How Strong Are International Standards in Practice?

Evidence from Cryptocurrency Transactions*

Karen Nershi†

August 9, 2022

Abstract

The rise of cryptocurrency (decentralized digital currency) presents challenges for state regulators given its connection to illegal activity and pseudonymous nature, which allows both individuals and businesses to engage in regulatory arbitrage. In this paper, I assess the degree to which states have managed 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 must 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 allow for 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

In February 2022, the Department of Justice charged two 30-somethings with conspiring to money launder (i.e., integrate illegally-obtained funds into the legitimate economy) $4.5 billion worth of stolen cryptocurrency from a 2016 hack of Bitfinex, a cryptocurrency exchange. Crucial to the success of these investigative efforts, exchanges, which allow individuals to convert cryptocurrency to fiat (government-issued) currency and vice versa, had recently implemented new anti-money laundering measures.[1] This example highlights the ambiguous implications of cryptocurrency for money launderers: on the one hand, cryptocurrency transactions are largely obscured from government scrutiny because a person's cryptocurrency wallet can rarely be linked to her legal identity. On the other hand, the open-source and decentralized nature of this technology provides a permanent record that states can leverage to investigate cryptocurrency-related crimes months or even years after they have taken place. Yet in order to leverage these records, states must implement effective anti-money laundering regulation, which requires them to overcome the challenge of regulatory arbitrage as both individuals and exchanges may otherwise circumvent national regulations by accessing (or providing) services from other jurisdictions. Thus, a coordinated international response is necessary to overcome the challenge posed by regulatory arbitrage; in this paper, I assess the success of one such recent effort.

Since the introduction of Bitcoin in 2009, cryptocurrency has attracted attention due to its unique features that offer high levels of secrecy. Specifically, cryptocurrency requires users to create a digital wallet (a unique numerical key) to send or receive currency from others; these digital wallets are not linked to public identities, which has allowed cybercriminals to transact cryptocurrency mostly free of the fear that authorities will ascertain their identities. However, the introduction of anti-money laundering laws offers states a way to chip away at this secrecy by requiring cryptocurrency exchanges to collect and keep records of a user's

[1] I refer to government-issued currency as "fiat" throughout the paper.

legal identity tied to a digital wallet for some types of transactions. Authorities can later access these records during money laundering investigations.

Although cryptocurrency has helped give rise to a new ecosystem of cybercrime,[2] governments were initially slow to regulate the sector. This changed in 2019 when the Financial Action Task Force (FATF) – an intergovernmental organization dedicated to setting international anti-money laundering standards – issued a new set of regulatory guidelines for cryptocurrency exchanges. The FATF's directive stipulates that cryptocurrency exchanges must adopt new measures to screen their customers for money laundering risk (FATF 2019). All 36 FATF member states (including the United States, many European Union countries, China, Japan, and others) agreed to incorporate these standards into national law within a year.

Cryptocurrency presents a good case to study cross-national efforts to enforce common international standards because unique factors around the adoption of these laws eliminate many of the confounders present in similar cases. Specifically, a common group of countries (FATF members) agreed to implement common standards (stipulated in the directive) (FATF 2019) within a given time period (one year) for an issue without much prior regulation. This helps to mitigate concerns about selection bias, temporal bias, time-varying treatment effects, and path dependence by offering a clear one-to-one comparison of adoption and enforcement by FATF members. Cryptocurrency also presents a good case due to the availability of transaction-level data that is typically unattainable for other types of businesses that enforce anti-money laundering laws. Thus, while most other businesses like banks and law firms are notoriously secretive with customer data, most cryptocurrency exchanges, by contrast, share information about the time, amount, and type of each transaction through public application programming interfaces (APIs). Accordingly, I leverage this publicly available data to collect a new dataset of crypto-to-fiat transactions across 66 exchanges during a two-month period in 2020.

[2]Cryptocurrency-related crime is estimated to have totaled $14 billion in 2021, although it is worth noting that this is still a relatively small portion of all cryptocurrency activity (Chainalysis 2022, p. 3).

I use this new dataset along with bunching estimation – an econometric strategy that employs the mass of a distribution to study how individuals respond strategically to an incentive by sorting below it – to measure the excess number of transactions (bunching) below the threshold above which exchanges are required by law to perform *customer due diligence*, a screening protocol for money laundering risk. I provide country-level estimates of bunching within exchanges and find that most, but not all, regulated countries show statistically significant bunching below the due diligence threshold, although I find no similar pattern in the trades of unregulated countries. I find similar results in both Bitcoin-to-fiat and Ethereum-to-fiat transactions (the two highest volume cryptocurrencies), and the results are robust to the testing of placebo thresholds. These findings are consistent despite varying crypto-to-fiat prices over time and across exchanges as well as the fact that some trades are made into non-threshold fiat currencies (e.g., Japanese yen, Turkish lira, etc.).

Based on these results, I draw two broad conclusions about the success of countries' efforts to enforce anti-money laundering standards in the cryptocurrency sector. First, the presence of bunching across most countries suggests that exchanges in regulated countries are enforcing customer due diligence at the threshold, which creates an incentive for users to shift transactions below it. This represents an important accomplishment, as most exchanges were unlicensed and unregulated before 2020. Second, the persistence of bunching over time suggests that exchanges are not adequately enforcing *risk-based measures*, which are additional measures that require exchanges to identify and address suspicious trends. Thus, although countries have made significant progress in implementing anti-money laundering standards for cryptocurrency exchanges, gaps in enforcement across countries allow for regulatory arbitrage.

These findings add to the small but growing body of literature that documents enforcement gaps in the international anti-money laundering regime (Findley, Nielson, and Sharman 2014; Findley, Nielson, and Sharman 2015; Levi, Reuter, and Halliday 2018; Ferwerda and Reuter 2019). These findings are important because one of the primary ways the FATF

has assessed states' efforts is by technical compliance with legal standards, which tells us little about how well laws are enforced in practice. Indeed, these findings add to evidence from large-scale data leaks like the Panama Papers and high profile money laundering cases to support the conclusion that even though most countries have adopted tough anti-money laundering laws, enforcement across countries remains varied and in some cases lax. Accordingly, this research underscores the need for national-level assessments based on enforcement in order to understand how well countries' systems function in practice, something the FATF has begun to shift toward in recent years (Financial Action Task Force 2013-2021).

These findings also hold significance for the international cooperation literature more broadly, as a key line of inquiry focuses on how international organizations shape state behavior. One major challenge for this literature, however, is that many of the contexts in which researchers might study these questions are subject to selection bias (as countries' adoption of new laws or standards is rarely exogenous) or other potential confounding factors (Ashworth, Berry, and Mesquita 2021, Ch. 5). Accordingly, this study offers a causally-identified way to study the cross-national enforcement of common standards whose adoption was prompted by an intergovernmental organization, the FATF. My results show that states have made significant progress toward implementing the new standards, supporting the conclusion that the FATF has had an important impact on state behavior. However, the results also suggest that the organization struggles to push countries to achieve high levels of enforcement for measures that are subject to greater discretion and more difficult for outsiders to objectively assess.

The rest of the paper is organized as follows: in section 2, I provide an overview of the way that cryptocurrency has challenged traditional notions of state power as well as the challenges states face in regulating this new technology. In section 3, I present the new anti-money laundering standards in more detail and predict trends that may emerge as states adopt the new standards. In section 4, I detail my data collection strategy, and in section 5, I outline the empirical strategy. Finally, in sections 6 and 7, I provide the results and a

discussion, followed by concluding thoughts in section 8.

2 Cryptocurrency: A Threat to State Power

Political scientists have long defined states by their monopoly over the legitimate use of force within a territory (Weber 2013), but for at least the last 500 years, one might add an additional function – issuing a national currency. National currencies have helped solidify the power of sovereign rulers and aided in the process of state building. Modern states in particular have come to depend on control of the money supply as a vital policy tool to moderate the impact of economic cycles within capitalist systems. And although many have come to view managing a currency as a state's right, a few argue that access to third-party "private currencies" would help correct inefficiencies in government management of the money supply (e.g., inflation) and offer individuals greater control over their daily lives. Below, I briefly recount the evolution of currency as a tool for sovereigns and state building, as well as arguments by those who claim that this control should no longer be afforded exclusively to states. I then provide an overview of the primary challenges states face when seeking to regulate cryptocurrency, which has emerged as a potential challenger to state-backed currencies.

2.1 National Currencies and State Building

The modern relationship between sovereigns and money began modestly, with sovereigns during the Middle Ages serving to verify the weight and validity of precious metals in coins as part of a standardization process (Naismith 2018, pp. 3–5); however, over time, sovereigns realized that control over the money supply could offer certain advantages that would aid in their efforts to consolidate wealth and power (Hayek 2009). Some began diluting the amount of precious metals in coins while continuing to stamp the coins with an official seal, forcing citizens to accept coins that were worth less in material terms as legal tender (Hayek 2009).

Others seized control of minting privileges and then charged segniorage (a fee for minting new coins) that often far exceeded the costs of manufacturing the coins themselves. National currencies also aided rulers in consolidating their power militarily, as the introduction of national currencies made it easier to tax citizens and provided a line of credit that allowed rulers to fund wars by running a deficit (Hayek 1976; Hayek 2009; Glasner 2020).

Maintaining a national currency also helped rulers secure prestige. Although initially, rulers conferred legitimacy onto coins through the use of a royal seal (often depicting the sovereign) that verified the veracity of the coin, the circulation of coins bearing the sovereign's seal often came to confer legitimacy onto the sovereigns themselves (Hayek 2009). In particular, coins allowed the sovereign's image to circulate to all reaches of the empire, which served as a daily reminder to her citizens of the ruler's power and prestige (Hayek 2009; Helleiner 1998). Some superstitious peasants even came to believe that it was the royal seal itself that conferred value onto coins rather than the precious metals from which they were made (Hayek 2009).

Beyond bestowing legitimacy on rulers, national currencies have helped solidify the development of modern states (Polanyi 2001; Helleiner 1998; Helleiner 1999; Helleiner 2018; Lauer 2008). In particular, national currencies have aided the horizontal integration of states by providing a common medium of exchange to ease transactions within a state's geographic boundaries; this "common national economic language" has helped to create a sense of a shared economic identity among citizens while also creating a clear distinction between a country and its neighbors (Helleiner 1998; Lauer 2008, p. 1414). National currencies have also aided the vertical integration between rich and poor members of society by binding all citizens' economic fortunes together and making them dependent on the success of a common national currency (Helleiner 1998). At an even more fundamental level, the introduction of a national currency has helped foster trust among citizens, as it requires citizens to trust that their compatriots will honor the national currency as a store of value – trust that ultimately flows from belief in the state as a guarantor of the national currency (Lauer 2008). In addi-

tion to material factors, a national currency can help create common national identities by sharing common symbols, patriotic imagery, and the depiction of important moments in a country's history on paper money (Lauer 2008; Helleiner 1998).

More recently, national monetary policy has emerged as an important policy tool. Since the end of World War II, most liberal democracies have adopted counter-cyclical monetary policy, leading central banks to *increase* the money supply (lower interest rates) during economic recessions to stimulate consumer spending and *decrease* the money supply (raise interest rates) during economic booms in order to stem frenzied spending. Accordingly, monetary policy provides countries with a powerful tool that can be used to mitigate the impact of booms and busts that are common within a capitalist system. For all these reasons, national currencies played an integral role in state power for hundreds of years and received little scrutiny as a state's inherent right until the middle of the 20^{th} century.

2.2 Private Currencies

One of the first dissenting voices in the modern debate over states' control of the money supply came in 1976 with Friedrich Hayek's *Choice in Currency: A Way to Stop Inflation* (Hayek 1976). Hayek, a well-known advocate of free markets and limited government intervention in the economy, argues that citizens' dependence on national currencies has allowed governments to increase the money supply leading to inflation. He argues that if citizens instead had access to alternative "private currencies," governments would be forced to adhere to fiscal discipline or else risk that citizens will abandon the national currency in favor of a better store of value during inflationary periods. Interestingly, Hayek argues that the most revolutionary part of his proposal is simply the idea that a state's exclusive right to issue money can be challenged, as this has been so widely accepted as a state's right and duty (Hayek 1976).

Two decades later, a group known as the Cypherpunks embraced the idea of private currency as part of a broader government-limiting agenda. The group, which included prominent

mathematicians and computer programmers and was influenced by libertarian and even anarchist ideals, coalesced on an online anonymous message board and shared thoughts on how new developments in cryptography might offer a "technological solution to the problem of too much government" (May and Hughes 1992; May 1994; May 1992). The culmination of their libertarian ideology is the concept of *crypto anarchy* – a Utopia in cyberspace in which governments would be "forbidden" and individuals could speak and transact freely through the use of pseudonymous identities. Central to this idea was the belief that an individual must be able to maintain her right to pseudonymity and reveal her true name and location only if she pleased (Hughes 1993). If individuals were not required to reveal their true identities, the Cypherpunks argued, the role of governments would become defunct, because there could be no coercion or physical violence without knowledge of an individual's true identity or location (May 1992; Dai 1998). In addition to encrypted communication, the Cypherpunks viewed the ability to transact pseudonymously as a key component of individual autonomy that must be developed in order to pave the way for crypto anarchy (May 1994; Dai 1998).

Although the Cypherpunks believed that states would try to regulate crypto-technologies, they predicted that states would prove unsuccessful due to a form of *regulatory arbitrage*. Specifically, they reasoned that because crypto-technology is accessed through cyberspace (which is untethered to a geographic location) and encryption provides the ability to obfuscate one's geographic location, any state's efforts to impose laws in cyberspace might be avoided by a savvy digital actor who disguises her physical location in order to access services from "another jurisdiction " (Hughes 1993; May 1994). Further, they argued that the non-physical nature of cyberspace would create legal ambiguity about which country's laws should apply in transactions involving citizens and businesses in different countries (May 1994). Accordingly, the Cypherpunks predicted that any state's attempt to exert power in cyberspace would be rendered impotent by the power of cryptographic technology and the transnational nature of cyberspace.

In addition to the risk of regulatory arbitrage by individuals, cryptocurrency exchanges have shown a willingness to avoid national regulation by changing jurisdictions. In particular, cryptocurrency exchanges have taken advantage of the fact that they operate mostly or entirely online to change national headquarters in response to new regulation. One case that illustrates this well is Binance, which is also one of the biggest cryptocurrency exchanges. Binance was formed in China in 2017 and moved to Japan the same year following new Chinese restrictions for cryptocurrency. After the Japanese government also introduced new regulations in 2018, Binance relocated to Malta. In 2019, however, Maltese regulators took the unusual step of issuing a statement denying that Binance was registered in the country. At various other times, Binance has claimed it was registered in the Cayman Islands and the Seychelles (Roberts 2021). Throughout Binance's many changing locations, it was often unclear what physical presence if any the company maintained in these countries.

In case Binance's frequently changing addresses did not appear suspicious enough, the company's CEO, Changpeng Zhao, refused to disclose the exchange's location during a 2020 interview. Far from a one-time gaffe, Zhao came to promote non-disclosure of the company's headquarters as an official company position, arguing that Binance was a new type of company without company headquarters and accordingly, should not be subject to regulation (Baker 2020). Although Binance has since registered specific branches of the company within several countries (e.g., Binance US is registered in the United States), the company's bold denial of a state's rights to regulate cryptocurrency companies seems to have left an impression among other cryptocurrency exchanges, with at least one other exchange (Coinbase) claiming that it has no headquarters and thus is not subject to any country's jurisdiction (Roberts 2021).

Although regulatory arbitrage and actions by cryptocurrency exchanges present major challenges for national regulators, the regulatory efforts examined in this paper are unique in that they involve a *coordinated international effort* led by some of the world's wealthiest and most powerful countries. This effort began in June 2019, when the FATF issued new

guidance for cryptocurrency exchanges. The 36 FATF member countries pledged to incorporate these standards into national law and begin enforcing them within one year, a pledge that was later affirmed by the Organization for Economic Co-operation and Development (OECD) countries. Accordingly, the coordinated nature of these efforts provides a chance to overcome regulatory arbitrage and attempts to evade regulations by exchanges themselves, but ultimately the success of these efforts will depend on how well all participating countries enforce these standards in practice.

3 New Regulations for Cryptocurrency Exchanges

The FATF's new regulatory standards for cryptocurrency exchanges are implemented in a top-down fashion by states. At the highest level, national legislators incorporate the new recommendations into law. One level down, national regulators supervise cryptocurrency exchanges to ensure they adhere to the standards, and they hold the power to fine exchanges (or impose other penalties) for failures to comply with national laws. At the lowest level, cryptocurrency exchanges must change their operating procedures to ensure they comply with the new standards.

The FATF's regulatory guidelines for cyrptocurrency articulate two main obligations for cryptocurrency 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 that exchanges 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 diligence for transactions below the threshold that are deemed high

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

risk (FATF 2019, p. 15).[4] Thus, although customer due diligence is clearly articulated with a clear rationale for when to apply it, 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, and requires a company to invest in highly skilled personnel, employee training, and often outside consultants or evaluators. Further, many of these measures may be difficult for national regulators (who supervise exchanges) to assess, which may lead some exchanges to minimize investment in these measures. Below, I detail two specific predictions for countries' efforts to implement anti-money laundering regulations for cryptocurrency exchanges.

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 some by prominent members of the cryptocurrency community, who have argued that anti-money laundering regulations will drive criminals away from laundering in 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 reacted to anti-money laundering laws for other sectors, I argue that at least some criminals will likely adapt their behavior to launder funds in regulated exchanges because of the *secrecy-security paradox* (Masciandaro, Takats, and Unger 2007, p. 155).

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

[5] I use this same definition for the remainder of this section.

Money launderers across all sectors face a tradeoff between the secrecy and security of a potential investment. 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 as many of the world's safest and most lucrative investments are located in wealthy Western countries that also have strict anti-money laundering laws in place as well as governments strong enough to investigate and prosecute money laundering crimes (Masciandaro, Takats, and Unger 2007, p. 155). Thus, while a criminal *could* invest in real estate in Lebanon (one of the most corrupt countries in the world) (Transparency International n.d.) and likely bribe bank employees to avoid due diligence screening, holding real estate in Beirut is generally far less attractive to investors than holding real estate in New York, London, or Paris. When faced with this tradeoff, many money launderers have responded by exploiting weaknesses in anti-money laundering enforcement within wealthy countries in order to access investments that offer a high level of security and an acceptable level of secrecy.[6]

For launderers of cryptocurrency, the security-secrecy paradox suggests that at least some criminals will continue to use regulated exchanges because the only alternatives are less secure and more difficult to use (Deer 2022). Criminals are unlikely to shift a majority of their activity to more secretive peer-to-peer trading sites on the dark web 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). 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 safer, regulated exchanges as the cryptocurrency sector has been rife with scams, theft, and the misappropriation of users' funds within exchanges. Given these constraints, it is likely

[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. See Konotey-Ahulu (2020), Osborne (2020), Stokel-Walker (2019), Story and Saul (2015), Levinson-King (2019), and Hoekstra (2019).

that some cryptocurrency launderers will strategically adapt their behavior within regulated exchanges to minimize the risk of detection rather than abandoning them altogether.

3.2 Wealthy Countries Are Not Immune to Laundering Risks

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, including: their extensive capabilities make implementing these measures possible (Verdugo Yepes 2011, p. 12); they have reputations for low levels of corruption and high rule of law; and these countries seek to safeguard their international reputations (Morse 2019). However, there is little evidence that OECD countries are better enforcers of anti-money laundering laws than other countries (Willebois et al. 2011; Sharman 2010; Findley, Nielson, and Sharman 2014). Instead, audit-based tests show that for one particular type of business (corporate service providers), businesses in so-called tax havens more actively enforced customer due diligence measures than exchanges in OECD countries, which enforced these laws at similar levels as businesses in developing countries (Findley, Nielson, and Sharman 2014). Accordingly, I predict that OECD countries will show lapses in the enforcement of anti-money laundering laws for cryptocurrency, which is also important since these countries process a high proportion of all cryptocurrency transactions.

4 Data

One of the chief challenges of analyzing cryptocurrency transactions is obtaining and ensuring the reliability of the data. Although prior studies have used data obtained from third-party aggregator sites, one major concern is that exchanges may share fake data with these sites. In particular, exchanges face an incentive to artificially inflate the number of

transactions they share as this gives the appearance of greater liquidity (an important attribute for cryptocurrency exchanges) and moves the exchange higher in industry rankings such as *CoinMarketCap*; both these factors can help exchanges attract and retain customers (Chen, Lin, and Wu 2022; Hougan, Kim, and Lerner 2019; Varshney 2021). In fact, one report estimates that 95% of transactions reported to site aggregators are fake (Bitwise Asset Management 2019). To minimize the risk of unreliable data, I bypassed third-party sites altogether by collecting data in real time directly from exchanges.

I collected a dataset of cryptocurrency trades from virtually all exchanges offering trades from Bitcoin or Ethereum to fiat currency between June 22, 2020 and September 2, 2020. The dataset includes 128 million transactions collected from 66 cryptocurrency exchanges. This data collection was possible because most exchanges share transaction-level data through an application programming interface (API), including the time, date, quantity of cryptocurrency, and the exchange rate of the currency pair at the time the trade was executed.[7] To collect the data, I wrote a Python script for each site and set up remote servers through Amazon Web Services to continually query the APIs at intervals of 15, 30, 60, or 150 seconds (depending on the volume and number of trades available from each site).

I then 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 250 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 6.3).

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

Table 1: 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.

After cleaning the data, the sample includes 65 trading pairs across 27 exchanges located in 9 countries. Table 1 shows summary statistics for each trading pair, where the count represents the number of exchanges that offered that trade. To compare bunching close to the threshold, I converted the fiat value of all non-euro and non-dollar trades into euros (for European-based exchanges) and dollars (for all others) based on the hourly exchange rate at the time of each trade using historical Forex rates from Dukascopy: Swiss Banking Group (n.d.). To tag each exchange by country, I used information from each exchange's website during the summer of 2020 to identify the country in which it was registered. 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 so-called tax haven (the British Virgin Islands).

5 Estimation Strategy

I use bunching estimation to measure activity within exchanges consistent with efforts to avoid due diligence screening. Previous studies have traced the laundering process for specific cases of cryptocurrency crime, but these studies have been limited in scope to only a relatively small number of transactions (Meiklejohn et al. 2013; Apuzzo 2014). Using bunching estimation, I am able to analyze a much broader sample of cryptocurrency activity – virtually all Bitcoin and Ethereum crypto-to-fiat trades within high volume, regulated exchanges during a two-month period. Accordingly, this study offers a macro-level view of activity within regulated exchanges that would be infeasible by tracing cryptocurrency linked to individual crimes. However, one tradeoff of this approach is that not all the activity uncovered using bunching estimation may be indicative of users avoiding screening for criminal reasons, a point I discuss in detail in Section 6.3.

Bunching estimation is an econometric strategy introduced by Saez (2010) and further developed by Chetty et al. (2011) that has been used to study phenomena involving avoidance

or evasion. Specifically, this method exploits a discontinuity in incentives in a context where individuals can sort below a cutoff and employs the mass of a distribution to measure how individuals strategically respond to this discontinuity in incentives (Figure 1). In this set up, the distribution of the number of trades in a given period is represented by a smooth density distribution $h(z)$ across a continuous variable z, which denotes the total fiat amount of each trade. 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 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 bunching in exponential distributions with 5, 2, and 1 percent excess mass below a threshold.

To estimate bunching, I follow the procedure outlined by Chetty et al. (2011) and summarized by Mavrokonstantis (2019). I wish 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). 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 due to 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.

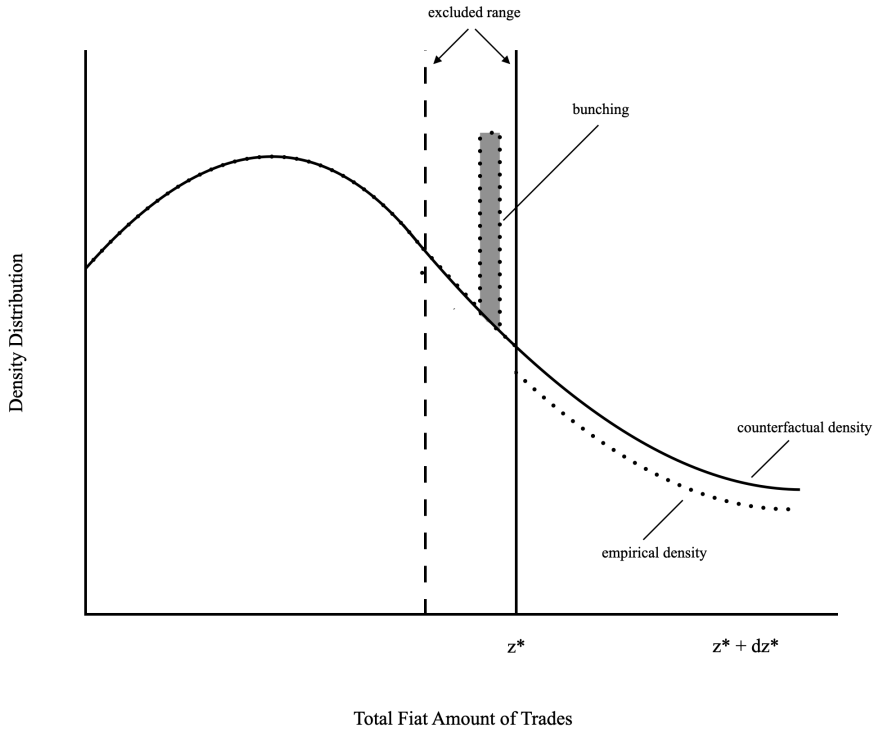
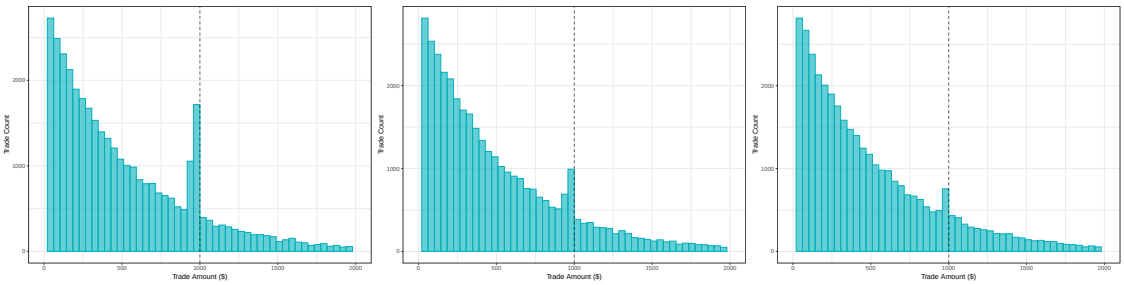


Figure 1: Graph illustrating bunching estimation. The solid line denotes a distribution function ($h(z)$) across values of trades in dollars. The rectangle denotes "bunching" below the threshold ($z*$), and the dotted line denotes the downward shift in the distribution beyond $z*$ caused by bunching.



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

Figure 2: Density plots showing simulated bunching at 5%, 2%, and 1% excess mass below the threshold (dashed line) for simulations using an exponential distribution of 10,000 trades with a mean of 500.

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:

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

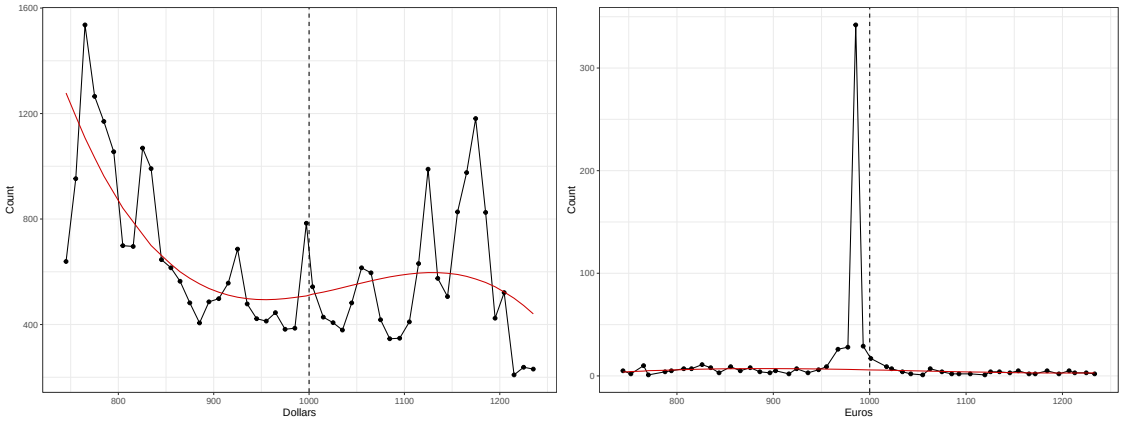
I then estimate the difference between the counterfactual and observed bin values within the bunching window ($\widehat{B}_N = \sum_{j=z_L}^{z_U} C_j - \widehat{C}_j$) (Kleven 2016). Finally, I estimate excess mass in the bunching region relative to the average height of the counterfactual distribution in the band $[z_L, z_u]$, 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). Nonparametric bootstrapping provides a way to estimate standard errors for estimates of bunching as it does not require the researcher to assume *a priori* the distribution of the data or use a known formula to calculate parameters of the distribution (i.e., the standard deviation) (Mooney et al. 1993, pp. 7–9). Accordingly, I estimate standard errors for bunching estimates by drawing 1,000 samples with replacement from the vector of errors (ϵ_i) in Equation 1. For each sample, I then calculate a bunching estimate ($\widehat{b}$) as 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 illustrates this approach with trades from two exchanges – Binance US, based in the United States (3a), and Coinmetro, based in Estonia (3b). These graphs show the distribution of trades for two exchanges with 10 unit-wide bins centered at the threshold and including 500 units surrounding the threshold. I fit a third-degree polynomial to each sample's data (excluding the 100 units below the threshold where bunching may occur) to provide a counterfactual estimate of the distribution. For Binance US, the counterfactual distribution fits the empirical distribution fairly well, and there is no significant excess mass below the due diligence threshold. This intuition is borne out in an estimate of $\widehat{b} = 0.04$,

Figure 3: Bunching in Two Exchanges



(a) Binance US (b) Coinmetro

Notes: Graphs show examples of bunching below the threshold in two exchanges: Binance US, a U.S.-based exchange offering Bitcoin-to-dollar trades, and Coinmetro, an Estonia-based exchange offering Bitcoin-to-euro trades. The red line denotes the counterfactual distribution.

which is not statistically significant (standard error = 1.96). In Coinmetro, by contrast, there is a high level of bunching below the due diligence threshold. The estimate of $\widehat{b}$ in this exchange is 58.80, which means that there were nearly 59 times more transactions in the range below the threshold than predicted based on the rest of the distribution. This result is statistically significant, with a standard error of 8.36 ($p < 0.00001$).

5.1 Optimization Friction and Potential Threats to Inference

One important finding of the literature on bunching estimation is that people often face *optimization friction* – costs for adjusting their behavior to take advantage of an incentive. For example, a self-employed worker who wishes to take advantage of a lower tax rate in a bracket capped at a certain income must forfeit the income she *would have earned* had she worked more hours. Accordingly, studies of income tax rates assume that only individuals in a small band above a tax bracket will respond to the lower tax rate incentive, since the amount of optimization friction increases the further a person's income would have fallen from the cutoff point (Chetty et al. 2011; Bastani and Selin 2014; Kleven and Waseem

2013). In my analysis, I dispense with the assumption that only people whose transactions would have fallen in a narrow band above the due diligence threshold will respond to the incentive as the optimization friction for cryptocurrency transactions is low; indeed, the only optimization friction cryptocurrency users face by responding to the threshold is the additional time it takes to carry out multiple transactions below the threshold rather than one large transaction above it.[8]

Importantly, there are two potential threats to inference using bunching estimation (Kleven 2016), but neither pose a problem for this research design. The first is the possible presence of another policy that also makes use of the 1,000 euro/dollar cutoff, which would confound estimates of excess mass; however, there are no other policies that affect cryptocurrency transactions at these thresholds. The second is that the threshold also serves as a natural reference point, which could also confound estimates by leading to a greater number of transactions at that value for unrelated reasons. Although both 1,000 dollars and euros are natural reference points, this does not confound estimates because I examine bunching *below* the threshold. Accordingly, this feature actually introduces bias *against* finding bunching, 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.

6 Results

To assess bunching in regulated countries, I present results across several levels of aggregation. First, I compare bunching below the threshold in regulated exchanges for trades from

[8]Importantly, fees do not create an incentive for users to carry out transactions at smaller amounts (or below the due diligence threshold). Cryptocurrency exchanges typically charge transaction fees that are a percentage of the trade value (Francis 2022; Ramberg 2020). Exchanges occasionally offer volume discounts, service fees, or flat rate fees, all of which encourage users to carry out larger rather than smaller transactions. See Appendix B for a list of transaction fees by exchange.

Bitcoin and Ethereum to fiat currency with results aggregated according to whether the exchange enforced due diligence at 1,000 euros (European exchanges) or 1,000 dollars (all others), yielding four types of trades: Bitcoin-to-dollars, Bitcoin-to-euros, Ethereum-to-dollars, and Ethereum-to-euros. I also consider bunching below 1,000 euros (European exchanges) and 1,000 dollars (all others) for unregulated exchanges, as well as estimates of bunching below two placebo thresholds – 500 and 1,500 dollars/euros – in regulated exchanges. I then measure bunching at the country level for trades from Bitcoin and Ethereum to fiat currency by aggregating transactions from a country's exchanges to produce a country-level estimate. For all country-level estimates, I also estimate bunching below two placebo thresholds (500 and 1,500 dollars/euros).[9]

Table 2 presents aggregate estimates of bunching for trades from Bitcoin and Ethereum into fiat currency in both regulated and unregulated exchanges, with the number of exchanges and trading pairs included in each estimate listed below it. The results show statistically significant bunching in both Bitcoin and Ethereum trades to fiat currency in regulated exchanges, with levels ranging from five times greater excess mass below the threshold in Bitcoin-to-dollar transactions to about twice the expected mass below the threshold in Ethereum-to-euro transactions. In unregulated exchanges, meanwhile, there is no statistically significant excess mass below the 1,000 dollar/euro thresholds for Bitcoin and Ethereum trades to fiat currency. Thus, these results show bunching below the 1,000 dollar/euro threshold in regulated exchanges with no similar pattern in unregulated exchanges, which suggests that this activity is driven by customers' efforts to avoid due diligence screening.

Next, I compare levels of bunching below two placebo thresholds for regulated exchanges. Because customer due diligence is not applied above these arbitrary thresholds, I do not expect users to sort their transactions below them. Conversely, if some other factor unrelated to customer due diligence led users to sort transactions below the 1,000 dollar/euro threshold

[9]Although the British Virgin Islands is *not* an FATF member, I include it in my analysis as the country issued new regulatory guidance for the cryptocurrency sector in line with the FATF's standards on July 10, 2020, during the data collection period (British Virgin Islands Financial Services Commission 2020; Law of Virgin Islands 2020).

Table 2: 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***	0.114	1.418	−0.922	−0.595
(*Threshold*)	(1.759)	(0.683)	(0.637)	(0.431)	(1.037)	(0.916)	(1.462)	(0.493)
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. 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.

in regulated exchanges, we might expect to see similar behavior below other round number values like 500 or 1,500 dollars/euros. As expected, there is no robust evidence of statistically significant bunching below the placebo thresholds in regulated exchanges, which is visible in Table 3. This finding lends support to the interpretation that bunching below the 1,000 euro/dollar threshold in regulated exchanges is driven by users' reaction to the due diligence threshold.

6.1 Country-Level Estimates

Next, I estimate levels of bunching in Bitcoin-to-fiat trades at the country level by aggregating transactions for all exchanges within regulated countries and calculating estimates for each. The middle row of Table 4 presents estimates of bunching below the due diligence threshold (1,000 dollars/euros), while the first and third row present estimates of bunching below the placebo thresholds of 500 and 1,500 dollars/euros. Once again, I include standard

Table 3: 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*)	(1.129)	(0.216)	(0.713)	(0.377)
1,500	−1.152*	0.028	−0.845*	0.367
(*Placebo*)	(0.542)	(0.143)	(0.486)	(0.295)
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. 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.

Table 4: Bunching in Bitcoin Trades by Country

	Estonia	**Brazil**	**Japan**	**Australia**	**BVI†**	**UK**	**Netherlands**	**Turkey**	**USA**
500	3.638*	−2.357***	2.852**	−2.131	0.282	−0.134	13.162	4.858***	4.476**
(*Placebo*)	(1.891)	(0.552)	(1.179)	(2.316)	(1.904)	(0.220)	(15.070)	(1.360)	(1.884)
1,000	**58.797*****	**6.670*****	**5.234****	**3.191****	**2.341*****	**2.628*****	**2.266****	**0.521**	**−0.266**
(*Threshold*)	**(8.363)**	**(0.803)**	**(1.955)**	**(1.371)**	**(0.775)**	**(0.637)**	**(0.969)**	**(0.790)**	**(3.504)**
1,500	0.808	1.706*	−1.329*	6.045***	−0.851**	0.020	0.195	1.132*	2.137**
(*Placebo*)	(1.936)	(0.791)	(0.602)	(1.478)	(0.301)	(0.141)	(1.065)	(0.663)	(0.762)
Exchanges	1	3	4	1	2	3	1	2	3
Pairs	1	3	6	1	2	6	1	2	3

Notes: Bunching by country in Bitcoin-to-fiat trades between 06/21/20 and 09/02/20. 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. † stands for British Virgin Islands.

errors and present the number of exchanges and trading pairs included in each estimate. The results show statistically significant bunching below the due diligence threshold in nearly all countries, but there is no robust cross-country evidence of statistically significant bunching (or the absence thereof) below the two placebo thresholds.

Bunching estimates vary by orders of magnitude across countries. At the most extreme, an exchange in Estonia showed excess mass that was nearly 59 times greater than predicted based on the rest of the distribution, while at the other extreme, exchanges in the United States and Turkey showed no statistically significant excess mass below the threshold. In between, Brazil, Japan, Australia, the British Virgin Islands, the United Kingdom, and the Netherlands all show some level of statistically significant bunching. Importantly, the United States is the only country in the sample for which exchanges do not enforce customer due diligence at the 1,000 dollar threshold; instead, U.S.-based exchanges perform customer due diligence for all new customers at the time they create an account, clearing customers to perform crypto-to-fiat transactions of any amount without additional screening. Thus, the

Table 5: 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

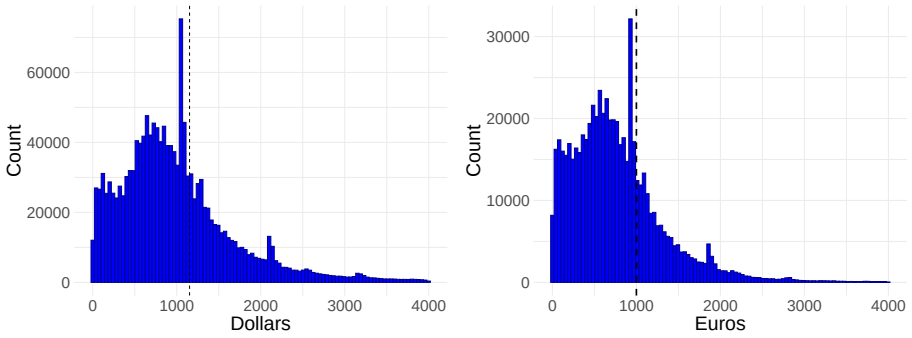
Notes: Bunching by country between 06/21/20 and 09/02/20 in the 7 bins (70 dollars/euros) below the threshold. Pairs denotes the number of trading pairs and exchanges denotes the number of exchanges included in each estimate; standard errors are in parentheses and stars indicate the statistical significance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

United States is the only country in the sample in which customers do not face an incentive to shift transactions below the 1,000 dollar threshold and is one of only two countries without statistically significant excess mass below the threshold.

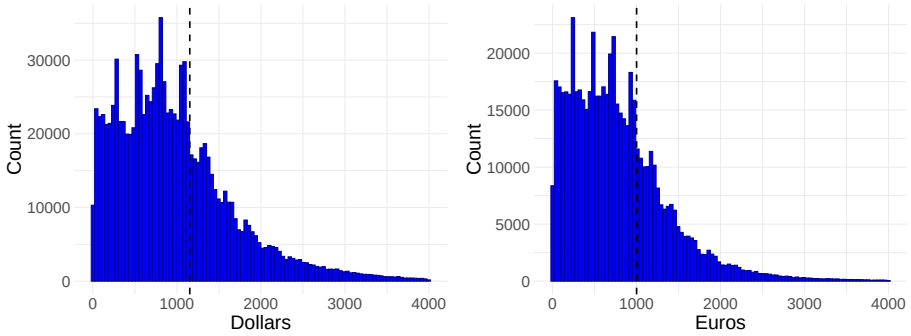
I conduct a similar analysis by country for Ethereum-to-fiat trades (Table 5). These results show statistically significant bunching below the threshold in some countries' exchanges – the British Virgin Islands, the United Kingdom, and Brazil – but not others – Japan, the Netherlands, Turkey, and the United States. Once again, there is no statistically significant bunching below the threshold in U.S. or Turkish-based exchanges. Estimates of excess mass range from 2.6 times greater 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 bunching (or the absence thereof) below the placebo thresholds of 500 and 1,500 dollars/euros.

In sum, these results show a pattern of statistically significant bunching below the due

Figure 4: Distribution of Trades in Extstock Exchange



(A) Bitcoin



(B) Ethereum

Notes: The height of each bin marks the number of transactions at each 10 dollar/euro increment for all trades between 07/01/20 and 08/03/20. The dashed line denotes the 1,000 euro threshold (for trades to euros) or the average 1,000 euro threshold based on the exchange rate between euros and dollars during the 34 day period.

diligence threshold in regulated exchanges with no similar pattern in unregulated exchanges or below placebo thresholds in regulated exchanges. It is also notable that the pattern of bunching within an exchange depends on whether that exchange enforces the threshold in euros or dollars. For example, in Extstock (based in Europe), transactions between Bitcoin and euros show bunching below 1,000 euros, while transactions between Bitcoin and dollars show bunching around 1,125 dollars in July 2020, which happened to be just below 1,000 euros based on the average exchange rate between dollars and euros for that month (Figure 4).

These results are also robust given varying crypto-to-fiat prices across exchanges and over time. Specifically, because there is no standardized exchange rate between cryptocurrencies and fiat currencies, the price for each trading pair fluctuates independently and can vary widely across exchanges (Pieters and Vivanco 2017). Further, because cryptocurrency exchanges do not close and execute trades at any time of the day, there are many minutes worth of price fluctuations included in the two-months worth of data. Thus, wide variation in crypto-to-fiat prices across exchanges and over time underscores that bunching below the due diligence threshold in regulated exchanges is most plausibly driven by the trade's fiat value – and, specifically, a response to the due diligence threshold – rather than characteristics of the cryptocurrency itself.[10]

6.2 Interpreting Excess Bunching

What does evidence of excess bunching below the due diligence threshold mean in substantive terms? I argue that bunching suggests countries are enforcing customer due diligence at the required threshold, otherwise there would be no incentive for users to keep their transactions below that specific value. However, the persistence of bunching in exchanges over time suggests that exchanges are not adequately performing risk-based measures, which compel exchanges to detect and combat suspicious trends. For example, one might expect that an

[10]In Appendix E, I test bunching within a different bunching window (i.e., 70 rather than 100 units below the threshold) for both Bitcoin-to-fiat and Ethereum-to-fiat trades by country. I find that the results of these robustness tests generally confirm those found in the main specification.

exchange performing risk-based measures would identify the presence of bunching below the threshold, interpret the activity as suspicious, and then take action to address it (for example, by performing randomized due diligence screening for transactions below the threshold). Over time, we should expect that the exchange's additional screening would discourage criminals or others avoiding scrutiny from keeping transactions below the threshold and either drive them to use other exchanges or change tactics, prompting a decrease in bunching over time. Thus, the fact that many exchanges show persistent bunching over time suggests that they are not adequately enforcing risk-based measures.

Conversely, one might interpret the *absence of bunching* in an exchange as supporting a different conclusion – the exchange is not enforcing due diligence at the threshold, so users have no incentive to keep their transactions below it. I argue this explanation is unlikely to be correct since regulators can check an exchange's records to determine whether it is enforcing due diligence, and failure to perform this duty could lead to fines or other penalties. Therefore, I argue that most exchanges will be unlikely to risk potential fines for failing to perform a duty that can be verified by regulators through a check of the company's records.

It is also important to note that bunching is not necessarily evidence of criminal activity. For example, a customer may seek to avoid due diligence screening because she greatly values her privacy and wishes to avoid sharing information with the government. However, I argue that non-criminal activity is unlikely to account for a large portion of bunching since the costs of avoiding due diligence screening are likely to discourage all but the most committed customers from avoiding it.

First, the costs to customers of undergoing due diligence screening are relatively low. Screening requires a customer to share her legal name, address, occupation, and a copy of a government-issued identification document with an exchange; this process does not require any additional costs for customers and can generally be performed within a matter of minutes. Undergoing due diligence screening also clears a customer to perform future

transactions of any amount without undergoing additional screening.

Second, avoiding due diligence screening requires specialized knowledge. Specifically, a customer must be aware that the exchange enforces customer due diligence for transactions above a specific value (a new development for most exchanges) and must also know whether the exchange enforces the threshold at 1,000 dollars or 1,000 euros. On top of that, some transactions require knowledge of the exchange rate between two fiat currencies to keep transactions below the threshold, such as an exchange enforcing the threshold in euros that offers crypto-to-dollar transactions (i.e., the customer must calculate the value of the dollar trade in euros to ensure it stays below the 1,000 euro threshold). Taken together, the costs to customers of undergoing due diligence screening are relatively low while avoiding it requires specialized knowledge; thus, I argue that most non-criminal customers are unlikely to avoid due diligence screening contributing to bunching below the threshold.

Finally, it is important to note that regardless of whether criminal or non-criminal behavior contributes to bunching, bunching itself is evidence of a lapse in enforcement by exchanges as defined by the new laws. Specifically, risk-based measures require exchanges to "'identify, assess, and take effective action to mitigate their money laundering/terrorist financing risks" (Mnuchin 2019). Given that the persistence of bunching over time – often several or many times greater than expected based on the rest of the distribution – is evidence of a potential money laundering risk, then a failure to address bunching represents a lapse in the enforcement of risk-based measures.

6.3 Fake Data, Exchange Closures, and Allegations of Fraud

Several other pieces of evidence suggest that exchanges with high levels of bunching are poorly regulated. For one, a country with high levels of bunching in Bitcoin-to-fiat trades – Estonia – was (as of July 2020) the location of exchanges that appear to have shared fake transaction data. Specifically, while the distribution of transactions from most exchanges

feature bunching at round numbers of cryptocurrency and fiat currency and other idiosyncrasies, the data from four Estonia-based exchanges feature distributions that resemble either a perfect exponential distribution or other highly idealized distributions (see Appendix D).[11] As discussed previously, exchanges face an incentive to artificially inflate their trading volume to appear to have greater liquidity and attract new customers; accordingly, the presence of suspected fake data shared by these exchanges suggests that national regulators have not limited this activity by exchanges.

Further, in the time since I collected the data in the summer of 2020, several exchanges with high levels of bunching have faced allegations of "scamming" customers out of money. Three Estonia-based exchanges (Coinsbit, P2PB2B, and Folgory) and one UK-based exchange (Extstock) have faced allegations that they routinely prevent customers from withdrawing funds under the guise of anti-money laundering concerns; specifically, reports state that the sites will flag a user's withdrawal request as suspicious, request additional identity verification measures, but then fail to release the funds to the customer even after she has provided additional information. A second UK-based exchange (Exmo) has received mixed reviews online, with some claiming it has also prevented customers from withdrawing funds.

Taken together, the suspected fake data and allegations of fraud provide evidence consistent with the idea the idea that exchanges in countries with high levels of bunching are subject to lax regulatory environments. Specifically, one would expect financial regulators in a country with active supervision to investigate and address reports of fraud in the cryptocurrency sector, yet none of these companies appear to have faced investigations or discipline by national regulators.

7 Discussion

Based on the results, I draw two broad conclusions in response to my predictions. First, the results suggest that individuals have strategically adapted their behavior to avoid screening

[11] Given these concerns, these exchanges were excluded from the analysis.

under the new law. Although prior research has considered problems with the implementation of national laws by 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), few consider the role of individuals. These results suggest that just as with tax laws (Saez 2010; Chetty et al. 2011), individual strategic behavior plays an important role in how well anti-money laundering laws function in practice, and, consequently, incentives and the possibility for strategic manipulation should be taken into account in the design of these laws. For example, one way to mitigate the impact of strategic behavior could be to perform randomized due diligence screening for transactions rather than screening all transactions above a cutoff, thereby making it harder for criminals to avoid due diligence screening.

A second broad conclusion is that developed countries – like developing countries and tax havens – are not immune to money laundering risk in the cryptocurrency sector. Countries with high levels of bunching include the United Kingdom, which has suffered a decade-long run of major money laundering scandals,[12] and Japan, which has been the location of several cryptocurrency exchanges that were victims of multi-million dollar thefts (McMillan 2018; Partz 2018; Partz 2021; Hickey 2019). This finding is significant for normative reasons, as some members of the international community have adopted the stance that developed countries are reliable enforcers of anti-money laundering laws and the international regime's true weakness lie in developing countries and tax havens (Schwarz 2011). For example, a recent ranking of 110 countries in terms of their money laundering and terrorist financing risk by the Basel Institute on Governance placed 16 OECD countries, 15 countries in continental Europe, and 11 EU members within the top 20 best performing countries. By contrast, 10 of the bottom 20 "riskiest" countries were classified as low income countries according to the World Bank's criteria, with another 4 in the bottom 20 classified as lower middle income countries (Basel Institute on Governance 2021). By contrast, my findings suggest that at

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

least for the cryptocurrency sector, it is less clear cut which countries are most susceptible to money laundering risk, and national resources alone cannot adequately predict a country's success.

Table 6: Bitcoin Trades Bunching Dollar Values by Country

Country	**Trades Value** (M USD)	**Bunching Volume** (% of All Transactions)
Japan	214.7	1.20
British Virgin Islands	86.3	0.40
United Kingdom	73.5	0.42
Netherlands	2.8	1.42
Brazil	2.5	1.44
Estonia	0.4	0.06
Australia	0.3	0.29

Notes: Dollar values in millions of statistically significant bunching by country for Bitcoin-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.

Table 7: Ethereum Trades Bunching Dollar Value by Country

Country	**Trades Value** (M USD)	**Bunching Volume** (% of All Transactions)
United Kingdom	44.8	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.

Evidence of bunching in developed countries is also significant because developed countries account for a high proportion of all transactions in the cryptocurrency sector. This relationship is displayed in Table 6, which shows the dollar value of statistically significant bunching estimates by country from Table 4. Accordingly, Japan, which falls near the middle

of countries in terms of the magnitude of bunching, accounts for the greatest overall dollar value, with bunching trades accounting for roughly $215 million during the two month period. The United Kingdom is third, with bunching in its sole exchange accounting for $73.5 million. The dollar values of bunching in the sole developing country with bunching is considerably lower, at $2.5 million for Brazil. Similar results are present in trades from Ethereum (Table 7), as bunching in UK-based exchanges totaled $44.8 million with $60,000 worth of bunching in Ethereum-to-fiat trades in Brazil-based exchanges. Accordingly, these results underscore the importance of improving enforcement in developed countries in order to minimize over all levels of money laundering risk.

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 (particularly risk-based) measures at varying levels. Prior research has established that the quality of national regulation plays an important role in how well businesses enforce anti-money laundering laws, but national regulators often vary greatly in their resources and methods across countries (Levi, Halliday, and Reuter 2014; Willebois et al. 2011, p. 30). However, even countries with sufficient resources may fail to adequately regulate the private sector in the context of anti-money laundering laws, as some wealthy countries with strong financial regulation in other areas have shown significant failures (Financial Action Task Force n.d.[b]; Financial Action Task Force n.d.[a], pp. 201, 199). Thus, variation in the approaches of national regulators could help explain varying levels of bunching across countries based on exchanges' enforcement of risk-based measures.

A second potential explanation emerges from demand-side theories of money laundering. Specifically, because Western countries have developed economies and offer safe and lucrative investment opportunities, they attract more criminal money than developing countries (Walker and Unger 2009, p. 833). Additionally, the features that make doing business difficult in many developing countries – such as long wait times for slow-moving bureaucracies and calls for bribes or other red tape – may also discourage *criminal* actors from conducting

business or investing in developing countries (Findley, Nielson, and Sharman 2014, p. 82). In the context of cryptocurrency exchanges, the factors discouraging the use of exchanges in developing countries are likely lower than for other types of businesses, although some aspects of these dynamics may still be at play. Thus, although varying levels of money laundering globally (and the factors driving them) remain poorly understood, this paper provides additional data points around the performance of countries within the cryptocurrency sector.

8 Conclusion

This paper has sought to assess how well a group of powerful countries have implemented a common set of anti-money laundering standards for cryptocurrency exchanges. The results suggest that while countries have made significant progress toward implementing these standards, important gaps in enforcement remain.

On the one hand, the presence of bunching across most transaction pairs in regulated exchanges suggests that exchanges in regulated countries are enforcing customer due diligence at the required threshold (creating an incentive for users to sort transactions below it). Given that cryptocurrency exchanges are typically mostly or entirely online businesses – and many have sought to evade regulation in the past, the fact that FATF countries managed to register exchanges and ensure they enforce customer due diligence represents significant progress. On the other hand, lapses in the enforcement of risk-based measures across countries creates conditions that allow enterprising criminals to launder funds in regulated exchanges. Consequently, the Cypherpunk's conception of regulatory arbitrage continues to present a challenge for cross-national efforts to regulate cryptocurrency exchanges.

Despite gaps in enforcement, there are several reasons to be optimistic about the long-term chances of effective anti-money laundering regulation in the cryptocurrency sector. In particular, the unique traceability of cryptocurrency transactions suggest that governments with enough resources can trace 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.[13] Finally, there is already evidence of broader adoption of these standards beyond FATF members, as 16 non-member states have now adopted these standards (Allison 2021). Thus, while there is still a long road to effective cross-national regulation of the cryptocurrency sector, states have proven themselves generally capable of regulating a technology that was once viewed (at least by some) as a viable challenge to state authority.

[13]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/.

Apuzzo, Matt (2014). "Secret Global Strike Kills 2 Malicious Web Viruses". In: *N.Y. Times*. ISSN: 0362-4331. URL: https://www.nytimes.com/2014/06/03/world/europe/battling-destructive-computer-viruses-agents-seize-networks-used-by-hackers.html.

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

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.

Dai, Wei (1998). "b-money". In: URL: https://nakamotoinstitute.org/b-money/.

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.

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

"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.

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.

— (2013-2021). *Methodology: for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*. [Online; accessed 18. Mar. 2021]. URL: http://www.fatf-gafi.org/media/fatf/documents/methodology/fatf%20methodology%2022%20feb%202013.pdf.

Financial Action Task Force (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.

Francis, Kelli (2022). "Crypto Fees: A Full Breakdown and How To Minimize Costs". In: URL: https://www.gobankingrates.com/investing/crypto/how-to-minimize-crypto-fees/#:~:text=Many\%20cryptocurrency\%20exchanges\%20charge\%20a,the\%20more\%20you'll\%20pay..

Glasner, David (2020). "An Evolutionary Theory of the State Monopoly over Money1". In: *Money and the nation state*. Routledge, pp. 21–45.

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.

Hayek, Friedrich August (1976). *Choice in currency: a way to stop inflation*. Vol. 48. Ludwig von Mises Institute.

— (2009). *Denationalisation of money: the argument refined*. Ludwig von Mises Institute.

Helleiner, Eric (1998). "National currencies and national identities". In: *American Behavioral Scientist* 41.10, pp. 1409–1436.

Helleiner, Eric (1999). "Historicizing territorial currencies: monetary space and the nation-state in North America". In: *Political Geography* 18.3, pp. 309–339.

— (2018). "The making of national money". In: *The Making of National Money*. Cornell University Press.

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.

Hoekstra, Gordon (2019). "Anatomy of money laundering in B.C. real estate: 12 cases, $1.7 billion, 20 countries and 30 banks". In: *Vancouver Sun*. URL: https://vancouversun.com/business/local-business/money-laundering-in-real-estate-in-bc-not-new-multiple-ways-to-get-money-into-financial-system.

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.

Hughes, Eric (1993). "A cypherpunk's manifesto". In.

Kleven, Henrik J and Mazhar Waseem (2013). "Using notches to uncover optimization frictions and structural elasticities: Theory and evidence from Pakistan". In: *The Quarterly Journal of Economics* 128.2, pp. 669–723.

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.

Konotey-Ahulu, Olivia (2020). "London Luxury Homes Are a Prime Location to Hide Dirty Money". In: *Bloomberg*. URL: https://www.bloomberg.com/news/articles/2020-12-21/london-luxury-homes-are-a-prime-location-to-hide-dirty-money.

Lauer, Josh (2008). "Money as mass communication: US paper currency and the iconography of nationalism". In: *The Communication Review* 11.2, pp. 109–132.

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.

Levinson-King, Robin (2019). "How gangs used Vancouver's real estate market to launder $5bn". In: *BBC News Online*. URL: https://www.bbc.com/news/world-us-canada-48231558.

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. (1992). "Libertaria in Cyberspace". In: *URL (accessed 2 Feb 2021): https://nakamotoinstitute.org/libertaria-in-cyberspace/*.

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

May, Timothy C. and Eric Hughes (1992). "Crypto Glossary". In: *URL (accessed 2 Feb 2021): https://nakamotoinstitute.org/crypto-glossary/*.

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.

Meiklejohn, Sarah et al. (2013). "A fistful of bitcoins: characterizing payments among men with no names". In: *Proceedings of the 2013 conference on Internet measurement conference*. ACM, pp. 127–140.

Mnuchin, Steven (2019). *Remarks of Secretary Steven T. Mnuchin FATF Plenary Session Orlando, Florida | U.S. Department of the Treasury*. [Online; accessed 24. Nov. 2019]. URL: https://home.treasury.gov/news/press-releases/sm713.

Mooney, Christopher Z et al. (1993). *Bootstrapping: A nonparametric approach to statistical inference*. 95. sage.

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*.

Naismith, Rory (2018). *Money and coinage in the Middle Ages*. Brill.

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.

Polanyi, Karl (2001). *The great transformation: The political and economic origins of our time*. Beacon press.

Ramberg, Richard (2020). "Cryptocurrency Exchange Fees". In: URL: https://www.cryptowisser.com/news/cryptocurrency-exchange-fees/.

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.

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.

Stokel-Walker, Chris (2019). "New data shows London's property boom is a money laundering horror". In: *WIRED*. URL: https://www.wired.co.uk/article/money-laundering-hmrc-tax-update.

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

Story, Louise and Stephanie Saul (2015). "Towers of Secrecy: Stream of Foreign Wealth Flows to Elite New York Real Estate". In: *N.Y. Times*. URL: https://www.nytimes.com/2015/02/08/nyregion/stream-of-foreign-wealth-flows-to-time-warner-condos.html.

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*.

Weber, Max (2013). *From Max Weber: essays in sociology*. Routledge.

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/.

A FATF Recommendations

A.1 Customer Due Diligence

Recommendation 5[14]

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.[15]

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 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

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

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

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[16]

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

[16]Text copied from Financial Action Task Force 2015, p. 2.

SECTION IV – APPLICATION OF FATF STANDARDS TO COVERED ENTITIES[17]

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 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

[17]Text copied from Financial Action Task Force 2015, pp. 14–16.

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 reasonable 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 Recom-

mendation 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.

B Fees by Cryptocurrency Exchange

Table 8 shows fees at select major cryptocurrency exchanges as of January 1, 2021.[18] 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, which should both encourage traders to execute larger rather than smaller transactions.

C Crypto-to-Fiat Price Changes

Figures 5a and 5b show variation in the average Bitcoin-to-dollar and Ethereum-to-dollar exchange rates during the data collection period.[19] Figures 6b and 6a show variation in the average Bitcoin-to-dollar and Ethereum-to-dollar exchange rate by exchange for a selection of exchanges included in the sample.

D Fake Data

Typical transaction data from cryptocurrency exchanges features 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 highlight examples of anomalies present in cryptocurrency transaction distributions (Figure 7).

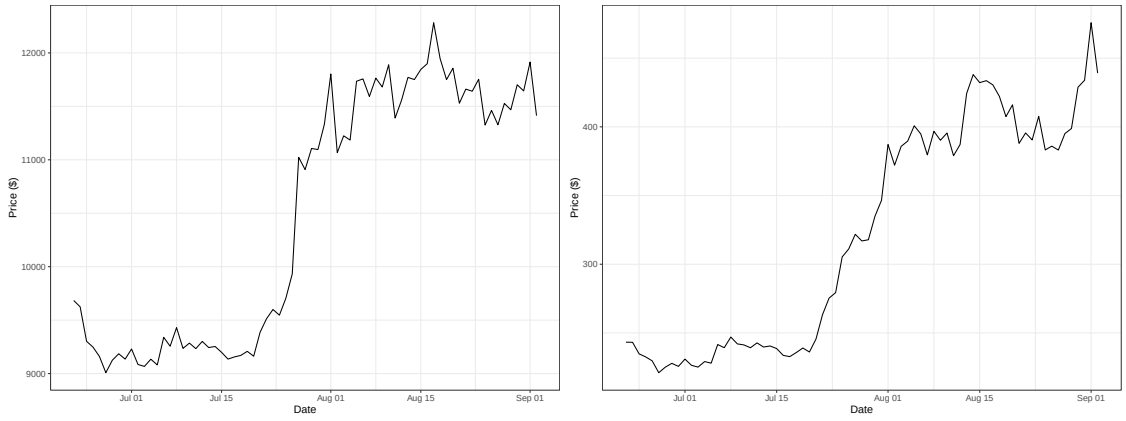
[18] Text taken from Stone 2022.

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

Table 8: 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

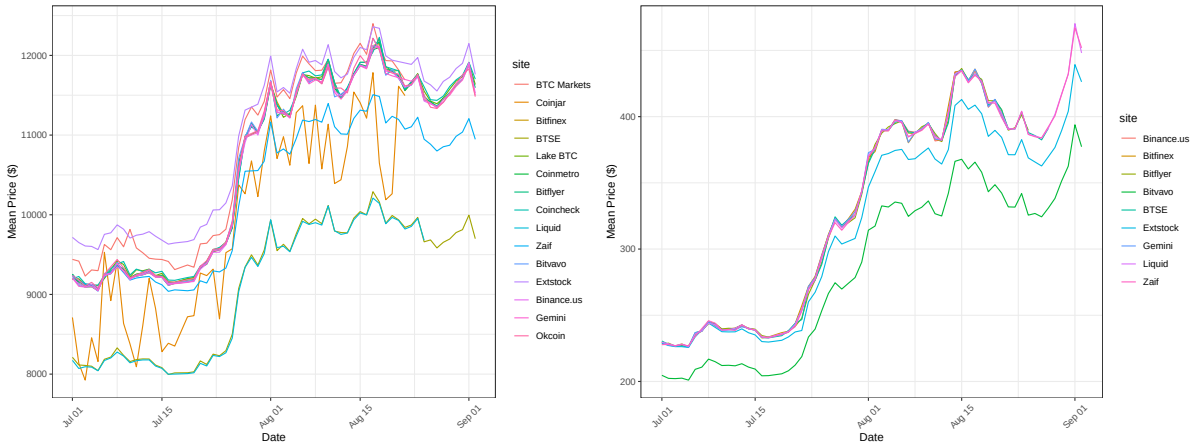
Figure 5: Caption



(a) Bitcoin Prices

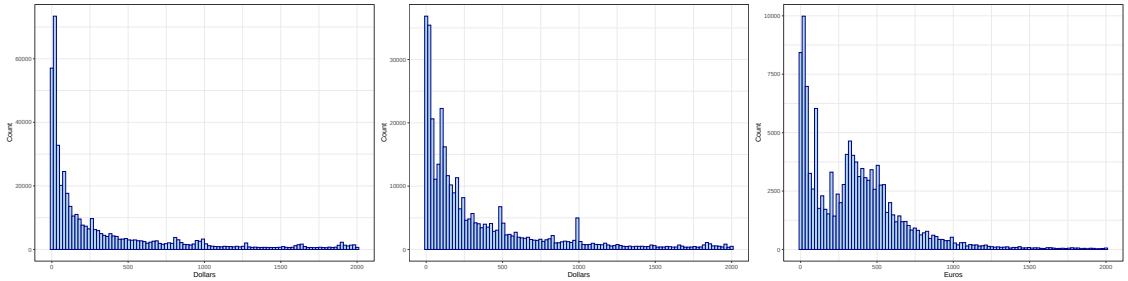
(b) Ethereum Prices

Figure 6: Caption



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

Figure 7: Example Distributions Across Trading Pairs



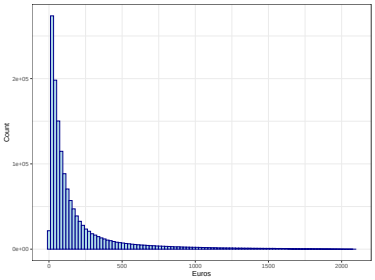
(a) Bittrex: Bitcoin-Dollar (b) Gemini: Bitcoin-Dollar (c) Bitvavo: Ethereum-Euro

I suspect that four exchanges in the sample feature fake transaction data as the distributions resemble an exponential distribution or other unusual distribution. Figure 8 shows distributions for trading pairs in Coinsbit, Figure 9 for pairs in Cryptology, Figure 10 for pairs in Folgory, Figure 11 and for pairs in Whitebit. All of these exchanges were registered in Estonia during the data collection period.

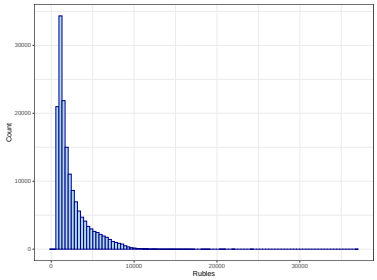
The graphs show that trading pairs in Coinsbit, Cryptology, and Whitebit resemble an exponential distribution, while trades in Folgory feature an unusual pattern in which the number of transactions decrease significantly past a certain fiat value. Further, the trading pairs within each exchange follow a similar distribution, which is unusual as there is often variation in the distributions of transactions across trading pairs.[20] For a more detailed discussion of fake transaction volume within exchanges, see Chen, Lin, and Wu (2022).

[20]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.

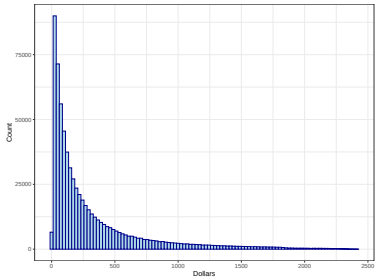
Figure 8: Coinsbit



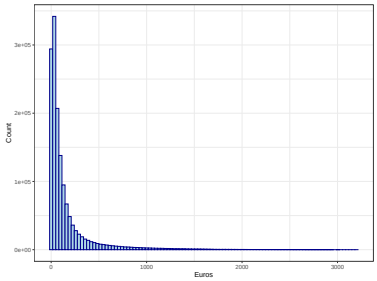
(a) Bitcoin-Euro



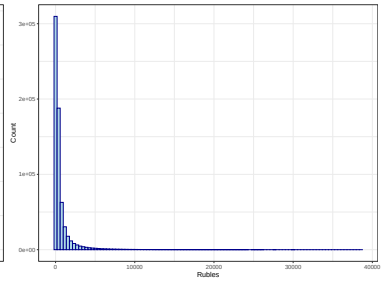
(b) Bitcoin-Ruble



(c) Bitcoin-Dollar

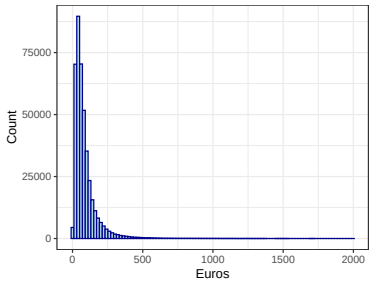


(d) Ethereum-Euro

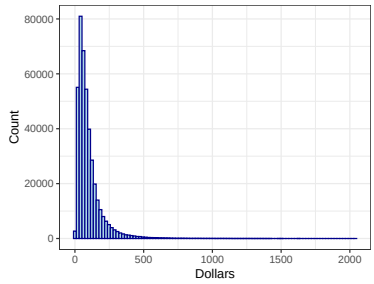


(e) Ethereum-Ruble

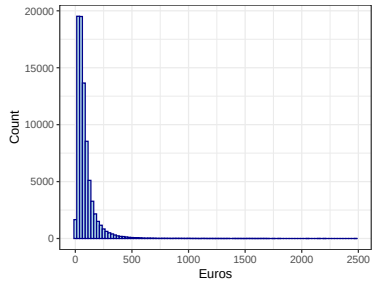
Figure 9: Cryptology



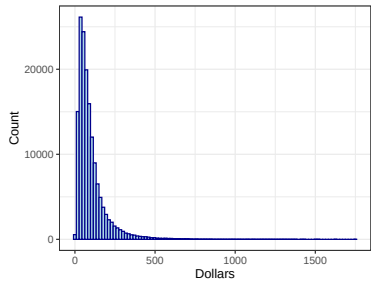
(a) Bitcoin-Euro



(b) Bitcoin-Dollar

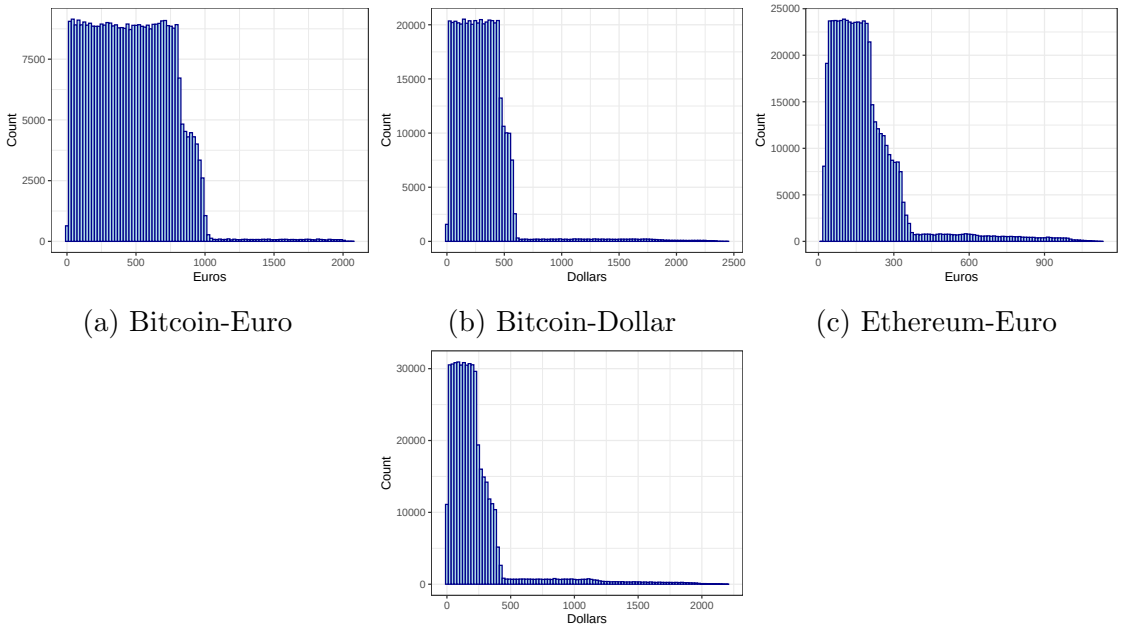


(c) Ethereum-Euro



(d) Ethereum-Dollar

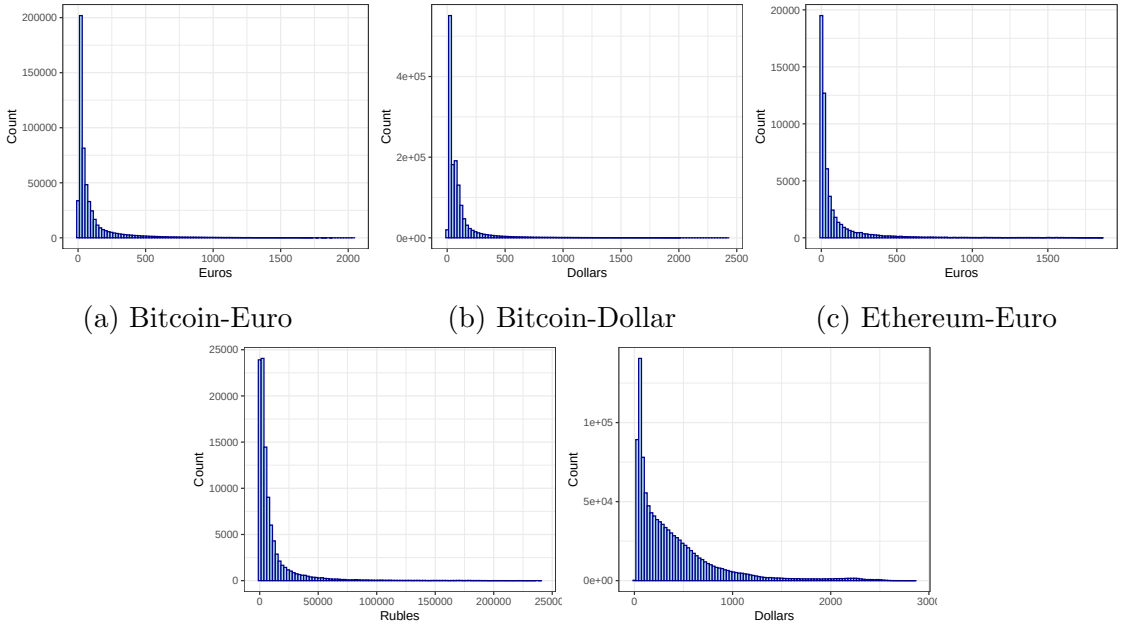
Figure 10: Folgory



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

(d) Ethereum-Dollar

Figure 11: Whitebit



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

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

Table 9: 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)	(7.964)	(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. † stands for British Virgin Islands.

E 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 9 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 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 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.

Table 10: 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. † stands for British Virgin Islands.