How Strong Are International Standards in Practice?

Evidence from Cryptocurrency Transactions*

Karen Nershi†

February 18, 2023

Abstract

The rise of cryptocurrency presents challenges for state regulators given its connection to illegal activity and pseudonymous nature, which has allowed both individuals and businesses to circumvent national laws through regulatory arbitrage. In this paper, I assess the degree to which states have cooperated to regulate cryptocurrency exchanges, providing a detailed study of international efforts to impose common regulatory standards for a new technology. To do so, I introduce a dataset of cryptocurrency transactions collected during a two-month period in 2020 from exchanges in countries around the world and employ bunching estimation to compare levels of unusual activity below a threshold at which exchanges screen customers for money laundering risk. I find that exchanges in some, but not all, countries show substantial unusual activity below the threshold; these findings suggest that while countries have made progress toward regulating cryptocurrency exchanges, gaps in enforcement across countries continue to allow regulatory arbitrage.

*I am grateful to Robert A. Bridges, Devin Case-Ruchala, Matthew Collins, Hadi S. Elzayn, Julia Gray, Robert Heverly, David Hoffman, Michael Levi, Charles Littrell, Edward D. Mansfield, Daniel Nielson, Molly Roberts, Kirsten Rodine-Hardy, Jason Sharman, Beth Simmons, Kevin Werbach, participants of the Second International Research Conference on Empirical Approaches to AML and Financial Crime Suppression, and members of the CISAC Social Science Reading Group at Stanford University for very helpful comments.

†Postdoctoral Fellow, Stanford Internet Observatory, Stanford Univeristy; nershi@stanford.edu.

1 Introduction

The rise of cryptocurrency, a new form of digital currency, holds ambiguous implications for states. On the one hand, cryptocurrency is a decentralized technology that is independent from a centralized authority, and individuals can transact it using pseudo-anonymous digital keys that are not linked to their legal identities; this has attracted the attention of criminals, non-state actors, and rogue states evading sanctions, who have used cryptocurrency to buy and sell illegal goods and services and carry out other types of crime. On the other hand, the open source, ledger-based technology behind cryptocurrency creates a permanent record of all transactions that governments can use to trace transactions (including ones linked to crime) months or even years after they happen. Yet in order to leverage these records at scale by identifying the person behind a transaction, states must implement effective anti-money laundering regulation; this requires states to overcome the challenge of regulatory arbitrage – efforts by individuals or businesses to circumvent national regulations – by cooperating to enforce common standards. In this paper, I measure how successfully states have cooperated to regulate the cryptocurrency sector.

Since the introduction of the first cryptocurrency, Bitcoin, in 2010, law enforcement agencies have raised concerns about its potential misuse by criminals (Federal Bureau of Investigation 2012). Indeed, cryptocurrency has helped engender a new ecosystem of cybercrime in recent years by offering a digital and pseudo-anonymous means of payment that directly enables some types of crime (e.g., thefts of cryptocurrency exchanges) and enables others to be carried out on a large scale (e.g., ransomware attacks). And while cryptocurrency connected to crime makes up only a small portion of all cryptocurrency transactions, it is large in absolute terms, totaling an estimated $14 billion in 2021 (Chainalysis 2022, p. 3).

Because cryptocurrency currently has limited use as a means of exchange, cryptocurrency obtained through crime must be converted to fiat currency before it can be used in the

broader economy. For example, a criminal that sells illegal weapons on the dark web and receives a payment in Bitcoin must find a way to convert it to dollars (or another currency) before using these funds more widely. Cryptocurrency exchanges, which allow people to trade cryptocurrency for fiat currency and vice versa, are the primary way that criminals have made these conversions (Chainalysis 2022, p. 11); specifically, exchanges act as the "middle man" in transactions by pairing those who wish to buy (or sell) cryptocurrency with those who wish to sell (or buy) fiat. Thus, cryptocurrency presents a new type of money laundering risk, as criminals seek to disguise and integrate illegally-obtained cryptocurrency within the legitimate economy.

Addressing this new type of money laundering risk requires regulation, but importantly, individual states cannot regulate the sector alone. Enabled by cryptocurrency's digital nature, both individuals and exchanges have engaged in *regulatory arbitrage* – circumventing national regulation by accessing (or providing) services from "other jurisdictions" (May 1994). For individuals, this has primarily taken the form of encryption that disguises a user's physical location, while cryptocurrency exchanges have frequently changed the jurisdiction of their headquarters or refused to reveal the company's physical location altogether in an effort to avoid national regulation (Roberts 2021; Baker 2020). Thus, international cooperation to regulate the cryptocurrency sector is necessary to mitigate the risk of regulatory arbitrage.

International cooperation in this area is made difficult by the fact that anti-money laundering enforcement functions as a global public good; specifically, enforcing anti-money laundering laws is costly for states, and the benefits of enforcement cannot be internalized within individual states or groups of states (Olson 2012). Regulation is costly because states must pass and enforce new laws, including training and equipping regulators to oversee the implementation of new standards by the private sector. The primary benefits of enforcement, meanwhile, include stemming the flow of funds to criminal or terrorist groups and discouraging future crimes from being committed. However, states experience these related harms at

varying levels, such that some states are greatly affected while others experience relatively few harms. For example, Latin American countries face much higher crime rates stemming from the illegal drug trade than the United States or Western European countries. Thus, while anti-money laundering enforcement provides benefits at the international level, these benefits are experienced unevenly across states, and efforts to impose common regulatory standards for cryptocurrency hinge crucially on the success of international cooperation to overcome this collective action problem.

In this paper, I measure the success of one such recent effort to impose common regulatory standards for cryptocurrency. In 2019, the Financial Action Task Force (FATF), an intergovernmental organization dedicated to combating money laundering, issued new anti-money laundering regulatory guidelines for the cryptocurrency sector; its 36 member states (including the United States and many European Union countries) agreed to incorporate these standards into national law within one year. To assess the success of this effort, I measure activity at the firm level (cryptocurrency exchanges), which I aggregate to provide insight into the effectiveness of regulation at the country level. Accordingly, this paper is the first to measure the success of recent international efforts to regulate the cryptocurrency sector.

To enable this research, I collected a dataset of cryptocurrency-to-fiat transactions directly from cryptocurrency exchanges. Although most studies of anti-money laundering enforcement are constrained by limited access to relevant data from businesses like banks or other financial institutions, cryptocurrency exchanges, by contrast, offer much greater access to data (even transaction level data) thanks to the open-source nature of cryptocurrency technology. Accordingly, I collected a dataset of 150 million transactions containing virtually all trades from the two most widely used cryptocurrencies (Bitcoin and Ethereum) to fiat offered by exchanges during a two-month period in 2020, which was soon after the date by which FATF countries should have fully implemented the new standards.

Using this data, I measure states' regulatory efforts by exploiting a threshold above

which exchanges are required to screen their customers for money laundering risk. I quantify unusual activity below the threshold using bunching estimation, which allows me to estimate how many more transactions there are in the range below the threshold than would be expected based on the rest of the distribution. My findings suggest that FATF countries have made significant progress in regulating the cryptocurrency sector but struggle to achieve high levels of enforcement for some measures, which in turn creates an opening for criminals to continue using regulated exchanges while avoiding anti-money laundering screening.

The rest of the paper is organized as follows: in section two, I situate this study within the literature on international cooperation. In section three, I discuss the FATF recommendation and offer predictions about how states will implement these measures. In sections four and five, I describe my data collection and empirical strategies. In sections six and seven, I provide my results and a discussion, followed by concluding thoughts in section eight.

2 International Organizations and Cooperation

One of the overarching questions within the international cooperation literature focuses on whether (and how) international organizations shape state behavior. International organizations are believed to be particularly important for issues that present a collective action problem, as states have an incentive to free ride on the provision of a public good by others; this leads to an underprovision of the public good in equilibrium (Olson 2012). However, proponents argue that international organizations can help states overcome collective action problems by *lowering* the costs of cooperation (e.g., by sharing common regulatory standards) and *increasing* the costs of defection (e.g., sharing information about states' compliance with common standards, which allows group members to punish defecting states) (Axelrod and Keohane 1985; Keohane 2005).

Critics, meanwhile, argue that international organizations often have limited impact on state behavior due to selection bias and power dynamics within international organizations.

Selection bias can play a role because a state's decision to join an international organization (or adopt international standards) may be largely endogenous to a state's underlying preferences on a given issue, such that the organization (or standards) themselves have little independent influence on state behavior (Downs, Rocke, and Barsoom 1996). Power dynamics can also play an important role because wealthy and powerful countries often have greater influence over processes and outcomes within organizations (Krasner 1991); stated most strongly, some argue that international organizations may serve as little more than platforms through which powerful states pursue their agendas while maintaining a veneer of multilateralism (Mearsheimer 2017, p. 7).

In response to critiques, scholars have employed empirical evidence to highlight the ways that international organizations can shape state behavior and encourage cooperation. Specifically, international organizations can provide a forum for resolving disputes (Kono 2007), empower domestic audiences to hold their leaders to account (Simmons 2009), spur healthy competition among states through the use of public rankings (Kelley and Simmons 2015; Kelley and Simmons 2020; Honig, Weaver, et al. 2019), produce market pressure directed against states that fail to comply with international standards (Morse 2019), and create synergy across issue areas by forging agreements that tie cooperation on challenging issues with cooperation on other issues that provide clear opportunities for mutual gain (Davis 2004; Poast 2012; Hafner-Burton 2005). While this literature highlights important ways that international organizations can encourage cooperation, broader measures of an international organization's impact on state *behavior* generally remain elusive due to methodological challenges.[1]

Indeed, measuring the impact of an international organization on state behavior presents a methodological challenge because the primary unit of observation is the state, which makes it difficult to employ a causally-identified empirical strategy.[2] Specifically, given the phenom-

[1]Here, I distinguish between countries' adoption of specific laws or standards (which is the focus of a number of studies) and actual enforcement of these measures, which is typically much harder to measure.

[2]See Ashworth, Berry, and Mesquita (2021, Ch. 5) for a discussion of these challenges.

ena of interest (states' efforts to regulate a new sector), any type of experimental approach would likely prove infeasible. Thus, researchers must rely on observational data to measure an effect, but there are a number of potential confounders that may bias estimates. These potential confounders include selection bias (countries are more likely to adopt international standards that align with their values), variation in the standards adopted (which may produce subtle but important differences across countries), temporal trends (states often adopt new standards at different times, so time-specific trends may influence a country's outcomes), and path dependence (a country's prior history of regulation may influence its current efforts in unknown ways).

In light of these challenges, countries' efforts to regulate the cryptocurrency sector presents an interesting opportunity to measure cooperation because the circumstances surrounding the adoption of these measures serve to mitigate many potential confounders. Specifically, the FATF issued new regulatory guidelines for the cryptocurrency sector and urged its members to adopt and implement them; thus, a group of countries (FATF member states) agreed to implement similar regulatory standards (closely mirroring the FATF's guidelines) within a given time period (one year after the guidelines were issued) for a sector without much prior regulation. This enables a comparison of regulatory efforts among FATF countries by mitigating concerns over selection bias, varying temporal trends, and path dependence.

My results suggest that the FATF's success in influencing state behavior falls somewhere between the expectations of international organization optimists and skeptics. On the one hand, my findings suggest that countries have implemented part of the new regulatory standards, which represents significant progress given that cryptocurrency was a previously unregulated sector with a high potential for regulatory arbitrage. On the other hand, my findings suggest that states have struggled to achieve high levels of enforcement for measures subject to greater discretion, which creates openings for individuals to exploit enforcement lapses across regulated countries. Thus, while the FATF has successfully encouraged cooperation among its members, achieving high levels of enforcement remains a significant

challenge.

Dynamics within the FATF are also informative. Specifically, the organization's members include primarily wealthy, industrialized countries; this was no accident, as key FATF members sought to circumvent the influence of developing countries present in other organizations by creating a smaller organization to tackle the global money laundering challenge (Drezner 2003). The FATF has also used noncompliance lists to pressure non-member states into adopting the group's standards; further, the choice of which countries to include on these lists was the result of a political process, leading the FATF to lose credibility with some developing countries (Sharman 2011; Drezner 2003; Eggenberger 2018; Hülsse 2008). Thus, while the FATF has achieved at least partial success in promoting international cooperation to regulate the cryptocurrency sector, the terms of cooperation within this and other areas of anti-money laundering regulation continue to be largely guided by the interests of powerful countries within the FATF.

3 New Regulations for Cryptocurrency Exchanges

Following release of the FATF's new guidelines, FATF members pledged to incorporate these standards into national law and oversee implementation of new screening measures by cryptocurrency exchanges. The standards articulate two main obligations for exchanges: (1) perform *customer due diligence* for transactions of 1,000 euros/dollars or more and, (2) design and implement *risk based measures* that are appropriate for the scale and type of money laundering risk they face. The first of these obligations, customer due diligence, requires exchanges to obtain information about a customer's identity "using reliable, independent source documents, data or information," understand the nature of a customer's business, and maintain records of this information.[3] The second obligation, risk based measures, requires exchanges to "identify, assess, and take effective action to mitigate their money laundering/terrorist financing risks" (FATF 2019, p. 78), including conducting customer due

[3]See Appendix A.1 for the FATF directive.

diligence for transactions below the threshold that are deemed high risk (FATF 2019, p. 15).[4] Thus, while the duties involved in customer due diligence screening are clearly articulated along with a clear rationale for when to apply them, the obligations involved in risk based measures are vaguer and rely on the proactive efforts of exchanges (and the regulators that oversee them) to address money laundering risk.

Importantly, exchanges face mixed incentives to comply with these standards. On the one hand, exchanges are compelled to perform these duties by law, and failure to do so could result in fines or other penalties from national regulators. Some scholars also argue that businesses (like exchanges) face an incentive to actively guard against money laundering risk in order to safeguard their institutional reputations (Morse 2019). On the other hand, establishing and maintaining an effective compliance program is costly, often requiring a company to hire highly skilled personnel, purchase access to compliance databases or other systems, and train employees. Further, many of these measures may be difficult for national regulators to assess, which may lead some exchanges to minimize investment in these measures. Drawing on these insights, I present two predictions about countries' implementation of these new measures.

3.1 Suspicious Activity in Regulated Exchanges

First (and fundamental to this research design), I predict that exchanges in regulated countries will show *suspicious activity*, which I define as activity consistent with efforts to avoid due diligence screening.[5] This prediction differs from one by prominent members of the cryptocurrency community, who have argued that anti-money laundering regulation will drive criminals away from regulated exchanges and to dark web peer-to-peer sites, making it harder for law enforcement to trace cryptocurrency connected to crime (Havilland 2019; Aguilar 2019). However, given how criminals have responded to anti-money laundering laws in other sectors, I argue that at least some criminals will likely adapt their behavior to

[4]See Appendix A.2 for the FATF directive.

[5]I use this same definition throughout this section.

continue using regulated exchanges because of the *secrecy-security paradox* (Masciandaro, Takats, and Unger 2007, p. 155).

The secrecy-security paradox highlights that money launderers across all sectors face a tradeoff between the secrecy and security of a potential investment (Masciandaro, Takats, and Unger 2007, p. 155). Money launderers, like legal investors, seek investments that are secure (i.e., little risk of expropriation or financial collapse), profitable, and convenient. However, unlike most legal investors, money launderers place a premium on secrecy, and thus face a dilemma because many of the world's safest and most lucrative investments are located in wealthy Western countries that have strict anti-money laundering laws in place and governments strong enough to enforce them (Masciandaro, Takats, and Unger 2007, p. 155). For example, a money launderer could use criminal proceeds to purchase real estate in Beirut, and because Lebanon is one of the most corrupt countries in the world (Transparency International n.d.), likely bribe bank or government employees to avoid due diligence screening; however, holding real estate in Lebanon is generally less attractive to investors (including criminal ones) than holding real estate in a wealthy, Western country because of the country's political and economic uncertainty. Thus, when faced with this type of tradeoff, many money launderers have chosen to exploit weaknesses in the global anti-money laundering regime to access investments that offer a high level of security and an acceptable level of secrecy.[6]

For those seeking to launder cryptocurrency, the security-secrecy paradox suggests that at least some criminals will continue to use regulated exchanges because the next best alternatives that allow conversions of cryptocurrency to fiat are less secure and more difficult to use for large-scale conversions (Deer 2022). Specifically, criminals are unlikely to shift a majority of their activity to more secretive peer-to-peer trading sites on the dark web

[6]For example, many kleptocrats have taken advantage of laxer anti-money laundering standards in the real estate sector to purchase luxury properties in developed countries (Collin, Hollenbach, and Szakonyi 2023).

because they are less convenient (users must arrange each transaction without the help of a third party to facilitate matching) and riskier (there is no third-party guarantee behind transactions). And while some criminals may shift activity to unregulated exchanges (i.e., exchanges located in non-FATF member states), security concerns are likely to continue to play a role in driving launderers to use regulated exchanges, which are recognized as more secure than unregulated ones. Indeed, security is an especially pertinent concern within the cryptocurrency sector, which has been rife with scams, theft, and the misappropriation of funds leading to significant losses for cryptocurrency users. Given these constraints, I predict that at least some launderers of cryptocurrency will strategically adapt their behavior to minimize their risk of detection within regulated exchanges rather than exiting them altogether, resulting in the presence of suspicious activity within regulated exchanges.

3.2 Enforcement by OECD Countries

Second, I predict that exchanges in at least some OECD countries will show substantial levels of suspicious activity. This inquiry is significant since much of the anti-money laundering literature assumes that OECD countries have strong anti-money laundering systems for a number of theoretical reasons; these reasons include (1) OECD countries possess the resources necessary to effectively enforce these regulations (Verdugo Yepes 2011, p. 12); (2) OECD countries have performed well in other related areas (e.g., low levels of corruption and high rule of law), which suggests their success may transfer into the area of anti-money laundering enforcement; and (3) OECD countries are committed to preserving their international reputations, and so will enforce regulations to avoid potential reputational harm caused by association with money laundering (Morse 2019).

Despite this theoretical debate, there is little documented evidence that OECD countries provide better enforcement of anti-money laundering laws than than other countries (Willebois et al. 2011; Sharman 2010; Findley, Nielson, and Sharman 2014). In fact, several

audit-style field experiments show that for at least one important type of anti-money laundering law, "tax haven" countries showed higher levels of enforcement than OECD countries; further, OECD countries enforced this law at levels on par with developing countries (Findley, Nielson, and Sharman 2014). Accordingly, I predict that OECD countries will not show better enforcement of new measures for cryptocurrency than other countries.

4 Data

One of the chief challenges of analyzing cryptocurrency transactions lies in obtaining reliable data. Although most studies have used data from third-party aggregator sites, data from these sites may be unreliable because some exchanges share fake data. Specifically, exchanges have an incentive to artificially inflate their transaction volume to give the appearance of high liquidity, which allows them to attract new customers (Chen, Lin, and Wu 2022; Hougan, Kim, and Lerner 2019; Varshney 2021). In fact, one report estimates that as much as 95% of all transactions reported to aggregator sites are fake (Bitwise Asset Management 2019). To minimize this risk, I bypassed third-party sites altogether by collecting data in real time directly from exchanges using each exchange's application programming interface (API). APIs should offer a more reliable source of data than other alternatives because individuals can use them to execute trades.

Using APIs, I collected a dataset of transactions from Bitcoin and Ethereum (the two most widely used cryptocurrencies) to fiat currencies from virtually all exchanges offering these trades between June 22, 2020 and September 2, 2020. I used remote servers to query the APIs at intervals of 15, 30, 60, or 150 seconds (depending on the volume and number of trades available from each site), as APIs have limited caches that store information about recent trades. For each transaction, I collected the time, date, quantity of cryptocurrency, and the exchange rate of the currency pair at the time the trade was executed.[7]

[7]Prices for each trading pair vary by site and fluctuate over time.

After collecting the data, I classified each exchange by the country in which it was registered (the country responsible for regulation) according to the exchange's website in July 2020. To clean the data, I removed low volume trading pairs (i.e., a specific combination of cryptocurrency to fiat trades such as Bitcoin to dollars, Bitcoin to euros, etc.) and transactions from several exchanges for which the regulating country could not be determined.[8] I also converted the fiat value of all transactions to either dollars or euros depending on the currency at which the exchange enforces the threshold (euros for European-based exchanges and dollars for all others) using hourly exchange rates (Dukascopy: Swiss Banking Group n.d.). After cleaning the data, the final sample contains 65 trading pairs from 27 exchanges located across 9 regulated countries.[9] This sample presents a diverse cross-section of countries including wealthy, industrialized countries (US, UK, and Japan), a middle-upper income country (Estonia), several developing countries (Turkey, Brazil), and a tax haven (British Virgin Islands).

5 Estimation Strategy

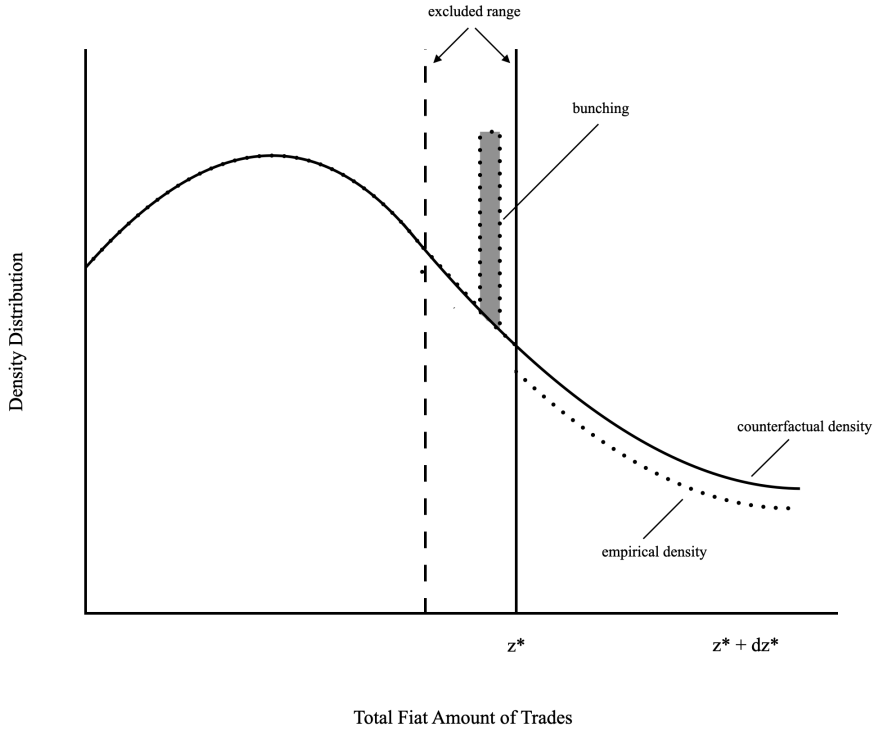
I use bunching estimation to measure activity within exchanges consistent with efforts to avoid due diligence screening. Bunching estimation is an econometric strategy introduced by Saez (2010) and further developed by Chetty et al. (2011) that is used to study phenomena involving avoidance or evasion. This method uses the mass of a distribution to measure how individuals strategically respond to a discontinuity in incentives in a context where they can adjust something (e.g., a transaction) below a threshold (Figure 1). In this context, the distribution of the number of trades within a given range is represented by a smooth density distribution $h(z)$ across a continuous variable z, which denotes the transaction size. The variation in incentives is marked by the due diligence threshold, which is represented by z^*; if users respond strategically to z^*, they will shift transactions that would have fallen in the

[8] Appendix G provides details on the data cleaning process.

[9] Appendix D shows the number and type of trading pairs across exchanges.

range $[z^*,\ z^* + d(z)]$ below z^* leading to bunching and shifting the empirical distribution beyond z^* downward. Because there is some randomness in how individuals choose to adjust their transactions, bunching may more closely resemble a hump than a spike (Bastani and Selin 2014). Figure 2 shows simulated distributions with bunching equal to 5, 2, and 1 percent excess mass below a threshold.

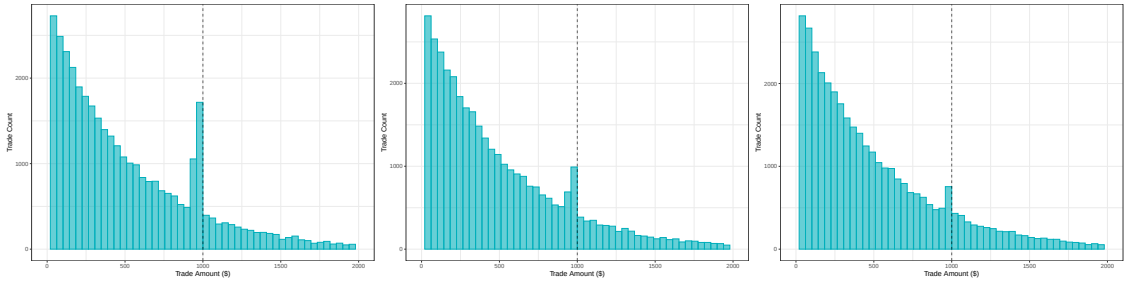
Figure 1: Bunching Illustration



Notes: The solid line denotes a distribution function ($h(z)$) across values of trades in dollars. The rectangle denotes "bunching" below the threshold ($z*$), and the dotted line denotes the downward shift in the distribution beyond $z*$ caused by bunching.

To estimate bunching, I follow the procedure outlined by Chetty et al. (2011) and summarized by Mavrokonstantis (2019), which allows me to estimate the level of excess mass relative to the predicted mass in a defined range below the threshold. Importantly, this method does not require knowledge of the global distribution of trades but rather the ability to approximate the local distribution within a smaller bunching window (Kleven 2016).

Figure 2: Bunching Simulations



(a) 5% Bunching (b) 2% Bunching (c) 1% Bunching

Notes: Simulated density plots show bunching at 5%, 2%, and 1% excess mass below the threshold (dashed line) for exponential distributions of 10,000 trades with a mean of 500.

Accordingly, I estimate the counterfactual distribution by fitting a polynomial to the distribution of binned data within the bunching window excluding the contribution of bins close to the threshold (to avoid introducing bias driven by bunching itself). The counterfactual distribution corresponds to the expected distribution if there were no bunching below the threshold and is given by the following equation:

$$C_j = \sum_{i=0}^{p} \beta_i \cdot (Z_j)^i + \sum_{i=z_L}^{z_U} \gamma_i \cdot \mathbb{1}[Z_j = i] + \epsilon_j, \tag{1}$$

where c_j denotes the number of transactions in each bin j, Z_j denotes the position of each bin relative to z^* in 10 unit increments ($Z_j = -25, -24, .., 25$), p is the order of the polynomial, and z_L and z_U denote the lower and upper bound of the excluded bunching area respectively. Thus, the counterfactual distribution is obtained from the predicted values of Equation 1 while omitting the contribution of the dummies in the excluded range, formally:

$$\widehat{C}_j = \sum_{i=0}^{p} \widehat{\beta}_i \cdot (Z_j)^i. \tag{2}$$

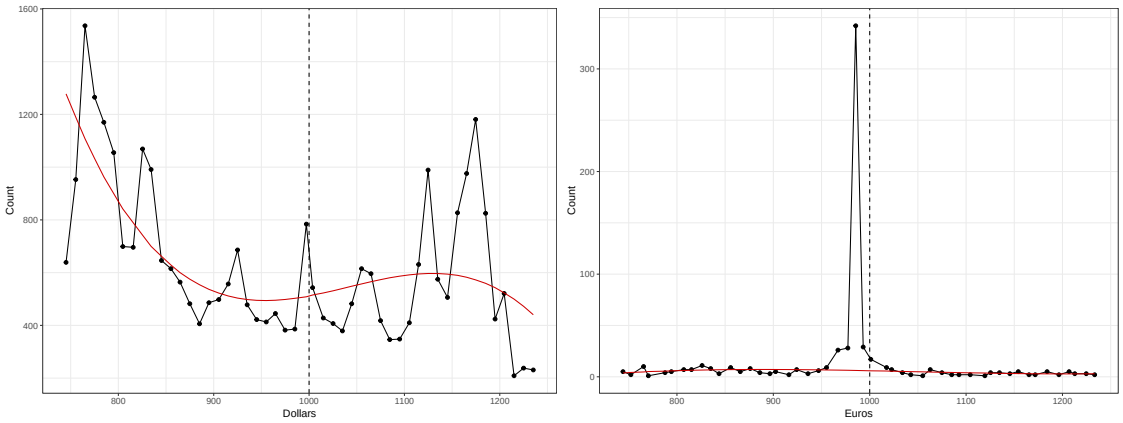
I then estimate the difference between the counterfactual and observed values in each bin within the bunching window ($\widehat{B}_N = \sum_{j=z_L}^{z_U} C_j - \widehat{C}_j$) (Kleven 2016). Finally, I estimate excess

mass in the bunching region relative to the average height of the counterfactual distribution in the excluded range $[z_L, z_u]$, formally:

$$\widehat{b} = \frac{\widehat{B}}{\frac{\sum_{j=z_L}^{z_U} \widehat{C}_j}{z_U - z_L + 1}} = \widehat{B} \cdot \frac{z_U - z_L + 1}{\sum_{j=z_L}^{z_U} \widehat{C}_j}. \tag{3}$$

I estimate bootstrapped standard errors following the procedure described by Chetty et al. (2011). Accordingly, I draw 1,000 samples with replacement from the vector of errors (ϵ_i) in Equation 1. For each sample, I calculate a bunching estimate $(\widehat{b})$ following the procedure described described above. I then define the standard error of the original estimate as the standard deviation of the distribution of $\widehat{b}^k$s (Chetty et al. 2011). This process allows me to ascertain whether an estimate of excess mass is statistically significant using a one-sided t-test.

Figure 3: Bunching in Two Exchanges



(a) Binance US (b) Coinmetro

Notes: Graphs show examples of the distribution of transactions close to the threshold in two exchanges: Binance US, an exchange offering Bitcoin-to-dollar trades, and Coinmetro, an exchange offering Bitcoin-to-euro trades. The red lines denote the counterfactual distribution, while the dashed lines denote the due diligence threshold.

Figure 3 illustrates this method with data from two exchanges – Binance US, located in the United States (3a), and Coinmetro, located in Estonia (3b). These graphs show the number of transactions in each exchanges within 10 dollar/euro bins between 750 and 1,250

dollars/euros with the graphs centered at the due diligence threshold. For each distribution, I fit a third-degree polynomial to the data (excluding the 100 units below the threshold where bunching may occur) to provide a counterfactual estimate of the distribution. The counterfactual distribution roughly matches the empirical distribution for Binance US with no significant excess mass below the threshold; this intuition is borne out in the estimate of $\widehat{b} = 0.04$, which is not statistically significant (standard error = 1.96). In Coinmetro, meanwhile, there are a large number of transactions below the threshold that diverge from the counterfactual fit line indicating bunching; indeed, the estimate of $\widehat{b}$ is 58.80 and is statistically significant, with a standard error of 8.36 ($p < 0.00001$). This indicates that there are nearly 59 times more transactions in the range below the threshold than predicted based on the rest of the distribution.

Importantly, there are two potential threats to inference using bunching estimation (Kleven 2016), but neither poses a significant problem for this research design. The first potential threat to inference is the presence of another policy that makes use of the same threshold, which could confound bunching estimates; however, there are no other policies that affect cryptocurrency transactions at the 1,000 dollar/euro threshold. The second potential threat to inference is that the threshold also serves as a natural reference point, which could lead to a higher number of transactions for an unrelated reason. Although 1,000 dollars/euros *is* a natural reference point, this does not present a problem for this design because I examine bunching *below* the threshold. Accordingly, this feature actually introduces bias *against* finding bunching below the threshold, since a higher number of transactions in the rest of the distribution (i.e., outside the excluded range) shifts the distribution upwards, making evidence of excess bunching below the threshold meet a higher level of robustness than would be necessary without a natural reference point outside the excluded range.

Similarly, bunching could occur at round quantities of cryptocurrency, but this behavior is unlikely to explain bunching below the threshold given widely varying crypto-to-fiat prices across exchanges and over time. Specifically, there are persistent price discrepancies across

exchanges (Pieters and Vivanco 2017) and many minutes worth of price fluctuations included in the data because exchanges, unlike trading houses on Wall Street, never officially close. Further variation is introduced by the fact that I measure bunching in trades from two different cryptocurrencies. Thus, variation in crypto-to-fiat prices across exchanges and over time suggests that bunching below the threshold is unlikely to be driven by bunching at specific round quantities of cryptocurrency.

5.1 Interpreting bunching

Given that at least some exchanges show bunching, how can we interpret the presence of bunching in substantive terms? First and foremost, bunching shows that there is an incentive for users to conduct transactions below the threshold, a finding I argue is most plausibly driven by users' efforts to avoid screening in regulated exchanges. Thus, the presence of bunching suggests that regulated exchanges *are* enforcing customer due diligence for transaction above the threshold, which creates an incentive for users to shift transactions below it. However, the presence of bunching within exchanges over time also supports a second conclusion about exchanges' efforts to enforce the new regulations. Specifically, I argue that the presence of bunching over time suggests that exchanges are not adequately performing risk based measures, which require exchanges to identify suspicious patterns and trends within their business and take effective measures to mitigate these risks. This conclusion follows from the fact that the presence of an abnormal number of transactions below the due diligence threshold appears suspicious, and an exchange that is adequately performing risk based measures should identify this risk and take additional steps to mitigate it (e.g., additional screening below the threshold), which would lead to a decrease in the amount of bunching over time.

Although the presence of bunching indicates behavior consistent with efforts to avoid screening, bunching itself *is not* direct evidence of criminal activity. However, I argue that

most lawful users are unlikely to avoid screening as the costs of undergoing screening are generally low and avoiding it can require specific knowledge. Indeed, undergoing due diligence screening as a customer is a relatively simple process – requiring a customer to share her legal name, address, occupation, and a copy of a government-issued identification document – that can generally be performed within minutes and requires no additional fees. Further, once screened, a customer is cleared to convert cryptocurrency to any fiat amount without undergoing additional screening.

Conversely, avoiding screening requires specific knowledge; a customer must be aware that an exchange enforces due diligence at the threshold as well as whether this threshold is enforced in dollars or euros. In some cases, a customer may even need to know a specific exchange rate, such as if a customer seeks to convert Bitcoin to dollars in a UK-based exchange (which enforces the threshold in euros). In this example, the customer would also need to know the exchange rate between euros and dollars to ensure that her transaction remains below the due diligence threshold. Importantly, regardless of whether the activity captured by bunching is criminal or non-criminal, it represents a lapse in enforcement by exchanges, as they are charged with guarding against suspicious trends (like bunching) and taking effective action to mitigate these risks.

What then does the *absence* of bunching suggest? First and foremost, it shows that there *is not* an incentive to shift transactions below the threshold, which, in turn, could be explained by one of two scenarios. First, the absence of bunching could indicate that an exchange is adequately enforcing risk based measures; in this case, an exchange addresses behavior consistent with efforts to avoid screening through additional proactive measures that lead to a decrease in bunching over time as customers either adopt new strategies to avoid screening or exit the exchange altogether. Second, the absence of bunching could indicate a very poor regulatory environment – an exchanges not only fails to enforce risk based measures, but it also fails to perform due diligence screening for transactions above the threshold so that customers have no incentive to sort transactions below it. Although

logically sound, I argue the second scenario is unlikely to occur in practice as national regulators can easily verify whether an exchange is performing due diligence by checking its records; further, an exchange that fails to perform this obligation will face potential fines or other penalties from regulators.

6 Results

To measure how well states have cooperated to enforce new standards for cryptocurrency, I use bunching estimation to quantify suspicious activity within exchanges and provide three points of comparison. First, I compare bunching below the threshold in both regulated and unregulated exchanges for trades from Bitcoin and Ethereum to fiat with results aggregated according to whether the exchange enforces due diligence at 1,000 euros (European exchanges) or 1,000 dollars (all others). This offers a comparison of activity below the relevant threshold between regulated and unregulated exchanges. Second, I compare bunching within regulated exchanges below two placebo thresholds: 500 and 1,500 dollars/euros; this offers a comparison of activity below the actual and placebo thresholds within regulated exchanges. Third, I compare bunching across regulated countries below the actual and placebo thresholds, which offers a comparison of the amount of unusual activity across all regulated countries.

Table 1 presents bunching estimates below the due diligence threshold (1,000 dollars/euros) for transactions from Bitcoin and Ethereum to fiat in both regulated and unregulated exchanges.[10] The results show that for both cryptocurrencies, there is positive and statistically significant bunching below the due diligence threshold in *regulated* exchanges, with no statistically significant bunching below the threshold in *unregulated* countries. Thus, activity below the threshold diverges between regulated and unregulated exchanges, a finding I argue is driven by customers' efforts to avoid due diligence screening in regulated exchanges.

[10] I exclude U.S. exchanges from these estimates because they screen all customers rather than screening above a threshold (see Section 6).

Table 1: Bunching in Regulated and Unregulated Exchanges

	Regulated Exchanges				**Unregulated Exchanges**			
	Bitcoin		Ethereum		Bitcoin		Ethereum	
	USD	*EUR*	*USD*	*EUR*	*USD*	*EUR*	*USD*	*EUR*
1,000	4.989**	2.627***	1.448*	2.284***	−1.482	1.418	−0.922	−0.595
(*Threshold*)	(1.759)	(0.683)	(0.637)	(0.431)	(1.800)	(0.916)	(1.462)	(0.493)
N	3,114,869	2,478,797	202,597	2,033,957	1,885,454	84,587	1,084,613	30,361
Exchanges	10	5	8	3	3	2	3	2
Pairs	17	8	8	6	3	4	3	2

Notes: Bunching in regulated and unregulated exchanges by trading pair between 06/21/20 and 09/02/20. *N* denotes the number of transactions, *Exchanges* denotes the number of exchanges, and *Pairs* denotes the number of trading pairs included in each estimate; standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

Meanwhile, there is no policy-driven incentive to sort transactions below the threshold in unregulated exchanges (as no screening is performed above it), and, consistent with my expectations, there is no statistically significant bunching below the threshold. Bunching estimates within regulated exchanges range from 4.155 for Bitcoin-to-dollar transactions to 1.448 in Ethereum-to-dollar transactions, with results indicating that there are nearly five and roughly one and a half times as many transactions in the range below the threshold as would be expected based on the rest of the distribution.

Table 2 shows bunching estimates below two placebo thresholds within regulated exchanges, providing a test of whether there is often bunching below round fiat values within regulated exchanges. Conversely, the absence of bunching or negative bunching (which may occur if there is bunching at the round fiat value) below placebo thresholds suggests that the results in Table 1 are unusual. Estimate of bunching are not statistically significant for transactions from Ethereum and Bitcoin to euros below both placebo thresholds. Estimates of bunching below the second placebo threshold (1,500 dollars/euros) are negative and

Table 2: Bunching in Regulated Exchanges at Placebo Thresholds

	Regulated Exchanges			
	Bitcoin		Ethereum	
	USD	*EUR*	*USD*	*EUR*
500	2.754**	0.009	−0.462	0.348
(*Placebo 1*)	(1.129)	(0.216)	(0.713)	(0.377)
1,500	−1.152*	0.028	−0.845*	0.367
(*Placebo 2*)	(0.542)	(0.143)	(0.486)	(0.295)
N (Placebo 1)	6,115,430	2,691,652	420,279	2,294,970
N (Placebo 2)	1,074,106	1,566,341	126,997	1,460,312
Exchanges	10	5	8	3
Pairs	17	8	8	6

Notes: Bunching below placebo thresholds in regulated exchanges between 06/21/20 and 09/02/20. *N* denotes the number of transactions, *Exchanges* denotes the number of exchanges, and *Pairs* denotes the number of trading pairs included in each estimate; standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

statistically significant for transactions from Bitcoin and Ethereum to dollars, and positive and statistically significant for transactions from Bitcoin to dollars below the first placebo threshold (500 dollars/euros). Although there is positive and significant bunching below a placebo threshold in one crypto-to-fiat pair, the results generally conform to my expectations as there is no consistent pattern of positive and statistically significant bunching below placebo thresholds in regulated exchanges.

Table 3 shows estimates of bunching below the actual and placebo thresholds across regulated countries for trades from Bitcoin to fiat currency.[11] Nearly all regulated countries show

[11]The British Virgin Islands is not an FATF member, but the country issued new regulatory guidance for the cryptocurrency sector in line with the FATF's standards on July 10, 2020 (British Virgin Islands Financial Services Commission 2020; Law of Virgin Islands 2020). I include transactions after this date in

statistically significant bunching below the due diligence threshold, and these estimates vary by orders of magnitude across countries. At the most extreme, Estonia's lone exchange shows bunching that is equal to nearly 59 greater transactions in the range below the threshold than predicted based on the rest of the distribution, followed by Brazil (7 times greater), Japan (5 times greater), and Australia (3 times greater). Exchanges in the United Kingdom, British Virgin Islands, and the Netherlands, meanwhile, show bunching roughly two to three times greater than expected below the threshold, while there is no statistically significant bunching below the threshold in exchanges in Turkey and the United States.

Although it is unclear what drives a lack of bunching in Turkey's exchanges, the United States' lack of bunching can be explained by a policy choice of U.S. exchanges: specifically, the U.S. is unique among regulated countries because exchanges perform customer due diligence screening as soon as a new a customer is registered rather than performing screening above a transaction threshold. Thus, customers in U.S.-based exchanges *do not* face an incentive to shift transactions below the $1,000 threshold, and consistent with this, there is no statistically significant bunching below it. I also test for bunching below two placebo thresholds across regulated countries, and while there is some statistically significant bunching below placebo thresholds (both positive and negative), there is no robust pattern of bunching below placebo thresholds across countries.

In sum, results across all three comparisons show a pattern of statistically significant bunching below the due diligence threshold in regulated exchanges with no similar pattern of bunching below the threshold in unregulated exchanges or below placebo thresholds in regulated exchanges. Each of these findings is consistent with the interpretation that users of cryptocurrency exchanges have responded to the introduction of new regulations in FATF countries by shifting a substantial number of crypto-to-fiat transactions below the due diligence threshold to avoid screening. These results are robust to different specifications of bunching estimation, which I present in Appendix C.

the country's estimate.

Table 3: Bunching in Bitcoin Trades by Country

	Estonia	**Brazil**	**Japan**	**Australia**	**UK**	**BVI†**	**Netherlands**	**Turkey**	**USA**
500	3.665*	−2.357***	2.852**	−2.131	−0.134	0.282	13.162	4.891***	4.485**
(*Placebo 1*)	(1.903)	(0.552)	(1.179)	(2.316)	(0.220)	(1.904)	(15.069)	(1.359)	(1.892)
1,000	**58.459*****	**6.670*****	**5.231****	**3.191****	**2.628*****	**2.341*****	**2.266****	**0.520**	**−0.220**
(*Threshold*)	**(8.079)**	**(0.803)**	**(1.955)**	**(1.371)**	**(0.712)**	**(0.637)**	**(0.969)**	**(0.790)**	**(3.531)**
1,500	0.831	1.706*	−1.329*	6.045***	0.020	−0.851**	0.195	1.137*	2.134**
(*Placebo 2*)	(1.949)	(0.791)	(0.602)	(1.478)	(0.141)	(0.301)	(1.065)	(0.664)	(0.762)
N (Placebo 1)	244	144,166	5,659,192	15,767	2,660,012	114,061	31,384	158,483	203,965
N (Threshold)	648	100,282	2,764,050	7,998	2,428,099	143,278	50,049	80,934	111,656
N (Placebo 2)	208	85,428	842,130	5,830	1,544,984	70,797	21,149	65,924	30,674
Exchanges	1	3	4	1	3	2	1	2	3
Pairs	1	3	6	1	6	2	1	2	3

Notes: Bunching by country in Bitcoin-to-fiat trades between 06/21/20 and 09/02/20. *N* denotes the number of transactions, *Exchanges* denotes the number of exchanges, and *Pairs* denotes the number of trading pairs included in each estimate; standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001. † British Virgin Islands

7 Discussion

Based on the results, I draw two broad conclusions about the success of FATF-led regulation. First, the presence of suspicious activity within regulated exchanges (measured through bunching) suggests that at least some individuals have strategically adapted their behavior to avoid screening under the new law. This finding is important because while prior research has highlighted enforcement challenges at the level of countries (Levi, Reuter, and Halliday 2018; Takats 2011; Ferwerda, Deleanu, and Unger 2019; Deleanu 2017; Ferwerda and Reuter 2019) and businesses (Sharman 2010; Sharman 2011; Findley, Nielson, and Sharman 2014; Findley, Nielson, and Sharman 2015), relatively little research has considered how the behavior of individuals may influence the way regulations function in practice. Specifically, my findings suggest that national and international anti-money laundering standards should take into account the potential for strategic behavior by individuals. For example, laws could require

exchanges to perform randomized due diligence screening rather than screening above a transaction threshold, which would make it harder for criminals to avoid screening.

A second broad conclusion drawn from these results is that developed countries – like developing countries and tax havens – struggle to adequately enforce anti-money laundering laws for the cryptocurrency sector. I draw this conclusion based on the fact that both developed and developing countries within the FATF showed similar outcomes (i.e., statistically significant bunching below the threshold). Developed countries with high levels of bunching include Japan, which was home to several cryptocurrency exchanges that experienced multi-million dollar thefts (McMillan 2018; Partz 2018; Partz 2021; Hickey 2019), and the United Kingdom, which has suffered a decade of money laundering scandals in other sectors.[12]

Table 4: Total Dollar Value of Bunching in Bitcoin Trades by Country

Country	**Trades Value** (M USD)	**Bunching Volume** (% of All Transactions)
Japan	214.7	1.20
United Kingdom	73.5	0.42
British Virgin Islands	6.5	0.30
Netherlands	2.8	1.42
Brazil	2.5	1.44
Estonia	0.4	0.06
Australia	0.3	0.29

Notes: Table shows the dollar value (in millions) of the statistically significant bunching within each country's exchange(s) between 06/21/20 and 09/02/20 for all trades from Bitcoin to fiat. Column 3 shows this dollar value as a percent of the total value of all transactions within a country's exchange(s).

This finding is important in substantive terms because developed countries often handle much larger transaction volumes than developing ones, which is true both in the financial sector more broadly and the cryptocurrency sector. Table 4 highlights this relationship by showing the dollar value of each country's statistically significant bunching estimate from

[12]See for example Harding, Hopkins, and Barr (2017), Osborne (2020), Withers (2021), and Spence, Browning, and Hoije (2022).

Table 3. Accordingly, Japan, which is third in terms of the magnitude of its bunching estimate, accounts for the greatest dollar value of bunching with roughly $215 million worth of transactions during the two month period. The United Kingdom is second, with bunching in its exchange totaling $73.5 million. The dollar values of bunching in the sole developing country, Brazil, is considerably lower at $2.5 million. Similar results are also present in trades from Ethereum (Appendix B.1). These results highlight that if a key goal of the international community is to reduce the over all amount of suspicious money in the global financial system, focusing on enforcement by developed countries is key because they handle a large portion of the financial system's transaction volume.

This finding is also important for normative reasons, as OECD countries often hold greater influence in international organizations and play an important role in shaping the dialog around key international issues. In the context of the global anti-money laundering fight, OECD countries make up a majority of FATF members and have helped promote the view that developed countries have effectively addressed money laundering risks, while the true areas of weakness globally lie in poor enforcement by developing countries and tax havens (Schwarz 2011). For example, the Basel Institute on Governance recently ranked 110 countries in terms of their money laundering and terrorist financing risks and placed 16 OECD countries (including 15 European countries) within the top 20 lowest risk countries. By contrast, 10 low income countries and 4 lower middle income countries were listed among the 20 riskiest countries (Basel Institute on Governance 2021).[13] Instead, my findings support the conclusion that both developed and developing countries struggle to adequately enforce anti-money laundering laws and that countries which present the greatest risk is less clear.

One additional finding is that regulated countries show varying levels of bunching, which may emerge for two reasons. The first is that regulatory stringency may vary across countries leading exchanges to enforce risk based measures at varying levels, which in turn leads to

[13]Income categories are based on the World Banks' classification scheme (Hamadeh, Van Rompaey, and Metreau 2021).

varying levels of suspicious activity. Prior research shows that the quality of national regulation plays an important role in determining the level of anti-money laundering enforcement by businesses, but the resources and methods used by national regulators vary widely across countries (Levi, Halliday, and Reuter 2014; Willebois et al. 2011, p. 30). Importantly, even countries that successfully enforce other types of financial regulation may struggle to enforce anti-money laundering standards, highlighting that the quality of national regulation is not solely determined by a country's wealth or performance in other areas.[14] Thus, variation in the quality of national regulation could help explain varying levels of bunching across countries.

A second potential explanation for varying levels of suspicious activity across countries is that certain markets may attract more suspicious money. Indeed, some argue that because Western countries have developed economies and offer safe and lucrative investment opportunities, they tend to attract a greater share of criminal money than developing countries (Walker and Unger 2009, p. 833). Additionally, features that make doing business in developing countries more difficult – such as long wait times for slow-moving bureaucracies, red tape, corruption, and bribery – may discourage *criminal* actors (in additional to non-criminal ones) from investing (Findley, Nielson, and Sharman 2014, p. 82). Although I expect that factors limiting the ease of doing business in developing countries are likely much lower for the cryptocurrency sector than for other sectors, it is possible that patterns of activity in other sectors continue to influence how actors behave in the cryptocurrency sector. Thus, while levels of money laundering remain poorly understood globally, this paper provides insight into the levels of suspicious money across countries within the cryptocurrency sector.

[14]See for example Financial Action Task Force (n.d.[b]) and Financial Action Task Force (n.d.[a], pp. 201, 199).

8 Conclusion

This paper assesses how well a group of countries has cooperated to enforce new regulatory standards for the cryptocurrency sector. My results suggest that FATF members have made significant progress by pushing cryptocurrency exchanges to perform due diligence screening for transactions above a key threshold. Given that most exchanges are majority online businesses and many have sought to evade regulation in the past, this represents a significant achievement for FATF countries in a short period of time. However, my results also suggest that countries struggle to ensure exchanges enforce discretion-based measures at high levels, creating weaknesses within the international system. These weaknesses provide an opening for criminals to continue laundering funds in regulated exchanges while avoiding due diligence screening.

Despite these challenges, there is cause to be optimistic about the long-term chances of effective international anti-money laundering regulation of the cryptocurrency sector. Specifically, the unique traceability of cryptocurrency transactions suggest that governments with enough resources will be able to trace all or most criminal activity through the laundering process. Further, advanced techniques for tracing transactions on the blockchain suggest that detecting suspicious activity in the cryptocurrency space will likely become easier over time.[15] Finally, there is already evidence of broader adoption of these standards by 16 non-member states (Allison 2021), and the process of anti-money laundering regulation for other sectors suggests that adoption of these new standards will likely to continue to spread among non-FATF countries. Thus, although there is still a long road ahead, states have made significant progress in their efforts to regulate the cryptocurrency sector through international cooperation.

[15]For examples, see Weber et al. (2019), Fanusie and Robinson (2018), Koerhuis, Kechadi, and Le-Khac (2020), and Möser et al. (2017).

References

Aguilar, Diana (2019). "Regulators Debate Cryptocurrency Legislation Ahead of G20 Summit - CoinDesk". In: *CoinDesk*. URL: https://www.coindesk.com/regulators-begin-to-debate-cryptocurrency-legislation-ahead-of-g20-summit.

Allison, Ian (2021). "FATF Says Majority of Countries Still Haven't Implemented Watchdog's Crypto Guidance". In: *CoinDesk*. URL: https://www.coindesk.com/policy/2021/06/25/fatf-says-majority-of-countries-still-havent-implemented-watchdogs-crypto-guidance/.

Ashworth, Scott, Christopher R Berry, and Ethan Bueno de Mesquita (2021). *Theory and Credibility: Integrating Theoretical and Empirical Social Science*. Princeton University Press.

Axelrod, Robert and Robert O Keohane (1985). "Achieving cooperation under anarchy: Strategies and institutions". In: *World Politics: A Quarterly Journal of International Relations*, pp. 226–254.

Baker, Paddy (2020). "Binance Doesn't Have a Headquarters Because Bitcoin Doesn't, Says CEO". In: URL: https://www.coindesk.com/markets/2020/05/08/binance-doesnt-have-a-headquarters-because-bitcoin-doesnt-says-ceo/.

Basel Institute on Governance (2021). *Basel AML Index 2021: 10th Public Edition*. URL: https://baselgovernance.org/sites/default/files/2021-09/Basel_AML_Index_2021_10th\%20Edition.pdf.

Bastani, Spencer and Håkan Selin (2014). "Bunching and non-bunching at kink points of the Swedish tax schedule". In: *Journal of Public Economics* 109, pp. 36–49.

"Bitcoin" (n.d.). In: (). [Online; accessed 18.Jul. 2022]. URL: https://www.investing.com/crypto/bitcoin/historical-data.

Bitwise Asset Management (2019). *Analysis of Real Bitcoin Trade Volume*. [Online; accessed 14. Apr. 2021]. URL: https://static.bitwiseinvestments.com/Research/Bitwise-Asset-Management-Analysis-of-Real-Bitcoin-Trade-Volume.pdf.

British Virgin Islands Financial Services Commission (2020). *Guidance on Regulation of Virtual Assets in the Virgin Islands (BVI)*. URL: https://www.bvifsc.vg/sites/default/files/guidance_on_regulation_of_virtual_assets_in_the_virgin_islands_bvi_final.pdf.

Chainalysis (2022). *The 2022 Crypto Crime Report: Original data and research into cryptocurrency-based crime*. URL: https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

Chen, Jialan, Dan Lin, and Jiajing Wu (2022). "Do cryptocurrency exchanges fake trading volumes? An empirical analysis of wash trading based on data mining". In: *Physica A: Statistical Mechanics and its Applications* 586, p. 126405.

Chetty, Raj et al. (2011). "Adjustment costs, firm responses, and micro vs. macro labor supply elasticities: Evidence from Danish tax records". In: *The quarterly journal of economics* 126.2, pp. 749–804.

Collin, Matthew, Florian M. Hollenbach, and David Szakonyi (2023). *The end of Londongrad? The impact of beneficial ownership transparency on offshore investment in UK property*. Tech. rep.

Davis, Christina L (2004). "International institutions and issue linkage: Building support for agricultural trade liberalization". In: *American Political Science Review* 98.1, pp. 153–169.

Deer, Marcel (2022). "What is P2P trading, and how does it work in peer-to-peer crypto exchanges?" In: *Cointelegraph*. URL: https://cointelegraph.com/news/what-is-p2p-trading-and-how-does-it-work-in-peer-to-peer-crypto-exchanges.

Deleanu, Ioana Sorina (2017). "Do countries consistently engage in misinforming the international community about their efforts to combat money laundering? Evidence using Benford's law". In: *PloS one* 12.1.

Downs, George W, David M Rocke, and Peter N Barsoom (1996). "Is the good news about compliance good news about cooperation?" In: *International Organization* 50.3, pp. 379–406.

Drezner, Daniel W (2003). "Clubs, Neighborhoods and Universes: The Governance of Global Finance". In: *University of Chicago. Paper prepared for the Annual Meeting of the American Political Science Association (28-31 August)*.

Dukascopy: Swiss Banking Group (n.d.). *Historical Data Feed*. URL: https://www.dukascopy.com/swiss/english/marketwatch/historical/.

Eggenberger, Katrin (2018). "When is blacklisting effective? Stigma, sanctions and legitimacy: the reputational and financial costs of being blacklisted". In: *Review of International Political Economy* 25.4, pp. 483–504.

"Ethereum" (n.d.). In: (). [Online; accessed 18. Jul. 2022]. URL: https://www.investing.com/crypto/ethereum/historical-data.

Fanusie, Yaya and Tom Robinson (2018). "Bitcoin laundering: an analysis of illicit flows into digital currency services". In: *Center on Sanctions and Illicit Finance memorandum, January*.

FATF (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

Federal Bureau of Investigation (2012). *(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Tech. rep. [Online; accessed 21. Nov. 2019]. URL: https://cryptome.org/2012/05/fbi-bitcoin.pdf.

Ferwerda, Joras, Ioana Sorina Deleanu, and Brigitte Unger (2019). "Strategies to avoid blacklisting: The case of statistics on money laundering". In: *PloS one* 14.6, e0218532.

Ferwerda, Joras and Peter Reuter (2019). "Learning from money laundering National Risk Assessments: the case of Italy and Switzerland". In: *European Journal on Criminal Policy and Research* 25.1, pp. 5–20.

Financial Action Task Force (n.d.[a]). *Anti-money laundering and counter-terrorist financing measures, Denmark: Mutual Evaluation Report*. [Online; accessed 10. May 2019]. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Denmark-2017.pdf (visited on 2017).

— (n.d.[b]). *Anti-money laundering and counter-terrorist financing measures, Finland: Mutual Evaluation Report*. [Online; accessed 10. May 2019]. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Finland-2019.pdf (visited on 2019).

— (2003). *FATF 40 Recommendations*. FATF Secretariat. URL: https://www.fatf-gafi.org/media/fatf/documents/FATF\%20Standards\%20-\%2040\%20Recommendations\%20rc.pdf.

— (2015). *Guidance for a risk-based approach to virtual currencies*. URL: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

Findley, Michael G, Daniel L Nielson, and Jason C Sharman (2014). *Global shell games: Experiments in transnational relations, crime, and terrorism*. 128. Cambridge University Press.

Findley, Michael G, Daniel L Nielson, and JC Sharman (2015). "Causes of noncompliance with international law: A field experiment on anonymous incorporation". In: *American Journal of Political Science* 59.1, pp. 146–161.

Hafner-Burton, Emilie M (2005). "Trading human rights: How preferential trade agreements influence government repression". In: *International Organization* 59.3, pp. 593–629.

Hamadeh, Nada, Catherine Van Rompaey, and Eric Metreau (2021). *New World Bank country classifications by income level: 2021-2022*. [Online; accessed 2. Feb. 2023]. URL: https://blogs.worldbank.org/opendata/new-world-bank-country-classifications-income-level-2021-2022.

Harding, Luke, Nick Hopkins, and Caelainn Barr (2017). "British banks handled vast sums of laundered Russian money". In: *the Guardian*. URL: https://www.theguardian.com/

world/2017/mar/20/british-banks-handled-vast-sums-of-laundered-russian-money.

Havilland, Paul de (2019). "FATF Issues Draconian Crypto Recommendations: You Now Have 12 Months To Comply | Crypto Briefing". In: *Crypto Briefing*. [Online; accessed 24. Nov. 2019]. URL: https://cryptobriefing.com/fatf-draconian-crypto.

Hickey, Shane (2019). "$32m stolen from Tokyo cryptocurrency exchange in latest hack". In: URL: https://www.theguardian.com/technology/2019/jul/12/tokyo-cryptocurrency-exchange-hack-bitpoint-bitcoin.

Honig, Dan, Catherine Weaver, et al. (2019). "A race to the top? the aid transparency index and the social power of global performance indicators". In: *International Organization* 73.3, pp. 579–610.

Hougan, Matthew, Hong Kim, and Micah Lerner (2019). "Economic and Non-Economic Trading In Bitcoin: Exploring the Real Spot Market For The World's First Digital Commodity". In: URL: https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5574233-185408.pdf.

Hülsse, Rainer (2008). "Even clubs can't do without legitimacy: Why the anti-money laundering blacklist was suspended". In: *Regulation & Governance* 2.4, pp. 459–479.

Kelley, Judith G and Beth A Simmons (2015). "Politics by number: Indicators as social pressure in international relations". In: *American journal of political science* 59.1, pp. 55–70.

— (2020). *The power of global performance indicators*. Cambridge University Press.

Keohane, Robert O (2005). *After hegemony*. Princeton university press.

Kleven, Henrik Jacobsen (2016). "Bunching". In: *Annual Review of Economics* 8, pp. 435–464.

Koerhuis, Wiebe, Tahar Kechadi, and Nhien-An Le-Khac (2020). "Forensic analysis of privacy-oriented cryptocurrencies". In: *Forensic Science International: Digital Investigation* 33, p. 200891.

Kono, Daniel Y (2007). "Making anarchy work: International legal institutions and trade cooperation". In: *The Journal of Politics* 69.3, pp. 746–759.

Krasner, Stephen D (1991). "Global communications and national power: Life on the Pareto frontier". In: *World Politics: A Quarterly Journal of International Relations*, pp. 336–366.

Law of Virgin Islands (2020). *Anti-Money Laundering and Terrorist Financing Code of Practice*. URL: https://www.bvifsc.vg/sites/default/files/anti-money_laundering_and_terrorist_financing_code_of_practice.pdf.

Levi, Michael, Terence Halliday, and Peter Reuter (2014). "Global surveillance of dirty money: assessing assessments of regimes to control money-laundering and combat the financing of terrorism". In.

Levi, Michael, Peter Reuter, and Terence Halliday (2018). "Can the AML system be evaluated without better data?" In: *Crime, Law and Social Change* 69.2, pp. 307–328.

Masciandaro, Donato, Elod Takats, and Brigitte Unger (2007). *Black finance: the economics of money laundering*. Edward Elgar Publishing.

Mavrokonstantis, Panos (2019). "Introduction to the bunching Package". In.

May, Timothy C (1994). *Crypto anarchy and virtual communities*. Timothy C. May.

McMillan, Robert (2018). "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster". In: *Wired*. URL: https://www.wired.com/2014/03/bitcoin-exchange.

Mearsheimer, John J (2017). "The false promise of international institutions". In: *International Organization*. Routledge, pp. 237–282.

Morse, Julia C (2019). "Blacklists, market enforcement, and the global regime to combat terrorist financing". In: *International Organization* 73.3, pp. 511–545.

Möser, Malte et al. (2017). "An empirical analysis of traceability in the monero blockchain". In: *arXiv preprint arXiv:1704.04299*.

Olson, Mancur (2012). "The logic of collective action [1965]". In: *Contemporary Sociological Theory* 124.

Osborne, Hilary (2020). "Luxury London homes still used to launder illicit funds, says report". In: *The Guardian*. URL: https://www.theguardian.com/money/2020/dec/21/luxury-london-homes-still-used-to-launder-illicit-funds-says-report.

Partz, Helen (2018). "Japanese Cryptocurrency Exchange Hacked, $59 Million in Losses Reported". In: URL: https://cointelegraph.com/news/japanese-cryptocurrency-exchange-hacked-59-million-in-losses-reported.

— (2021). "Hacked Liquid exchange receives $120M debt funding from FTX". In: URL: https://cointelegraph.com/news/hacked-liquid-exchange-receives-120m-debt-funding-from-ftx.

Pieters, Gina and Sofia Vivanco (2017). "Financial regulations and price inconsistencies across Bitcoin markets". In: *Information Economics and Policy* 39, pp. 1–14.

Poast, Paul (2012). "Does issue linkage work? Evidence from European alliance negotiations, 1860 to 1945". In: *International Organization* 66.2, pp. 277–310.

Roberts, Daniel (2021). "Binance and Coinbase Say They Have No Headquarters—That's True and Untrue". In: *Decrypt*. URL: https://decrypt.co/70330/binance-cz-coinbase-say-they-have-no-headquarters-true-and-untrue.

Saez, Emmanuel (2010). "Do taxpayers bunch at kink points?" In: *American economic Journal: economic policy* 2.3, pp. 180–212.

Schwarz, Peter (2011). "Money launderers and tax havens: Two sides of the same coin?" In: *International Review of Law and Economics* 31.1, pp. 37–47.

Sharman, Jason C (2010). "Shopping for anonymous shell companies: An audit study of anonymity and crime in the international financial system". In: *Journal of Economic Perspectives* 24.4, pp. 127–40.

— (2011). "Testing the global financial transparency regime". In: *International Studies Quarterly* 55.4, pp. 981–1001.

Simmons, Beth A (2009). *Mobilizing for human rights: international law in domestic politics*. Cambridge University Press.

Spence, Eddie, Jonathan Browning, and Katarina Hoije (2022). "London Laundering Case May Hold Clues to Guinea's Gold". In: *Bloombeg*. URL: https://www.bloomberg.com/news/features/2022-05-13/where-is-guinea-s-gold-a-london-money-laundering-case-may-hold-clues.

Stone, Sam (2022). "2022 Crypto-Exchange Fee Comparison". In: URL: https://www.cointracker.io/blog/2019-crypto-exchange-fee-comparison.

Takats, Elod (2011). "A theory of "Crying Wolf": The economics of money laundering enforcement". In: *The Journal of Law, Economics, & Organization* 27.1, pp. 32–78.

Transparency International (n.d.). *Our Work in Lebanon*. URL: https://www.transparency.org/en/countries/lebanon.

Varshney, Anupam (2021). "Telling the truth? How crypto data aggregators fight fake exchange volumes". In: URL: https://cointelegraph.com/news/telling-the-truth-how-crypto-data-aggregators-fight-fake-exchange-volumes.

Verdugo Yepes, Concha (2011). "Compliance with the AML/CFT International Standard: Lessons from a Cross-Country Analysis". In: *IMF Working Papers*, pp. 1–75.

Walker, John and Brigitte Unger (2009). "Measuring Global Money Laundering:" The Walker Gravity Model"". In: *Review of Law & Economics* 5.2, pp. 821–853.

Weber, Mark et al. (2019). "Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics". In: *arXiv preprint arXiv:1908.02591*.

Willebois, Emile Van der Does de et al. (2011). *The puppet masters: How the corrupt use legal structures to hide stolen assets and what to do about it*. The World Bank.

Withers, Iain (2021). "Bin bags of cash: NatWest fined for dirty money breaches". In: *Retuers*. URL: https://www.reuters.com/business/finance/around-50-natwest-branches-involved-money-laundering-case-fca-2021-12-13/.

Appendices

A FATF Recommendations

A.1 Customer Due Diligence

Recommendation 5[16]

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.[17]

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows

[16] Text taken from Financial Action Task Force 2003, pp. 4–5

[17] Reliable, independent source documents, data or information will hereafter be referred to as "identification data"

who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

A.2 Risk Based Measures for Cryptocurrency Businesses

TABLE OF ACRONYMS[18]

AML	Anti-money laundering
CDD	Customer due diligence
CFT	Countering the financing of terrorism
DNFBP	Designated non-financial business and profession
ML	Money laundering
MVTS	Money value transfer service
NPPS	New Payment Products and Services
RBA	Risk-based approach
TF	Terrorist financing
VC	Virtual currency
VCPPS	VC payment products and services

[18]Text taken from Financial Action Task Force 2015, p. 2.

SECTION IV – APPLICATION OF FATF STANDARDS TO COVERED ENTITIES[19]

40. This section explains how specific FATF Recommendations should apply to Convertible VC exchanges and any other type of entities that act as nodes where convertible VC activities intersect with the regulated fiat currency financial system, to mitigate the ML/TF risks associated with VCPPSs. These should include applying a RBA (Recommendation 1), customer due diligence (CDD) (Recommendation 10); record-keeping (Recommendation 11); registration or licensing requirements for MVTS (Recommendation 14) identification and mitigation of risks associated with new technologies (Recommendation 15); AML/CFT program requirements (Recommendation 18) and suspicious transaction reporting (Recommendation 20). This section also examines current obstacles to applying some of these mitigating measures in the decentralised VC space. Recommendation 14 is discussed only in section III above, but as noted requires covered entities to comply with registration or licensing requirement in all jurisdiction where they provide VC MVTS.

41. **Recommendation 1.** The FATF Recommendations make clear that countries should require financial institutions and DNFBP to identify, assess, and take effective action to mitigate their ML/TF risks (including those associated with VCPPS). This includes ongoing efforts to refine technical processes used to reliably identify and verify customers. For AML/CFT purposes, where VC activities are permitted under national law, all jurisdictions, financial institutions and DNFPBs, including convertible virtual currency exchangers, should assess the ML/TF risks posed by VC activities and apply a RBA to ensure that appropriate measures to prevent or mitigate those risks are implemented. The RBA does not imply the automatic or wholesale denial of services to VCPPS without an adequate risks assessment.

42. **Recommendation 10**. CDD is an essential measure to mitigate the ML/TF risks

[19]Text taken from Financial Action Task Force 2015, pp. 14–16.

associated with convertible VC. In accordance with the FATF Standards, countries should require convertible VC exchangers to undertake customer due diligence when establishing business relations or when carrying out (non-wire) occasional transactions using reliable, independent source documents, data or information.9 For example, convertible VC exchangers should be required to conduct customer due diligence when exchanging VC for fiat currency or vice versa in a one-off transaction greater than the designated threshold of USD/EUR 15 000 of USD/EUR 15 000 or (b) carrying out occasional transactions that are wire transfers covered by Recommendation 16 and its Interpretive Note. Usually, convertible VC transactions will involve a wire transfer and therefore be subject to Recommendation 16.

43. Countries may wish to consider having a lower or no threshold for VC CDD requirements if appropriate, given the nature and level of identified ML/TF risks.

44. In light of the nature of VCPPS, in which customer relationships are established, funds loaded and transactions transmitted entirely through the internet, institutions must necessarily rely on nonface-to-face identification and verification. Countries should consider requiring entities providing VCPPS to follow the best practices suggested in the June 2013 NPPS Guidance. These, to the extent applicable, include: corroborating identity information received from the customer, such as a national identity number, with information in third party databases or other reliable sources; potentially tracing the customer's Internet Protocol (IP) address; and searching the Web for corroborating activity information consistent with the customer's transaction profile, provided that the data collection is in line with national privacy legislation.

45. Where convertible VCPPS are presenting higher risk, as ascertained on the basis of the RBA, convertible virtual currency exchangers should be required to conduct enhanced CDD in proportion to that risk, and encouraged to use multiple techniques to take reason-

able measures to verify customer identity. Where convertible virtual currency exchangers are permitted to complete verification after establishing the business relationship in order not to interrupt the normal conduct of business (in low risk cases), they should be required to complete verification before conducting occasional transactions above the threshold.

46. Countries should also expect financial institutions and DNFBP to consider risks associated with the source of funding convertible VCPPS. Decentralised convertible VCPPS allow anonymous sources of funding, including peer-to-peer (P2P) VC transfers and funding by NPPS that are themselves anonymous, increasing ML/TF risks. As with NPPS, VCPPS business should consider, for occasional transactions above a given threshold, limiting the source of funds to a bank account, credit or debit card, or at least applying such limitations to initial loading, or for a set period until a transaction pattern can be established, or for loading above a given threshold.

47. Transaction monitoring is a key risk mitigant in the convertible VC space because of the difficulty of non-face-to-face identity verification and because it is only recently that decentralised convertible VC technology allows certain risk mitigants that may be available for NPPS to be built into decentralised VCPPS in order to restrict functionality and reduce risk. For instance, multisignature (multi-sig) technology now enables VCPPS to effectively build in loading total wallet value, and value/velocity transaction limits into decentralised VCPPS. However, current decentralised VC technology does not make it possible to effectively build in geographic limits; limit use to the purchase of certain goods and services; or prevent person-to-person transfers.

48. It is recommended that countries encourage transaction monitoring, commensurate with the risk. The public nature of transaction information available on the blockchain theoretically facilitates transaction monitoring, but as noted in the *June 2014 VC Report*

(Appendix A), the lack of real world identity associated with many decentralised VC transactions limits the blockchain's usefulness for monitoring transactions and identifying suspicious activity, presenting serious challenges to effective AML/CFT compliance and supervision.

49. **Recommendation 11**, **Recommendation 20 and Recommendation 22. Record-keeping** and **Suspicious activity** reporting when VC transactions could involve the proceeds of criminal activity or be related to terrorist financing, in accordance with Recommendation 20, are also essential. At a minimum, financial institutions and DNFBP should be required to maintain transaction records that include: information to identify the parties; the public keys, addresses or accounts involved; the nature and date of the transaction, and the amount transferred. The public information available on the blockchain provides a beginning foundation for record keeping, provided institutions can adequately identify their customers. Countries should require institutions to be attentive to the type of suspicious activity they are in a position to detect.

50. **Recommendation 15 and Recommendation 22** specifically addresses new technologies and requires financial institutions and DNFBP to identify and assess ML/TF risks relating to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Recommendation 15 also requires financial institutions and DNFBP licensed by or operating in a jurisdiction to take appropriate measures to manage and mitigate risk before launching new products or business practices or using new or developing technologies. These measures apply in relation to VC as a new technology. National authorities are expected to enforce this obligation, and financial institutions and DNFBP should be proactive in fulfilling the expectations set forth in Recommendation 15.

Table 5: Bunching in Ethereum Trades by Country

	BVI†	**UK**	**Brazil**	**Japan**	**Netherlands**	**Turkey**	**USA**
500	0.148	0.387	−1.316*	−2.678**	−1.112*	2.819***	−2.006
(*Placebo 1*)	(0.790)	(0.360)	(0.571)	(1.113)	(0.519)	(0.776)	(2.207)
1,000	**2.641*****	**2.228*****	**1.893****	**2.198**	**0.281**	**−0.972***	**−4.908***
(*Threshold*)	**(0.636)**	**(0.416)**	**(0.733)**	**(1.360)**	**0.953**	**(0.564)**	**2.490**
1,500	−0.144	0.436	−2.872**	−1.792***	1.282	0.405	0.030
(*Placebo 2*)	(1.240)	(0.293)	(1.065)	(0.531)	(1.163)	(0.508)	(0.798)
N (Placebo 1)	129,240	2,349,026	23,053	141,606	126,380	62,020	92,642
N (Threshold)	63,760	2,085,235	17,497	62,899	58,436	9,443	35,359
N (Placebo 2)	23,049	1,491,636	16,353	47,308	40,287	1,850	10,150
Exchanges	1	2	2	3	3	2	2
Pairs	1	5	2	4	4	2	2

Notes: Bunching by country between 06/21/20 and 09/02/20 in the 10 bins (100 dollars/euros) below the threshold. Pairs denotes the number of trading pairs and exchanges denotes the number of exchanges included in each estimate; standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001. † British Virgin Islands.

B Results for Ethereum-to-fiat Trades

B.1 Dollar Value of Statistically Significant Bunching in Trades from Ethereum

I also calculate the total dollar value of statistically bunching with regulated exchanges for transactions from Ethereum. These results show statistically significant bunching below the threshold in some countries' exchanges – the British Virgin Islands, the United Kingdom, and Brazil – but not others – Japan, the Netherlands, Turkey, and the United States. Once again, there is no statistically significant bunching below the threshold in U.S. or Turkish-based exchanges. Estimates of bunching range from 2.6 times greater transactions than expected in British Virgin Islands-based exchanges to roughly twice greater in exchanges based in the

United Kingdom and Brazil. As with country-level estimates of Bitcoin-to-fiat trades, there is no robust evidence of positive or negative bunching below the placebo thresholds of 500 and 1,500 dollars/euros.

Table 6: Ethereum Trades Bunching Dollar Value by Country

Country	**Trades Value** (M USD)	**Bunching Volume** (% of All Transactions)
United Kingdom	45.8	0.37
British Virgin Islands	3.2	0.41
Brazil	0.06	0.53

Notes: Dollar values in millions of statistically significant bunching by country for Ethereum-to-fiat trades between 06/21/20 and 09/02/20. Column 3 shows this dollar value as a percent of the value of all transactions in the country during the data collection period.

C Robustness Checks

As a robustness check, I estimate bunching in the 70 units below the threshold for trades from Bitcoin and Ethereum to fiat currency by country. Looking at the 70 units below the threshold offers an alternate specification to the 100 units used in Table 4 and Table 5 and offers a robustness check by testing for bunching within a narrower band below the threshold.

Table 7 presents estimates of bunching in the 70 euros/dollars below the threshold or transactions from Bitcoin to fiat currency by country. As in Table 4, Estonia shows the highest levels of bunching, and Brazil, the United Kingdom, the British Virgin Islands, and the Netherlands also show statistically significant bunching. However, two countries (Japan and Australia) that show statistically significant bunching in the 100 units below the threshold do not show similar bunching in the 70 units below it. Once again, Turkey and the United States do not show statistically significant bunching below the threshold. These results generally confirm those found in Table 4, though with the exception of two countries

Table 7: Bunching in Bitcoin Trades by Country (70 units below threshold)

	Estonia	**Brazil**	**UK**	**BVI**†	**Netherlands**	**Japan**	**Turkey**	**USA**	**Australia**
500	1.651	−1.734***	0.203	1.073	10.775	3.707***	4.262***	4.662**	−0.931
(*Placebo*)	(1.370)	(0.522)	(0.198)	(1.895)	(7.965)	(1.065)	(1.121)	(1.608)	(2.328)
1,000	**66.791*****	**4.894*****	**2.149*****	**2.059*****	**1.769***	**1.392**	**0.750**	**0.453**	**0.172**
(*Threshold*)	**(9.630)**	**(0.718)**	**(0.560)**	**(0.637)**	**(0.788)**	**(1.282)**	**(0.677)**	**(2.870)**	**(1.029)**
1,500	2.174	0.947	−0.022	−0.320	−0.463	−1.895***	1.749**	1.701**	1.517
(*Placebo*)	(1.912)	(0.612)	(0.120)	(0.287)	(0.848)	(0.476)	(0.616)	(0.606)	(1.332)
Exchanges	1	3	3	2	1	4	2	3	1
Pairs	1	3	6	5	1	6	2	3	1

Notes: Bunching by country between 06/21/20 and 09/02/20 in the 7 bins (70 dollars/euros) below the threshold. Pairs denotes the number of trading pairs and exchanges denotes the number of exchanges included in each estimate; standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001. † British Virgin Islands.

that do not show bunching in the 70 units below the threshold.

I also test the robustness of the results in Table 5 by estimating bunching in the 70 units below the threshold for Ethereum-to-fiat trades by country. Two countries that show statistically significant bunching in Table 5 (the British Virgin Islands and the United Kingdom) also show bunching under this specification, while one that does not show bunching in Table 5 (Japan) shows bunching in the 70 units below the threshold. Though Brazil shows bunching in the 100 units below the threshold, it does not show bunching in the 70 units below the threshold. The remaining three countries (the Netherlands, Turkey, and the United States) once again do not show statistically significant bunching below the threshold. This robustness check generally confirms the results found in Table 5.

D Trading Pairs Summary

Table 8: Bunching in Ethereum Trades by Country (70 units below threshold)

	Japan	**BVI**†	**UK**	**Brazil**	**Netherlands**	**Turkey**	**USA**
500	−1.581	0.100	0.338	−1.781***	−0.324	2.329***	−1.046
(*Placebo*)	(1.056)	(0.663)	(0.294)	(0.477)	(0.507)	(0.633)	(2.181)
1,000	**3.200****	**2.507*****	**1.764****	**0.999**	**0.701**	**−0.272**	**−2.549**
(*Threshold*)	**(1.293)**	**(0.523)**	**(0.342)**	**(0.601)**	**0.857**	**(0.545)**	**8.421**
1,500	−1.630***	0.340	0.196	−2.039*	1.756	0.892	0.427
(*Placebo*)	(0.428)	(1.058)	(0.242)	(0.949)	(1.046)	(0.463)	(0.716)
Exchanges	3	2	2	1	1	2	2
Pairs	4	2	5	1	1	2	2

Notes: Bunching by country between 06/21/20 and 09/02/20 in the 7 bins (70 dollars/euros) below the threshold. Pairs denotes the number of trading pairs and exchanges denotes the number of exchanges included in each estimate; standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001. † British Virgin Islands.

E Fees by Cryptocurrency Exchange

Table 10 shows fees at select major cryptocurrency exchanges as of January 1, 2021.[20] Most exchanges operate on a percentage base fee structure, which should not influence incentives around the size of each trade. Several exchanges offer volume discounts or (occasionally) flat fees, measures that should encourage traders to execute larger rather than smaller transactions.

F Crypto-to-Fiat Price Changes

Figures 4a and 4b show variation in the average Bitcoin-to-dollar and Ethereum-to-dollar exchange rates during the data collection period.[21] Figures 5b and 5a show variation in the

[20] Text taken from Stone 2022.

[21] "Bitcoin" n.d.; "Ethereum" n.d.

Table 9: Trading Pairs Summary

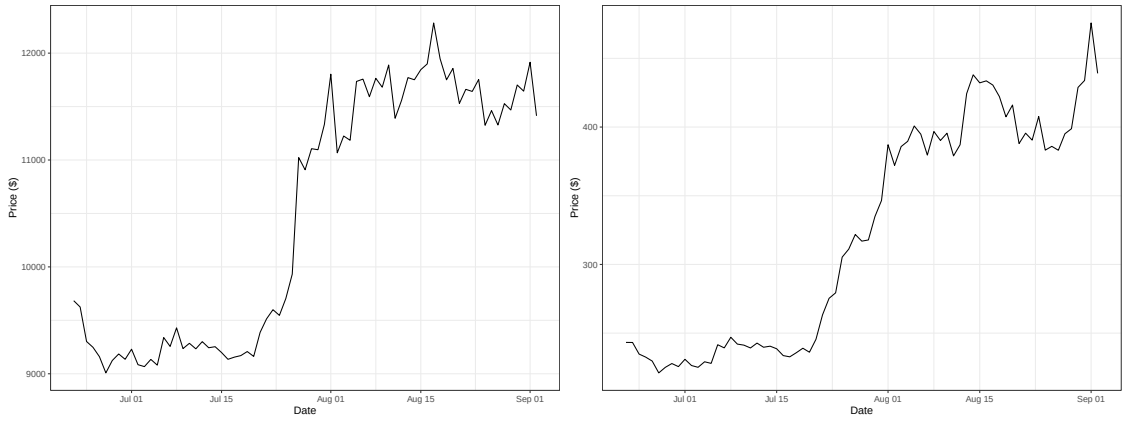
	Count of Trading Pairs	
Fiat Currency	**Bitcoin**	**Ethereum**
Australian Dollar	2	0
Brazilian Real	3	1
Euro	6	6
British Pound	2	1
Indian Rupee	1	1
Japanese Yen	5	4
South Korean Won	3	3
Russian Ruble	2	0
Turkish Lira	3	3
US Dollar	10	9
Total	37	28

Notes: Table shows the number of pairs in the sample for each crypto-to-fiat trade. Each count represents the number of exchanges that offered that trading pair.

Table 10: Fees by Cryptocurrency Exchange

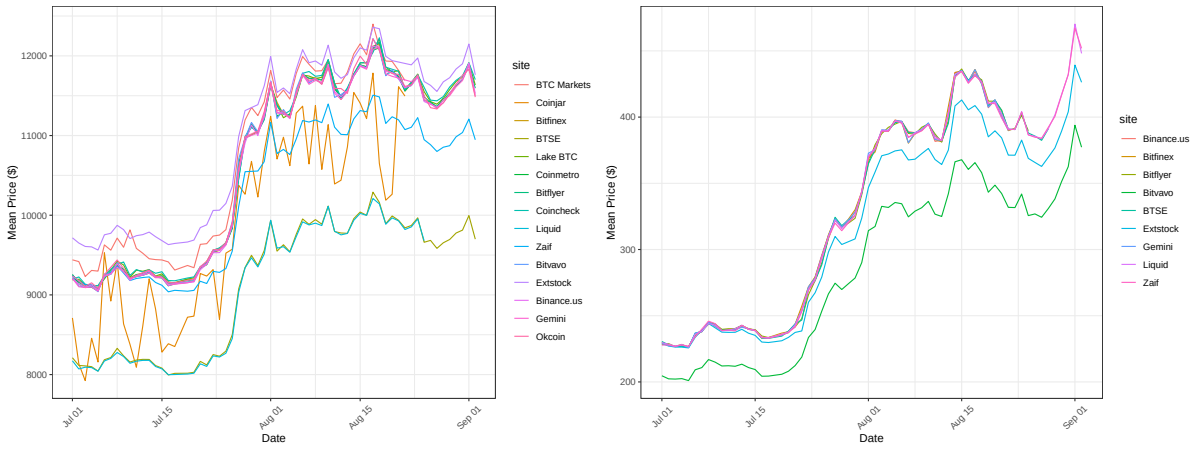
	Trading Fees			Funding Fees		Discounts	
Exchange	**Maker**	**Taker**	**Spread**	**Deposits**	**Withdrawals**	**Exchange Token Discount**	**Volume Discount**
Binance.us	0.1%	0.1%	No	No	No	Yes - 25%	Yes
Binance.com	0.1%	0.1%	No	No	Yes	Yes - 25%	Yes
Bitfinex	0.1%	0.2%	No	No	Yes	No	Yes
Bitstamp	0.5%	0.5%	No	No	Yes	No	Yes
Bittrex	0.35%	0.35%	No	No	Yes	No	Yes
Bitmex	0.025%	0.075%	No	No	No	No	Yes
BTC Markets	0.05%	0.2%	No	No	Yes (AUD Free)	No	Yes
Bybit.com	-0.025% (Rebate)	0.075%	No	No	No	No	No
CEX.IO	0.16%	0.25%	No	No	Yes	No	Yes
Coinbase	N/A	The greater of flat fee ($1.49, $1.99 & $2.99) or 1.49%	0.50% fiat 1.00% crypto	No	No	No	Yes
Coinbase Pro	0.5%	0.5%	No	No	No	No	Yes
crypto.com	0.1%	0.16%	No	No	Yes	No	Yes
Gemini	The greater of flat fee ($0.99, $1.49, $1.99 & $2.99) or 1.49%	The greater of flat fee ($0.99, $1.49, $1.99 & $2.99) or 1.49%	No	No	No	No	Yes
HitBTC	0.1%	0.25%	No	No	No	No	Yes
Huboi	0.2%	0.2%	No	No	No	Yes	Yes
Kraken	0.16%	0.26%	No	No	No	No	Yes
Liquid	0.29%	0.29%	No	No	Yes	Yes	Yes

Figure 4: Caption



(a) Bitcoin Prices (b) Ethereum Prices

Figure 5: Caption



(a) Bitcoin Prices by Exchange (b) Ethereum Prices by Exchange

average Bitcoin-to-dollar and Ethereum-to-dollar exchange rate by exchange for a selection of exchanges included in the sample.

G Data Cleaning Procedure

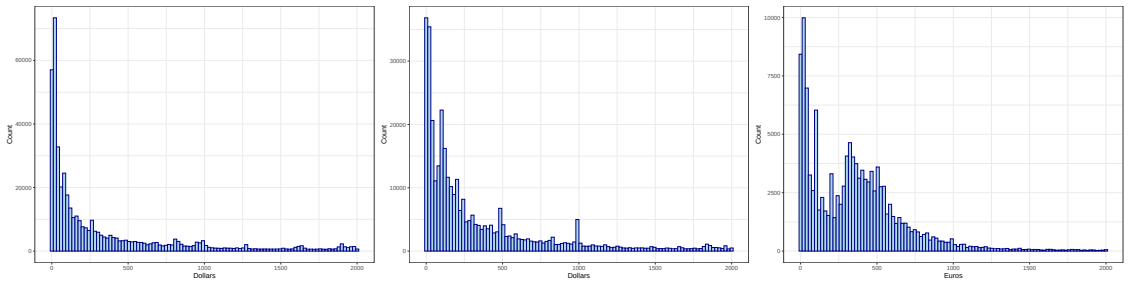
I performed several steps to prepare the data for analysis. First, I removed data from 5 exchanges where the country of registration could not be determined and from 3 exchanges with registrations in multiple jurisdictions. I also excluded trading pairs with low transaction

volumes (less than an average of 30 transactions per hour) because the statistical method I use (bunching estimation) requires sufficiently frequent observations to estimate valid parameters. In total, these low-volume pairs accounted for only 0.5% of all transactions close to the threshold (within 500 dollars/euros), assuaging concerns that their removal would substantially influence the results. Lastly, I excluded data from 5 exchanges that show abnormal distributions within their trading pairs given the high likelihood that they include fake data (more details are provided in Section H).

H Fake Data

Typical transaction data from cryptocurrency exchanges feature bunching at round quantities of cryptocurrency or values of fiat currency as well as other types of anomalies. Figure shows distributions from several exchanges that show bunching at round numbers and other idiosyncrasies present in most transaction data(Figure 6).

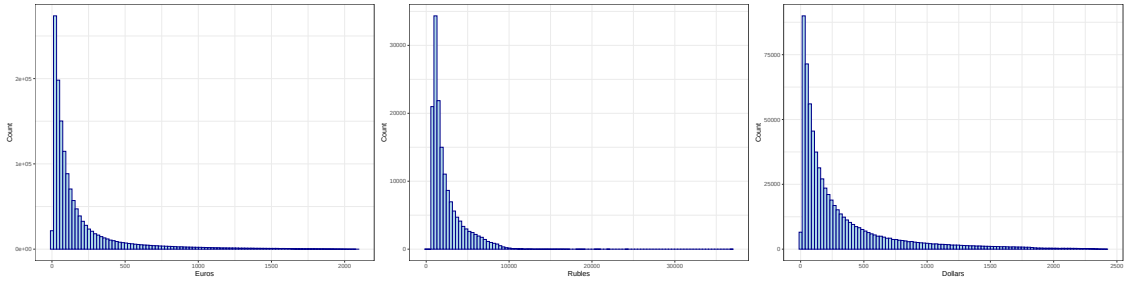
Figure 6: Example Distributions Across Trading Pairs



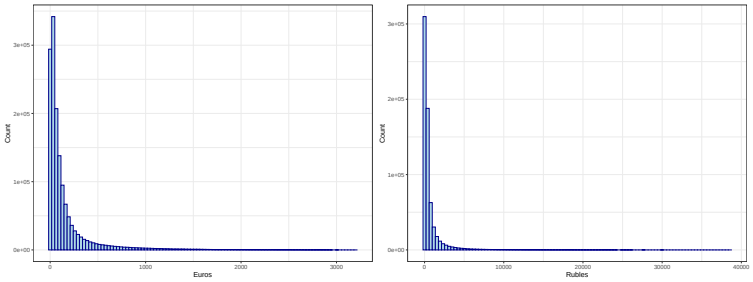
(a) Bittrex: Bitcoin-Dollar (b) Gemini: Bitcoin-Dollar (c) Bitvavo: Ethereum-Euro

I suspect that four exchanges in the sample feature fake transaction data as the distributions resemble an exponential distribution or other unusual distribution. Figure 7 shows distributions for trading pairs in Coinsbit, Figure 8 for pairs in Cryptology, Figure 9 for pairs in Folgory, Figure 10 and for pairs in Whitebit. All of these exchanges were registered in Estonia during the data collection period.

Figure 7: Coinsbit



(a) Bitcoin-Euro (b) Bitcoin-Ruble (c) Bitcoin-Dollar

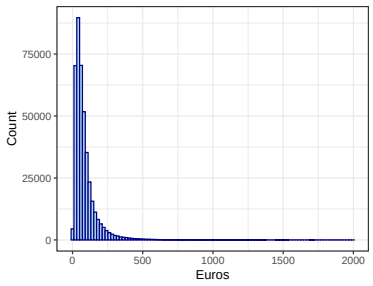


(d) Ethereum-Euro (e) Ethereum-Ruble

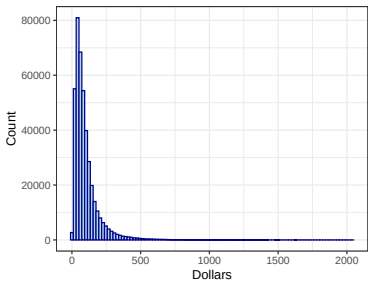
The graphs show that trading pairs in Coinsbit, Cryptology, and Whitebit resemble an exponential distribution, while trades in Folgory feature an unusual pattern in which the number of transactions decrease significantly past a certain fiat value. Further, the trading pairs within each exchange follow a similar distribution, which is unusual as there is often variation in the distributions of transactions across trading pairs.[22] For a more detailed discussion of fake transaction volume within exchanges, see Chen, Lin, and Wu (2022).

[22]For example, many exchanges feature higher transaction volumes for cryptocurrency trades to dollars or euros, which often results in a different distribution of transactions for these trading pairs than trades to other fiat currencies.

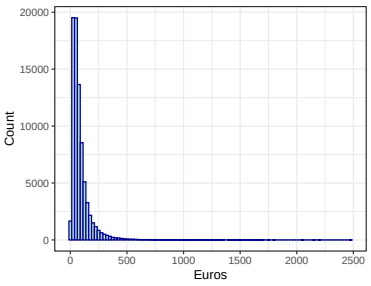
Figure 8: Cryptology



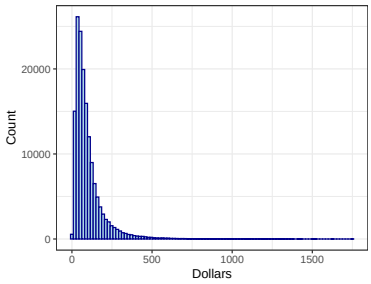
(a) Bitcoin-Euro



(b) Bitcoin-Dollar

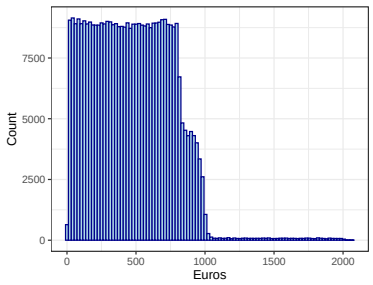


(c) Ethereum-Euro

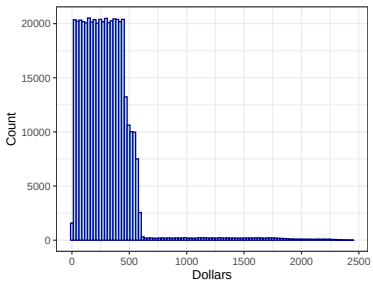


(d) Ethereum-Dollar

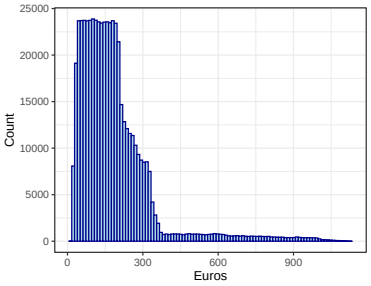
Figure 9: Folgory



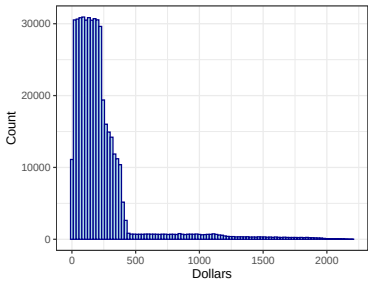
(a) Bitcoin-Euro



(b) Bitcoin-Dollar

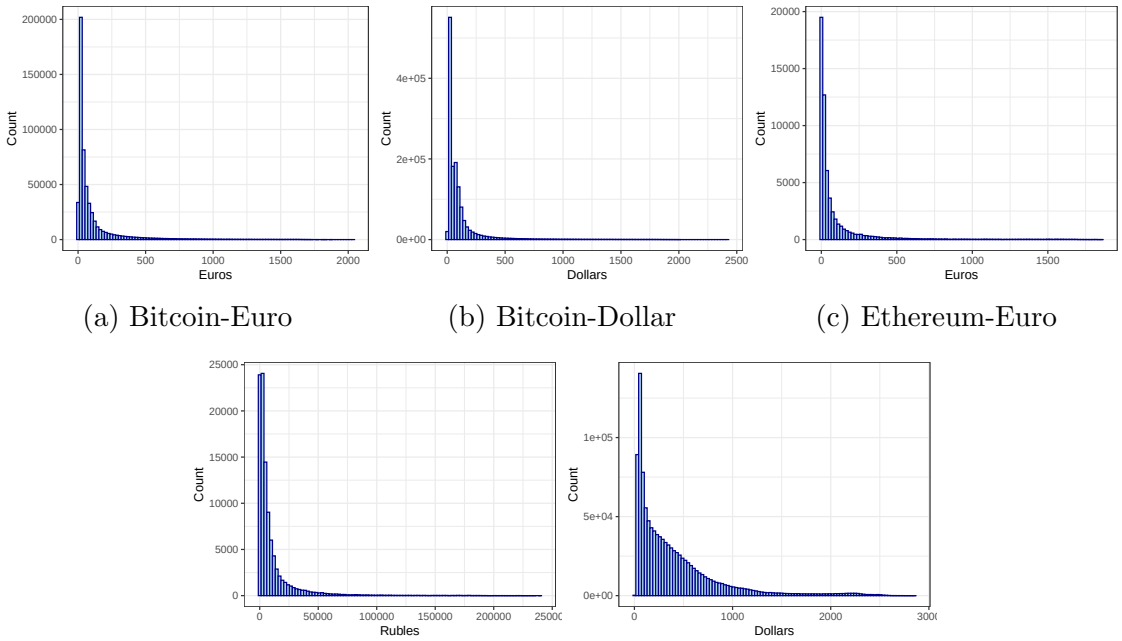


(c) Ethereum-Euro



(d) Ethereum-Dollar

Figure 10: Whitebit



(a) Bitcoin-Euro (b) Bitcoin-Dollar (c) Ethereum-Euro

(d) Ethereum-Ruble (e) Ethereum-Dollar