

# Sharing Economy for Tackling Crypto-Laundering: The Europol Associated ‘Global Conference on Criminal Finances and Cryptocurrencies’

Ethem Ilbiz <sup>1,\*</sup> and Christian Kaunert <sup>1,2</sup>

<sup>1</sup> Faculty of Life Sciences and Education, University of South Wales, Pontypridd CF37 1DL, UK; christian.kaunert@dcu.ie

<sup>2</sup> School of Law and Government, Dublin City University, Dublin 9, Ireland

\* Correspondence: ethem.ilbiz@southwales.ac.uk; Tel.: +44-(0)3455760101

**Abstract:** This article examines the compatibility of the Global Conference on Criminal Finances and Cryptocurrencies with a sharing economy model. The analysis is based on the claims presented in Europol documents and public statements of Europol executives that this initiative serves as a platform for knowledge exchange and building professional networks between public and private actors to tackle crypto-laundering. The article investigates the validity of these statements with the most prominent sharing economy concepts: low barrier accessibility, transaction cost and trust-building. The article employs each sharing economy concept on two beneficiaries of the platform—law enforcement agencies (LEAs) and non-governmental organizations—while scaling the platform’s sharing economy level. Based on Europol documents, an expert interview and participant observation of the 5th Global Cryptocurrency Conference, the article’s core argument is that these cryptocurrency conferences can be categorized as a ‘partial’ sharing economy platform. They reduce the transaction cost for public and private actors to share knowledge about the latest trends and threats about crypto-laundering and reduce transaction costs for networking. However, co-founders should consider integrating robust trust-building mechanisms that allow low barrier entry to the conference, which will facilitate more inclusive and optimized public-private partnerships (P3).

**Keywords:** sharing economy; crypto-laundering; Europol; public-private partnerships

**Citation:** Ilbiz, E.; Kaunert, C. Sharing Economy for Tackling Crypto-Laundering: The Europol Associated ‘Global Conference on Criminal Finances and Cryptocurrencies’. *Sustainability* **2022**, *14*, 6618. <https://doi.org/10.3390/su14116618>

Academic Editors: Vytautas Snieška, Vaida Pilinkienė, Daiva Dumciuvienė

Received: 27 April 2022

Accepted: 27 May 2022

Published: 28 May 2022

**Publisher’s Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Digitalization in socio-economic life has unexpected consequences on crime patterns. The internet as an international medium provides easy accessibility and anonymity for offenders, and many governments find themselves lacking resources to cope with the new security challenges happening in cyberspace. Therefore, in a changing cybersecurity ecosystem, governments are pushed to relinquish a certain level of their monopoly in public security and seek the support of non-governmental actors to exchange resources [1].

The paradigm shift in cybersecurity has also introduced new forms of public governance in which rigid organizational structures are replaced with network or informal governance [2]. The efficient use of public and non-governmental resources have become a priority to maintain public service delivery [3]. Governments can no longer instruct and monitor cyberspace with traditional and formal governance models [4]. On the contrary, the responsibility of governments turns into a coordinator, stimulator or partner in complex and fragmented cybersecurity networks where most of the tasks are delegated to the non-governmental actors [5].

The invention of cryptocurrencies in this context has had a disruptive impact on the global financial system and has added a new dimension to the money transaction pro-

cess. Cryptocurrencies are minted by non-governmental actors and are transferred through a decentralized online network without any intermediary like banks. Moreover, the use of encryption for value transactions has enabled a financial obfuscation for its users to hide their real identities. As a result, cryptocurrencies have become a new tool for crime groups to launder illegally obtained funds, often called crypto-laundering [6], and avoid law enforcement agency (LEA) investigations.

As tracing cryptocurrency transactions becomes more complicated for LEAs due to a lack of human and technical resources [7], new private sector initiatives emerge to offer LEAs cryptocurrency tracing and intelligence analysis [8,9]. Interconnecting private sector actors with LEAs become vital to efficiently use scarce public and private sector resources to tackle crypto-laundering and build strong public–private partnerships (P3).

In this respect, Europol is the first LEA to declare that they have adapted ‘sharing economy’ as a new P3 model to tackle cyber threats [10,11]. In broad terms, a sharing economy is the exchange of under-utilized or scarce resources with others in an online platform in return for money or altruistic purposes [12–15]. According to the executive director of Europol, Catherine De Bolle, the European policing agency is on the way to becoming an innovation hub for policing solutions with different online platforms [16]. In these platforms, Europol, along with its other founding partners, intermediate between LEAs and non-government actors to tackle cybercrimes [17]. One of these platforms that aims to enhance P3 are cryptocurrency conferences organized by Europol, Interpol and the Basel Institute of Governance. According to Europol documents, the platform aims to be a gathering site where public and private actors share their expertise and build networks for robust partnerships [18–20].

Although a sharing economy is a popular topic in many disciplines such as business, finance, marketing and law, only a handful of studies have examined a sharing economy in public governance. In this limited literature, opportunities and challenges associated with sharing economy for the public sector [21] and the different roles the public sector may play within sharing economy platforms have been systematically conceptualized [22]. Nevertheless, in this newly developing academic field, very little is known about any adaptation of online platforms in public service delivery. In such an example, we know little on to what extent online sharing economy platforms governed by public administrations comply with this theoretical concept.

Based on the knowledge gap in the literature, this article takes public statements of Europol executives and publicly available Europol documents as evidence that Europol adapts the sharing economy platform principles in cryptocurrency events for knowledge exchange and building networks [10,16–19]. Relying on these official statements, the core objective of this article is to explore ‘to what extent does the Europol associated ‘Global Conference on Cryptocurrencies’ comply with sharing economy principles to facilitate knowledge sharing and professional network building in the crypto-laundering struggle?’

The article qualitatively explores the sharing economy scale of the platform triangulating the knowledge acquired from a semi-structured elite interview, Europol official documents and the structured observation of the 5th Global Conference on Criminal Finances Cryptocurrencies held on 07 December 2021. This article contributes to both research and practices twofold. First, it is the first empirical study where a P3 initiative in crypto-laundering has been examined through the sharing economy conceptual framework. This article may inspire other empirical works to use the same analytical framework for other P3 initiatives, not only crypto-laundering, but also other public administration fields. Second, the study’s empirical findings can help both Europol and other LEAs develop their current P3 initiatives according to sharing economy principles.

The following section will describe the methodological approach employed in the article. The subsequent section will introduce the sharing economy theoretical framework and its variables. In the discussion section, brief information regarding crypto-laundering and the background of Europol associated cryptocurrency platform will be

provided. In addition to both, the platform's compatibility will be debated through the sharing economy concepts. The concluding section will summarize the research findings and propose new research ideas and policy recommendations for the public and private actors involved in these initiatives.

## 2. Methodology

The research data obtained for this study is gleaned from three data sources. These are a semi-structured interview conducted with an expert who was a former LEA agent and currently working on cryptocurrency industry, publicly available Europol documents, and structured participation observation of the 5th Global Conference on Criminal Finances and Cryptocurrency held on 7 December 2021. The conference is one of the largest P3 events in crypto-laundering (with around 2000 experts participating in the open event in 2021) [20]. It is the most significant gathering that shows sharing dynamics in the cryptocurrency community concerned with the dark side of digital currencies.

In this article, three sharing economy concepts, namely, 'low barrier accessibility', 'transaction cost' and 'trust-building', were employed while structuring the empirical investigation. These are the most prominent sharing economy concepts in the literature, and they roughly appear with similar names. In the section on 'low barrier accessibility', the article discusses the participation process to the platform [23,24]. The 'transaction cost' variable examines whether the platform reduces searching, contacting, and contracting costs for the platform community [25–27]. In the context of 'trust-building', the article inspects the existence of trust-building mechanisms such as regulation, vetting and rating [28–30].

One researcher from the research team observed the conference session as a covert observer [31], and observations were noted according to pre-defined sharing economy variables built during the literature review stage. The observation also solely focused on the formal space of the event rather than informal networking activities during the conference, which are not possible to observe. Several measurable metrics were developed to strengthen the objectivity of the observations, such as the existence of trust-building mechanisms (vetting, regulation, rating), the promotion of private sector services (showcasing product and services) and low barrier accessibility (invitation process).

During the data collection stage, semi-structured interview requests were also sent to event organizers such as Europol, Interpol, the Basel Institute on Governance and private companies providing blockchain analytics to LEAs. However, only one of the research participant candidates responded positively to our invitation. The interviewee is highly knowledgeable about conferences because of his former public and recent private-sector career in the cryptocurrency industry. The remaining candidates refrained from participating for confidentiality reasons, or were unresponsive to the interview requests. Being able to do only one elite interview for this study is an unavoidable limitation of this article.

To scale the compatibility of the cryptocurrency initiative according to sharing economy platform principles, three parameters, 'fully', 'partial' and 'no equivalent', have been identified in this article. Full compliance means conforming to all three sharing economy principles. Partial compliance corresponds to fulfilling at least one but no more than two criteria. The no equivalent implies an absence of sharing economy principles.

## 3. Sharing Economy for Public–Private Partnerships

Sharing is an altruistic behaviour aimed at the mutual use of resources or space [32,33] and at benefiting and supporting one another [12,34]. Sharing provides an alternative solution to ownership by offering temporary access to a good or service [35]. In recent years, sharing has shown a remarkable transition. Globalization, economic crises, environmental concerns and exponential developments in digital technologies have changed the prominent patterns in customer behaviour [34]. The new economic ex-

change focuses on sharing resources or temporary access through digital platforms [36]. As a result of this transition, a new generation of sharing economy was born that has had a disruptive impact on many sectors, including transportation (Uber, Lyft), accommodation (Airbnb) and freelancer services (Upwork, Fiverr) [37]. The new digitalized sharing economy model has proven that many services could be acquired without ownership [36,38–40]. The rise of sharing economy platforms has also initiated a discussion of whether similar platforms can solve environmental and economic sustainability [21,41,42].

In the existing literature, there are a plethora of terms and definitions referred to as the sharing economy [34,43–45], and these descriptive attempts generally overlap with each other [21,27]. Despite various definitions, the sharing economy can simply be identified as sharing under-utilized or scarce resources with others through an online platform for money and non-material benefits [12–15]. The success of a sharing economy also depends on the existence of a community concerned with sustainability and the use of resources in a mutual and altruistic way [25,46]. Being part of the community is one of the important motivational factors for sharing [46]. It creates a synergy and enables community members to access products without ownership that saves their time and money [13]. As the sharing economy has the potential to facilitate the use of under-utilized or scarce resources, it can be a sustainable solution for public sector actors to fill their resource gap [47]. Whether the public or private sector utilizes it, the success of this model relies on three major factors, including low barrier accessibility, reduction of transaction cost and the existence of trust-building mechanisms.

### *3.1. Low Barrier Accessibility*

One of the important advantages of the sharing economy is the fact that the technological infrastructure provided by the online platform enables a low barrier entry for its users to share their resources [24]. Anyone with an internet connection can access these platforms after a simple sign-up process and interact with other platform users. The online platform, thus, eases network participation [21] and facilitates underutilized resource sharing [48].

The easy access provided by sharing economy allows the participation of new and alternative players in the market [49]. An increasing number of players in online platforms create a competition that positively impacts customers to acquire the best value product and services [50].

The online interaction between peers also removes geographical barriers [12,14]. The members of the online platform can maintain communication and resource exchange from distant locations. By bringing together service providers and customers in one marketplace, the platforms ease the accessibility to a more extensive online network.

### *3.2. Transaction Cost*

The second important feature of a sharing economy is that it reduces the transaction cost for platform members. The transaction cost is often regarded as all costs for searching, contacting, and contracting with the right partner [33,51,52]. The online platforms have matchmaking mechanisms to exchange goods and services efficiently [53]. The sharing economy platforms collect and aggregate massive metadata [54]. When users need to reach a particular product or service, these matchmaking mechanisms (integrated with big data) assist users in finding what they are looking for quickly [55]. As online sharing platforms are designed for low barrier entry and have matchmaking mechanisms, they reduce the transaction cost for platform members when seeking the right partner [53]. Peers using online platforms do not need to search for their ideal partner in different places. They can detect the right partner with the help of 'keyword algorithms' [56].

The technological infrastructure utilized by platforms eases listing and distribution costs [50] and offers low-cost alternatives to customers [49,53]. The price gap between al-

ternative products creates a consumer surplus, the difference between the highest amount the customer is willing to pay and the actual amount paid [55]. As online sharing economy platforms facilitate the reduction of transaction costs, they increase consumer surplus and customer satisfaction, making them more popular while seeking service and products [57,58].

### 3.3. Building Trust

In online platforms, trusting a peer is not easy because of the absence of physical contact and uncertainties about who is behind the online profile [59,60]. As traditional trust mechanisms are not responding to eliminate these uncertainties, sharing economy platforms developed new trust-building mechanisms such as vetting, regulation and rating [61].

The first mechanism, vetting, aims to verify the real identity of platform members and to check their background [62]. In this context, online platforms collect personal data from participants such as their IDs, driving licenses, criminal records, financial information from banks or credit cards, social media footprint collected from Facebook or Google, or a selfie taken by mobile applications. In addition to the data identifying platform members, some of the sharing economy platforms require the qualifications of suppliers because customer trust is also associated with increasing service quality [63]. Therefore, sharing economy platforms prefer to work with high standard suppliers to attract more customers. Some platforms also occasionally test the qualifications of their service providers to keep service quality higher [64].

The second trust-building mechanism in sharing economy platforms is regulation. Regulation is often described as the management of complex systems using rules [65]. The main objective of regulation in the market is to create a 'level playing field' where all market players know how the game should be played [65]. The regulation aims to correct market failure, which are inefficiencies in the market regarding the distribution of goods and services associated with the pursuit of individual interest [66]. Market failures like monopolies undermining competition or lack of correct information while buying and selling the product can be corrected by regulation [55]. In this regard, as an online marketplace, online platforms regulate their members' interaction to facilitate trust between platform members [67]. In case of a violation of rules, the platform intervenes the disagreement based on its regulation, and, if necessary, dismisses the platform member violating platform regulation.

The third mechanism for building trust is the rating that accumulates and measures platform users' reputation [30]. There is no efficient mechanism for suppliers to pay for their poor service in many traditional industries. For instance, for efficient food safety in a restaurant, each restaurant should be inspected by a full-time inspector [55]. Classical monitoring procedures are generally time-consuming, and resolution takes longer [65]. Therefore, sharing economy platforms developed a reputation system, where customers and suppliers rate each other [29]. When potential customer's access sharing economy platforms, they find evaluations and criticisms of previous customers who already shared their experiences [68,69]. These ratings influence customer decisions distinguishing high- and poor-quality service suppliers [70]. Ratings can also favour some suppliers because a higher score can be capitalized by better prices [71,72]. As a result, rating incentivizes suppliers to provide higher quality services [73]. Even though there are many problems associated with ratings, such as underreporting, a reluctance to rate [74], biases with earlier ratings [75] or the manipulation of ratings [76], only a tiny reliable group of customers comments sometimes be enough to impact on undermining the reputation of the supplier [76].

## 4. Empirical Analysis of 'Global Conference on Criminal Finances and Cryptocurrencies'

Based on a sharing economy conceptual framework, in the following subsections the ‘Global Conference on Criminal Finances and Cryptocurrencies’ will be discussed according to the three major sharing economy concepts: ‘low barrier accessibility’, ‘transaction costs’ and ‘trust building’. In each concept, the platform’s compatibility with sharing economy principles will be explored through the lenses of two beneficiaries, including LEAs and private companies. However, prior to the empirical discussion, the concept of crypto-laundering will be provided in order to explain why sharing knowledge and building networks are important between public and private actors to tackle crypto-laundering. This section will be followed by how this platform has initiated with Europol and its partners.

#### 4.1. Crypto-Laundering

Money laundering is often referred to as a process of disguising the origin of illegally obtained funds and integrating them into the mainstream financial system to appear as a legitimate source of income [77]. It is considered one of the biggest threats to a well-established economy and public safety [78]. Money laundering has three stages, namely, placement, layering and integration. Placement involves introducing illicitly acquired funds into the financial system [79]. In the layering stage, illicit funds previously deposited into the financial system are obfuscated with complex transactions to frustrate auditing traceability [80,81]. The integration stage is channelling the ‘washed’ money that appears legitimate to mainstream investments [82].

Since the fintech industry introduced new payment technologies that enable complex money transactions, money laundering has been identified as ‘cyber laundering’ [83]. If cryptocurrencies are used in the money laundering process, it is named ‘crypto-laundering’ [6] or ‘virtual money laundering’ [84]. According to Financial Action Task Force (FATF), cryptocurrencies are digital representations of value issued by the non-public authority and do not have legal tender status. They are digitally traded and function as a medium of exchange’, ‘a unit of account’ and ‘a store of value’ [85]. These currencies, however, differ from other virtual currencies like bonus points or loyalty rewards because they are minted and transferred in a peer to peer (P2P) network without the supervision of a central authority [86].

The first cryptocurrency Bitcoin was introduced by a pseudonym inventor, Satoshi Nakamoto, following the 2008 financial crisis [87]. Since its launch, Bitcoin has had a disruptive effect on the global financial system and proved that digital asset transactions could be possible without a central authority and by hiding user identity. The protocol of Bitcoin is based on a ‘distributed ledger system’ or also known as ‘blockchain’. It is run by a decentralized network of computers (nodes). Their role is validating, recording, storing, and broadcasting the transactions in an open-access ledger [88].

In a blockchain, a digital currency transaction is made through digital wallets. Without disclosing personal identifying information, these wallets can be obtained from different online service providers. Each wallet is associated with public and private keys. Public key works like a bank account to which a cryptocurrency transaction is addressed. The sender uses the private key to encrypt the transaction, whereas the receiver uses it for decryption [89]. When cryptocurrencies are transferred from one wallet to another, these transactions are checked by nodes on a larger blockchain network to prevent double-spending. Nodes record the validated transactions between two wallets on a blockchain ledger as random numbers and letters [90]. So, transaction records cannot be associated with the real identity of the sender and the recipient by outsiders through this metadata [91]. Additionally, once nodes confirm a transaction, it is irreversible [6,79]. Nodes also aggregate the validated transaction within a data block, and each block is chained to each with reference to the previous one [88,92]. Any attempt to change these records necessitate a substantial computational power which is very unlikely to happen in the current computational standards of the world [93]. Therefore, cryptocurrencies

such as Bitcoin or Ethereum with a strong network of nodes are also immune from hacking and infiltration.

Tracing back illegitimate resource of cryptocurrency becomes more challenging if criminals use ‘mixing’ and ‘tumbler’ services. Mixing and tumbler services put another obfuscation layer to cryptocurrency transactions [8]. These services pool crypto assets from many users and randomly send mixed coins to the recipient wallet addresses after deducting a transaction fee [94]. The difference between the two services is that while tumblers distribute the same kind of cryptocurrency to the client’s wallet, mixers send a different cryptocurrency, making blockchain analysis more complicated [95]. Some mixing and tumbler services use random delay times and randomized fees to make correlation analysis more difficult for investigators [89].

Privacy coins are another way to obfuscate cryptocurrency transactions. These cryptocurrencies are released to the market as privacy by default to provide anonymity to their users. Most popular privacy coins such as Zcash and Monero use shielded pools or one-time public keys that hides details of transactions which are difficult to trace by LEAs [8,96,97]. The anonymity feature of Zcash, for instance, has been praised by Edward Snowden, a prominent privacy advocate and a former National Security Agency (NSA) employee who revealed global surveillance programs of the US [98].

Money laundering with cryptocurrencies has similar stages with fiat currencies. At the placement stage, cryptocurrencies are purchased from unregulated cryptocurrency exchanges, ATMs or online-platforms where peers exchange cryptocurrencies [8]. Crime groups also recruit money mules to buy cryptocurrencies on their behalf [99]. During the layering stage, the source of cryptocurrencies is obfuscated with mixing and tumbler services, or they are converted to privacy coins to make them untraceable [100]. The initial coin offerings (ICO) are another method exploited in the layering stage in which dirty cryptocurrencies are exchanged with newly minted coins [101,102]. The use of non-fungible tokens (NFTs) in layering is another technique of recent times that there is increasing suspicion of their role in crypto-laundering. These tokens are collectables that represents a digital art piece in the blockchain. Perpetrators buy their self-created NFT through an anonymous account, declaring that they have sold their piece to a higher bid. Their unpredictable valuation makes them a perfect tool to clean illegitimate proceeds [103]. In the integration stage, the cleansed cryptocurrencies are cashed out by money mules in a regulated cryptocurrency exchange offering cryptocurrency exchange with fiat currencies [104].

The problems associated with using cryptocurrencies in money laundering led to the emergence of blockchain tracing and intelligence companies as part of the reg-tech industry [8,9]. These companies use clustering techniques to examine complex cryptocurrency transactions and map money laundering patterns in blockchain ledgers. They flag unusual transactions and use visualization tools to simplify statistical data to help investigators follow the source and destination of suspicious transactions of illegal funding [105]. They also correlate these transactions with wallet addresses that cryptocurrency exchanges know their owners [7]. Based on their knowledge of blockchain analysis and sophisticated software analysis, these companies became new outsourcing partners of LEAs and revenue services in many countries struggling to tackle crypto-laundering [97,106]. Engaging these private sector actors with LEAs became vital to tackle the global crypto-laundering threat. Europol is one of the intermediaries vocal to resource sharing and supports a strong P3 in this context.

#### *4.2. Europol, Crypto-Laundering and Global Conference on Criminal Finances and Cryptocurrencies*

Even though the anti-money laundering efforts in the EU goes back to the early 1990s [107,108], the threat posed by cryptocurrency to use in money laundering was first voiced by European Central Bank (ECB) in 2012 [109]. The first appearance of crypto-laundering in Europol’s cybercrime agenda was also seen in the 2014 Interned Orga-

nized Crime Threats Assessment report that explained the possible use of cryptocurrencies to launder illegal proceeds obtained from cybercrime activities [110].

The first step taken by Europol to organize a cryptocurrency conference was the creation of a working group partnering with Interpol and the Basel Institute on Governance in 2016 [111]. The tripartite partnership aimed to serve as a platform to build a bridge between LEAs and cryptocurrency experts and create an expert community with the participation of both [18,19]. Since January 2017, the working group has organized global conferences on countering money laundering with cryptocurrencies [112]. Conferences were held in different locations, including Doha (Qatar), Basel (Switzerland) and the Hague (The Netherlands), and became an online event following COVID-19 travel limitations [20,113,114]. In these events, Europol and its partners aimed to facilitate a closer cooperation opportunity for LEAs and private actors to prevent and detect cryptocurrency-facilitated crimes and assist asset recovery [115]. The platform not only helps the exchanging of knowledge and expertise but also serves as a networking opportunity for public and private actors to contact each other for future collaboration [116]. In these conferences, only non-operational information is shared with private actors, and private parties cannot participate in LEA-only sessions [18,113]. According to Europol's publicly available documents, cooperation facilitated between public and private actors through the platform has increased the effectiveness of investigations on cryptocurrency-related crimes [113].

#### *4.3. Low Barrier Accessibility of Global Conference on Criminal Finances and Cryptocurrencies*

The conferences organized by tripartite partnership opened their venue as a face to face gathering in the early years of the event. However, the conference began to be organized as an online event following the COVID-19 outbreak. Since then, even though it removed the geographical barriers between law enforcement agencies and private industry engagement, not all public and private actors welcomed the event, which raised the barrier to conference participation.

According to our expert interview, private sector companies under investigation for operating illegally, violating anti-money laundering rules, and having a bad reputation in the industry are not invited to the conference because their participation would jeopardize the investigations. In addition, LEAs from Russia and China are not invited to the event because of the trust issues between these countries and organizers [117].

The high barrier to entry to the conference is also linked with the limited space for participation. The Europol and organizers discuss who they should allow participation each year. The companies that are useful for law enforcement agencies or provide new solutions and have specific investigation tools are invited to the conference after an informal selection process [117].

Even though during the COVID-19 pandemic, the conference was held online, its digital accessibility is still uncertain in the following years. The conference committee has been thinking of starting with a hybrid version of panels and returning to face-to-face meetings as soon as travel limitations are lifted [117].

Considering the low barrier entry requirement of the sharing economy model, the conference organized by Europol and its partners does not provide easy accessibility for participants because of security reasons and limited space. Their choice is understandable not to jeopardize LEA investigations in a sensitive security area. However, as long as a high barrier entry remains, knowledge exchange and networking opportunities would stay limited between public and private actors. Some of the companies which remain in the grey area that their operations are not illegal but illegitimate can be very helpful for law enforcement agencies in their investigations. Nevertheless, these companies will be left out of the platform until a low barrier entry is provided.

#### *4.4. Transaction Cost in Global Conference on Criminal Finances and Cryptocurrencies*



The reduction of transaction cost is vital for LEAs to find the right outsourcing partner in crypto-laundering cases easily, quickly and, if possible, more reasonable prices in the absence of talent and resource gaps. Apart from LEAs, calculating the transaction cost is also crucial for the small and medium-sized enterprises (SMEs) experiencing significant barriers to market entry [65]. The sharing economy platforms help SMEs reach a more extensive customer network through one big online market with little or no cost [55]. Therefore, sharing economy platform developed for P3 can reduce transaction costs for SMEs. They can easily engage with LEAs, increase their revenues and gain experience while competing with incumbent players in the market.

According to our participant observation and an elite interview [117], the conference has no modern matchmaking mechanism that accelerates transaction cost reduction for LEAs and private industry. The only way the LEAs and private actors can engage is by watching the presentations. Then, if LEAs see any potential for collaboration, they can either contact the email or the website address of the private actor provided in the presentation. Even though the platform is far behind its non-governmental examples for developing an innovative matchmaking mechanism, its traditional method still reduces the transaction cost for all parties.

As a conference presenter, our interviewee confirmed that he had received numerous emails from many LEAs requesting information about crypto-laundering and offering to collaborate on different P3 projects after his presentation. The interviewee also indicated that he approached public sector institutions to ask for their help with his work [117]. So, based on the interview data, the conference reduces the transaction cost of knowledge exchange both for LEAs and the private sector in the crypto-laundering context. The knowledge exchange, in that sense, is a mutual process in which demand comes not only from LEAs but also from the private sector.

Regarding promoting private sector products and services to LEAs, the conference also reduces the transaction cost for the private industry. Although advertisement is not allowed at the conference, some companies inevitably showcase their solution to LEAs as part of their intelligence-gathering method during their presentations. The conference committee also excuses these presentations as far as it is helpful for LEAs [117]. As a result, the platform helps these companies promote their brand and make their name more visible in the LEA market. Following the conference, if the LEAs acquire a license from these companies, the conference brings a competitive advantage in financial terms for its private sector members over those who remain out of it [117].

As for LEAs, the conference reduces the transaction cost while looking for an outsourcing partner. Several vendors participate in the conference who are qualified in tracing products, and LEAs find the opportunity to approach different companies more easily. Moreover, these companies sometimes provide demo licenses for the LEAs to help them during their investigations [117]. So, the low-cost alternatives in the conference and demo licenses create a customer surplus for LEAs. In that sense, the conference helps LEAs reduce their outsourcing costs.

#### *4.5. Trust Building in Global Conference on Criminal Finances and Cryptocurrencies*

The high-barrier entry to cryptocurrency conferences indicates that there should be a robust vetting mechanism when choosing and inviting public and private actors. However, based on our different data resources, including a review of Europol documents, participant observation and an elite interview [117], the committee has an informal vetting process in which the selection process is not well defined. In the absence of a well-written vetting mechanism, participant invitations are open to interpretation by committee members. They might overlook some potential participants whose contribution can add value to knowledge exchange and reduce the transaction cost for conference participants. Furthermore, the lack of a formal vetting mechanism undermines the inclusivity principles of sharing platform. It can cause selection bias critics for Europol and its partners, who have an intermediary role between public and private actors.

Based on the same data resources, there is also no guidelines that orders the interaction of public and private actors during the conference. In general, the moderators of the sessions set some housekeeping rules to maintain the interaction between presenter and audience without any disruption. However, comparing with other sharing economy platform examples, these rules are temporary and not well-defined rules to regulate the collaboration between public and private actors.

Finally, according to our participant observation and the elite interview [117], the platform has no rating mechanism to build trust between public and private actors either. The polling tool used in the conference only serves to learn audience's opinion on specific content questions. It does not build a reputational record for public and private actors on whether their knowledge exchange was functional and are they approachable for networking opportunities. The addition of a rating mechanism for the conference, in that sense, can motivate both public and private actors to engage more with their stakeholders to share their ideas and provide more evidence about their expertise and experience. The effective engagement between LEAs and the private industry will also accelerate networking opportunities for future collaborations.

## 5. Conclusions

This article has shown that the Europol associated 'Global Conference on Criminal Finances and Cryptocurrencies' serves as a platform for public and private actors to exchange knowledge about crypto-laundering and provides a networking opportunity. However, its compatibility with sharing economy is still 'partial', unlike the claims represented in Europol resources. As summarized in Table 1, the conference reduces the transaction cost for P3. However, due to the absence of robust trust-building mechanisms, the conference does not provide low barrier access to all public and private actors. Although the security concerns of Europol and its partners are reasonable not to jeopardize LEA investigations in the crypto-laundering context, it becomes harder to build an inclusive platform with a high-barrier entry. The increasing barrier to accessibility also hinders optimum resource sharing between LEAs and the private sector. As a result, compared with other non-governmental sharing economy platforms, the conference needs some adjustments for an efficient P3.

**Table 1.** The summary of empirical investigation.

<b>The Global Conference on Criminal Finances and Cryptocurrencies</b>				
Sharing Economy Variables				Dependent Variable
Platform Community	Low Barrier Accessibility	Transaction Cost	Trust-Building Mechanisms	To what extent the conference is compatible with sharing economy variables?
LEAs	-	+	-	Partial
Private Companies	-	+	-	Partial

Based on the empirical analysis, this study also found that optimum resource sharing in a P3 platform is highly dependent on a coherent adaption of sharing economy concepts. The Europol associated cryptocurrency conference reveals that the absence of trust-building solid mechanisms causes higher barrier entry that inevitably increases the transaction cost for LEAs and the private sector to share their scarce resources. As a result, public authorities who are willing to create online platforms but have security concerns about private sector participation should start their initiative by developing robust trust-building mechanisms first. Building trust mechanisms will undoubtedly clarify the eligibility criteria for outside actors and guide them on how to access the platform easily. As the number of public and private actors participate in the platform, the transaction

cost of resource sharing will be low for all participants. This platform model, in the end, will be a more sustainable solution for efficient P3 not only in the crypto-laundering context but also in other public service domains.

This work was one of the first attempts to examine the knowledge exchange and networking platform for P3 through the sharing economy concept. The empirical analysis of crypto-laundering P3 can also be expanded to other online platforms where public and private actors share their resources for a better partnership. Furthermore, considering the data collection limitations of the study, new studies can also contribute to the same research context by doing more interviews with stakeholders of the platform to refine the sharing economy level of the conference.

**Author Contributions:** E.I. was responsible for data collection, conceptualization, empirical analysis, and synthesis. C.K. was responsible for supervision, conceptualization, review and analysis, synthesis and editing. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 886141 as well as Jean Monnet research funding (Module, Chair, Centre, Network and Teacher Training).

**Institutional Review Board Statement:** The study was conducted in accordance with the Declaration of Helsinki and approved by the Research and Ethics Committee of University of South Wales (protocol code 210321LR and 25 February 2021).

**Informed Consent Statement:** Informed consent was obtained from the interviewee involved in the study. Regarding the conference participants, informed consent was waived due to research data were made publicly available by the data controllers (Europol, Interpol and the Basel Institute on Governance).

**Data Availability Statement:** Conference data is accessible via the link. [https://www.youtube.com/watch?v=zI4WCXy6vtQ&list=PLYRnhpCcnLP\\_4ZHA3Fg0xu2FY6QhQg8YT&ab\\_channel=BaselInstituteonGovernance](https://www.youtube.com/watch?v=zI4WCXy6vtQ&list=PLYRnhpCcnLP_4ZHA3Fg0xu2FY6QhQg8YT&ab_channel=BaselInstituteonGovernance) (accessed on 8 December 2021).

**Conflicts of Interest:** The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

## References

1. Dunn-Cavelty, M.; Suter, M. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 179–187. <https://doi.org/10.1016/j.ijcip.2009.08.006>.
2. Rainey, H.G.; Bozeman, B. Comparing Public and Private Organizations: Empirical Research and the Power of the A Priori. *J. Public Adm. Res. Theory* **2000**, *10*, 447–470. <https://doi.org/10.1093/oxfordjournals.jpart.a024276>.
3. Hoggett, P. New Modes of Control in the Public Service. *Public Adm.* **1996**, *74*, 9–32. <https://doi.org/10.1111/j.1467-9299.1996.tb00855.x>.
4. Salamon, L.M. The Tools Approach and the New Governance: Conclusion and Implications In *The Tools of Government: A Guide to the New Governance*, Salamon, L.M., Ed.; Oxford University Press: Oxford, UK, 2002; pp. 600–610.
5. Sørensen, E. Metagovernance: The Changing Role of Politicians in Processes of Democratic Governance. *Am. Rev. Public Adm.* **2006**, *36*, 98–114. <https://doi.org/10.1177/0275074005282584>.
6. Mabunda, S. Cryptocurrency: The New Face of Cyber Money Laundering. In Proceedings of the 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 6–7 August 2018; pp. 1–6.
7. Crawford, J.; Guan, Y. Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy. In Proceedings of the 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE), New York, NY, USA, 15 May 2020; pp. 38–45.
8. Buttigieg, C.P.; Efthymiopoulos, C.; Attard, A.; Cuyle, S. Anti-money laundering regulation of crypto assets in Europe’s smallest member state. *Law Financ. Mark. Rev.* **2019**, *13*, 211–227. <https://doi.org/10.1080/17521440.2019.1663996>.
9. Möser, M.; Narayanan, A. Effective cryptocurrency regulation through blacklisting. 2019. Available online: <https://allquantor.at/blockchainbib/pdf/moser2019effective.pdf> (accessed on 9 January 2022)
10. Wainright, R. The ‘Uberisation’ of International Police Work. 2016. Available online: <https://www.linkedin.com/pulse/uberisation-international-police-work-rob-wainwright/> (accessed on 4 May 2021).

11. Wainright, R.; Cilluffo, F.J. *Responding to Cybercrime at Scale: Operation Avalanche—A Case Study*; Center for Cyber and Homeland Security at Auburn University: Alabama: USA, 2017.
12. Belk, R. You are what you can access: Sharing and collaborative consumption online. *J. Bus. Res.* **2014**, *67*, 1595–1600. <https://doi.org/10.1016/j.jbusres.2013.10.001>.
13. Botsman, R.; Rogers, R. *What's Mine Is Yours: The Rise of Collaborative Consumption*; Harper Business: New York, NY, USA, 2010.
14. Gansky, L. *The Mesh: Why the Future of Business Is Sharing*; Portfolio: New York, NY, USA, 2010.
15. Schor, J.B. Getting sharing right. *Context* **2015**, *14*, 14–15.
16. De Bolle, C. The role of Europol in international interdisciplinary European cooperation. *Eur. Law Enforc. Res. Bull.* **2020**, *19*, 13–24.
17. Amann, P. NoMoreRansom 5th Anniversary. 2021. Available online: <https://www.linkedin.com/video/live/urn:li:ugcPost:6823996525824290816/?isInternal=true> (accessed on 26 July 2021)
18. Europol. In Proceedings of the 3rd Global Conference on Criminal Finances and Cryptocurrencies, The Hague, The Netherlands, 6–7 March 2019. Available online: <https://www.europol.europa.eu/publications-events/events/3rd-global-conference-criminal-finances-and-cryptocurrencies> (accessed on 8 December 2021).
19. Europol. In Proceedings of the Cryptocurrency Meets Law Enforcement at Europol's 5th Virtual Currencies Conference, The Hague, The Netherlands, 19–21 June 2018. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrency-meets-law-enforcement-europol%e2%80%99s-5th-virtual-currencies-conference> (accessed on 8 December 2021).
20. Europol. Thousands gather virtually to share knowledge of virtual assets-based money laundering and other crypto-enabled crimes. 2021. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/thousands-gather-virtually-to-share-knowledge-of-virtual-assets-based-money-laundering-and-other-crypto-enabled-crimes> (accessed on 9 December 2021)
21. Ganapati, S.; Reddick, C.G. Prospects and challenges of sharing economy for the public sector. *Gov. Inf. Q.* **2018**, *35*, 77–87. <https://doi.org/10.1016/j.giq.2018.01.001>.
22. Hofmann, S.; Sæbø, Ø.; Braccini, A.M.; Za, S. The public sector's roles in the sharing economy and the implications for public values. *Gov. Inf. Q.* **2019**, *36*, 101399. <https://doi.org/10.1016/j.giq.2019.101399>.
23. Rose, J.; Persson, J.S.; Heeager, L.T.; Irani, Z. Managing e-Government: Value positions and relationships. *Inf. Syst. J.* **2015**, *25*, 531–571. <https://doi.org/10.1111/isj.12052>.
24. Rifkin, J. *Age of Access: The New Culture of Hypercapitalism, Where All of Life is a Paid for Experience*; Penguin Putnam: New York, NY, USA, 2001; p. 320.
25. Hamari, J.; Sjöklint, M.; Ukkonen, A. The sharing economy: Why people participate in collaborative consumption. *J. Assoc. Inf. Sci. Technol.* **2016**, *67*, 2047–2059. <https://doi.org/10.1002/asi.23552>.
26. Hansen Henten, A.; Maria Windekilde, I. Transaction costs and the sharing economy. *INFO* **2016**, *18*, 1–15. <https://doi.org/10.1108/info-09-2015-0044>.
27. Martin, C.J. The sharing economy: A pathway to sustainability or a nightmarish form of neoliberal capitalism? *Ecol. Econ.* **2016**, *121*, 149–159. <https://doi.org/10.1016/j.ecolecon.2015.11.027>.
28. Ert, E.; Fleischer, A.; Magen, N. Trust and reputation in the sharing economy: The role of personal photos in Airbnb. *Tour. Manag.* **2016**, *55*, 62–73. <https://doi.org/10.1016/j.tourman.2016.01.013>.
29. Dambrine, B.; Jerome, J.; Ambrose, B. User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy. *Future Priv. Forums* **2015**. Available online: [https://fpf.org/wp-content/uploads/2021/05/FPF\\_SharingEconomySurvey\\_06\\_08\\_15.pdf](https://fpf.org/wp-content/uploads/2021/05/FPF_SharingEconomySurvey_06_08_15.pdf) (accessed on 7 January 2022)
30. Thierer, A.D.; Koopman, C.; Hobson, A.; Kuiper, C. How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the 'Lemons Problem'. *Univ. Miami Law Rev.* **2015**, *70*, 830–878.
31. Fyfe, N.R. Observations on observations. *J. Geogr. High. Educ.* **1992**, *16*, 127–133. <https://doi.org/10.1080/03098269208709185>.
32. Cohen, M.; Zehngbot, C. What's Old Becomes New: Regulating the Sharing Economy. *Boston Bar J.* **2014**, *58*, 6–9.
33. Munger, M.C. *Tomorrow 3.0: Transaction Costs and the Sharing Economy*; Cambridge University Press: Cambridge, UK, 2018.
34. Sedkaoui, S.; Khelfaoui, M. *Sharing Economy and Big Data Analytics*; Wiley and Sons: London, UK, 2020; p. 268.
35. John, N.A. Sharing and Web 2.0: The emergence of a keyword. *New Media Soc.* **2013**, *15*, 167–182. <https://doi.org/10.1177/1461444812450684>.
36. Bardhi, F.; Eckhardt, G.M. Access-Based Consumption: The Case of Car Sharing. *J. Consum. Res.* **2012**, *39*, 881–898. <https://doi.org/10.1086/666376>.
37. Christensen, C.M.; Raynor, M.E.; McDonald, R. What is Disruptive Innovation? *Harv. Bus. Rev.* **2015**. Available online: <https://hbr.org/2015/12/what-is-disruptive-innovation> (accessed on 11 January 2022)
38. Hodkinson, P. *Media, Culture and Society: An Introduction*; SAGE: London, UK.; Los Angeles, CA, USA, 2011.
39. John, N.A. The Social Logics of Sharing. *Commun. Rev.* **2013**, *16*, 113–131. <https://doi.org/10.1080/10714421.2013.807119>.
40. O'Rourke, D.; Lollo, N. Transforming Consumption: From Decoupling, to Behavior Change, to System Changes for Sustainable Consumption. *Annu. Rev. Environ. Resour.* **2015**, *40*, 233–259. <https://doi.org/10.1146/annurev-environ-102014-021224>.
41. Avital, M.; Carroll, J.M.; Hjalmarsson, A.; Levinat, N.; Arvind, M.; Sundararajan, A. The Sharing Economy: Friend or Foe? In Proceedings of the The Thirty Sixth International Conference on Information Systems, ICIS 2015, Atlanta, GA, USA, 13–16 December 2015.

42. Heinrichs, H. Sharing Economy: A Potential New Pathway to Sustainability. *GAIA—Ecol. Perspect. Sci. Soc.* **2013**, *22*, 228–231.
43. Botsman, R. The Sharing Economy Lacks A Shared Definition. 2013. Available online: <https://www.fastcompany.com/3022028/the-sharing-economy-lacks-a-shared-definition> (accessed on 3 January 2021)
44. Codagnone, C.; Martens, B. *Scoping the Sharing Economy: Origins, Definitions, Impact and Regulatory Issues*; Institute for Prospective Technological Studies: Seville, Spain, 2016.
45. Gussen, B.F. Sharing City Seoul and the Future of City Governance. In *Legal Tech and the New Sharing Economy*; Corrales Compagnucci, M., Forgó, N., Kono, T., Teramoto, S., Vermeulen, E.P.M., Eds.; Springer Singapore: Singapore, 2020; pp. 21–45.
46. Albinsson, P.A.; Yasanthi Perera, B. Alternative marketplaces in the 21st century: Building community through sharing events. *J. Consum. Behav.* **2012**, *11*, 303–315. <https://doi.org/10.1002/cb.1389>.
47. Chasin, F.; Scholta, H. Taking Peer-to-Peer Sharing and Collaborative Consumption onto the Next Level—New Opportunities and Challenges for E-Government. *Compleat. Res. Pap.* **2015**. doi:10.18151/7217288
48. Benoit, S.; Baker, T.L.; Bolton, R.N.; Gruber, T.; Kandampully, J. A triadic framework for collaborative consumption (CC): Motives, activities and resources & capabilities of actors. *J. Bus. Res.* **2017**, *79*, 219–227. <https://doi.org/10.1016/j.jbusres.2017.05.004>.
49. Van Alstyne, M.; Parker, G.; Choudary, S.P. Pipelines, Platforms, and the New Rules of Strategy. *Harv. Bus. Rev.* **2016**, *62*, 54–60.
50. Wirtz, J.; So, K.K.F.; Mody, M.A.; Liu, S.Q.; Chun, H.H. Platforms in the peer-to-peer sharing economy. *J. Serv. Manag.* **2019**, *30*, 452–483. <https://doi.org/10.1108/JOSM-11-2018-0369>.
51. Aigrain, P.; Aigrain, S. *Sharing: Culture and the Economy in the Internet Age*; Amsterdam University Press: Amsterdam, Netherlands, 2012.
52. Williamson, O.E. *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*; Free Press: New York, NY, USA; Collier Macmillan: London, UK, 1985.
53. Evans, D.S.; Schmalensee, R. *Matchmakers: The New Economics of Multisided Platforms*; Harvard Business Review Press: Boston, MA, USA, 2016.
54. Andrei Andreia, G.; Gazzola, P.; Zbucea, A.; Alexandru Vlad, A. Modeling socially responsible consumption and the need for uniqueness: A PLS-SEM approach. *Kybernetes* **2017**, *46*, 1325–1340. <https://doi.org/10.1108/K-03-2017-0103>.
55. Sundararajan, A. *The Sharing Economy: The End of Employment and the Rise of Crowd-Based Capitalism*; MIT Press: Cambridge, MA, USA, 2016.
56. Marr, B. The Sharing Economy—What It Is, Examples, and How Big Data, Platforms and Algorithms Fuel It. *Forbes* **2016**. Available online: <https://www.forbes.com/sites/bernardmarr/2016/10/21/the-sharing-economy-what-it-is-examples-and-how-big-data-platforms-and-algorithms-fuel/?sh=378acc3a7c5a> (accessed on 3 January 2022).
57. Cohen, P.; Hahn, R.; Hall, J.; Levitt, S.; Metcalfe, R. Using Big Data to Estimate Consumer Surplus: The Case of Uber. *Natl. Bur. Econ. Res. Work. Pap. Ser.* **2016**. doi:10.3386/w22627
58. Fraiberger, S.P.; Sundararajan, A. Peer-to-Peer Rental Markets in the Sharing Economy. *NYU Stern Sch. Bus. Res. Pap.* **2017**. <https://dx.doi.org/10.2139/ssrn.2574337>
59. Benkler, Y. Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production. *Yale Law J.* **2004**, *114*, 273–358. <https://doi.org/10.2307/4135731>.
60. Bratianu, C. The Crazy New World of the Sharing Economy. In *Knowledge Management in the Sharing Economy: Cross-Sectoral Insights into the Future of Competitive Advantage*; Vătămănescu, E.-M., Pînzaru, F.M., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 3–18.
61. Calcaterra, C.; Kaal, W.A. Reputation Protocol for the Internet of Trust. In *Legal Tech and the New Sharing Economy*; Corrales Compagnucci, M., Forgó, N., Kono, T., Teramoto, S., Vermeulen, E.P.M., Eds.; Springer Singapore: Singapore, 2020; pp. 123–147.
62. Ravenelle, A.J. *Hustle and Gig: Struggling and Surviving in the Sharing Economy*; University of California Press: Oakland: CA, USA, 2019.
63. Teubner, T.; Hawlitschek, F. The Economics of Peer-to-Peer Online Sharing. In *The Rise of the Sharing Economy: Exploring the Challenges and Opportunities of Collaborative Consumption*; Albinsson, P.A., Perera, Y., Eds.; Praeger: Santa Barbara, CA, USA, 2018; pp. 129–156.
64. Allon, G.; Bassamboo, A.; Çil, E.B. Large-Scale Service Marketplaces: The Role of the Moderating Firm. In *Sharing Economy: Making Supply Meet Demand*; Hu, M., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 165–192.
65. Schneider, H. *Creative Destruction and the Sharing Economy: Uber as Disruptive Innovation*; Edward Elgar Pub.: Northampton, MA, USA, 2017.
66. Cohen, M.; Sundararajan, A. Self-Regulation and Innovation in the Peer-to-Peer Sharing Economy. *Univ. Chic. Law Rev. Online* **2015**, *42*, 116–133.
67. Constantiou, I.; Eaton, B.; Tuunainen, V.K. The Evolution of a Sharing Platform into a Sustainable Business. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016, 2016; pp. 1297–1306.
68. Parigi, P.; Cook, K. Trust and Relationships in the Sharing Economy. *Contexts* **2015**, *14*, 18–19.
69. Resnick, P.; Kuwabara, K.; Zeckhauser, R.; Friedman, E. Reputation systems. *Commun. ACM* **2000**, *43*, 45–48. <https://doi.org/10.1145/355112.355122>.

70. Sundararajan, A. Why the Government Doesn't Need to Regulate the Sharing Economy. *Wired* **2012**. Available online: <https://www.wired.com/2012/10/from-airbnb-to-coursera-why-the-government-shouldnt-regulate-the-sharing-economy/> (accessed on 11 January 2021)
71. Gutt, D.; Herrmann, P. Sharing Means Caring? Hosts' Price Reaction to Rating Visibility. In Proceedings of the European Conference on Information Systems, Munster, Germany, 26–29 May 2015.
72. Teubner, T.; Flath, C.M. Privacy in Sharing Economy. *J. Assoc. Inf. Syst.* **2019**, *20*, 2.
73. Benkler, Y. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*; Yale University Press: New Haven, CT, USA, 2006.
74. Resnick, P.; Zeckhauser, R. Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system. In *The Economics of the Internet and E-Commerce*; Michael, R.B., Ed.; Advances in Applied Microeconomics; Emerald Group Publishing Limited: Bingley, UK, 2002; Volume 11, pp. 127–157.
75. Zervas, G.; Proserpio, D.; Byers, J.A. A First Look at Online Reputation on Airbnb, Where Every Stay is Above Average. *Mark. Lett.* **2021**, *32*, 1–16.
76. Slee, T. *What's Yours Is Mine: Against the Sharing Economy*; OR Books: New York, NY, USA; London, UK, 2017.
77. Levi, M. Money Laundering and Its Regulation. *Ann. Am. Acad. Political Soc. Sci.* **2002**, *582*, 181–194.
78. McDowell, J.; Novis, G. Consequences of Money Laundering and Financial Crime. *Econ. Perspect.* **2001**, *6*, 6–8.
79. Brenig, C.; Accorsi, R.; Lüller, G. Economic Analysis of Cryptocurrency Backed Money Laundering. In Proceedings of the European Conference on Information Systems 2015, Munster, Germany, 26–29 May 2015.
80. Compin, F. The role of accounting in money laundering and money dirtying. *Crit. Perspect. Account.* **2008**, *19*, 591–602. <https://doi.org/>
81. Kepli, M.Y.b.Z.; Nasir, M.A. Money Laundering: Analysis on the Placement Methods. *Int. J. Bus. Econ. Law* **2016**, *11*, 32–40.
82. Albrecht, C.; Duffin, K.M.; Hawkins, S.; Morales Rocha, V.M. The use of cryptocurrencies in the money laundering process. *J. Money Laund. Control* **2019**, *22*, 210–216. <https://doi.org/10.1108/JMLC-12-2017-0074>.
83. Stokes, R. Virtual money laundering: The case of Bitcoin and the Linden dollar. *Inf. Commun. Technol. Law* **2012**, *21*, 221–236. <https://doi.org/10.1080/13600834.2012.744225>.
84. Filipkowski, W. Cyber Laundering: An Analysis of Typology and Techniques. *Int. J. Crim. Justice Sci.* **2008**, *3*, 15–27.
85. FATF. *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*; FATF: Paris, France, 2014.
86. Nian, L.P.; Chuen, D.L.E.E.K. Introduction to Bitcoin. In *Handbook of Digital Currency*; Lee Kuo Chuen, D., Ed.; Academic Press: San Diego, CA, USA, 2015; pp. 5–30.
87. Lansky, J. Possible State Approaches to Cryptocurrencies. *J. Syst. Integr.* **2018**, *9*, 19–31.
88. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: [https://www.usssc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging\\_Tech\\_Bitcoin\\_Crypto.pdf](https://www.usssc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf) (accessed on 14 January 2022)
89. Möser, M.; Böhme, R.; Breuker, D. An inquiry into money laundering tools in the Bitcoin ecosystem. In Proceedings of the 2013 APWG eCrime Researchers Summit, San Francisco, CA, USA, 17–18 September 2013; pp. 1–14.
90. Bebris, A.V. Anti-Money Laundering and Counter-Terrorism Financing methodology for cryptocurrency exchanges in the European Union. Copenhagen, 2018. Available online: [https://research-api.cbs.dk/ws/portalfiles/portal/59782893/454560\\_Master\\_s\\_Thesis\\_project\\_Anrijs\\_Valts\\_Bebri\\_Final\\_v2.pdf](https://research-api.cbs.dk/ws/portalfiles/portal/59782893/454560_Master_s_Thesis_project_Anrijs_Valts_Bebri_Final_v2.pdf) (accessed on 7 January 2022)
91. Cancelli, L. *The Growing Crypto-assets Threat to Anti-money Laundering: How Institutions Are Coping with This Phenomenon*; Ca'Foscari University Venice: Venice, Italy, 2020; pp. 1–21.
92. Krishnan, H.; Saketh, S.; Tej Vaibhav, G. Cryptocurrency Mining—Transition to Cloud. *Int. J. Adv. Comput. Sci. Appl.* **2015**, *6*, 115–124.
93. Teichmann, F.M.J.; Falker, M.-C. Money laundering via cryptocurrencies—potential solutions from Liechtenstein. *J. Money Laund. Control* **2021**, *24*, 91–101. <https://doi.org/10.1108/JMLC-04-2020-0041>.
94. Drainville, D. An Analysis of the Bitcoin Electronic Cash System. 2012. Available online: [https://uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/drainville\\_danielle.pdf](https://uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/drainville_danielle.pdf) (accessed on 14 January 2022)
95. Fanusie, Y.J.; Robinson, T. Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services. *Memorandum* **2018**. Available online: <https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf> (accessed on 14 January 2022)
96. Ilbiz, E. The Uberization of the United Nations' regime to prevent the online financing of terrorism: Tackling the problem of obfuscation in virtual currencies. *J. Cyber Policy* **2019**, *4*, 404–424. <https://doi.org/10.1080/23738871.2019.1666892>.
97. Dupuis, D.; Gleason, K. Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *J. Financ. Crime* **2021**, *28*, 60–74.
98. O'leary, R.-R. Edward Snowden: Zcash Is 'Most Interesting Bitcoin Alternative'. *Coindesk* 2017.
99. Custers, B.; Oerlemans, J.-J.; Pool, R. Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *Eur. J. Crime Crim. Law Crim. Justice* **2020**, *28*, 121–152. <https://doi.org/10.1163/15718174-02802002>.
100. Wronka, C. "Cyber-laundering": The change of money laundering in the digital age. *J. Money Laund. Control.* 2021, *ahead-of-print*. <https://doi.org/10.1108/JMLC-04-2021-0035>.

101. Haffke, L.; Fromberger, M.; Zimmermann, P. Cryptocurrencies and anti-money laundering: The shortcomings of the fifth AML Directive (EU) and how to address them. *J. Bank. Regul.* **2019**, *21*, 125–138.
102. Wronka, C. Anti-money laundering regimes: A comparison between Germany, Switzerland and the UK with a focus on the crypto business. *J. Money Laund. Control* **2021**, *ahead-of-print*. <https://doi.org/10.1108/JMLC-06-2021-0060>.
103. Owen, A.; Chase, I. NFTs: A New Frontier for Money Laundering? **2021**. Available online: <https://rusi.org/explore-our-research/publications/commentary/nfts-new-frontier-money-laundering> (accessed on 14 January 2022)
104. Desmond, D.B.; Lacey, D.; Salmon, P. Evaluating cryptocurrency laundering as a complex socio-technical system. *J. Money Laund. Control* **2019**, *22*, 480–497. <https://doi.org/10.1108/JMLC-10-2018-0063>.
105. Forgang, G. *Money Laundering Through Cryptocurrencies*; La Salle University: Philadelphia, PA, USA, 2019.
106. Campbell-Verduyn, M. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law Soc. Change* **2018**, *69*, 283–305. <https://doi.org/10.1007/s10611-017-9756-5>.
107. Faccia, A.; Moşteanu, N.R.; Cavaliere, L.P.L.; Mataruna-Dos-Santos, L.J. Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases. In Proceedings of the 2020 12th International Conference on Information Management and Engineering, Amsterdam, The Netherlands, 16–18 September, 2020; pp. 29–34.
108. Wronka, C. Money laundering through cryptocurrencies—analysis of the phenomenon and appropriate prevention measures. *J. Money Laund. Control* **2022**, *25*, 79–94. <https://doi.org/10.1108/JMLC-02-2021-0017>.
109. Ramalho, D.S.; Matos, N.I. What we do in the (digital) shadows: Anti-money laundering regulation and a bitcoin-mixing criminal problem. *ERA Forum* **2021**, *22*, 487–506. <https://doi.org/10.1007/s12027-021-00676-4>.
110. Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2014*; Europol: Hague, The Netherlands, 2014.
111. Europol. Money Laundering with Digital Currencies: Working group established. 2016. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/money-laundering-digital-currencies-working-group-established> (accessed on 15 January 2022)
112. Europol. In Proceedings of the Global Conference on Countering Money Laundering and the Misuse of Digital Currencies, Doha, Qatar, 19 January 2017. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/global-conference-countering-money-laundering-and-misuse-of-digital-currencies> (accessed on 8 December 2021).
113. Europol. In Proceedings of the Over 2000 participants from 132 countries logged on for the 4th Global Conference on Criminal Finances and Cryptocurrencies, Online Event, 18–19 November 2020. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/over-2-000-participants-132-countries-logged-for-4th-global-conference-criminal-finances-and-cryptocurrencies> (accessed on 8 December 2021).
114. Europol. In Proceedings of the Europol hosted 4th Conference on Virtual Currencies, The Hague: The Netherlands, 22–23 June 2017. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/europol-hosted-4th-conference-virtual-currencies> (accessed on 8 December 2021).
115. Europol. In Proceedings of the Cryptocurrency Experts Meet at Europol to Stengthen Ties Between Law Enforcement and Private Sector, The Hague, The Netherlands, 12–14 June 2019. Available online: <https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrency-experts-meet-europol-to-strengthen-ties-between-law-enforcement-and-private-sector> (accessed on 8 December 2021).
116. Europol. In Proceedings of the 4th Global Conference on Criminal Finances and Cryptocurrencies, Online, 18–19 November 2020. Available online: <https://baselgovernance.org/news/4th-global-conference-criminal-finances-and-cryptocurrencies-interpol> (accessed on 8 December 2021).
117. Former LEA Agent and Senior Investigation Officer in a Global Cryptocurrency Exchange. Semi-Structured Interview. 2022.