Kim *et al. Financ Innov* (2021) 7:78
https://doi.org/10.1186/s40854-021-00294-6

Financial Innovation

RESEARCH Open Access

Are suspicious activity reporting requirements for cryptocurrency exchanges effective?

Daehan Kim[1], Mehmet Huseyin Bilgin[2] and Doojin Ryu[1*]

*Correspondence:
sharpjin@skku.edu
[1] College of Economics, Sungkyunkwan University, Seoul 03063, Republic of Korea
Full list of author information is available at the end of the article

Abstract

This study analyzes the impact of a newly emerging type of anti-money laundering regulation that obligates cryptocurrency exchanges to report suspicious transactions to financial authorities. We build a theoretical model for the reporting decision structure of a private bank or cryptocurrency exchange and show that an inferior ability to detect money laundering (ML) increases the ratio of reported transactions to unreported transactions. If a representative money launderer makes an optimal portfolio choice, then this ratio increases further. Our findings suggest that cryptocurrency exchanges will exhibit more excessive reporting behavior under this regulation than private banks. We attribute this result to cryptocurrency exchanges' inferior ML detection abilities and their proximity to the underground economy.

Keywords: Cryptocurrency, Cryptocurrency exchange, Financial regulation, Money laundering, Portfolio choice

JEL Classification: E26 (informal economy · underground economy), G11 (portfolio choice· investment decisions), K42 (illegal behavior and the enforcement of law)

Introduction

During the current cryptocurrency boom, numerous cryptocurrency exchanges have emerged, and they now comprise a considerable fraction of the financial industry. These new exchanges must be considered, in order to accurately analyze the recent banking and financial sectors. As regulatory authorities worldwide extend the application of financial regulations from traditional financial institutions to cryptocurrency exchanges, there is an urgent need to study the regulation of cryptocurrency transactions.

Theoretically, cryptocurrency market regulations have two conflicting effects. On the one hand, regulations can function as restrictions for market participants, negatively impacting the market. On the other hand, they may boost the market by strengthening its credibility and stability. Under this framework, empirical studies assess the impact of regulations on the cryptocurrency market. Borri and Shakhnov (2020) identify that cryptocurrency investors react negatively to regulations or announcements about forthcoming regulations. Chokor and Alfieri (2021) and Shanaev et al. (2020) also draw

Springer Open

© The Author(s), 2021. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

similar conclusions, using the reaction of price movements as a proxy for the impact of regulations on the cryptocurrency market. In contrast, Feinstein and Werbach (2021) investigate the reaction of trading volume, criticizing the use of price movements as a proxy, and find no sufficient evidence to assert the significant impact of the regulations. In addition, Borri and Shakhnov (2020) and Feinstein and Werbach (2021) draw inconsistent results on the international spillover of regulations. However, compared to studies on other financial assets, those on cryptocurrency regulations are in an early phase. To integrate the conflicting ideas suggested by existing studies, more in-depth theoretical research considering both the investor and exchange intermediary sides is required.

One of the most important purposes of cryptocurrency regulations is to prevent money laundering (ML). Owing to the decentralized nature of cryptocurrencies, criminals can use cryptocurrency exchanges to launder dirty money; proper anti-money laundering (AML) actions in the cryptocurrency market can, therefore, improve overall AML performance in the economy.

This study specifically focuses on the duty to report suspicious activities imposed upon cryptocurrency exchanges. Governments do not directly detect ML activities. For several reasons, such as privacy rights, governments do not have the right to directly monitor all transactions made through private banks or cryptocurrency exchanges. Even if a government did have the right to do so, it would not be able to thoroughly check every individual transaction. Thus, although the exact processes may vary by country, financial authorities usually require banks and exchanges to monitor and report transactions for which ML activities are suspected. The authorities then analyze the reports of suspicious transactions thoroughly and identify whether they are true ML transactions. Some studies, such as those of Brenig et al. (2015) and Dupuis and Gleason (2020) particularly investigate cryptocurrency-backed ML activities. Furthermore, Bhaskar and Chuen's (2015) study implies that exchanges may go out of business because they are not capable of complying with strict AML regulations. Unfortunately, no prior studies have focused on the duty of cryptocurrency exchanges to report suspicious activities. The lack of research explicitly studying whether a cryptocurrency exchange can faithfully comply with this reporting duty may stem from the fact that such exchanges are still in the early stages of adoption. Compared to traditional private financial institutions, cryptocurrency exchanges are new, small, and illiquid. This study pays attention to these distinct characteristics.

We analyze the impact of a newly emerging type of AML regulation requiring cryptocurrency exchanges to report transactions for which ML is suspected. Based on background information on ML practices, the structure of the AML regulations, and the characteristics of cryptocurrency exchanges, we build two models to derive some findings on exchanges' behavior. The first model illustrates a cryptocurrency exchange's decision structure to report a transaction as an ML-suspected case. The second model describes the proportion of total illegal gains that a money launderer chooses to launder. Whereas the first model focuses on the decision of a representative cryptocurrency exchange, the second model focuses on the decision of a representative money launderer. The second model extends the discussion of the first model by endogenizing the money launderer, which is treated as an exogenous actor in the first model. We claim that when cryptocurrency exchanges are obligated to report suspicious transactions,

they will not faithfully comply with this regulation, but rather will report an excessive number of transactions, which is uninformative to the regulatory authority.

Our models suggest two main findings on the potential consequences of applying AML regulations to cryptocurrency exchanges. First, the relatively short history, small exchange size, and illiquidity of the cryptocurrency market increase the threat that a cryptocurrency exchange will be punished by authorities for reporting an excessive number of ML-suspected cases. Second, some cryptocurrency exchanges that largely depend on revenues from ML transactions may intentionally lower the ML detection probability by increasing the number of reports of suspected ML.

This study makes some additional contributions to the literature. We develop a model describing the reporting decision structure of a financial institution entrusted with monitoring ML. Furthermore, this study relaxes the assumption in the existing literature that all illegal pecuniary gains must be laundered for use. With this assumption relaxed, our study attempts to make a novel approach to analyze ML using portfolio choice theory.

Our study is also expected to provide policy implications for global financial regulatory authorities. Financial authorities around the world have already begun to design AML regulations for cryptocurrency exchanges. The Financial Action Task Force (FATF), an intergovernmental organization to combat ML, suggests guidelines on how financial authorities worldwide should respond to cryptocurrency technology (FATF 2012, 2019). To mitigate the risk associated with this new technology, it recommends that global financial authorities encourage cryptocurrency exchanges to be licensed or registered and subject to ML monitoring compliance. In accordance with the FATF's recommendation, global authorities are expected to arrange measures to adopt reporting obligations for cryptocurrency exchanges.

The remainder of this paper is organized as follows. "Research background" section provides background information; Cryptocurrency exchange's decision" section explains the model of a cryptocurrency exchange decision; "Money launderer's portfolio choice problem" section incorporates the portfolio choice model of a money launderer; "Policy implications" section suggests policy implications based on the findings; "Conclusion" section concludes the paper.

Research background

One of the aims of this study is to analyze the impact of a newly emerging type of AML regulation that obligates cryptocurrency exchanges to report suspicious transactions to financial authorities. Whereas there are many websites or documents on the AML regulation of cryptocurrency and suspicious activity reports, the academic literature on this topic is limited.

Nevertheless, to sustain a money-making process, a criminal with illegal pecuniary gains (e.g., profits from drug sales) does not leave the money as is, but instead prefers to reinvest it. For the gains to be reinvested into either legal or illegal sectors, the money needs to be laundered (Masciandaro 1999). Dirty money that remains dirty cannot be utilized outside the sector from which it originated. In this sense, ML is a practice of changing potential purchasing power into actual purchasing power (Masciandaro 1998). Once the government notices that certain money is dirty, it will not allow the money to be used for any purpose. Money laundering is the act of concealing the source of dirty

money, increasing the information asymmetry between the supervising authority and the owner of the money (Brenig et al. 2015).

An ML process consists of three stages: placement, layering, and integration (Brenig et al. 2015; Albrecht et al. 2008). Suppose that a criminal has obtained money by selling illegal drugs. The criminal takes this money to the financial sector by depositing the money into a bank. This initial stage is called placement. This money then moves repeatedly from place to place in multiple layers to prevent the government from tracing its source. Therefore, this process is referred to as layering. Finally, the money settles in a clean zone and can be used for a new business. This final stage is called integration.

In the past, the placement and layering stages only involved traditional types of the financial institution, such as private banks and stock exchanges, but ML processes now often involve cryptocurrency transactions. Cryptocurrency is a currency that allows digital payments, but cryptocurrencies differ significantly from traditional fiat-money-based digital payment systems. When a dollar is transferred, a financial intermediary, such as a credit card company, must verify the validity of the transaction. Cryptocurrency payments do not depend on such third parties; instead, the peer-to-peer network of blockchain technology verifies the transaction. This process resolves the famous "double spending problem" (Dwyer 2015; Nakamoto 2008). A cryptocurrency remittance is verifiable for the receiver, but is not easily observable by traditional financial institutions under government supervision. With services provided by some companies, such as Chainalysis, authorities can trace transfers of money to some extent (Dupuis and Gleason 2020), but this traceability is certainly limited compared to that of traditional online payments. Cryptocurrency, therefore, offers a huge opportunity for illegal market participants. Foley et al. (2019) estimate that a quarter of bitcoin users are involved in illegal activities. Although they mention that the popularity of cryptocurrency reduces the proportion used for illegal activities, it is natural to expect that the proximity of cryptocurrency to illegal activities is higher than that in the case of fiat money. Thus, the portion of ML transactions within a cryptocurrency exchange may be higher than that within a private bank. If criminals have sufficient information, they will not use a cryptocurrency exchange that cooperates with the government. Thus, a cryptocurrency exchange that is highly dependent on fee revenues from ML transactions may not actively participate in AML actions led by authorities, but may instead choose to be helpful to money launderers.

In an indirect ML monitoring structure, in which the government delegates ML obligations to private banks, the principal-agent problem of ML monitoring proposed by Masciandaro (1999) is inevitable. The principal, which is the government authority, wants to maximize the detected number of ML attempts. Conversely, the agent, which is a private bank in the study, tries to maximize its profits, considering the possibility of government sanctions. Takáts (2011) reports that the discrepancy between the principal and the agent causes excessive reporting. Sometimes, the government identifies ML transactions that are not reported by banks. In these cases, the government imposes sanctions on the bank for failing to properly report suspicious transactions. A bank that

dislikes being fined by the authority for its failures tends to report transactions that are less suspicious along with sufficiently suspicious transactions, making the reports uninformative. Likening the private bank to the boy who cried wolf, Takáts (2011) describes this overreporting tendency as "crying wolf." Banks may excessively report not only to avoid the threat of penalties, but also because of the high cost of careful monitoring (Masciandaro and Filotto 2001).

To combat ML, authorities worldwide have set up legal devices that require not only private banks, but also cryptocurrency exchanges to monitor and report suspicious transactions. For instance, the US Financial Crimes Enforcement Network (FinCEN) has worked on extending its longstanding AML regulation to cryptocurrency exchanges. It requires that cryptocurrency exchanges comply with AML regulations including setting registration, record keeping, and reporting obligations (Böhme et al. 2015; FinCEN 2019). Similarly, a recently amended South Korean law[1] was enacted in March 2021. The newly enforced rule mandates that cryptocurrency exchanges must be registered to Korea Financial Intelligence Unit under Financial Services Commission and report transactions that raise suspicions of ML attempts.

After ML processes, dirty bitcoins can be reinvested as clean bitcoins and dirty dollars can be reinvested as clean dollars. However, in some cases, a criminal may want to convert its bitcoins to dollars, and vice versa. In these cases, the financial authority can catch ML practices backed by cryptocurrencies if proper regulations are applied to cryptocurrency exchanges in a way that regulations are imposed on traditional financial institutions. To analyze the impacts of these regulations, we need to understand the business structures of cryptocurrency exchanges.

In fact, it is difficult to identify a single form of cryptocurrency exchange business. Each cryptocurrency exchange has a different affiliation, profit system, supported fiats, cryptocurrencies, and so on. Nonetheless, all exchanges have one common feature: every exchange receives transaction fees as a basic source of revenue. When a transaction is made, both seller and buyer pay the fees. Revenue is directly related to total trading volume. This relationship also holds for private banks because a private bank making money through the lending deposit spread ultimately benefits from a greater number of transactions as well. However, it may be true that the cryptocurrency exchange business depends more directly on trading volumes.

The most important difference between a cryptocurrency exchange and a general private bank in the context of this study is that they have different ML monitoring abilities. As most cryptocurrency exchanges have emerged recently, they are likely to lack data and experience in analyzing those data. Dupuis and Gleason (2020) mention that decentralized exchanges that allow users to control their own private keys, which are expected to be good ML channels, are still in their early stages. Thus, even if they are obligated by law to monitor transactions, they are not expected to carry out monitoring practices successfully. The fact that they are focused on stabilizing their profit systems and surviving in the volatile cryptocurrency market further worsens the problem.

[1] Act on reporting and using specific financial transaction information, §§ 3–6-8. [Republic of Korea, Enforcement Date Mar. 25, 2021].

Cryptocurrency exchange's decision

The concept of "crying wolf," that is, private banks' excessive reporting tendency introduced by Takáts (2011), can also appear when cryptocurrency exchanges are subject to analogous requirements. Under a regulation system, in which a high rate of type II error is punished explicitly and a high rate of type I error is not explicitly punished, a cryptocurrency exchange will decide to overreport transactions.

Furthermore, the degree of this excessive reporting may be higher for cryptocurrency exchanges compared to the behavior of private banks. The first reason for this is the exchange's lack of ability. Unlike the private banking system, cryptocurrency is a relatively novel concept, and nearly all cryptocurrency exchanges are newly established with relatively low trading volumes compared to traditional financial exchanges. Thus, a cryptocurrency exchange business faces an inevitable problem, in that it lacks experience in detecting ML transactions. In other words, it is not accustomed to carrying out ML analyses using its own detection model. Owing to the drawbacks of a rule-based system, machine learning techniques are currently widely used for detecting anomalies, including ML (Chen et al. 2018). However, statistical analyses using models, particularly machine learning models, require rich data. Even if a cryptocurrency exchange has a good detection model, it may not make good use of it, given that newly launched and illiquid exchanges generally have accumulated too little data. According to previous studies, cryptocurrency markets are often illiquid (Loi 2018; Smales 2019; Yermack 2015). Cryptocurrencies and exchanges addressed in the prior academic literature are usually major cryptocurrencies and major exchanges; thus, the illiquidity problem of cryptocurrency markets in the real world would be more severe than what is reported in the literature. Coinmarketcap (https://coinmarketcap.com) provides information on the liquidity of various cryptocurrency exchanges using its average liquidity score ranging from 0 to 1000. Binance is one of the most liquid and popular exchanges, with a score of 720, as of July 31, 2021. This is an overwhelmingly high score compared to many illiquid exchanges. For example, OTCBTC has a liquidity score of 1. As of July 31, there are almost no sell orders and no buy orders in the BTC/USD market[2] of OTCBTC. These severely illiquid exchanges are unlikely to have sufficient data. In addition, few of them are expected to have sufficient personnel to dedicate to ML detection. Creating a new cryptocurrency exchange is not complicated, and small groups of people or individuals can easily develop new exchanges. These small businesses may not be able to afford personnel for ML detection. In sum, cryptocurrency exchanges lack a variety of necessary resources to meet reporting requirements, leading to overall inferiority in ML detection. The following model explains why an ML monitoring institution with an inferior detection ability overreports to a high degree.

We define the indicator function I_i, which represents the true characteristic of transaction i, as follows:

$$I_i = \begin{cases} 0, & i \text{ is a normal transaction} \\ 1, & i \text{ is an ML transaction} \end{cases}. \tag{1}$$

[2] The BTC/USD market indicates bitcoin market in dollars.

The signal $P_i = \widehat{I_i}$ is an estimator of I_i, indicating the strength of the signal that transaction i is an ML transaction, measured by the detecting ability of a bank or cryptocurrency exchange. A high value of P_i implies that transaction i is highly suspicious. Whereas I_i has a fixed value for a given transaction i, P_i is a random variable. The accumulated data and detection technique determine the effectiveness of P_i as an estimator for I_i. Here, effectiveness can be evaluated in terms of measures, such as bias, relative efficiency, and the mean squared error. As the detection ability improves, $Bias(P_i) = E[P_i] - I_i$ and $Var(P_i)$ will generally decrease.

When the signal from transaction i is observed, an institution entrusted with monitoring decides whether to report the transaction based on the following standard:

$$\begin{aligned} &Report\ i \quad if \quad P^{min} \leq P_i \\ &Do\ not\ report\ i \quad if \quad P^{min} \geq P_i \end{aligned} \tag{2}$$

The threshold P^{min} is the minimum strength at which i is reported to the financial authority. The exchange can set a value of P^{min} between zero and one. This reporting system is rational because otherwise, the monitoring institution would end up leaving a transaction likely to be an ML action and reporting a less likely one. The excessive reporting tendency is defined by a low value of P^{min}. This study aims to show that P^{min} is lower for cryptocurrency exchanges than for private banks.

Assume that the financial authority that practices AML regulation can still identify an ML transaction, even if that transaction is not reported by the monitoring institution. In his model, Takáts (2011) assumes that an unreported case, as well as a reported case, is subject to a positive investigation effort.[3] When the authority imposes fines for any unreported ML cases that it identifies, a monitoring institution cares about type II errors. The type II error probability in this model is defined as the probability that a transaction is not reported, given that it is actually an ML attempt. This conditional probability is given by

$$Pr(not\ reported|ML) = Pr\Big(P_i \leq P^{min}|I_i = 1\Big). \tag{3}$$

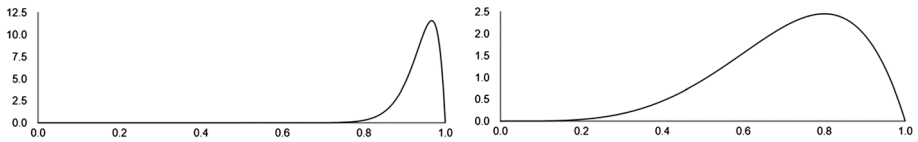
Let the strength of the signal P_i be a random variable, such that

$$P_i \sim Beta(\alpha, \beta), where\, \alpha, \beta \in (0, \infty). \tag{4}$$

A greater value of α relative to β moves the expected value $\mathrm{E}[P_i] = \frac{\alpha}{\alpha+\beta}$ toward one, shifting the overall weight of the beta distribution curve to the right. $\mathrm{E}[P_i] = \frac{\alpha}{\alpha+\beta}$ approaches I_i as the detection ability increases. When $I_i = 1$, the overall weight is shifted to the right when the ability is higher.

Using the mathematical property of $\frac{\alpha}{\alpha+\beta} \rightarrow_{monotonically} 1\, as\, \alpha \rightarrow \infty$, we can create distributions under $I_i = 1$ by fixing β and varying α to illustrate different detection ability

[3] Some may argue that governments usually do not investigate transactions that are not reported. However, we can use the following interpretation to justify positive investigation efforts. For two transactions i and j by the same money launderer, if i is reported and an authority catches the launderer, then j may also be uncovered by a further investigation. Here, j is not reported but is identified.



Panel A. Beta distribution with α=30 and β=2 **Panel B.** Beta distribution with α=5 and β=2

Fig. 1 **a** (Left panel) shows the beta distribution for $\boldsymbol{\alpha} = 30, \boldsymbol{\beta} = 2$. **b** (Right panel) shows the beta distribution for $\boldsymbol{\alpha} = 5, \boldsymbol{\beta} = 2$. The left and right graphs are the PDFs of the random variable $\boldsymbol{P_i}$ when $\boldsymbol{I_i} = 1$for monitoring institutions with superior and inferior ML detection abilities, respectively

levels.[4] When β is fixed, α can be used as a proxy for detection ability, as it is larger when the ability is higher if $I_i = 1$. Two different detection ability levels are indicated by this model, as shown in Fig. 1. Both distributions in the figure indicate the probability density function (PDF) of P_i when transaction i is an ML case. In particular, Panel A of Fig. 1 shows the distribution curve of P_i when the goodness of the estimator is high, that is, when the detection ability is superior. In contrast, Panel B shows the distribution curve of P_i when the goodness of the estimator is relatively low, that is, when the ability is relatively inferior.

Recall that the probability of committing a type II error is given by $Pr\left(P_i \leq P^{min} | I_i = 1\right)$. For both superior and inferior exchanges, it is straightforward to see that the probability of a type II error is greater for the inferior exchange for a given level of P^{min} (e.g., $P^{min} = 0.9$). To maintain its type II error probability similar to that of a superior exchange, an inferior exchange lowers its level of P^{min}, the minimum strength for reporting.

As already stated, cryptocurrency exchanges have lower detection abilities than private banks have, considering their limitations due to their short histories, small sizes, and illiquidity. Thus, we can consider ordinary private banks as superior exchanges and cryptocurrency exchanges as inferior exchanges. Under a similar reporting system, the excessive reporting behavior observed in private banks is likely to be even greater among cryptocurrency exchanges. In addition, by matching the two panels in Fig. 1 to an old, large, liquid exchange and a new, small, illiquid exchange, we can infer that the magnitude of overreporting is greater for newer, smaller, and less liquid exchanges.

A cryptocurrency exchange will try to reduce the probability of type II errors as much as possible, but not to an extreme amount. Although no direct sanctions are applied, exchanges face reporting costs. If the reporting cost were zero, private banks under the longstanding regulation would report every transaction. Each financial authority already has a preset form and guideline and, crucially, it often requires monitoring institutions to describe the transaction. When an exchange reports a transaction for being suspicious, it needs to state why the transaction is regarded as ML, so that the exchange is not punished for an intentional reporting insincerity. This reporting cost does not appear only when the transaction being reported is a true ML case, but also when the transaction is actually a normal case. Due to the trade-off relationship between increasing the number of reports and reducing reporting costs, P^{min} will not fall to zero, but to a certain optimal point where

[4] As $\frac{\alpha}{\alpha+\beta} = 1 - \frac{\beta}{\alpha+\beta}$ holds, fixing α and varying β also works.

the total loss is minimized. The total loss is the sum of the expected reporting failure sanctions and expected total reporting costs.

The loss of expected reporting failure sanction is a function of P^{min}, defined by

$$\begin{aligned}\mathcal{L}_{fail}\left(P^{min}\right) &= \gamma nPr(ML \wedge not\ reported) = \gamma nPr(ML)Pr(not\ reported|ML) \\ &= \gamma nPr(I_i = 1)Pr\left(P_i \le P^{min}|I_i = 1\right) = \gamma n\delta \int_0^{P^{min}} f_1(P_i)dP_i\end{aligned} \tag{5}$$

where n refers to the number of transactions on the exchange, δ denotes the probability that transaction i is an ML transaction, and γ is an authority constant implying government sanctions caused by an unreported ML case. In reality, the authority constant may be related to the identification of reported cases, but we set it as a constant for simplicity. $f_1(P_i)$ is the probability density function of P_i when i is an ML transaction. Differentiating $\mathcal{L}_{fail}$ with respect to P^{min} yields

$$\mathcal{L}'_{fail}\left(P^{min}\right) = \gamma n\delta f_1\left(P^{min}\right). \tag{6}$$

The loss of total reporting cost is also a function of P^{min}, defined by

$$\mathcal{L}_{cost}\left(P^{min}\right) = n\left[\delta \int_{P^{min}}^{1} C(P_i)f_1(P_i)dP_i + (1-\delta) \int_{P^{min}}^{1} C(P_i)f_0(P_i)dP_i\right], \tag{7}$$

where $C(P_i)$ is the cost function which depends on P_i. If P_i is small, it is difficult for an exchange to justify its reporting. Thus, the smaller the P_i, the higher the cost $C(P_i)$ will be. $f_0(P_i)$ is the probability density function of P_i when i is a normal transaction. Differentiating $\mathcal{L}_{cost}$ with respect to P^{min} yields

$$\mathcal{L}'_{cost}\left(P^{min}\right) = -n\left[\delta C\left(P^{min}\right)f_1\left(P^{min}\right) + (1-\delta)C\left(P^{min}\right)f_0\left(P^{min}\right)\right]. \tag{8}$$

The total loss is the sum of two kinds of loss:

$$\mathcal{L}\left(P^{min}\right) = \mathcal{L}_{fail} + \mathcal{L}_{cost}. \tag{9}$$

By the first-order condition, the total loss is minimized when

$$\mathcal{L}'_{fail}\left(P^{min}\right) + \mathcal{L}'_{cost}\left(P^{min}\right) = 0. \tag{10}$$

It follows that the optimal threshold P^{min*} satisfies the following condition:

$$\left(\frac{\gamma}{C\left(P^{min*}\right)} - 1\right) = \frac{(1-\delta)f_0\left(P^{min*}\right)}{\delta f_1\left(P^{min*}\right)}. \tag{11}$$

This is the extent to which a cryptocurrency exchange will adjust P^{min} down.

Money launderer's portfolio choice problem

In the model depicting a cryptocurrency exchange's decision in the previous section, we do not discuss the behavior of money launderers. The number of ML transactions is given and $\delta = \Pr(ML)$ is treated as exogenous. However, a cryptocurrency exchange considers not only the financial authority's behavior, but also the money launderers' behavior. Thus, we build a second model using portfolio choice theory to analyze the decision of a representative money launderer and its effect on the cryptocurrency exchange's decision.

Cryptocurrencies are known to be favored by illegal market participants. A criminal who wants to launder illegal gains and convert them to fiat money is likely to use a cryptocurrency exchange. We can infer that the fraction of ML transactions performed on a cryptocurrency exchange is much greater than that of ML transactions performed through ordinary private banks. Assuming that money launderers are aware of which exchanges are safer or riskier for performing ML activities than others and, thus, can choose the safest cryptocurrency exchange as an ML channel, an exchange that is highly reliant on revenue from ML transactions may try to conceal money launderers' activities from being detected. We call these types of businesses ML-friendly cryptocurrency exchanges. An ML-friendly exchange can be aware that excessive reporting is uninformative to the government. Then, the exchange may prefer to overreport suspicious transactions because it still fears penalties for reporting failures. This can be better understood by addressing an example. Suppose ten transactions are made through an exchange and two of them, denoted as A and B, are actual ML cases. A and B are estimated by the exchange to be the most and second-most suspicious transactions. The exchange is contemplating whether to change the currently set P^{min}, which lets A and B be reported. Raising P^{min} to report only B runs the risk of a reporting failure sanction caused by A. On the other hand, lowering P^{min} to include other less suspicious cases dilutes the report without making further reporting failure sanction risk. The government has limited resources; thereby it can waste its resources on insignificant reports if P^{min} is lowered. By setting the threshold P^{min} low, the exchange can deter the apprehension of money launderers.

Masciandaro (1998, 1999) assumes that dirty money must be laundered before it can be reinvested. The reason for this is that those who are willing to reinvest illegal gains try to maintain secrecy by using an ML process. However, the assumption that reinvestment must always be preceded by ML seems inadequate. It is true that reinvesting dirty money into another sector requires ML, but one can still invest the money in the sector in which it originated. For example, profits from drug sales can be reinvested to expand the drug business. This process does not necessarily require ML, and ML may expose the money to the risk of identification by the authority. Ferwerda (2009) concedes that not all gains need to be laundered in practice; however, for simplicity, he assumes that unlaundered gains can be incorporated in the ML detection probability by lowering the probability value. This study distinguishes money that does not need to be laundered from money that needs to be laundered.

In our study, the money launderer is the same person as the criminal. McCarthy et al. (2015) include a professional money launderer in their model, whereas, in our discussion, we assume that the money launderer is the criminal for simplicity. As we allow for the possibility of reinvestment in the original sector without ML, we assume that a

money launderer with dirty money compares the profitability of investing in the original sector or investing in other sectors that require ML. We refer to investment in another sector as an investment in a clean zone. Although laundered money can become dirty again, we use the term *clean zone* to denote outside sectors in general. In this model, there are only two distinct zones: a dirty underground zone and a clean zone (Fig. 2).

Let m denote an initial amount of illegal money held by a representative would-be money launderer. The money launderer with the fixed illegal fund m divides the fund into two parts for diversification. Defining θ $(0 < \theta < 1)$ as a proportion of the initial fund that the launderer chooses to send to the clean zone, θm goes to the clean zone via a cryptocurrency exchange. The transaction fee τ determined by the exchange is lost in the ML process. In practice, dirty money has to go through several institutions to set up layers, but, for simplicity, we assume that the ML is implemented through a single cryptocurrency exchange. When θm is laundered, the successfully washed money can be invested outside of the original sector with a return of r_C. Considering the loss of τ and the return of r_C, we express r_{ML}, the total return from the ML process, as follows:

$$\theta m(1 + r_{ML}) = \theta m(1 - \tau)(1 + r_C) \tag{12}$$

However, ML is not certain to succeed, but rather involves some risk. Hinterseer (2002) suggests that each financial investment can be framed in an R^3 space of $(return, risk, secrecy)$. The risk is the embedded financial risk describing the deviations caused by the upward and downward movements of an asset. In addition to the traditional dimensions of financial return and risk, this space includes a secrecy dimension. Associated with legal risk, this dimension signifies concealment from the public and supervising authority. A financial decision, such as ML, needs enough secrecy to avoid detection. In fact, the risk and secrecy dimensions used by Hinterseer (2002) do not necessarily need to be thoroughly separated, but they both imply probabilities. In this sense, the model in this study treats detection risk as if it is a financial risk.

In this model, D denotes the probability that an ML attempt is detected by the authority and the launderer forfeits the money. Even in this case, the money launderer pays the transaction fee τ to the cryptocurrency exchange.[5] Incorporating this probability into the previous equality yields

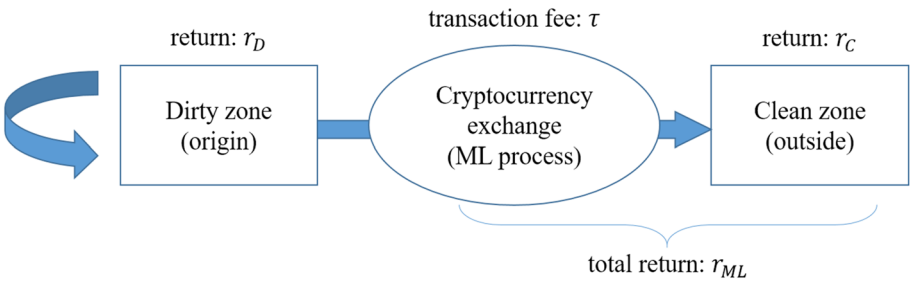


Fig. 2 Model describing the two choices available to a money launderer

[5] It is intricate to construct a benchmark model because the punishment implementation can vary by country or even by individual case. Instead of considering a representative form of the punishment implementation, we assume that the money launderer has to pay off the whole amount of ML attempted money when identified, irrespective of the transaction fee. This assumption is convincing, in that it makes sure illegal gains are forfeited, even if they are consumed.

$$\theta m(1+r_{ML}) = \begin{cases} \theta m(-\tau)(1+r_C), \textit{with probability } D \\ \theta m(1-\tau)(1+r_C), \textit{with probability } (1-D) \end{cases} \tag{13}$$

We note that because the money confiscated by the authority was expected to earn a return of r_C, it is more accurate to convert the confiscated amount θ_m into future value using r_C rather than r_D. The expectation and variance of r_{ML} is computed as

$$\mu_{ML} = E[r_{ML}] = (1-D-\tau)(1+r_C) - 1, \sigma_{ML}^2 = Var(r_{ML}) = D(1-D). \tag{14}$$

The remaining fraction of the fund, $(1-\theta)m$, stays at the original sector. Whereas the clean money earns a return of r_{ML}, $(1-\theta)m$ is assumed to be invested without any risk. This dirty money grows to be $(1-\theta)m(1+r_D)$, where r_D is the return in the origin sector.

By considering θm and $(1-\theta)m$ as funds invested in risky and riskless assets, respectively, the money launderer's investment decision can be interpreted as a financial portfolio. This model uses the mean–variance framework introduced by Markowitz (1952). In the portfolio, the money launderer decides the share θ to transfer to the clean zone through the ML process. The portfolio return is constructed as

$$w = \theta r_{ML} + (1-\theta) r_D. \tag{15}$$

It follows that

$$\mu = E[w] = E[\theta r_{ML} + (1-\theta) r_D] = \theta \mu_{ML} + (1-\theta) r_D, \tag{16}$$

and

$$\sigma^2 = Var(w) = Var(\theta r_{ML} + (1-\theta) r_D) = \theta^2 Var(r_{ML}) = \theta^2 \sigma_{ML}^2. \tag{17}$$

Then, we can obtain a capital allocation line (CAL) as follows:

$$\mu = \frac{\mu_{ML} - r_D}{\sigma_{ML}} \sigma + r_D. \tag{18}$$

The optimal pair (σ^*, μ^*) is the solution to the following utility maximization problem:

$$\max_{\sigma,\mu} U(\sigma, \mu), \quad s.t. \mu = \frac{\mu_{ML} - r_D}{\sigma_{ML}} \sigma + r_D. \tag{19}$$

By equating the $MRS_{\sigma,\mu}$ to the slope of the CAL, we can determine the optimal pair.

We are not interested in (σ^*, μ^*) per se, but rather in how a cryptocurrency exchange's manipulation of D affects θ. In fact, a cryptocurrency exchange can control not only D, but also the transaction fee τ. Thus, we can also check the relative effects of τ and D. The transaction fee that must be paid to the cryptocurrency exchange only affects μ_{ML} and not σ_{ML}. The inequality $\frac{\partial \mu_{ML}}{\partial f} = -(1+r_C) < 0$ holds and, thus, lowering τ positively affects μ_{ML}. The partial derivative of the slope of CAL with respect to τ is negative:

$$\frac{\partial}{\partial f}\left(\frac{\mu_{ML}-r_D}{\sigma_{ML}}\right)=\frac{1}{\sigma_{ML}}\frac{\partial \mu_{ML}}{\partial f}<0. \tag{20}$$

Thus, a reduction in τ causes the slope to increase. Then, the substitution effect increases θm, the fraction of funds that undergo ML. The sign of the income effect depends on the degree of absolute risk aversion. However, because money launderers are aggressive agents who bear the risk of punishment, we assume that a representative money launderer's degree of absolute risk aversion is decreasing or at least constant. Based on this assumption of non-increasing absolute risk aversion, we can conclude that both substitution and income effects are positive for θm.

Now, let τ be fixed, so that we can focus on the impact of changes in D. A cryptocurrency exchange can reduce D through excessive reporting. We check how D affects $\frac{\mu_{ML}-r_D}{\sigma_{ML}}$, the slope of the CAL. The partial derivative of the slope of the CAL with respect to D is calculated as

$$\frac{\partial}{\partial D}\left(\frac{\mu_{ML}-r_D}{\sigma_{ML}}\right)=\frac{[(D+\tau-1)(1+r_C)+1]\frac{1-2D}{2\sqrt{D(1-D)}}}{D(1-D)}, \quad \textit{where} \quad D\in(0,1). \tag{21}$$

This derivative is negative if and only if

$$4(1+r_C)D^2+[(2\tau-5)((1+r_C))+2]D+(1-\tau)(1+r_C)-1>0. \tag{22}$$

This quadratic inequality seems complicated, but it is only complicated for $0.5<D$. μ_{ML} is a monotonically decreasing function of D, whereas σ_{ML} is not a monotonic function of D. σ_{ML} is maximized when $D=0.5$. When $0<D<0.5$, a decrease in D leads to an increase in μ_{ML} and a decrease in σ_{ML}. In this interval, it is easy to see, without any complicated computation, that reducing D increases the slope of the CAL. The implications of lowering τ are the same as those of lowering D. Assuming that absolute risk aversion is non-increasing, reducing D increases the demand for ML, θm, when D is less than 0.5. In fact, it is difficult for D to exceed 0.5 when an ML monitoring is practiced by cryptocurrency exchanges with inferior techniques; thus, it is likely that intentionally reducing D through excessive reporting can be a tool for a cryptocurrency exchange business. Moreover, reducing τ does not always increase revenue, as revenue is calculated as $\theta m\tau$. To a certain extent, decreasing τ increases the demand for ML, θm, which leads to higher revenues. However, when τ is too small, a further decrease in τ leads to lower revenue. The effect of manipulating D is free of this problem occurring when controlling τ.

Ferwerda (2009), who incorporates ML into the market offense function proposed by Becker (1968), suggests that the ML detection probability negatively affects the amount of criminal activity, which is related to m in our study. Our model shows that the detection probability negatively affects the ML demand θm, for a fixed amount of illegal gain m. A cryptocurrency exchange sets the threshold P^{min} low enough not only to avoid sanctions, but also to reduce the detection probability to cater to money launderers. Then, P^{min} is lower in this model than in the first model. There is an additional effect. When the demand for ML increases owing to the lower detection probability, δ increases. Then, even when $Pr(notreported|ML)$ is given, the absolute number of reporting failure

cases increases. Consequently, the exchange reduces P^{min} even further, and this can be identified through Eq. (11). When we incorporate the behavior of money launderers into the analysis, we find that cryptocurrency exchanges in which ML activities comprise a large proportion of total transactions may reduce P^{min} below that indicated by the result in the first model. An excessively low P^{min} dilutes suspicious reports, making the naive application of existing private bank regulations to cryptocurrency exchanges ineffective.

Policy implications

Cryptocurrency is booming. Although opinions on its value or potential power may differ, its impact on the economy must be considered. In particular, governments worldwide are most concerned about its wide use in the underground economy and investor protections (Böhme et al. 2015). On the grounds that illegal pecuniary gains from the underground economy are followed by ML, governments are working to apply the AML regulation that originally targeted the traditional private financial sector to the cryptocurrency market. For example, in fact, regulations compelling cryptocurrency exchanges to report suspicious transactions are emerging.

The consequences of regulatory reforms or adoptions do not depend only on the current behavior of those being regulated. Because those affected by the regulations react to them, the regulator faces a new set of actions from those being regulated. For this reason, a regulator should not take the current set of actions for granted. Successful implementation of regulations requires the authorities to not only consider the problems faced in the present state, but also predict long-run consequences (Kane 1988). This lesson also applies to the design of regulations for cryptocurrency exchanges.

Takáts (2011) proposes that private banks taking on an ML monitoring role tend to report an excessive number of transactions to avoid punishment for reporting failures. To alleviate this behavior and make the set of reports to the government more informative, he suggests a few corrective policy measures, such as reducing the punishment for reporting failures and introducing reporting fees. In other words, measures that punish type II errors less and indirectly reduce type I errors can improve the effectiveness of regulations. Similar measures may be valid for cryptocurrency exchanges. However, given our finding that overreporting is expected to be greater for cryptocurrency exchanges, further policy measures are needed.

In addition, despite some conflicting views, there is a general consensus that the direction of regulatory impact on the cryptocurrency market is generally negative or, at least, non-positive (Borri and Shakhnov 2020; Chokor and Alfieri 2021; Feinstein and Werbach 2021; Shanaev et al. 2020). This implies that the cryptocurrency regulations should be elaborate and not excessively tight, so as to reduce the burdens caused by regulations.

The overreporting behavior of cryptocurrency exchanges is primarily attributed to their inferior detection abilities, and the fact that cryptocurrencies are heavily involved in illegal activities is likely to intensify the problem. Thus, the government needs to work to improve cryptocurrency exchange businesses' detection abilities and ensure transparency in the cryptocurrency world. To improve these abilities, we suggest providing financial and technological support to cryptocurrency exchanges. Anti-money laundering risk assessments can be performed for each exchange prior to the support. For example, financial risk, including ML risk, can be analyzed through clustering algorithms, as

suggested by Kou et al. (2014). Government support will be more effective when it concentrates on exchanges with high ML risk. An alternative is to set a capital requirement level for these exchanges, so that highly incompetent exchanges are prevented from entering the market.

We also suggest a differential application of regulations. Not all cryptocurrency exchanges registered on financial authorities' lists can immediately bear full monitoring and reporting obligations. Our model explaining the impacts of detection ability levels shows that newer, smaller, and less liquid exchanges tend to set lower reporting thresholds (i.e., P^{min}). Hence, reporting deadlines, fines, and reporting fees need to be applied differentially based on an exchange's age, size, and trading volume.

Conclusion

A governmental authority cannot directly manage entire societies and economies; thus, authorities often partially entrust their roles to private institutions to maximize the efficiency of regulations. However, this type of delegation system is bound to create agency problems caused by interest discrepancies. This discrepancy is intensified if a regulatory delegation imposes a compliance cost on the delegate that is partially responsible for the regulation practice. From this perspective, this study proposes the possibility that cryptocurrency exchanges will tend to report excessively if they are obligated to monitor ML transactions and report suspicious cases in the same way as private banks.

Beyond suggesting the mere possibility of overreporting, we claim that the magnitude of overreporting will be stronger for cryptocurrency exchange businesses. Cryptocurrency exchanges generally have short histories, small sizes, and low trading volumes; thus, they lack ML detection abilities. This study develops a model to understand the structure of ML monitoring institutions' reporting decisions. Through this model, we show that cryptocurrency exchanges with limited ML detection abilities choose to overreport suspicious cases more intensely to reduce type II errors, which can be explicitly punished. Moreover, we assume that some cryptocurrency exchanges rely heavily on revenues from ML and are friendly to money launderers. Based on this assumption, we use portfolio selection theory to show that reducing the detection probability through excessive reporting can be a tool for an exchange to increase ML transactions. In consideration of this additional finding, we conclude that cases reported by cryptocurrency exchanges will be even greater. We suggest some policy measures and expect that further studies can be conducted to design these measures in a more refined manner. Finally, we expect our argument that newer, smaller, and less liquid exchanges would report suspicious transactions more than older, larger, and more liquid exchanges to be empirically tested when the regulation is settled and the data are accessible for academia.

Abbreviations

AML: Anti-money laundering; CAL: Capital allocation line; FATF: Financial action task force; FinCEN: US Financial Crimes Enforcement Network; ML: Money laundering; PDF: Probability density function.

Acknowledgements

We appreciate helpful comments and discussions from Takanori Adachi (Tokyo Metropolitan Univ.), Kyoung Jin Choi (Univ. of Calgary), and Gang Kou (Southwestern Univ. of Finance and Economics).

Authors' contributions

DK: proposal and original idea. DR, MB: conceptualization; DK: modeling; DK, DR:methodology; DR: validation; DR: resources; DK, MB: literature review; DR, MB: economic and business implication; DK: writing—original draft preparation;

DR: writing—review and editing; MB: discussion; DR: project administration. All authors have read and agreed to the published version of the manuscript. All authors read and approved the final manuscript.

Author's information

Daehan Kim is currently a researcher at the College of Economics, Sungkyunkwan University (SKKU), Seoul, Republic of Korea.

Mehmet Huseyin Bilgin is a full professor of economics and the Chair of the Division of the International Economic Integration at Istanbul Medeniyet University. His current research interests include macroeconomics, international economics, and international finance. Bilgin has published many articles in reputable international journals.

Doojin Ryu, the corresponding author, is a full professor of finance at SKKU. Ryu has published 130 papers in SSCI journals, and globally ranked 4th (2018), 4th (2019), 9th (2020), 14th (2021) in the field of business and finance (Journal Citation Reports—Clarivate Analytics).

Funding

There is no specified project funding.

Availability of data and materials

The liquidity score of each cryptocurrency exchange is available in "exchanges" section of Coinmarketcap (https://coinmarketcap.com/rankings/exchanges/).

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1]College of Economics, Sungkyunkwan University, Seoul 03063, Republic of Korea. [2]Faculty of Political Sciences, Istanbul Medeniyet University, Istanbul, Turkey.

Received: 12 June 2021 Accepted: 8 September 2021
Published online: 04 October 2021

References

Albrecht WS, Albrecht CC, Albrecht CO, Zimbelman MF (2008) Fraud examination, 3rd edn. South-Western College Pub
Becker GS (1968) Crime and punishment: an economic approach. J Polit Econ 76(2):169–217. https://doi.org/10.1086/259394
Bhaskar ND, Chuen DL (2015) Bitcoin exchanges. Handb Digital Curr. https://doi.org/10.1016/b978-0-12-802117-0.00028-x
Böhme R, Christin N, Edelman B, Moore T (2015) Bitcoin: economics, technology, and governance. J Econ Perspect 29(2):213–238. https://doi.org/10.1257/jep.29.2.213
Borri N, Shakhnov K (2020) Regulation spillovers across cryptocurrency markets. Financ Res Lett 36:101333. https://doi.org/10.1016/j.frl.2019.101333
Brenig C, Accorsi R, Müller G (2015) Economic analysis of cryptocurrency backed money laundering. In: ECIS 2015 completed research papers 20. https://doi.org/10.18151/7217279
Chen Z, Khoa LD, Teoh EN, Nazir A, Karuppiah EK, Lam KS (2018) Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowl Inf Syst 57(2):245–285. https://doi.org/10.1007/s10115-017-1144-z
Chokor A, Alfieri E (2021) Long and short-term impacts of regulation in the cryptocurrency market. Q Rev Econ Finance 81:157–173. https://doi.org/10.1016/j.qref.2021.05.005
Dupuis D, Gleason K (2020) Money laundering with cryptocurrency: open doors and the regulatory dialectic. J Financ Crime 28(1):60–74. https://doi.org/10.1108/jfc-06-2020-0113
Dwyer GP (2015) The economics of bitcoin and similar private digital currencies. J Financ Stab 17:81–91. https://doi.org/10.1016/j.jfs.2014.11.006
Feinstein BD, Werbach K (2021) The impact of cryptocurrency regulation on trading markets. J Financ Regul 7(1):48–99. https://doi.org/10.1093/jfr/fjab003
Ferwerda J (2009) The economics of crime and money laundering: Does anti-money laundering policy reduce crime? Rev Law Econ. https://doi.org/10.2202/1555-5879.1421
Foley S, Karlsen JR, Putniņš TJ (2019) Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Rev Financ Stud 32(5):1798–1853. https://doi.org/10.1093/rfs/hhz015
Financial Action Task Force (2012) International standards on combating money laundering and the financing of terrorism and proliferation: the FATF recommendations, FATF/OECD, Paris, France (updated as of October 2020). www.fatf-gafi.org/recommendations.html
Financial Action Task Force (2019) Guidance for a risk-based approach to virtual assets and virtual asset service providers
Financial Crimes Enforcement Network, Public Affairs (2019) New FinCEN guidance affirms its longstanding regulatory framework for virtual currencies and a new FinCEN advisory warns of threats posed by virtual currency misuse [press release]. Retrieved from https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual

Hinterseer K (2002) Criminal finance: the political economy of money laundering in a comparative legal context. Kluwer Law International, Hague
Kane EJ (1988) Interaction of financial and regulatory innovation. Am Econ Rev 78(2):328–334
Kou G, Peng Y, Wang G (2014) Evaluation of clustering algorithms for financial risk analysis using MCDM methods. Inf Sci 275:1–12. https://doi.org/10.1016/j.ins.2014.02.137
Loi H (2018) The liquidity of bitcoin. Int J Econ Financ 10(1):13–22. https://doi.org/10.5539/ijef.v10n1p13
Markowitz H (1952) Portfolio selection. J Finance 7(1):77. https://doi.org/10.2307/2975974
Masciandaro D (1998) Money laundering regulation: The micro economics. Journal of Money Laundering Control 2(1):49–58. https://doi.org/10.1108/eb027170
Masciandaro D (1999) Money laundering: the economics of regulation. Eur J Law Econ 7:225–240. https://doi.org/10.1023/A:1008776629651
Masciandaro D, Filotto U (2001) Money laundering regulation and bank compliance costs: What do your customers know? Economics and the Italian experience. J Money Laundering Control 5(2):133–145. https://doi.org/10.1108/eb027299
Mccarthy KJ, Santen PV, Fiedler I (2015) Modeling the money launderer: microtheoretical arguments on anti-money laundering policy. Int Rev Law Econ 43:148–155. https://doi.org/10.1016/j.irle.2014.04.006
Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
Shanaev S, Sharma S, Ghimire B, Shuraeva A (2020) Taming the blockchain beast? Regulatory implications for the cryptocurrency market. Res Int Bus Financ 51:101080. https://doi.org/10.1016/j.ribaf.2019.101080
Smales L (2019) Bitcoin as a safe haven: Is it even worth considering? Financ Res Lett 30:385–393. https://doi.org/10.1016/j.frl.2018.11.002
Takáts E (2011) A theory of "crying wolf": the economics of money laundering enforcement. J Law Econ Organ 27(1):32–78. https://doi.org/10.1093/jleo/ewp018
Yermack D (2015) Is bitcoin a real currency? An economic appraisal. Handb Digital Curr. https://doi.org/10.1016/b978-0-12-802117-0.00002-3

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com