# Money for Nothing, Supervision for a Fee

## Investigating the Effects of the 5th Anti-Money Laundering Directive on Cryptocurrency Exchanges in the Netherlands

Volten, Cécile; van Eeten, Michel; van Wegberg, Rolf

**DOI**
10.1007/s10610-025-09640-1

**Publication date**
2025

**Document Version**
Final published version

**Published in**
European Journal on Criminal Policy and Research

European Journal on Criminal Policy and Research
https://doi.org/10.1007/s10610-025-09640-1

ORIGINAL RESEARCH

# Money for Nothing, Supervision for a Fee: Investigating the Effects of the 5th Anti-Money Laundering Directive on Cryptocurrency Exchanges in the Netherlands

**Cécile Volten**[1] · **Michel van Eeten**[1] · **Rolf van Wegberg**[1]

Accepted: 22 July 2025


**Abstract**
By converting between currencies, cryptocurrency exchanges provide access between the traditional and cryptocurrency ecosystem, making them susceptible to money laundering. The European Union extended the scope of the 5$^{th}$ Anti-Money Laundering Directive (AMLD5) to include cryptocurrency exchanges, requiring them to obtain a registration, conduct customer due diligence, and report unusual transactions. It is, however, unknown whether the measures introduced by the implementation of AMLD5 lead to less risk exposure and what impact it has on cryptocurrency exchanges. This paper uses a mixed-methods approach to explore the effects of the Dutch implementation of AMLD5 measures on cryptocurrency exchanges active in the Netherlands. We analyzed over 335,000 transactions and complemented them with seven qualitative interviews with Dutch cryptocurrency exchanges and the supervisory authority. We find that the Dutch implementation of AMLD5 imposed high administrative burdens and substantial fees on relatively small exchanges that do not pose high money laundering risks. This raises questions about the alignment of the goals and consequences of the regulation.

**Keywords** AMLD5 · Cryptocurrency · Cryptocurrency exchanges · Money laundering · Regulation

✉ Cécile Volten
c.j.volten-1@tudelft.nl

[1] Faculty of Technology, Policy & Management, Delft University of Technology, Jaffalaan 5, Delft 2628BX, the Netherlands

Published online: 13 September 2025

## Introduction[1]

Cryptocurrency exchanges act as gatekeepers between the traditional financial and decentralized cryptocurrency ecosystem. Their role in converting fiat to cryptocurrency makes them susceptible to money laundering, a risk amplified by cryptocurrency transactions' inherent pseudonymous, global, and irreversible nature. As a result, money laundering risks in the cryptocurrency ecosystem can extend into the traditional financial system. This possibility places cryptocurrency exchanges at the center of global regulatory debates on financial crime and digital asset governance (Stokes, 2012; United States Attorney's Office, 2023).

In response to these concerns, the European Union adopted the 5$^{th}$ Anti-Money Laundering Directive (AMLD5), which extended the scope of anti-money laundering (AML) regulations to cryptocurrency exchanges and custodian wallet providers. AMLD5 requires the so-called obliged entities to register with national financial authorities, conduct customer due diligence (CDD), and report unusual transactions. However, its transposition has varied across EU member states. The Netherlands, positioned as a pioneer in combating money laundering, took a particularly proactive stance, introducing a strict registration regime through its national transposition of AMLD5. This led to a tumultuous response in the cryptocurrency exchange sector, leading to legal disputes on the proportionality of introduced measures, particularly regarding the proposed wallet verification procedures (van Spengen, 2021). Moreover, controversy arose regarding the design of the registration regime, which, according to the sector, better resembled a permit regime (van Spengen et al., 2023).

Previous literature has examined the AML regulations' limitations in both traditional finance and cryptocurrency markets (see Kirillova et al., 2018; Haffke et al., 2020; De Vido, 2020). Moreover, studies have tried to understand the effectiveness of AML policies but have shown that the lack of available metrics provides difficulties in establishing this (Chaikin, 2009; Pol, 2018, 2020a). Still, few empirical studies have evaluated the actual impact of AMLD5 on cryptocurrency exchanges (with regards to AML effectiveness in general see Usman Kemal, 2014; Soudijn, 2019). Moreover, there is limited evidence on whether the measures introduced by AMLD5 reduce exposure to money laundering risks or how they affect the business operations of compliant firms.

This paper addresses this gap by examining the Dutch implementation of AMLD5 and its effects on the country's cryptocurrency exchanges. In particular, we focus on the following research questions: 1) Which parties obtained a registration at the Dutch National Bank? 2) What changes in transaction patterns of Dutch cryptocurrency exchanges can be observed? 3) What is the business impact of the new oversight on the Dutch cryptocurrency exchanges?. We employ a mixed-methods approach to answer these open questions, combining blockchain transaction analysis of over 335,000 Bitcoin transfers with qualitative interviews conducted with seven employees at Dutch exchanges and the Dutch National Bank (DNB), the supervisory authority.

Our findings suggest that the exchanges that comply with registration requirements represent only a small subset of the global and Dutch markets, which are not at a significant risk of being exploited for money laundering. Nevertheless, they face high compliance costs and administrative burdens. This raises the question of whether the Dutch transposition of

[1] Here, we would like to acknowledge the contributions of one of the reviewers, which significantly helped in shaping the introduction in its current state.

AMLD5 actually reduces possible money laundering risks. Moreover, it highlights a potential misalignment between AML objectives and outcomes.

## Countering Crypto Crime

Before analyzing the effects of the Dutch implementation of AMLD5 on cryptocurrency exchanges, we first examine the perceived risks of cryptocurrencies. We then assess anti-money laundering legislation's objectives, measures, and effectiveness.

### Cryptocurrencies

Cryptocurrencies are a digital representation of value not issued or guaranteed by a central authority (FATF, 2014), typically operating in a decentralized system lacking a responsible authority (Stokes, 2012). They serve various functions, including acting as a measure of value, medium of exchange, means of payment, and storage of value (Kirillova et al., 2018). Bitcoin is the most prominent example and the most adopted cryptocurrency.

The Bitcoin system exhibits two key features that differentiate it from traditional banking. First, unlike in the traditional system, all Bitcoin transactions are publicly recorded on a transparent blockchain (Böhme et al., 2015). This offers pseudo-anonymity: while transaction details are public, user identities remain concealed (Meiklejohn et al., 2013). This duality enhances privacy for legitimate users but also facilitates illicit activity. Second, Bitcoin enables near-instant, irreversible, and transnational transactions (Leuprecht et al., 2023), allowing criminals to bypass cross-border restrictions (FATF, 2014).

Intermediaries provide market access between the seemingly disconnected traditional and Bitcoin systems by converting cryptocurrency to fiat currency and vice versa. This linkage increases systemic risk, particularly in the context of money laundering (Stokes, 2012).

### Money Laundering

Money laundering involves concealing the illicit origin of funds to make them appear legitimate (Interpol, n.d.). This process typically includes three stages: *placement* into the financial system, *layering* to obscure the origin, and *integration* into the legal economy through spending or investment (Levi & Soudijn, 2020). The methods adopted for this vary widely (Nazzari, 2023).

Cryptocurrencies pose money laundering risks due to their pseudonymity and limited transaction oversight (Limba et al., 2019). Various laundering techniques exploit these features (Tsuchiya & Hiramoto, 2021; Van Wegberg et al., 2018). Common methods include using mixers or tumblers to obscure transaction trails (Kruisbergen et al., 2019; Crawford & Guan, 2020) and converting cryptocurrency through exchanges. Both crypto-to-crypto and fiat-to-crypto exchanges can be used for this purpose (Haffke et al., 2020), though fiat-to-crypto exchanges are necessary for integration into the traditional financial system. Additionally, laundered cryptocurrency can be spent on goods such as gift cards or NFTs (Garretsen, 2022). These practices highlighted the need for updated regulatory frameworks.

## The 5th Anti-Money Laundering Directive

The regulation of cryptocurrencies has been widely debated. As early as Stokes, identified the money laundering risks associated with Bitcoin and questioned whether existing AML frameworks would apply. With growing concerns over AML risks and the increasing adoption of cryptocurrencies, scholars have explored their legal classification as currencies, assets, or commodities (De Filippi, 2014; Kirillova et al., 2018; Fletcher et al., 2021), and assessed regulatory frameworks across jurisdictions (Parasol, 2022; Kepli & Zulhuda, 2019; Alekseenko, 2022).

The 4th Anti-Money Laundering Directive (AMLD4), introduced in 2015 (Directive (EU), 2015), set out key measures in the fields of AML and countering the financing of terrorism (CFT). It defined obliged entities required to conduct customer due diligence in specific situations (Article 2(1)) and formally recognized Politically Exposed Persons as carrying elevated risk profiles. AMLD4 also established a register of ultimate beneficial owners to improve transparency and prevent the misuse of corporate structures for financial crime. Additionally, it mandated risk assessments at the EU, national, and institutional levels, requiring appropriate mitigation strategies. The directive further introduced Financial Intelligence Units (FIUs) in each member state and promoted systematic information exchange among them.

In 2018 (Directive (EU), 2018), the EU amended AMLD4 through AMLD5 to address money laundering risks related to cryptocurrencies (see Fig. 1). The directive's scope was expanded to draw a parallel between cryptocurrency exchanges and traditional payment service providers (see Amuso and Baron, 2023). Specifically, Article 2(1) point 3 introduced two new obliged entities: (g) providers of exchange services between virtual and fiat currencies, and (h) custodian wallet providers. These additions extended AML obligations to key cryptocurrency service providers. Furthermore, Article 3 formally defined "virtual currencies" and "custodian wallet providers".

AMLD5 requires Member States to ensure the registration of providers offering exchange services between virtual and fiat currencies, as well as custodian wallet providers (Article 47). The expanded scope obliges these entities to conduct risk assessments (Article 8), apply customer due diligence throughout the business relationship based on customer risk profiles

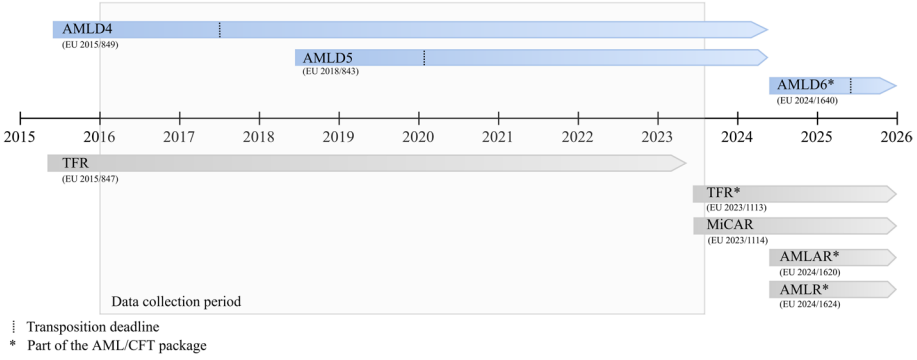


**Fig. 1** Timeline providing an overview of EU regulations related to anti-money laundering. The regulations highlighted in blue represent the anti-money laundering framework central to this study, where AMLD5 introduces requirements for cryptocurrency exchanges. Those in grey indicate related EU regulations that fall outside the scope of this research

(Article 14), and report suspicious transactions to the FIU, including attempted transactions (Article 33).

Member States were required to transpose the directive by January 10, 2020. The Netherlands implemented the legislation later, on May 20, 2020. This research focuses on the Dutch implementation, as national transpositions can vary. AMLD5 measures had to be applied at the national level and directed toward domestic companies.

Despite AMLD5's expansion of the AML framework, the regulatory landscape continued to evolve. On July 20, 2021, the European Commission proposed a comprehensive AML/CFT package comprising four legislative initiatives. These proposals aimed to address persistent gaps, including fragmented supervision, inconsistent rule application, and weak FIU coordination (European Commission, 2021), and to further harmonize AML measures across the EU.

The first component, adopted on May 31, 2023 (Regulation (EU), 2023), was the Regulation on information accompanying transfers of funds and certain crypto-assets (TFR). This regulation ensures that identifying information on both the sender and recipient accompanies crypto-asset transfers (Murphy, 2024), and it replaces the earlier TFR, which did not cover crypto-assets.

The remaining three components were also adopted on May 31, 2024. The second element, the 6$^{th}$ Anti-Money Laundering Directive (AMLD6), repeals AMLD4 (and by extension, AMLD5) and redefines AML requirements at the national level. Member States must transpose AMLD6 into national law by July 10, 2025. The third element, the Regulation establishing the EU Anti-Money Laundering Authority (AMLAR), creates a centralized body to promote supervisory convergence and a unified AML culture across Member States (European Commission, n.d.). The fourth element, the Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLR), sets AML compliance obligations for the private sector.

In parallel, the EU also introduced the Markets in Crypto-Assets Regulation (MiCAR). MiCAR seeks to harmonize crypto-asset regulation across Member States, foster innovation through regulatory clarity, and enhance consumer protection.

### Dutch Transposition AMLD5

In the Netherlands, the AMLD5 was transposed into national legislation through the *Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)* (2023). The Dutch implementation of AMLD5 had two primary objectives. First, it aimed to protect financial institutions from integrity risks such as money laundering. Second, it sought to enhance the effective detection and prosecution of criminal activities. During the parliamentary debates, the need was emphasized to prevent a crowding-out effect in the sector. This meant limiting the number of companies that might be forced to close due to the burdens of the new legislation (Alkaya & van der Linde, 2019).

The transposition of AMLD5 brought several amendments to the Wwft. In line with the directive, virtual currency exchange providers and custodian wallet providers were classified as obliged entities under Article 1. The responsibility for supervising these entities was assigned to DNB.

A key change introduced by the legislation was the requirement for registration. According to Article 23b of the Wwft, service providers must obtain registration from the dedicated

supervisory authority, in this case DNB, to operate legally in the Netherlands. Offering services without registration is prohibited. DNB is expected to process registration applications within two months, although this period can be extended if additional information is needed. Before granting registration, DNB must assess whether the company's directors are reliable and suitable, as stated in Article 23h. At the start of the regulatory implementation, existing companies were required to complete registration by the end of the transitional period on November 20, 2020. DNB must also publish a publicly accessible register of registered providers (Article 23f).

In the Netherlands, Wwft states that institutions must execute CDD and share information with the supervisor (Wwft, Article 2a). The legislation also prescribes at what time enhanced and simplified CDD can be executed, based on the assessed risk of a customer (Wwft, Article 3). CDD consists of monitoring clients in different phases of the transaction process (De Wit, 2007). During the Know Your Customer phase, the client needs to be identified. Next, when a client initiates a transaction, the transaction is monitored to identify unusual transactions. Cryptocurrency exchanges use tools to identify them (Möser & Narayanan, 2019). These tools can trace Bitcoin on the blockchain and attribute addresses to an entity (Crawford & Guan, 2020).

In terms of company organization, one director must be assigned to oversee compliance with AML legislation, and an independent audit function must be created. Companies must adopt policies that address the risks identified in national or supranational risk assessments. Moreover, they must investigate unusual transactions based on indicators established in a general administrative order (Article 15) and report these to the Dutch FIU. Companies are not permitted to share information about submitted reports. The FIU determines whether a transaction is suspicious and should be referred to law enforcement authorities (Directive (EU), 2015). If needed, they may share relevant information with enforcement or supervisory bodies.

In addition to the regulatory and operational requirements, institutions must also consider the financial costs of supervision. The *Regeling Bekostiging Financieel Toezicht* (2021) outlines the applicable fees. These include one-time costs for registration, which amount to €6300 excluding the assessment of directors, and annual supervision fees estimated at €29850.

### Effectiveness of Anti-Money Laundering Approaches

The governance of cryptocurrencies follows a risk-based approach, mirroring the strategy used in traditional AML frameworks. This approach, introduced to replace the more rigid rule-based system, is considered better suited to address money laundering risks (Bello & Harvey, 2017). However, as more assessments lead to the identification of more risks, regulatory measures tend to expand even further (Turner & Bainbridge, 2018).

Despite these efforts, the effectiveness of AML policies remains uncertain. Empirical evaluations show mixed results: for example, the reporting of unusual transactions appears to have minimal impact (Usman Kemal, 2014), and shifts in laundering methods have not clearly been linked to AML policies (Soudijn, 2019). The Financial Action Task Force (FATF), established in 1989, conducts mutual evaluations to assess national AML efforts (FATF, n.d.). However, these evaluations focus on outcomes rather than inputs (Chaikin, 2009), lack a global effectiveness metric (Pol, 2018), and are not designed for cross-coun-

try comparisons due to differing national objectives (Chaikin, 2009). Moreover, the AML regime lacks clear metrics for success, limiting its ability to demonstrate policy impact (Pol, 2020a, b).

Cryptocurrencies offer new opportunities to assess AML effectiveness through public transaction data. Ideally, AML success should be evaluated by reductions in predicate crimes and laundering opportunities (Harvey, 2008). Blockchain data enables the analysis of entities and transaction flows. Clustering techniques help identify addresses controlled by single entities (Liang et al., 2019; Meiklejohn et al., 2013), while transaction graphs reveal behavioral patterns (Möser et al., 2013; Ranshous et al., 2017). Additional metadata, such as IP addresses and public keys, can support identity inference (Reynolds & Irwin, 2017). In practice, AML efforts increasingly rely on combining these analytical tools (Crawford & Guan, 2020).

## Approach

We employed a mixed-methods approach to understand the effects of the Dutch implementation of AMLD5 on cryptocurrency exchanges active in the Netherlands. This approach allowed us to capture quantitative transaction trends and qualitative insights into business experiences (Wilkes et al., 2022). First, we analyzed transaction data from registered Dutch exchanges to identify patterns and changes over time. To complement this, we conducted interviews with employees of several Dutch exchanges and the DNB to explore the perceived business impact of the regulation.

### Transaction Analysis

Before conducting the transaction analysis, we compiled a list of cryptocurrency exchanges to include. We then collected and analyzed their transaction data. Figure 2 presents a schematic overview of this process.

### Selecting Cryptocurrency Exchanges

To conduct the transaction analysis, we compiled a list of Dutch cryptocurrency exchanges active between January 2016 and July 2023. This timeframe was selected to maximize data coverage and ensure a balanced period before and after the AMLD5 transposition deadline. Figure 1 illustrates how the dataset aligns with AML regulatory developments.

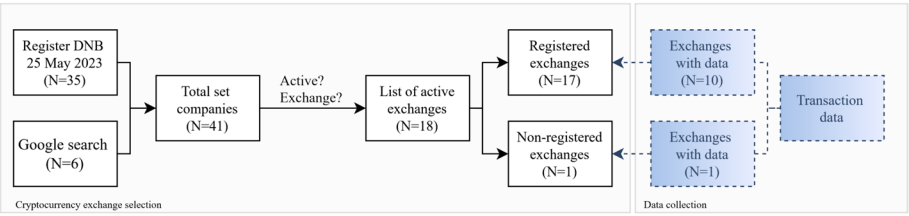


**Fig. 2** The selection process of the cryptocurrency exchanges started with the exploration of the DNB register. The active cryptocurrency exchanges were filtered from the complete set, and data was collected for those exchanges

We began by consulting the Dutch Central Bank (DNB) registry on 25 May 2023, which listed 35 registered cryptocurrency service providers. To supplement this, we conducted a Google search using the terms "Dutch," "Nederlands," "Exchange," "Crypto," and "stopped/gestopt." This search yielded six additional companies, verified through crypto websites, news sources, and forums.

To finalize the list, we applied two selection criteria. First, we verified whether the exchanges were active in the Netherlands according to the definition used by DNB, namely whether they have a Dutch website, iDeal payment support, or partnerships with local influencers (Ballegeer & Verhagen, 2023). Several unregistered exchanges had ceased operations, and one had relocated abroad to avoid EU regulations. Second, we confirmed that the selected entities provided fiat-to-crypto exchange services, excluding crypto-to-crypto exchanges, investment platforms, and global exchanges, due to data isolation constraints. We further limited the selection to platforms operating at a comparable scale and primarily targeting the Dutch market. Ultimately, 18 active Dutch cryptocurrency exchanges met the inclusion criteria for the analysis, one of which was unregistered with the DNB.

### Analysing Cryptocurrency Exchanges

After identifying active Dutch cryptocurrency exchanges, we focused on collecting their transaction data, limiting the analysis to Bitcoin due to its widespread adoption. Blockchain transaction data was obtained through Chainalysis, a leading blockchain analytics provider (Azevedo, 2021). Chainalysis links and labels addresses using heuristics and by interacting with known services, applying clustering techniques to group related addresses. Labels are only applied when the company is confident in the categorization. Although Chainalysis cannot offer complete coverage of transactions, clusters, or labels, its data is considered reliable and is widely used by law enforcement agencies.

Chainalysis did not supply data for all identified exchanges (see Fig. 2). Ultimately, we extracted transaction data for 11 active Dutch exchanges, including one that relocated abroad and did not register with the DNB. The dataset comprised over 335,000 transactions, including information on the type of origin and destination and the value of a transaction. Table 1 outlines the data fields. Identifiable information was removed, such as hash, receiving, and counterparty addresses. Chainalysis assigns a risk level to each transaction category; we used these classifications to label the risk level of each transaction (see Table 2).

To characterize Dutch exchanges, we analyzed monthly transaction volume and count as proxies for business size (see Brooksbank, 1991). This allowed us to assess the broader impact of Dutch exchanges within the Bitcoin ecosystem, where we anticipated relatively low volumes and transaction counts.

We then examined how transaction patterns evolved pre- and post-implementation of AMLD5, and compared registered exchanges with the unregistered one. To assess changes in transaction composition, we analyzed risk levels over two equal two-year periods before and after AMLD5 implementation. Transactions categorized as *unidentified*, *unnamed service*, *other*, and *exchange* were excluded due to the absence of risk classification, potentially leading to underestimating high-risk activity. Due to significant differences in transaction volumes across risk categories, we used logarithmic values for visualization. This approach highlights only substantial differences. A successful AMLD5 implementation would be reflected in a reduced share of high- or severe-risk transactions.

**Table 1** The available data per transaction provided by Chainalysis. The gray transaction features were discarded before executing the transaction analysis

| Column | Contains |
|---|---|
| Hash | The 32 byte hash of the transfer that contains the output. |
| Date | The date when the transfer was confirmed. |
| Receiving address | Address that received the payment. |
| Counterparty address | Address that the payment was sent from. |
| Counterparty category | Category of the peer cluster. |
| Value | The values in BTC. |
| USD value | The approximated USD value converted by using daily average prices. |

**Table 2** Risk level per identified category (adapted from: Chainalysis, 2020)

| Risk level | Type of service |
|---|---|
| Severe | Terrorist financing, Child abuse material, Sanctions |
| High | Mixers, Darknet markets, Hacks, Stolen funds, Scams and Ransomware |
| Medium | ICOs, Gambling, Cryptocurrency ATMs |
| Low | Exchanges, Merchant services, Mining pools |
| Unknown | Other |

Finally, we compared the risk profiles of the registered exchanges with the unregistered one over the full analysis period. Given indications that the unregistered exchange relocated to avoid regulatory compliance, we expected a higher proportion of high-risk transactions from this entity.

## Interviews

Between February and August 2021, we conducted five semi-structured interviews with stakeholders in the Dutch cryptocurrency ecosystem to assess the business impact of the Dutch implementation of AMLD5. The aim of these interviews was exploratory, seeking to gain insight into how different actors experienced and responded to the regulatory changes. Due to sector-wide turbulence and reluctance to speak openly, participants were difficult to reach. To facilitate access, we contacted the industry group Verenigde Bitcoinbedrijven Nederland (VBNL), whose members include both active firms and those that ceased operations following the regulation. After internal discussions during a general meeting, five representatives from Dutch cryptocurrency exchanges agreed to participate—four from registered exchanges and one from a company that closed due to AMLD5. Additionally, DNB was invited to participate through personal contact, after which two employees were selected to represent the regulator. Table 3 provides an overview of all participants.

The interviews were conducted online, lasting approximately 30 minutes. In two instances, respondents participated jointly: participants 1a and 1b requested a joint interview due to discomfort with individual participation, while 5a and 5b aimed to provide a comprehensive perspective by combining their views. Leading us to conduct five interviews in total.

Interview topics were based on an initial literature review on cryptocurrency regulation and anti-money laundering efforts. Topics varied according to the respondent's role and expertise, including: (i) virtual currency adoption, (ii) AML responsibilities, (iii) legislation,

**Table 3** Overview of interviewees. Two interviews were held with two interviewees, indicated by the gray rows

| Interview | Occupation participant(s) |
|---|---|
| 1 | Crypto supervision specialist at DNB |
| | Market access specialist at DNB |
| 2 | CFO of a registered cryptocurrency exchange |
| 3 | Co-founder of a non-registered exchange that altered the services they offered |
| 4 | Head of risk at a registered exchange |
| 5 | Co-founder of a registered cryptocurrency exchange |
| | Compliance officer at a registered cryptocurrency exchange |

(iv) transaction monitoring, and (v) registration and supervision. The interview protocol is included in Appendix A.

Interviews were transcribed and coded inductively using Atlas.Ti (Bernard et al., 2016, p.128). One researcher conducted the initial coding, followed by a collaborative review of the codebook to ensure reliability in line with McDonald et al. (2019). The final codebook included six themes: (i) Bitcoin adoption in cybercrime, (ii) future trends in illicit Bitcoin adoption, (iii) effects of AMLD5 implementation, (iv) AML practices prior to AMLD5, (v) registration and supervision, and (vi) contrasts between the traditional and new financial system. The complete codebook is available in Appendix B.

## Characterizing the Registered Cryptocurrency Exchanges

To characterize registered cryptocurrency exchanges, we examined their transaction volumes and the number of executed transactions. Figure 3 presents the monthly transaction volume (in USD) of ten registered exchanges from January 2016 to January 2023, with key AMLD5 implementation milestones indicated.

The figure reveals two distinct groups. The first, consisting of Huobi.com, Bitstamp.net, and BitPay.com, consistently shows significantly higher transaction volumes. The second group, comprising the remaining exchanges, exhibits lower but similarly patterned volumes over time.

Figure 4 shows the monthly number of transactions over the same period. The pattern aligns with the patterns of the transaction volumes. Huobi.com, Bitstamp.net, and BitPay.com process a substantially higher number of transactions, while the others handle consistently lower volumes.

In summary, the registered exchanges can be grouped into two categories: a high-volume segment (Huobi.com, Bitstamp.net, and BitPay.com) and a low-volume segment (the other seven exchanges), with both transaction volume and frequency reflecting this division.

## Changes in Transaction Patterns

To assess changes in transaction patterns following the implementation of AMLD5, we examine the risk composition of transaction portfolios across cryptocurrency exchanges and compare patterns between registered and non-registered entities.

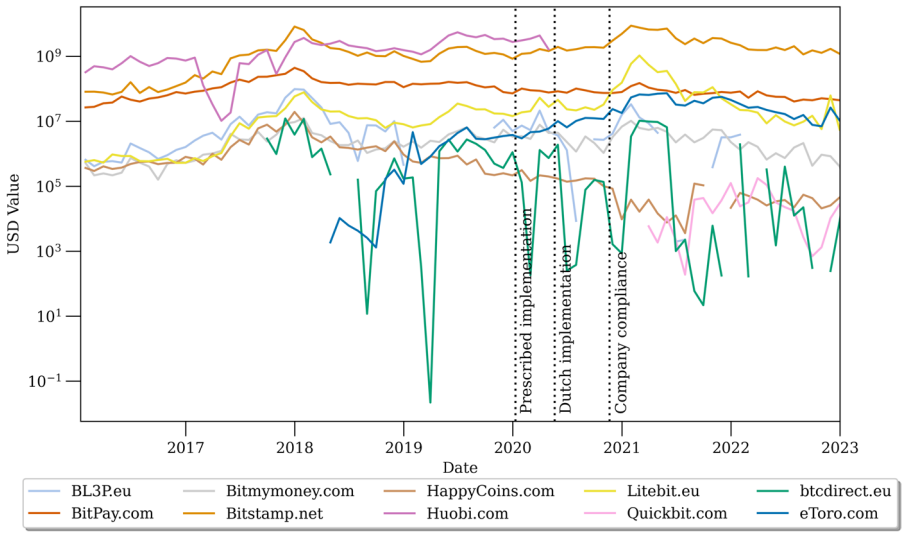


**Fig. 3** Monthly transaction volume in USD at active Dutch registered cryptocurrency exchanges (log) (N=10)

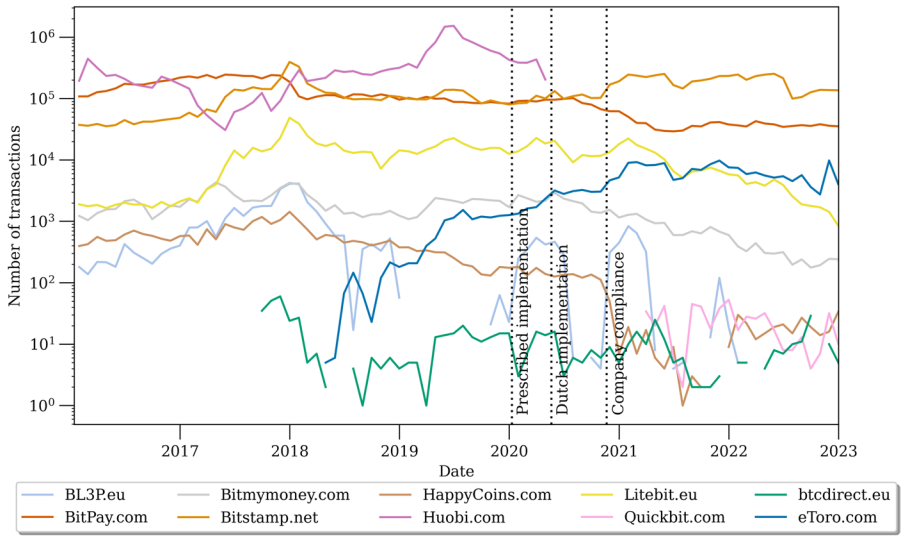


**Fig. 4** Monthly processed number of transactions at active Dutch registered cryptocurrency exchanges (log) (N=10)

## Transaction Portfolio at Registered Exchanges

Figure 5 presents the aggregated transaction portfolios of ten exchanges for the two years before (May 20, 2018 – May 20, 2020) and after (May 20, 2020 – May 20, 2022) AMLD5

implementation. Transactions are categorized by risk level. In both periods, low-risk transactions dominate, while severe-risk transactions constitute a minor share.

Contrary to expectations, the relative risk level distribution remains unchanged post-implementation. Due to the logarithmic scale, absolute volume differences are not visible in the figure; full values are provided in Appendix C. Overall, AMLD5 appears to have had limited effect on the relative risk composition of executed transactions.

### Differences in Transaction Behavior Between Registered and Non-registered Exchanges

To further explore AMLD5's effects, we analyze monthly transaction volumes by risk level for registered (Fig. 6) and non-registered (Fig. 7) exchanges from January 2016 to January 2023. Key legislative milestones are indicated in both figures. Data gaps reflect periods of missing transaction data. Risk levels of specific transaction types are detailed in Table 2.

Registered exchanges consistently processed few high- or severe-risk transactions. Over time, a decline in medium- and high-risk volumes is evident, suggesting increased compliance with AML obligations. In contrast, the non-registered exchange shows a different trajectory. Before AMLD5, it conducted a significant number of high-risk transactions. Following implementation, such transactions ceased, and total volumes sharply declined.

These findings highlight two key dynamics. First, registered exchanges already exhibited relatively low-risk profiles, which continued to decline under AMLD5. Second, the non-registered exchange, which initially facilitated higher-risk activity, was effectively pushed out of the Dutch market. High-risk transactions were reduced after AMLD5 implementation, but the transaction volumes also decreased sharply.

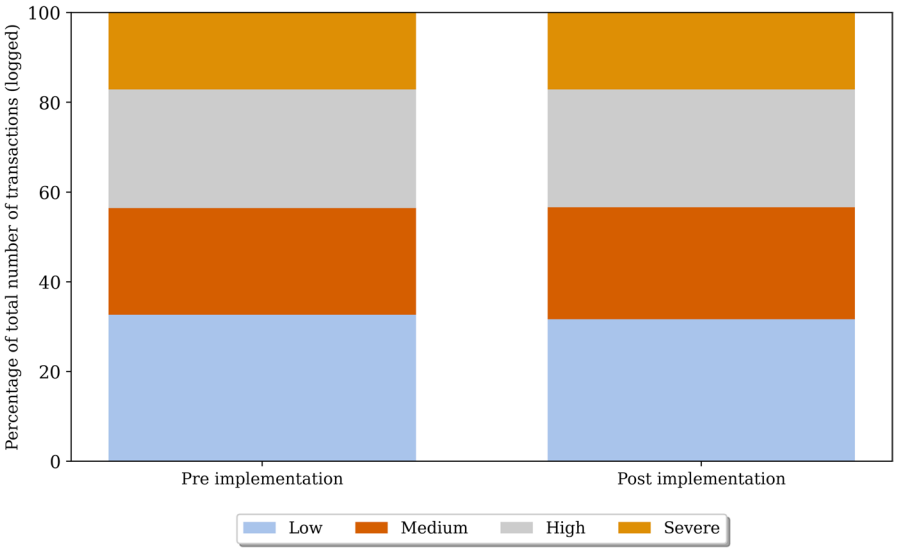


**Fig. 5** Transaction portfolio at registered cryptocurrency exchanges in percentage of the logged number of transactions categorized by risk level (n=10)

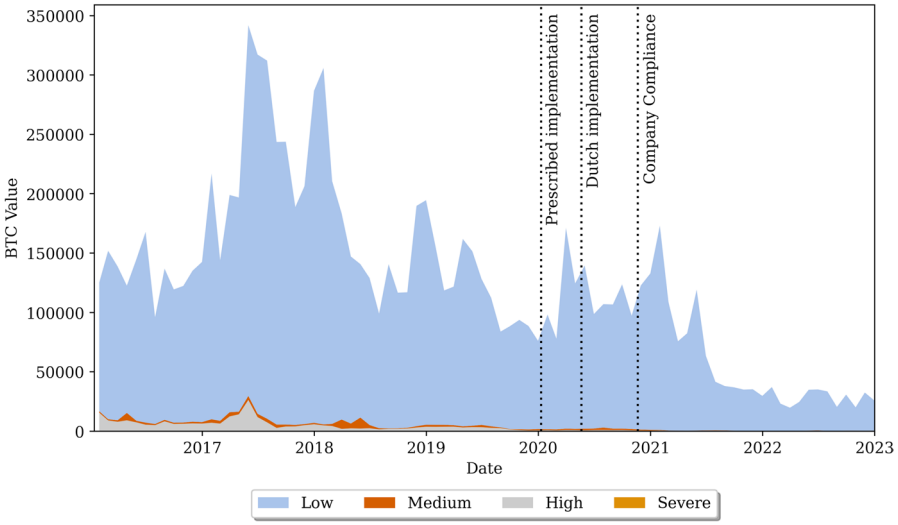


**Fig. 6** Monthly transaction volume in BTC at ten registered cryptocurrency exchanges grouped by risk level (N=10)

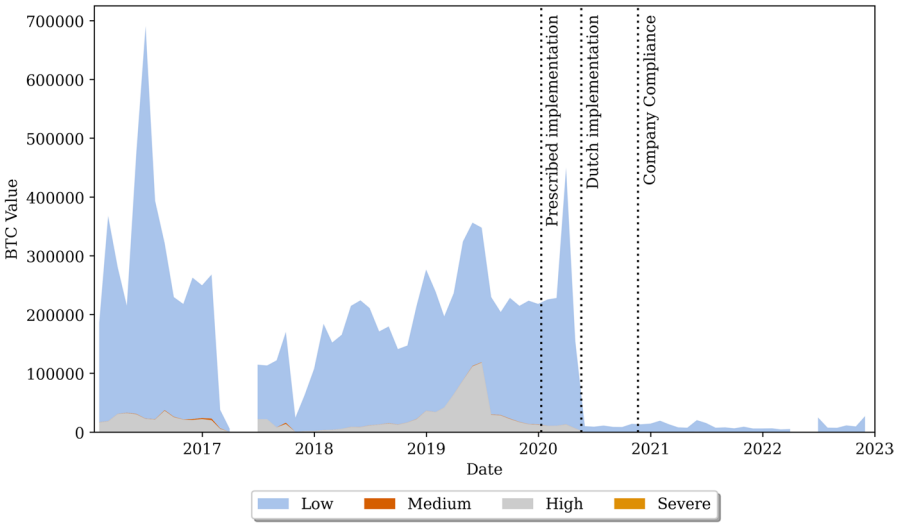


**Fig. 7** Monthly transaction volume in BTC at one non-registered cryptocurrency exchange grouped by risk level (N=1)

## Business Impact

The interviews with employees of the Dutch cryptocurrency exchanges and the regulator DNB led to an understanding of the impact of the legislation on the companies. First, the effects on a company level are discussed. Second, the impact on the Dutch cryptocurrency exchange sector is elaborated upon.

### Effects on the Company

Dutch cryptocurrency exchanges adopted AMLD5 measures before the legislation took effect, driven by both internal motivation and external incentives. In Interview 5, one interviewee stated that they had *"been preparing to conform to the Wwft since 2016/2017"*. The exchanges aimed to outperform the traditional financial system (Interviews 2 and 5). Aware of the risk of facilitating money laundering, all exchanges implemented CDD. Some exceeded the CDD standards by limiting transaction values and payment methods (Interviews 3 and 5) or requesting copies of identification documents without a legal mandate. Moreover, the exchanges had a compliance policy in place due to external incentives. *"We actually did that before because otherwise we couldn't get a bank account."* (Interview 4).

These efforts, however, were not recognized by the regulator DNB. They pronounce that the cryptocurrency exchange sector *"is a new sector that still has to get used to these new criteria, [...] That is still quite a challenge for this new sector."*. This highlights an apparent disconnect between the regulators' and regulatees' perspectives, as the sector's early AML efforts remain unacknowledged.

Although only limited technical adaptations were needed, with the reporting functionality being the main addition, exchanges underwent significant organizational changes. First, the companies faced increased administrative burdens. As part of the supervision, DNB requires the cryptocurrency exchanges to complete *"the integrity risks questionnaire, in which [they] inquire about the scope and risks of the activities and the control measures that are in place internally."* (Interview 1). One exchange explained, *"these are not things that you just write down in half an hour. For this, the compliance officer spends hours or even weeks to get that done"* (Interview 3). In addition to the large number of questions, which exceeds those asked for other financial institutions (Interview 4), some were seen as irrelevant (Interview 5). This contributed to the expansion of compliance departments. One exchange noted they *"were an organization of ten [before the implementation], and now [they] employ 70 people, of which compliance is with ten men and women"* (Interview 2).

In addition to the increased administrative burdens, the exchanges reported increased financial burdens due to substantial supervision costs. Under the supervision regime, registered exchanges were required to cover the costs of their own oversight. The Ministry of Finance expected that about 45 cryptocurrency exchanges would register, allowing the costs to be shared among them (Ministerie van Algemene Zaken, 2021). However, this estimate proved inaccurate. Only seven exchanges registered in time; by early 2020, only 15 had done so. As a result, the total supervision costs were divided among fewer firms, significantly increasing the fees per exchange. DNB noted, *"we try to have as few surprises as possible in such a [supervision] process. We provide as much information as possible in advance."* (Interview 1). Nonetheless, the exchanges experienced unexpectedly high costs, which was a complete surprise.

### Effects on the Sector

The implementation of AMLD5 brought significant changes to the Dutch cryptocurrency exchange sector. DNB acknowledged they could not assess the impact, as they lacked baseline knowledge of the sector before regulation. However, they expressed satisfaction with the number of registrations: *"21 is quite a lot of parties [that have registered themselves]. A year and a month ago there were 0. So I don't think that's a bad number."* (Interview 1). In reality, 43 exchanges were active when AMLD5 was introduced, and over 25% ceased operations following its announcement and implementation. Fewer than half of the original exchanges obtained registration; others who did not register moved abroad, changed their services, or shut down.

Still, registered exchanges recognize some benefits. They associate regulation with the professionalization of the market (Interview 4), improved transparency, and more standardized transaction monitoring (Interview 2). This enhances the understanding of money laundering risks (Interview 4).

Despite these advantages, the Dutch implementation also presents apparent drawbacks. All exchanges reported a decline in innovation, as smaller companies could not bear the supervision costs or meet requirements such as the separation of functions (Interview 5). This contradicts DNB's stated goal to support innovation, as they *"... also look closely at innovative parties and whether they have opportunities to gain access to the market."* (Interview 1). In practice, smaller innovative firms were excluded. Moreover, the competitive position of Dutch exchanges worsened. As one exchange noted, *"The new rules that we have to impose create a barrier which drives your Dutch customers abroad to parties that are purely focusing on the commerce and not concerned with their reputation."* (Interview 3).

The cryptocurrency exchanges compliant with AMLD5 performed low-risk transactions, meaning that the legislation does not contribute to countering money laundering. The benefits of the Dutch implementation of AMLD5 are thus meager. At the same time, the costs of supervision are excessive and are paid by those exchanges that have already implemented the legislation. Non-compliant cryptocurrency exchanges evaded the regime by moving abroad, giving them a competitive advantage over the registered cryptocurrency exchanges, as they do not have to pay the supervision costs.

## Discussion

This study explored the effects of the Dutch implementation of AMLD5, which has faced criticism in prior research. Scholars have noted its outdated nature at adoption (De Vido, 2020) and limited scope, excluding crypto-to-crypto exchanges (Dupuis & Gleason, 2020; Haffke et al., 2020; Wronka, 2022) and having a national focus (Kirillova et al., 2018). Baker and Shortland (2023) mentioned that legislation introduced in emerging sectors often becomes overly restrictive, counterproductive, or easily circumvented. The observations of this study support these concerns.

The first observation shows that registered Dutch exchanges are small-scale actors, with a low transaction volume and a limited number of executed transactions. Moreover, the registered exchanges primarily engage in low-risk transactions, while higher-risk activi-

ties remain prevalent among non-registered platforms outside the regulatory framework. As observed, these exchanges have already implemented measures and possibly averted high-risk clients. The low transaction volumes and risk aversion mean they do not face significant money laundering risks.

Secondly, no changes in the levels of high or severe risk transactions can be observed. The risk levels were already very low to start with. The exchanges had an intrinsic motivation to counter money laundering. Possibly because the exchanges were already doing what the legislation is now asking of the companies in this timeframe, no changes can be observed. Still, the fact that high and severe risk type transactions do occur means that the AML system is not waterproof, and high-risk transactions can still be executed. Our observations suggest that the first goal of the legislation, preventing financial institutions from being used in money laundering regimes, was not achieved.

Meanwhile, we have observed that cryptocurrency exchanges experience adverse effects attributable to the regulatory measures. They must pay enormous costs for their supervision, which led to companies closing down. The exchanges furthermore experience a high administrative burden. As Turner and Bainbridge (2018) state, the measures lead to a tick-box culture in which compliance is proven without showing the effectiveness of the measures taken and keeping the goal in mind, removing the before existing intrinsic motivation. Also, the supervision does not fit the dynamic, innovative cryptocurrency sector, leading to much dissatisfaction. The execution of the supervision, as does the general policy, seems to be copied and pasted from the traditional financial system. This could be an effect of the new role for DNB as Wang and Gao (2024) showed that regulators are likely to encounter challenges in resources, experience, and expertise to address the new system.

Lastly, we have observed diminished possibilities for innovation and competitiveness in the Dutch cryptocurrency sector. Compliance costs have increased substantially, leading to market exits and the relocation of some exchanges. Relocation leads to the advantage of not having to pay these costs. Moreover, it provides significant challenges to the second objective of AMLD5, which is to enable effective detection and prosecution of financial crime. The cryptocurrency sector being addressed by the regulation has shrunk, meaning that less influence can be exerted to address money laundering with cryptocurrencies.

**Limitations** Several limitations can be observed in this study. Due to the highly dynamic nature of the emerging cryptocurrency market, the composition of the players in the system can change quickly, partially influenced by changes in sanctioned entities, the occurrence of ransomware attacks, or the popularity of cryptocurrency in general. Therefore, this study reflects on the short-term effects of the Dutch implementation of AMLD5.

Moreover, the analysis focused on a small sample of Dutch exchanges, excluding global players. As a result, the findings cannot be generalized to larger or internationally operating platforms, whose regulatory responses and risk profiles may differ. While smaller firms may struggle with compliance costs, potentially leading to market consolidation and benefits of scale, the long-term structure of the sector remains uncertain. Notably, the Dutch exchanges studied did not exhibit significant risk levels at the outset, which may have influenced the limited observed impact.

Due to data limitations, only a subset of Dutch exchanges and one unregistered platform were included in the analysis, with some transactions unlabeled. Still, the data, sourced from Chainalysis, is well-suited for identifying transaction trends (Azevedo, 2021). Interviews were conducted with employees from companies affiliated with the VBNL, which may have introduced shared viewpoints. Still, participants held diverse roles, providing varied insights.

**Policy Implications** The variety in exchanges underscores the need for risk-based supervision. As Nazzari (2023) argues, it is impossible to apply the same AML regulation everywhere as actors, activities, and in this case, systems differ. Therefore, supervisory activities need to fit the dynamic cryptocurrency system, for example, by making use of the possibility of transaction analysis. Moreover, the administrative burdens observed can reduce companies' intrinsic motivation to counter money laundering. This can foster a tick-box culture, where demonstrating compliance outweighs the effectiveness of the measures, ultimately weakening the shared responsibility.

**Future research** Future research should examine global cryptocurrency exchanges with high transaction volumes, as these actors may pose greater money laundering risks and respond differently to regulation. Attention should also be given to the forthcoming effects of the MiCAR, particularly due to the EU-wide travel rule, which may influence regulatory outcomes across member states. In addition, further study is needed on decentralized exchanges and the crypto-to-crypto sector, which remain largely outside current regulatory scope but carry significant potential for illicit activity. Finally, broader and longitudinal research across EU member states is essential to gain a more comprehensive understanding of regulatory effectiveness over time.

## Conclusion

In conclusion, our analysis suggests that the Dutch implementation of AMLD5 imposed significant burdens on Dutch cryptocurrency exchanges that neither play a major role in the broader crypto ecosystem nor pose high money laundering risks. All unintended effects led to the deterioration of the Dutch virtual currency exchange sector. With MiCAR in place, future research should focus on the influence and impact of this new legislation and the effects of the AML/CFT package. Additionally, future research could explore what measures can be implemented to reduce the incidence of high-risk transactions, considering the inadequacy of transaction monitoring in addressing this issue.

## Appendix A Interview Protocol

This appendix provides the interview protocol that was adopted in the interviews with the virtual currency exchanges. The goal of the interview was to obtain new insights in the parties within the virtual currency exchange ecosystem and their perspectives on the introduction of the AMLD5. All questions ending in * were only asked to employees of the regulator the Dutch National Bank, and all questions marked with ** were only asked to employees of several virtual currency exchanges active in the Netherlands and member of the Dutch Bitcoin Companies in the Netherlands.

Virtual currency adoption

1. What is the potential of the use of virtual currencies in organized crime and what threat does this pose?
2. What do you come across in the flow of virtual currencies that may be prosecutable? Do you see certain patterns?

Legislation

3. What is your perspective on the introduction of the AMLD5?
4. Do you believe the AMLD5 implementation is effective?*
5. What impact do you observe following the implementation of the AMLD5:

   (a) In the landscape;
   (b) Within your organization.

Anti-money Laundering Responsibilities

5. How do you describe your role within the anti-money laundering chain?
6. What anti-money laundering measures did you adopt before the AMLD5 implementation?**
7. How did you have to adapt your daily operations after the AMLD5 implementation?**
8. What else could cryptocurrency companies do to combat money laundering?**
9. What are the biggest challenges in this?**
10. Does the AMLD5 implementation help you with your anti-money laundering responsibilities?**
11. What would you need from legislation to help you?**

Transaction Monitoring

12. How do you apply the following anti-money laundering principles:**

    (a) Know Your Customer
    (b) Customer Due Diligence

13. What tools do you use to monitor transactions?** If tools are adopted that analyse the blockchain:

    (a) How many steps do you look back to see if a coin is tainted? After how many steps is a coin clean?
    (b) Which heuristic is adopted in this tool?

14. When is a transaction marked as unusual? **

    (a) What do you do with this unusual transaction?
    (b) Is there some kind of feedback loop that comes back to you after you have reported the transaction?

Registration and Supervision

15. How did the registration process work?
16. How should you demonstrate compliance as a cryptocurrency exchange?**
17. How are you as a cryptocurrency exchange monitored by the supervisor? **
18. Are there opportunities for exchanges to operate without a registration in the Netherlands and what are the effects of this?
19. Which exchanges that did apply for registration have dropped out of the registration process? And why?*
20. The registry lists parent companies with their subsidiaries. Who is responsible for complying to the duty to notify and for ensuring the correct procedures are in place?*
21. How are virtual currency exchanges supervised?*
22. What tools are used to carry out supervision? If tools that look into the blockchain are used:*

    (a) How many steps do you look back to see if a coin is tainted? After how many steps is a coin clean?
    (b) Which heuristic is adopted in this research?

23. How do you expect the system to develop over the next 5 years based on:

    (a) Tools
    (b) Coins
    (c) Legislation

## Appendix B Codebook

**Table 4** Codebook - AML practices prior to AMLD5

| Pre AMLD5 | Respondents |
|---|---|
| Customer identification | 80% |
| Mitigating money laundering | 80% |
| Motivation for money laundering prevention | 80% |

**Table 5** Codebook - Efffects of Dutch implementation AMLD5

| Consequences of the AMLD5 | Respondents |
|---|---|
| Negative effects | 100% |
| Customer identification | 80% |
| Transaction monitoring | 80% |
| Mitigation of money laundering | 80% |
| Positive effects | 60% |
| Reporting duty | 60% |

**Table 6** Codebook - Bitcoin adoption in cybercrime

| Adoption | Respondents |
|---|---|
| Adoption of bitcoin | 60% |
| Traceability | 60% |
| Virtual currency risk | 60% |

**Table 7** Codebook - Contrasts traditional and new financial system

| Taditional vs new system | Respondents |
|---|---|
| Regular vs virtual market | 80% |
| New sector | 60% |
| Old rules on new system | 60% |

**Table 8** Codebook - Registration and supervision

| Regulation and supervision | Respondents |
|---|---|
| Process of registration | 100% |
| Process of supervision | 100% |
| Supervision costs | 80% |
| Role supervisor | 40% |

**Table 9** Codebook - future trends in illicit Bitcoin adoption

| Future outlook | Respondents |
|---|---|
| Legislation | 100% |
| Bitcoin developments | 80% |
| Changing tools | 80% |
| Focus on new coins | 80% |
| Gain experience | 40% |

This appendix provides the codebook adopted for analysing the interviews of which the results were provided in Section "Business Impact". The interview protocol that was used can be found in Appendix A. Table 4 contains the codes inferred about what cryptocurrency exchanges did before AMLD5. All respondents of virtual currency exchanges stressed their motivation and work on countering money laundering before the introduction of the legislation. Table 5 contains the codes pertaining the effects of the implementation of AMLD5. All respondents acknowledge the negative effects.

Table 6 contains codes about the adoption of Bitcoin in cybercrime and opportunities of this. The respondents sometimes saw bitcoin being adopted in cybercrime and saw some risks. However, they also noticed the opportunities of tracing to counter this.

Table 7 shows the codes used to describe the difference between the traditional and new financial system. All virtual currency exchanges stated the difference between the traditional an virtual currency system, most of them also mentioned how the new rules were merely copy-pasted.

The codes in Table 8 were used to identify statements on the registration and supervision process. The respondents had a lot to state about the process of registration and supervision, also the supervision costs were a topic of concern.

Table 9 provides the codes that contained information about possible future developments. All respondents mention that new legislation can be promising also they expect things to change in developments within the bitcoin system which might frustrate these promises, new tools for for example law enforcement could make up for this fact.

## Appendix C Absolute Values Per Risk Level

Section "Changes in Transaction Patterns" explored the relative composition of transaction patterns of active registered cryptocurrency exchanges. It was seen that the relative transaction portfolio was not altered due to AMLD5. Table 10 shows the absolute values during the period pre-implementation, May 20$^{th}$ 2018 till May 20$^{th}$ 2022, and post-implementation, May 20$^{th}$ 2020 till May 20$^{th}$ 2022. It can be observed that before and after the implementation of the regulation transactions were executed with a high or severe risk level.

**Table 10** Absolute BTC values per risk level

| Risk | Low | Medium | High | Severe | Unknown |
|---|---|---|---|---|---|
| Pre implementation | 402,548,316 | 1,781,571 | 9,340,466 | 32072 | 3,255,784,311 |
| Post implementation | 608,061,466 | 8,335,185 | 19,066,597 | 57774 | 5,498,329,448 |

**Author Contributions** All authors contributed to the study conception and design. Data collection and analysis were performed by C.J. Volten, The first draft was written by C.J. Volten. All authors commented on previous versions of the manuscript and rewrote sections of the manuscript. All authors read and approved the final manuscript.

**Funding** The work in this study has been partially supported by the Dutch Ministry of Finance, under grant M75B36.

**Availability of data and material** The data will not be deposited.

## Declarations

**Conflict of Interest** The author's declare no conflict of interest.

**Ethics approval and consent to participate** The interviewees provided informed consent for the interviews according to the institutions' IRB guidelines. All other parts of this work did not require IRB approval.

**Consent for publication** The authors declare consent for publication.



## References

Alekseenko, A. P. (2022). Ban of cryptocurrencies in china and judicial practice of chinese courts. *China and WTO Review, 8*(2), 361–384. https://doi.org/10.14330/cwr.2022.8.2.06

Alkaya, M., & van der Linde, R. (2019). Gewijzigde motie van de leden alkaya en van der linde over de monitoring van de uitwerking van de implementatiewet anti-witwasrichtlijn op kleine ondernemingen.

Amuso, V., & Baron, I. Z. (2023). Disruptive technology and regulatory conundrums: The emerging governance of virtual currencies. *Governance*. https://doi.org/10.1111/gove.12783

Azevedo, M. A. (2021). Crypto boom continues as chainalysis raises [CDATA[100m, doubles valuation to over ]]$100m, doublesvaluationtoover$2b. [Tech crunch]. Retrieved October 26, 2023, from https://techcrunch.com/2021/03/26/chainalysis-raises-100m-doubles-valuation-to-over-2b/

Baker, T., & Shortland, A. (2023). The government behind insurance governance: Lessons for ransomware. *Regulation & Governance, 17*(4), 1000–1020. https://doi.org/10.1111/rego.12505

Ballegeer, D., & Verhagen, L. (2023). Dit is de man die bij DNB toezicht houdt op de cryptomarkt: 'over twee jaar herinneren wij ons wie er over de schreef zijn gegaan'. *de Volkskrant*.

Bello, A. U., & Harvey, J. (2017). From a risk-based to an uncertainty-based approach to anti-money laundering compliance. *Security Journal, 30*, 24–38. https://doi.org/10.1057/s41284-016-0002-0

Bernard, H. R., Ryan, G. W., & Wutich, A. (2016). *Analyzing qualitative data: Systematic approaches* (2nd ed.). Los Angeles: SAGE.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brooksbank, R. (1991). Defining the small business: a new classification of company size. *Entrepreneurship & Regional Development, 3*(1), 17–31. https://doi.org/10.1080/08985629100000002

Chaikin, D. (2009). How effective are suspicious transaction reporting systems? *Journal of Money Laundering Control, 12*(3), 238–253. https://doi.org/10.1108/13685200910973628

Chainalysis. (2020). Cryptocurrency typologies guide: Who's who on the blockchains? Retrieved July 21, 2025, from https://www.chainalysis.com/blog/cryptocurrency-typologies-guide-2020/

Crawford, J., & Guan, Y. (2020). Knowing your bitcoin customer: Money laundering in the bitcoin economy. *In 2020 13th international conference on systematic approaches to digital forensic engineering (SADFE)* (pp. 38–45). 2020 13th international conference on systematic approaches to digital forensic engineering (SADFE). https://doi.org/10.1109/SADFE51007.2020.00013

De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review, 3*(2). https://doi.org/10.14763/2014.2.286

De Vido, S. (2020). Virtual currencies: New challenges to the right to privacy? an assessment under the v AML directive and the GDPR. *Global Jurist, 20*(2). https://doi.org/10.1515/gj-2019-0045

De Wit, J. (2007). A risk-based approach to AML: A controversy between financial institutions and regulators. *Journal of Financial Regulation and Compliance, 15*(2), 156–165. https://doi.org/10.1108/13581980710744048

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance). (2015, May 20). Retrieved October 26, 2023, from http://data.europa.eu/eli/dir/2015/849/oj/eng

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance). (2018, May 30). Retrieved October 26, 2023, from http://data.europa.eu/eli/dir/2018/843/oj/eng

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime, 28*(1), 60–74. https://doi.org/10.1108/JFC-06-2020-0113

European Commission. (n.d.). Anti-money laundering and countering the financing of terrorism at EU level [Finance european commission]. Retrieved August 2, 2023, from https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en

European Commission. (2021). Impact assessment accompanying the anti-money laundering package.

FATF. (n.d.). History of the FATF. Retrieved January 31, 2025, from https://www.fatfgafi.org/en/the-fatf/history-of-the-fatf.html

FATF. (2014). Virtual currencies - key definitions and potential AML/CFT risks. Retrieved from https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance,* 56. https://doi.org/10.1016/j.ribaf.2021.101387

Garretsen. (2022). Echtpaar verdacht van witwassen 120.000 bitcoin: wat is witwassen? [AllesOverCrypto]. Retrieved April 12, 2024, from https://allesovercrypto.nl/blog/echtpaar-verdacht-witwassen-120000-bitcoin-witwassen

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

Harvey, J. (2008). Just how effective is money laundering legislation? *Security Journal, 21*, 189–211. https://doi.org/10.1057/palgrave.sj.8350054

Interpol (n.d.). Money laundering. Retrieved August 3, 2023, from https://www.interpol.int/en/Crimes/Financial-crime/Money-laundering

Kepli, M.Y.B.Z., & Zulhuda, S. (2019). Cryptocurrencies and anti-money laundering laws: The need for an integrated approach. In U.A. Oseni, M.K. Hassan, and R. Hassan (Eds.), Emerging issues in islamic finance law and practice in malaysia (pp. 247–263). https://doi.org/10.1108/978-1-78973-545-120191020

Kirillova, E. A., Pavlyuk, A. V., Mikhaylova, I. A., Zulfugarzade, T. E., & Zenin, S. S. (2018). Bitcoin, lifecoin, namecoin: The legal nature of virtual currency. *Journal of Advanced Research in Law and Economics, 9*(1), 119–126. https://journals.aserspublishing.eu/jarle/article/view/2294

Kruisbergen, E., Leukfeldt, E., Kleemans, E., & Roks, R. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice, 42*(5), 569–581. https://doi.org/10.1080/0735648X.2019.1692420

Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime, 30*(4), 1036–1054. https://doi.org/10.1108/JFC-07-2022-0161

Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice, 49*, 579–631. https://doi.org/10.1086/708047

Liang, J., Li, L., Chen, W., & Zeng, D. (2019). Targeted addresses identification for bitcoin with network representation learning. *In 2019 IEEE international conference on intelligence and security informatics (ISI)* (pp. 158–160). 2019 IEEE international conference on intelligence and security informatics (ISI). https://doi.org/10.1109/ISI.2019.8823249

Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Towards sustainable cryptocurrency: risk mitigations from a perspective of national security. *Journal of Security and Sustainability Issues, 9*(2), 374–389. https://doi.org/10.9770/jssi.2019.9.2(2)

McDonald, N., Schoenebeck, S., & Forte, A. (2019). Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction, 3*, 1–23. https://doi.org/10.1145/3359174

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. *In Proceedings of the 2013 conference on internet measurement conference* (pp. 127–140). IMC'13: Internet measurement conference. https://doi.org/10.1145/2504730.2504747

Ministerie van Algemene Zaken. (2021, September 23). 1e deelbesluit Wob-verzoek aanbevelingen en regelgeving cryptodienstverlening - Wob-verzoek - Rijksoverheid.nl. Retrieved July 31, 2023, from https://www.rijksoverheid.nl/documenten/wob-verzoeken/2021/09/23/1e-deelbesluit-wob-verzoek-aanbevelingen-en-regelgevingcryptodienstverlening

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. *In 2013 APWG eCrime researchers summit* (pp. 1–14). 2013 eCrime researchers summit (eCRS). https://doi.org/10.1109/eCRS.2013.6805780

Möser, M., & Narayanan, A. (2019). Effective cryptocurrency regulation through blacklisting

Murphy, C. (2024). Proposal for a regulation on information accompanying transfers of funds and certain crypto-assets (recast). [Legislative train schedule]. Retrieved August 1, 2024, from https://www.europarl.europa.eu/legislativetrain/theme-an-economy-that-works-for-people/file-revision-of-the-regulation-ontransfers-of-funds

Nazzari, M. (2023). Lost in the maze: Disentangling the behavioral variety of money laundering. *European Journal on Criminal Policy and Research, 30*, 379–397. https://doi.org/10.1007/s10610-023-09572-8

Parasol, M. (2022). Avoiding the wholesale de-banking of cryptocurrency exchanges in australia. *University of New South Wales Law Journal, 45*(4). https://doi.org/10.53637/WJQH3341

Pol, R. F. (2018). Anti-money laundering effectiveness: assessing outcomes or ticking boxes? *Journal of Money Laundering Control, 21*(2), 215–230. https://doi.org/10.1108/JMLC-07-2017-0029

Pol, R. F. (2020a). Anti-money laundering: The world's least effective policy experiment? together, we can fix it. *Policy Design and Practice, 3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Pol, R. F. (2020b). Response to money laundering scandal: evidence-informed or perception-driven? *Journal of Money Laundering Control, 23*(1), 103–121. https://doi.org/10.1108/JMLC-01-2019-0007

Ranshous, S., Joslyn, C. A., Kreyling, S., Nowak, K., Samatova, N. F., West, C.L., & Winters, S. (2017). Exchange pattern mining in the bitcoin transaction directed hypergraph. In M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, . . . M. Jakobsson (Eds.), Financial cryptography and data security (Vol. 10323, pp. 248–263). Cham: Springer International Publishing. Retrieved July 21, 2023, from http://link.springer.com/10.1007/978-3-319-70278-0_16

Regeling bekostiging financieel toezicht eenmalige handelingen. (2021). Last Modified: 2024-07-18. Retrieved February 7, 2025, from https://wetten.overheid.nl/BWBR0041647/2021-05-01#Paragraaf3

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. (2023). Retrieved February 12, 2025, from https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

Reynolds, P., & Irwin, A. S. (2017). Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control, 20*(2), 172–189. https://doi.org/10.1108/JMLC-07-2016-0027

Soudijn, M. (2019). Using police reports to monitor money laundering developments. continuity and change in 12 years of dutch money laundering crime pattern analyses. *European Journal on Criminal Policy and Research, 25*, 83–97. https://doi.org/10.1007/s10610-018-9379-0

Stokes, R. (2012). Virtual money laundering: the case of bitcoin and the linden dollar. *Information & Communications Technology Law, 21*(3), 221–236. https://doi.org/10.1080/13600834.2012.744225

Tsuchiya, Y., & Hiramoto, N. (2021). How cryptocurrency is laundered: Case study of coincheck hacking incident. *Forensic Science International: Reports, 4*, Article 100241. https://doi.org/10.1016/j.fsir.2021.100241

Turner, S., & Bainbridge, J. (2018). An anti-money laundering timeline and the relentless regulatory response. *The Journal of Criminal Law, 82*(3), 215–231. https://doi.org/10.1177/0022018318773205

United States Attorney's Office. (2023). FBI disrupts virtual currency exchanges used to facilitate criminal activity [United states attorney's office]. Retrieved July 31, 2023, from https://www.justice.gov/usao-edmi/pr/fbi-disrupts-virtual-currencyexchanges-used-facilitate-criminal-activity

Usman Kemal, M. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control, 17*(4), 416–427. https://doi.org/10.1108/JMLC-06-2013-0022
van Spengen, A. (2021, April 7). ECLI:NL:RBROT:2021:2968
van Spengen, A., Boonstra, N., & van Velzen, B. . (2023, October 4). ECLI:NL:RBROT:2023:9157
Van Wegberg, R., Oerlemans, J.-J., & Van Deventer, O. (2018). Bitcoin money laundering: mixed results? an explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime, 25*(2), 419–435. https://doi.org/10.1108/JFC-11-2016-0067
Wang, H., & Gao, S. (2024). The future of the international financial system: The emerging network and its impact on regulation. *Regulation & Governance, 18*(1), 288–306. https://doi.org/10.1111/rego.12520
Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). (2023). Last Modified: 2023-10-26. Retrieved October 26, 2023, from https://wetten.overheid.nl/BWBR0024282/2022-11-01
Wilkes, N., Anderson, V. R., Johnson, C. L., & Bedell, L. M. (2022). Mixed methods research in criminology and criminal justice: a systematic review. *American Journal of Criminal Justice, 47*, 526–546. https://doi.org/10.1007/s12103-020-09593-7
Wronka, C. (2022). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control, 25*(1), 79–94. https://doi.org/10.1108/JMLC-02-2021-0017