Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency

Christian Leuprecht
Royal Military College of Canada, Kingston, Canada; School of Policy Studies, Queen's University, Kingston, Canada and Australian Graduate School of Policing and Security, Charles Sturt University – Canberra Campus, Barton, Australia, and

Caitlyn Jenkins and Rhianna Hamilton
School of Policy Studies, Queen's University, Kingston, Canada

Abstract

Purpose – This study aims to explain how cryptocurrency is leveraged for illicit purposes across the global financial system. Specifically, it establishes how cryptocurrency has been changing the nature of transnational and domestic money laundering (ML). It then assesses the effectiveness of conventional anti-money laundering (AML) policy and legislation against the proliferation of crypto laundering, using Canada as a critical case study.

Design/methodology/approach – Data was collected from court cases and secondary sources to build cross-case trends of cryptocurrency use in ML. Illicit International Political Economy forms the theoretical foundation for this study, whose contribution is situated in the current literature on crypto-ML.

Findings – This study finds that Bitcoin is common among crypto-money launderers, though most also use some form of alt-coin, and that the use of third-party currency exchanges is a prevalent method to create illicit funds and conceal proceeds of crime. The findings validate two hypotheses that illicit use of crypto is prevalent in the first two stages of ML, and that crypto is most often used in conjunction with other fiat currencies. Although law enforcement is improving on monitoring and understanding popular cryptocurrencies such as Bitcoin, alt-coins pose a significant challenge for criminal intelligence. New regulations for third-party currency exchanges are having a positive impact on curtailing crypto-laundering but are shown to be insufficient per se to contain the use of crypto in criminal activity.

Originality/value – This study contributes to a more robust understanding of the use of virtual currency in transnational and domestic ML. It contributes to an emerging body of literature on the role of technological change in enabling the global flow of illicit funds. It also informs public policy on virtual currency in general, and on AML regulation in Canada in particular.

Keywords Canada, USA, Money laundering, FATF, Cryptocurrency, Transnational crime

Paper type Research paper

Introduction

This article investigates the role of cryptocurrency and its impact on transnational and domestic money laundering (ML). It assesses the effectiveness of conventional anti-ML

Funding: Research for this article was supported by the Social Sciences and Humanities Research Council of Canada, Insight Grants 435-2022-0862 and 435-2019-1333.

Journal of Financial Crime
Vol. 30 No. 4, 2023
pp. 1036-1054
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-07-2022-0161

(AML) policy in containing the illicit use of cryptocurrency through a small-*n* comparison of a dozen court cases that involve crypto-ML. The sample reveals Bitcoin as the most popular cryptocurrency used in ML schemes, although private alt-coins feature prominently and cryptocurrency exchanges are key financial mechanisms in crypto-ML. The article makes a novel empirical contribution to a largely theoretical body of literature on technological change in the global flow of illicit funds. It also contributes to the emerging field of Illicit International Political Economy (IIPE) and develops a more systematic approach to study the poorly understood realm of crypto-ML. Initially, the article explains cryptocurrency and its relevance to ML. Second, it introduces the method used, the theory that informs it and then situates the article among key debates. Third, it provides empirical observations, followed by analysis. The final section assesses implications for the efficacy of crypto-AML policy by applying the results to Canadian policy on ML and cryptocurrency.

Laying the groundwork: money laundering, crypto and current research

ML is a global challenge that undermines public safety by enabling organized crime, taxation to pay for public services and regional stability by incentivizing state capture. The global illicit economy is estimated to account for about US$2.2tn or 3.6% of the global GDP per year (World Economic Forum, 2015). However, other figures peg it closer to 10% of global GDP (The High-Level Panel on International Financial Accountability Transparency and Integrity for Achieving the 2030 Agenda, 2020).

Financial crime, and ML specifically, is difficult to measure: it is illicit and, therefore, opaque, often disguised as legitimate in appearance and only a full picture of associated transnational transactions reveals their illicit nature and criminal intent (Leuprecht *et al.*, 2019). As a result, globalization has proven an accelerant for ML (Legrand and Leuprecht, 2021). Criminals adapt their strategies according to emerging economic trends to turn a profit and avoid detection by law enforcement (Dupuis and Gleason, 2021).

One trend to emerge in the global economy in recent years is virtual currency, also referred to as cryptocurrency or crypto. In 2009, the creation of Bitcoin opened the possibility of a new global financial order in which currency need not be backed by any one government (Parkin, 2020). In the legitimate economy, cryptocurrencies are beginning to be integrated as investments and securities, as well as a medium of exchange (Maume and Fromberger, 2019; Trzcionka, 2019; Shovkhalov and Idrisov, 2021). While cryptocurrencies and blockchain technology are not about to replace the traditional banking system, their prevalence presents a host of new security challenges. Due to their decentralized nature, cryptocurrency circumvents government regulation and operates almost independently from traditional financial systems. It is anonymous and notoriously difficult to track – which makes it appealing to criminals.

Unlike "fiat" currencies that are used as legal tender and the principal medium of exchange by issuing countries, virtual currencies are stateless and intangible. Instead of banks and a centralized financial system, cryptocurrencies rely on a virtual ledger, known as a blockchain, to ensure stability (Adachi and Aoyagi, 2020).

The Criminal Intelligence Service Canada and the OECD's international Financial Action Task Force (FATF) have both flagged cryptocurrency for its use in ML and terrorist financing (ML/TF) (Financial Action Task Force, 2016; Criminal Intelligence Service Canada, 2020). In the illicit economy, a single cryptocurrency, Bitcoin, accounts for nearly one-quarter of all users and close to one-half of all transactions. Users that primarily use Bitcoin for illegal activity conduct around 37 million transactions annually, valued at more than US$76bn (Foley *et al.*, 2019). This is on par with the size of the combined illegal drug markets in the USA and Europe (Barone and Masciandaro, 2011). Although cryptocurrency

is fairly new, its deregulated and stateless nature has made it a commodity to launder money and enables criminal transactions on a global scale (Kethineni and Cao, 2020).

Notwithstanding its popularity and attention heaped by domestic and international regulatory bodies, cryptocurrency remains largely unaccounted for in Canada's AML regime. By way of example, ML features prominently in British Columbia's real estate and gambling industries (German, 2018, 2019); so, in 2020, the government launched the Cullen Commission into Money Laundering in British Columbia, which reflects heightened concern with domestic ML. Its final report, published in June 2022, made extensive commentary on the danger that virtual assets pose as a tool for ML in British Columbia's economy (Cullen, 2022). Beyond the Commission, scholarly attempts to present a picture of Canada's ML market are outdated and fail to include cryptocurrency in their empirical accounts (Beare and Schneider, 2007).

In studying the nexus between cryptocurrency and ML, this article makes an important contribution to understanding the options available to decision-makers and law enforcement to contain the prevailing proliferation of cryptocurrency in the commission of financial crime.

Hypotheses. To this effect, the observations in this article generate two hypotheses. *H1* posits conventional approaches to ML as problematic insofar as cryptocurrency does not conform to the three traditional steps of ML: placement, layering and integration (Figure 1). Placement refers to proceeds of crime that are first placed into the financial system. Layering describes a sequence of financial transactions, often across borders, to conceal the origin of the illicit funds. During integration, illicit funds that now appear to be legitimate are returned to the criminal to be used in the legal economy.

There is little regulation of virtual currency; so, we hypothesize that the use of cryptocurrency should be common in the placement and layering stages of ML. The widespread appeal of cryptocurrency for criminal use due to its anonymity and relative ease with which to transfer funds across borders, suggests that crypto is likely to be used in stages where these traits are most beneficial to concealing illicit funds.

As the use of cryptocurrency is not yet widespread and has limited traction in the financial system, *H2* postulates that virtual currencies are rarely used exclusively in ML schemes. Instead, one would expect to see virtual currencies laundered alongside fiat currencies.

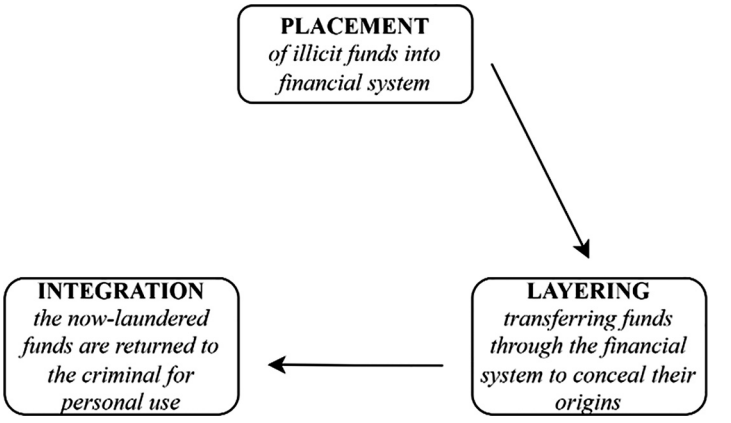

Figure 1.
Structure of typical ML scheme

Defining core concepts: what is cryptocurrency?

There are two kinds of cryptocurrency: centralized and decentralized. Centralized cryptocurrency relies on a third-party administrator to issue the currency, maintain its blockchain and decide the rules for its use (Financial Action Task Force, 2014): WebMoney "WM Units," PerfectMoney, Liberty Reserve dollars (defunct) and E-gold (defunct) are all examples of centralized cryptocurrency. Decentralized cryptocurrencies use open source and math-based peer-to-peer blockchains that function without a central administrator (Financial Action Task Force, 2014): Bitcoin, Litecoin, Ethereum and Monero are all examples of decentralized cryptocurrency.

The blockchain allows cryptocurrency to function, *inter alia*, as a medium of exchange, as an asset and as an investment (Hayes, 2019). This diversity in use, as well as the unprecedented nature of the technology, makes it difficult to categorize and, therefore, regulate cryptocurrency. As of January 2021, there were 7,812 cryptocurrencies in use (Kumru, 2021). That has prompted a range of regulatory responses across different national jurisdictions, from outright bans to more permissive attitudes that incorporate cryptocurrencies in national financial regulatory frameworks (Chohan, 2017). For example, on the one hand, El Salvador has adopted Bitcoin as legal tender alongside the US dollar. On the other hand, China has deemed all cryptocurrency transactions in the country illegal. In jurisdictions where cryptocurrencies are legal, their status varies from a currency to a security to a commodity (Desmond *et al.*, 2019). By design, however, cryptocurrency is meant to be global and thus beyond the control of any one jurisdiction.

The technology ensures greater anonymity than traditional financial mechanisms. In a blockchain, each "block" contains a timestamp, the details of the transaction and the information of the previous block in the chain. Ergo, it is possible to track the order of transactions and when they occurred depending on the level of privacy a certain crypto-coin provides (Adachi and Aoyagi, 2020). However, blockchains remain pseudo-anonymous as transactions do not require the identification of the sender or receiver, as is common for a conventional wire transfer (Egan, 2018). The Bitcoin blockchain in particular has limited anonymity, as the details of transactions are public, and only the identities of the sender and receiver are anonymous. In addition, law enforcement has succeeded in tracking Bitcoin users when they follow blockchain transactions until it reaches a Bitcoin address that is linked to a known identity (Greenberg, 2022). Other cryptocurrencies, such as Monero, have a higher degree of anonymity because their designs include added privacy features such as stealth addresses (Greenberg, 2018).

The pseudo-anonymous nature of the transactions, international decentralization and an incomplete patchwork of different regulations across national jurisdictions makes cryptocurrencies vulnerable to exploitation for the purposes of financial crime, specifically ML (Dyntu and Dykyi, 2018; Mabunda, 2018; Albrecht *et al.*, 2019). However, while the general vulnerability of cryptocurrency to financial crime is well-known, the exact nature of that vulnerability is poorly understood. How might cryptocurrency shape the conflict in Ukraine? Some herald its use as a democratizing tool to deliver aid to Ukraine and allow an alternative to the Moscow-controlled ruble. Others worry that crypto will be vulnerable to Russian actors intent on evading sanctions and moving money illegally (Arasasingham and DiPippo, 2022). Such geopolitical situations highlight an inchoate understanding of cryptocurrency's potential in compromising national and international security.

Illicit international political economy and the theorization of crypto-money laundering

This article is informed by a theoretical approach known as Illicit International Political Economy (IIPE). Much like IPE, IIPE asks questions regarding globalization, the balance of power between the state and the market and the flow of money among other things. However, they differ in that IPE theorizes about the legitimate, legal and licit political economy, whereas IIPE studies the unofficial, illegal and illicit dimensions of the discipline's core concepts (Andreas, 2004).

Andreas (2004) brought the study of the illicit dimensions of the global economy into IPE as its own independent sub-discipline. Scholars have since attempted to dissolve the artificial divide between the licit and illicit economies. Ryner (2006) and Hudson (2005, 2013, 2019) assert that these economies are two sides of the same coin. According to Hudson:

> Many, if not all, commodities in their passage along a circuit of commodity production may, and routinely do, pass through a variety of legally and illegally regulated spaces and may involve illegal activities and practices that are nonetheless seen as licit (Hudson, 2013, pp. 13-14).

This article seeks to re-evaluate the scope of these regulated spaces, as it pertains to new technologies and to provide evidence to dissolve the artificial divide between licit and illicit business dealings.

However, scholarship on IIPE remains limited. This is largely due to methodological and logistical challenges in acquiring access to the proper data necessary for thorough and accurate research (Legrand and Leuprecht, 2021). Empirical constraints of IIPE push political economists toward approaches that are reliant on widely accessible data on licit economic activity. To lessen these constraints and expand scholarship of IIPE, the sample of cases that informs this article thus makes a modest yet important contribution to a field that is plagued by a dearth of data: scholarship on illicit economic activity in general, and on cryptocurrency as an enabler of ML in particular.

Debates

The study of ML is an emerging field, and literature on the role of cryptocurrency in ML is scarce. Scholarship generally falls into one of two categories:

(1) policy and regulation (Albrecht *et al..,* 2019; Mancini, 2016; Neagu, 2019; Turpin, 2014); or

(2) investigation and policing (Ogunbadewa, 2014; Custers *et al..*, 2020; Farrugia *et al..*, 2020).

Proposed solutions consist of changing the way cryptocurrency or ML are regulated and policed.

On the one hand, Sanchez (2017) argues that to crack down on the illicit use of crypto in the USA, the status of cryptocurrencies under the law must change. Either cryptocurrencies become legal tender or cryptocurrency exchanges must maintain user-identification records. Sanchez argues that either of these solutions would align crypto policy with traditional financial instruments. This would discourage them being leveraged for criminal purposes while also ensuring that crypto-ML will be adequately regulated and investigated. On the other hand, Ogunbadewa (2014) suggests that investigators be equipped with the right technology and techniques to police cyberspace. He argues that the illicit use of cryptocurrency can be circumvented if governments invest in high-tech online surveillance programs as well as multilateral platforms to facilitate international cooperation in investigating the illicit use of cryptocurrency.

Differences in approach have prompted emerging debates in the literature. One debate concerns the vulnerability of cryptocurrency to perpetrate financial crime. One group of scholars attributes this vulnerability to the underlying technology of the blockchain (Campbell-Verduyn, 2018; Ducas and Wilner, 2017). These authors argue that the anonymous nature of private blockchains pose the greatest risk, rather than the use of cryptocurrencies themselves. Others instead propose that the blockchain is an unimportant point of risk in anti-ML methods. Hughes (2019) suggests that the main concern for adequate crypto-AML efforts is finding effective regulators that are equipped to handle the challenges that cryptocurrency presents.

However, the solutions proposed in these debates, and for illicit crypto use in general, lack empirical support. Most scholarship on the use of cryptocurrency in ML is based solely on previous literature and theory. Little scholarship is supported by actual empirical evidence (Farrugia *et al.*, 2020; Custers *et al.*, 2020; Ferwerda *et al.*, 2020). Within that subset, most empirical research focuses on investigating ways to detect the use of laundering money via cryptocurrency. Ferwerda *et al.* (2020), for instance, use an econometric gravity model estimation to simulate global illicit financial flows and identify the countries that money launderers prefer.

The few articles that do discuss concrete cases of crypto-ML tend to trade in single case studies rather than broader trends or comparative analysis. That gives us little traction on understanding the current reality of crypto use in financial crime.

Inclusion criteria and limitations of current data

This study uses small-*n* comparative case analysis, a method typical within social science, to examine cases that involve crypto-laundering and uncover greater relationships and networks. This study comprises 12 cases (Appendix).

Cases were collected from the US Department of Justice website and other legal databases. Inclusion criteria of cases was determined by whether they were transnational in nature, included the use of cryptocurrency and involved a charge or clear component of ML. Few crypto-laundering cases meet these scope conditions. In addition, public legal documents for crypto-laundering cases often involve redactions or lack of detail that disqualifies many potential cases. Due to the clarity and detail in public legal documents under US jurisdiction, the limited number of cases that fulfilled the research scope were found in American courts. The observations in this study are skewed accordingly.

We then look for patterns on how money launderers use cryptocurrency in relation to one another, the global financial system and various forms of centralized and decentralized currencies by dividing each legal document into 26 variables. If information for a variable could not be found in the primary text, we consulted secondary sources to fill the gap in knowledge. This includes news articles, academic papers, databases, government and business reports and occasionally social media platforms such as Instagram and LinkedIn. This method draws on similar studies conducted by Leuprecht *et al.* (2017) and Leuprecht *et al.* (2019). However, cases of crypto-laundering differ from other datasets of prosecuted ML cases in that they lack an apparent organizational structure and centralized social networks. In addition, many actors within these decentralized networks are unidentified and/or serve multiple functions within a given network, which makes it difficult to determine the role of key individuals and their relationship to a grand scheme. Pervasive anonymity within crypto-laundering cases detracts from mathematical clustering and makes it difficult to interpret the meaning of the networks revealed through this approach.

Patterns within transnational crypto-money laundering

Still, some pattern emerge. First, Bitcoin is the most prevalent form of cryptocurrency for ML. A total of 9 of 12 cases used Bitcoin to transfer illicit funds. However, as Figure 2 shows, there are plenty of other options (Figure 2). Bitcoin is the best-known cryptocurrency and the most accessible for a diverse array of uses. Although law enforcement's ability to track Bitcoin is improving, the design of Bitcoin's blockchain currently remains effective at preserving the anonymity of its users.

Second, diverse "alt-coins" are used 14 times across 12 cases. The term "alt-coin" refers to any cryptocurrency other than Bitcoin. Nearly every case studied used some form of alt-coin. While there is less opportunity to use them as a method of payment, the obscurity of alt-coins helps in transferring illicit funds undetected. Compared to Bitcoin, law enforcement and regulatory bodies are also less likely to track and have a full understanding of alt-coins.

Third, currency exchanges kept recurring within the data set. After wire transfer, the most popular mechanisms for moving illicit funds are currency conversion and third-party exchange: a third-party intermediary that converts fiat to crypto and vice versa for recipients and investors (Figure 3). Four main categories of currency exchange are used in ML schemes in this sample.

The first group (Figure 4) consists of USA v. Western Express and USA v. BTC-e and Vinnik. It concerns the prosecution of cryptocurrency exchanges, including charges of ML and the illegal operation of a money transmission business. In these schemes, the managers and employees of the business would facilitate laundering of their clients' funds by allowing them to bypass identity verification required by law and convert their currency in and out of crypto. The business would take a cut of their clients' ill-gotten gains for the conversion and the discretion of their service.

In the second group of cases (Figure 5), third-party cryptocurrency exchanges were integral to the functioning of the scheme. In USA v. Karlsson, for instance, Roger Karlsson created a fraudulent website claiming to offer investments, particularly for retirement purposes. To purchase a share, customers had to transfer their money into Bitcoin with a digital currency exchanger such as Perfect Money and C-Gold. The money would then be sent to Karlsson, who converted the Bitcoin into Baht and deposited the funds into his personal bank accounts in Thailand.

In the third group of cases (Figure 6), currency exchange businesses were not used to obtain illicit funds, but to layer and integrate illicit funds derived from other sources into the legitimate economy. For example, in USA v. Stoica *et al.*, members of the Alexandria Online

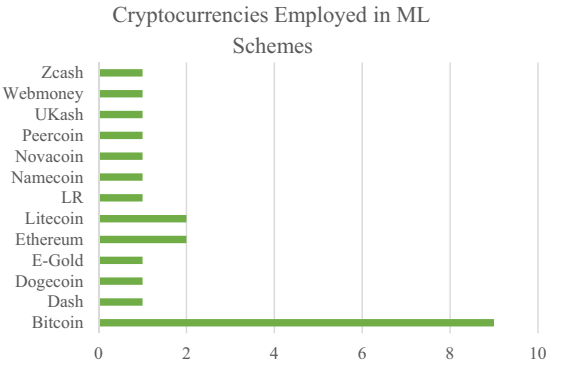

Figure 2.
Cryptocurrencies used in ML schemes

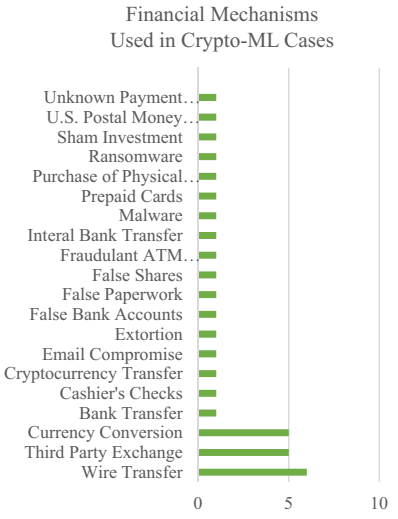

Figure 3.
Financial mechanisms used in crypto-ML cases

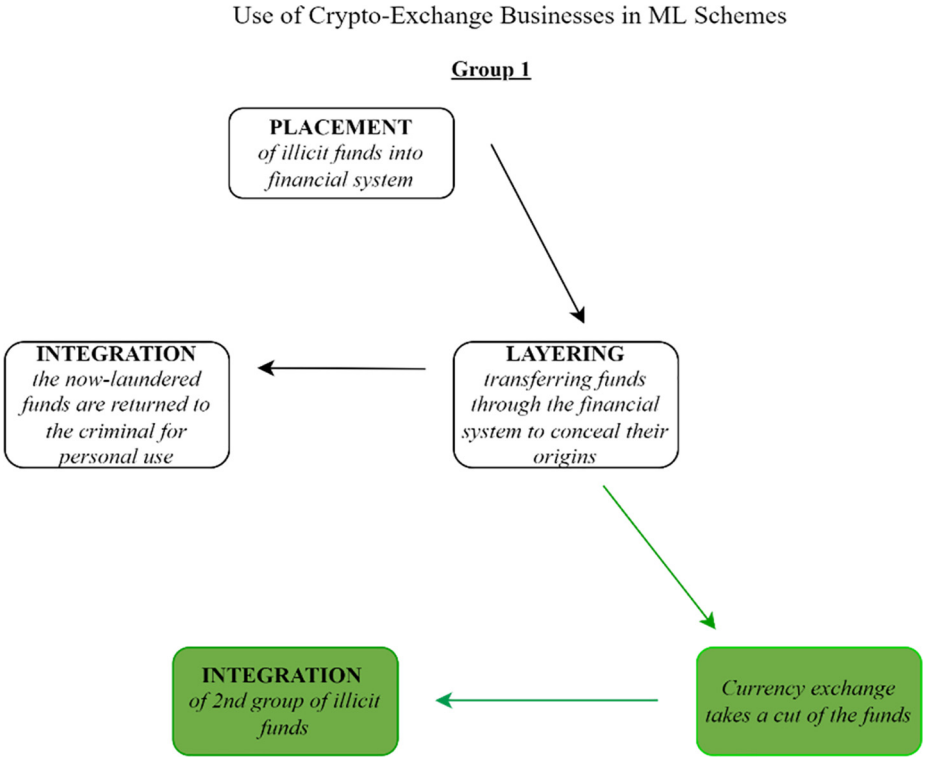

Figure 4.
Use of crypto-exchanges in ML schemes – Group 1

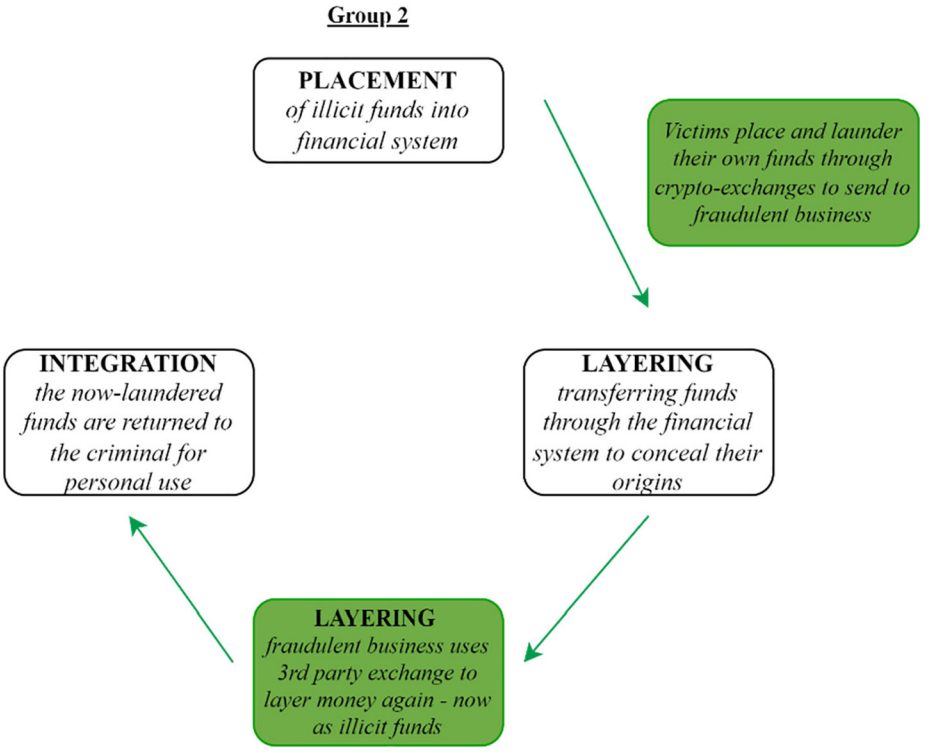

Figure 5.
Use of crypto-exchanges in ML schemes – Group 2

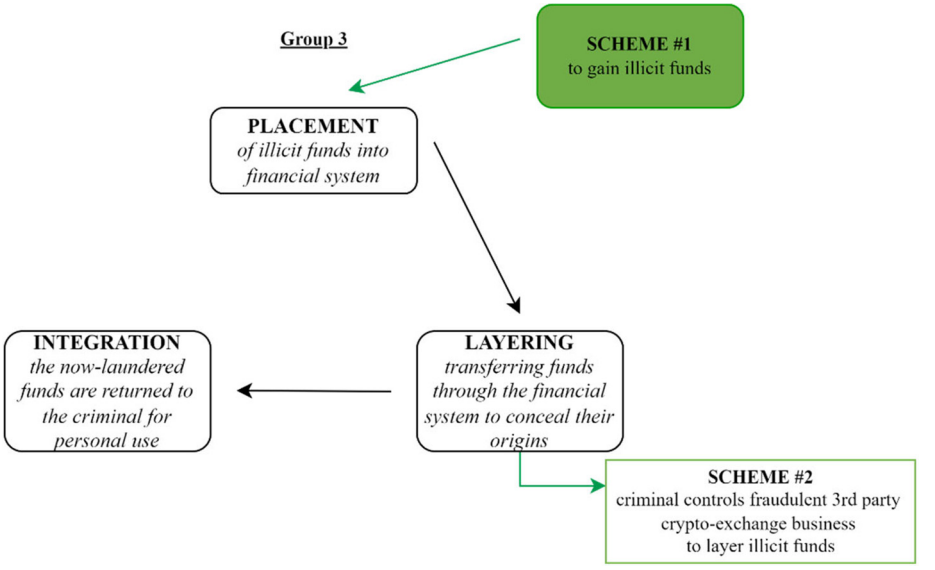

Figure 6.
Use of crypto-exchanges in ML schemes – Group 3

Auction Fraud Network ran secondary Bitcoin exchange businesses to convert funds gained from auction fraud schemes into cryptocurrency and hide their origins.

Finally, the fourth group of cases concerns cryptocurrency exchanges targeted as ML victims from external actors (Figure 7). In USA v. Yinyin and Jiadong, North Korean co-conspirators stole $48.5m worth of cryptocurrency from a South Korean virtual currency exchange business and subsequently laundered those funds through several other crypto exchanges, bypassing "know your customer" protocols with falsified documentation. According to a report from the North Korea Cyber working group at Harvard University, state-sponsored actors in North Korea have stolen approximately $316.4m in virtual assets between January 2019 and November 2020 (Kim *et al.*, 2022, p. 1). USA v. Yinyin and Jiadong is simply a representative case of a larger ongoing scheme.

All four groups of cases see the transfer of cryptocurrency between licit and illicit ventures. Although small, the data set clearly demonstrates the interconnectedness between legal and illegal economies: ill-gotten cryptocurrency was accepted by legitimate exchanges and banks, real investments and businesses were stolen from and fraudulent exchanges were operated in the same manner as their legitimate counterparts. As with the rest of the international economy, virtual currency's licit and illicit markets do not operate independently, and one must understand both to comprehend an industry as a whole.

Further, the cases analyzed in this sample substantiate that exchanges are a key component of transnational ML when criminals use cryptocurrency. In all 12 cases,

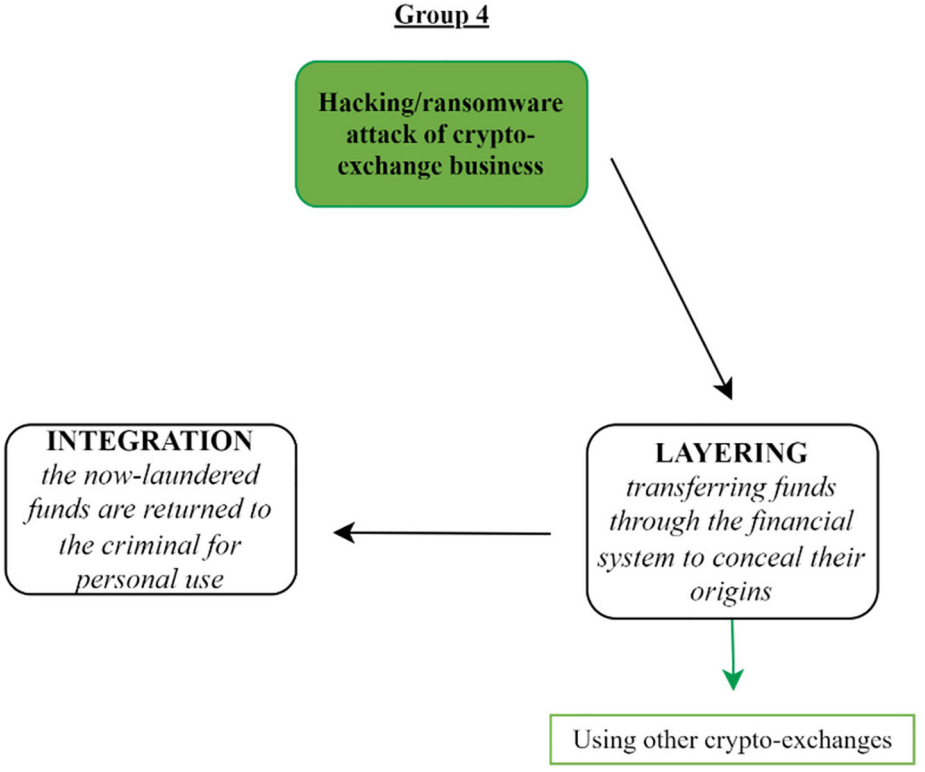

Figure 7.
Use of crypto-exchanges in ML schemes – Group 4

cryptocurrency was used in the placement stage, layering stage or both, which validates *H1*: that the use of cryptocurrency should be common in the placement and layering stages of ML. As anticipated, cryptocurrency allows for more anonymity and ease in transferring funds across borders.

Cryptocurrency is useful in the placement stage of ML because its high level of anonymity offsets the vulnerability associated with entering proceeds of crime into the legitimate economy. To conceal illicit funds, criminals can receive the proceeds of their crimes in cryptocurrency from the start. This is particularly effective for Web-based crimes such as hacking or ransomware. Criminals can also enter their funds into the economy by way of currency exchanges, as seen in the sample. By exchanging illegally acquired fiat currency into crypto coins, it is easier to begin layering the illicit funds to return them to the criminal in question. Although crypto exchanges across the world are required to implement "know your customer" procedures to prevent the transfer of illicit funds, this requirement can be circumvented in locations without strong regulatory bodies that closely govern the use and transfer of cryptocurrency.

Cryptocurrency is also useful for the layering stage of ML because of its virtual nature that puts it beyond the control of any one jurisdiction, which enables the transfer of funds internationally, the exchange of coins into other cryptocurrencies or fiat currencies, and its trade or investment. By using cryptocurrency, financial criminals can easily move their money across borders until the connection to the crime from which the funds derived is lost.

H1 holds that the use of cryptocurrency is more probable in the placement and layering stages of ML, rather than integration. As cryptocurrency is of limited use for everyday transactions, crypto is unlikely to be used as a method to return illicit funds to the criminal for legitimate use in the final stage of ML. A review of all countries in the sample where investors (including both criminals and victims) and recipients were located demonstrates the inaccessibility of cryptocurrency in everyday life. A majority of countries where illicit funds were invested or received had laws prohibiting cryptocurrency as a payment method or had unclear laws regarding their status. Due to these restrictions, it would be more beneficial for criminals to convert their illicit funds into fiat currency before returning the now "clean" money to themselves for personal use.

The limited functionality of cryptocurrency validates *H2*. A total of 3 out of 12 cases used only cryptocurrency in their ML scheme. Three quarters used a mix of cryptocurrency and fiat currency to steal and move funds. Although more countries are accepting crypto as mediums of exchange, its regular widespread use in tandem with fiat currency is some ways off. Money launderers thus receive both crypto and fiat currencies illegally and conceal their origins. The use of virtual currency expands opportunity for criminals to launder their illicit funds. However, given cryptocurrency's limited functionality, it would greatly limit ML opportunities if it were used alone; therefore, ML schemes involving cryptocurrency usually involve fiat currency as well.

Discussion: what does this mean for anti-money laundering regimes?

These findings have notable implications for AML regimes. Although many now incorporate cryptocurrency *pro forma*, in practice regimes falls short. AML regimes consist of different levels of regulation and enforcement. Some exist in a hierarchy while others work in tandem to identify and prevent acts of ML domestically and internationally. Canada's AML regime is an interesting example due to its alignment with international recommendations and its multitiered institutions that share the burden for ML prevention and prosecution. The introduction of crypto-laundering tests the flexibility and adaptability of such a multifaceted AML regime. Although the collected cases skew the data toward an

American legal context, the results are general enough to have global implications, especially for the Canadian AML. The following sections will identify existing levels of regulation in Canada's AML regime and analyze the implications of our findings.

Financial Action Task Force

The international Financial Action Task Force (FATF) is responsible for the promotion of policies that protect the global financial system from ML and TF. Recommendations by FATF are the global standard for AML/CTF measures. When FATF makes reports and recommends changes to a country's AML regime, if accepted, they are adopted as bills or as practice by national regulatory bodies.

By way of example, FATF's recommendations spurred significant change to Canada's AML approach at the turn of the new millennium: the creation of the Proceeds of Crime (ML) and Terrorist Financing Act (PCMLTFA) (Cooper and Stack, 2018). The PCMLTFA created a system for reporting suspicious financial transactions, established record keeping and client identification requirements for financial service providers, as well as established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) [Proceeds of Crime (Money Laundering) and Terrorist Financing Act c. 17, 2000]

Financial Transactions and Reports Analysis Centre of Canada and reporting entities

While the Department of Finance is responsible for Canada's AML regime, most of the work to combat ML/TF falls to Canada's Financial Intelligence Unit, FINTRAC. The aim of the Centre is to collect and analyze information to aid in the detection and prevention of ML/TF activities. To collect this information, FINTRAC receives reports from "mandatory reporting entities": financial institutions, money services companies, accountants, securities dealers, life insurance companies and casinos among other things. Akin to other AML regimes, the onus for ML prevention falls on the reporting entities. FINTRAC issues fines for non-compliance, requires reports to be submitted and training so that staff can identify potential ML/TF activity and understand mechanisms to report it (Cooper and Stack, 2018).

Financial Transactions and Reports Analysis Centre of Canada and partner agencies

The last level of regulation includes FINTRAC's partners at the federal and provincial levels to share intelligence and help enforce the PCMLTFA. Table 1 describes how each partner agency interacts with FINTRAC (Cooper and Stack, 2018).

Agency	Relationship to FINTRAC
Royal Canadian Mounted Police (RCMP)	Receives intelligence from FINTRAC to effectively prosecute individuals and entities engaging in ML/TF through their money laundering units (MIUs)
The Canadian Border Security Agency (CBSA)	Responsible for ensuring that anyone coming into or leaving the country with more than $10,000 in cash or monetary instruments files a proper report. Suspicious funds are seized and/or forfeited and this information is reported to the Centre. They collect the data and transfer it to the proper authorities
The Canada Revenue Agency (CRA)	Tax evasion is a common dimension of money laundering. When FINTRAC suspects the presence of tax or duty offense in their data, they relay that information to CRA's Enforcement and Disclosures Directorate
The Canadian Secret Intelligence Service (CSIS)	CSIS and FINTRAC share intelligence through reports and disclosures on actions that may be a threat to national security

Table 1. FINTRAC's partner agencies and their responsibilities

Canadian anti-money laundering and cryptocurrency

In 2016, Canada recognized virtual currency as part of its AML regime after the FATF had found Canada's AML measures on cryptocurrency wanting (Financial Action Task Force, 2016). Only in 2019 was virtual currency included in the PCMLTFA (Financial Transactions and Reports Analysis Centre of Canada, 2021). It states that those "dealing in virtual currencies," that is, virtual currency exchanges, digital wallet providers, value transfer services and the like, must register with FINTRAC and implement a robust compliance program. In addition, entities or people that receive more than $10,000 in cryptocurrency have to verify the identity of the entity that is the source of the funds, the identification number related to the funds and the transaction identifiers of the funds. Virtual funds received from another financial entity or public body are exempt (Abudulai, 2019). However, assessing the impact that these new regulations will have on the effectiveness of Canada's AML regime will take time: these amendments only came into effect in June of 2021 (Financial Transactions and Reports Analysis Centre of Canada, 2021).

New regulation under the PCMLTFA has brought virtual currency, including Bitcoin, within the scope of Canada's AML regime. The two main concerns from an AML standpoint are whether Bitcoin is regulated and the extent of law enforcement's knowledge to investigate and prosecute ML via Bitcoin, in light of its particular popularity as a cryptocurrency.

On the law enforcement side, the Royal Canadian Mounted Police (RCMP) and other investigative bureaus have taken steps to ensure that they are properly equipped to deal with Bitcoin. The RCMP has appointed a national cryptocurrency coordinator and implemented guidelines on the investigation and seizure of virtual assets. They offer training on all levels through courses on national financial crime, proceeds of crime, financial integrity and cybersecurity. The RCMP also collaborates with many partners to improve their awareness of cryptocurrency and its position in financial crime, including the National Cybercrime Coordination Centre (NC3). To improve the monitoring and investigation of the illicit use of Bitcoin, police departments across Canada have acquired software tracing tools that track the flow of funds (Cullen, 2020).

While the posture of law enforcement on Bitcoin is becoming more robust, alt-coins are a different story. Although Bitcoin is more popular, use of alt-coins features prominently in our sample. As law enforcement becomes more adept at tracing and monitoring the use of Bitcoin, criminals are likely to disperse to alt-coins that are more obscure with ledger technology that is more private. Tools used by law enforcement to track Bitcoin are limited in their ability to track private alt-coins (Cullen, 2020).

Third-party currency exchanges are another vulnerability. Although they have been brought under FINTRAC's regulatory framework, they remain vulnerable to exploitation by criminals for the purpose of ML.

First, the PCMLTFA requires transactions over $10,000 to have associated identification verification [Proceeds of Crime (Money Laundering) and Terrorist Financing Act c. 17, 2000]. Criminals can work around this requirement by exchanging smaller sums in and out of many crypto wallets. Because the onus for AML protocols is on these exchange businesses, they could simply lie about the suspicious activity of their clients. In USA v. Reynolds, funds were laundered out of a currency exchange in Vancouver. Canada, then, is not immune.

In USA v. BTC-e and USA v. Liberty Reserve, management flouted compliance laws to profit from laundering illicit funds. Law enforcement is able to track illicit crypto with the wallet addresses and key phrases provided by regulatory bodies, which in turn are provided

by currency exchanges. If businesses fail to comply with regulation, identifying those that launder funds through third-party exchange services becomes much more difficult.

The popularity of currency exchanges in financial crime calls into question whether money services businesses should be responsible for AML in the first place. Adrienne Vickery of the RCMP suggested that third-party exchanges should be eliminated entirely. He recommended that conversion to and from cryptocurrency should be organized through the Bank of Canada (Cullen, 2020). The Bank of Canada's Project Jasper experimented with distributed ledger technology to plan for a central bank digital currency should the need arise (Payments Canada, Bank of Canada and R3, 2017). It is thus possible to integrate virtual currency into the financial system instead of grafting it onto laws and regulation as an afterthought.

Another option is harsher punishments for non-compliance. Jail time and fines might deter third-party exchanges from the allure of criminal profit.

Conclusion

Although the study of the role of cryptocurrency in transnational ML is still in its infancy, sample cases can help us understand crypto-ML and the effectiveness of policies in countering it. Cross-case comparison of a sample of 12 cases of transnational crypto-ML in this study reveal two main conclusions. First, that Bitcoin is common among money launderers, though most also use some form of alt-coin. Second, the use of third-party currency exchanges is a prevalent method to create and hide illicit funds. The dozen cases also validate two hypotheses. Cryptocurrencies are used in the placement and layering stages of ML, rather than integration on account of their anonymity and ease of transfer, as well as the limitation as a method of payment in the legitimate economy. Second, because of this limitation of use, cryptocurrency will almost always be used alongside fiat currencies in ML schemes. The use of multiple currencies diversifies the illicit funds, which makes them harder to detect.

An assessment of Canada's AML posture on cryptocurrency revealed two important conclusions. First, although law enforcement is consistently improving on monitoring and understanding popular cryptocurrencies such as Bitcoin, they are challenged by alt-coins. Second, new regulations for third-party currency exchanges, though positive, are insufficient to deal with their use in criminal activity. The cases in this sample show that both owners of exchanges and independent money launderers are willing to use exchanges for proceeds of crime, irrespective of regulation. The article posits two possible ways to deter this activity: eliminate the need for third-party exchanges in AML regulation or punish non-compliance more thoroughly.

This article makes two contributions to this budding field of research. First, it expands the study of IIPE into more grounded, empirical evidence, while introducing cryptocurrency as a subject of study. It also develops an experimental method to study the illicit use of crypto notwithstanding limited access to cases and data. Among current debates on the cause of cryptocurrency's vulnerability to financial crime, this article demonstrates that currency exchanges and regulation more widely are to blame, rather than the technology itself. Current literature on crypto-ML is over-reliant on theory and limited previous literature. In introducing comparative empirical evidence to the investigation of crypto-ML patterns, this article makes an innovative contribution towards a more robust approach to the proliferating problem of crypto-ML. The findings are subject to subsequent scrutiny as more illicit crypto become available, including TF and drug smuggling, to paint a more fulsome picture of cryptocurrency's role in the Illicit International Political Economy.

References

Abudulai, S. (2019), "Amendments to the proceeds of crime (money laundering) and terrorist financing act", Cassels, available at: https://cassels.com/?export=pdfandpost_id=3016andforce

Adachi, D. and Aoyagi, J. (2020), "Blockchain and economic transactions", *Cryptocurrency and Blockchain Technology*, De Gruyter, Berlin, Boston, pp. 9-22, doi: 10.1515/9783110660807-002.

Albrecht, C., Duffin, K.M.K., Hawkins, S. and Morales Rocha, V.M. (2019), "The use of cryptocurrencies in the money laundering process", *Journal of Money Laundering Control*, Vol. 22 No. 2, pp. 210-216, doi: 10.1108/JMLC-12-2017-0074.

Andreas, P. (2004), "Review: Illicit international political economy: the clandestine side of globalization", *Review of International Political Economy*, Vol. 11 No. 3, pp. 641-652, doi: 10.1080/0969229042000252936.

Arasasingham, A. and DiPippo, G. (2022), "Cryptocurrency's role in the Russia-Ukraine crisis", Center for Strategic and International Studies, available at: www.csis.org/analysis/cryptocurrencys-role-russia-ukraine-crisis

Barone, R. and Masciandaro, D. (2011), "Organized crime, money laundering and legal economy: theory and simulations", *European Journal of Law and Economics*, Vol. 32 No. 1, pp. 115-142.

Beare, M. and Schneider, S. (2007), *Money Laundering in Canada: chasing Dirty and Dangerous Dollars*, University of Toronto Press, Toronto.

Campbell-Verduyn, M. (2018), "Laundering governance", *Crime, Law and Social Change*, Vol. 69 No. 2, pp. 283-305.

Chohan, U.W. (2017), "Assessing the differences in bitcoin and other cryptocurrency legality across national jurisdictions", *SSRN Electronic Journal*, doi: 10.2139/ssrn.3042248.

Cooper, T. and Stack, R. (2018), "A recent overview of anti-money laundering organizations within the United States, Canada and internationally", *Journal of Management Policy and Practice*, Vol. 19 No. 3, doi: 10.33423/jmpp.v19i3.53.

Criminal Intelligence Service Canada (2020), "National criminal intelligence estimate on the Canadian criminal marketplace: money laundering and fraud", available at https://cisc-scrc.gc.ca/media/2020/2020-09-28-eng.htm (accessed December 2021).

Cullen, A. (2020), "Commission of inquiry into money laundering November 23, 2020", available at: https://cullencommission.ca/data/transcripts/TranscriptNovember23,2020.pdf

Cullen, A. (2022), "Commission of inquiry into money laundering in British Columbia final report", available at: https://cullencommission.ca/files/reports/CullenCommission-FinalReport-Full.pdf

Custers, B., Oerlemans, J.J. and Pool, R. (2020), "Laundering the profits of ransomware; money laundering methods for vouchers and cryptocurrencies", *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 28 No. 2, pp. 121-152, doi: 10.1163/15718174-02802002.

Desmond, D.B., Lacey, D. and Salmon, P. (2019), "Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review", *Journal of Money Laundering Control*, Vol. 22 No. 3, pp. 480-497, doi: 10.1108/JMLC-10-2018-0063.

Ducas, E. and Wilner, A. (2017), "The security and financial implications of blockchain technologies: regulating emerging technologies in Canada", *International Journal: Canada's Journal of Global Policy Analysis*, Vol. 72 No. 4, pp. 538-562, doi: 10.1177/0020702017741909.

Dupuis, D. and Gleason, K. (2021), "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, Vol. 28 No. 1, pp. 60-74, doi: 10.1108/JFC-06-2020-0113.

Dyntu, V. and Dykyi, O. (2018), "Cryptocurrency in the system of money laundering", *Baltic Journal of Economic Studies*, Vol. 4 No. 5, pp. 75-81.

Egan, M. (2018), "A bit(coin) of a problem for the EU AML framework", in King, E., Walker, C. and Gurulé, J. (Eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Palgrave MacMillan, Cham, pp. 183-208.

Farrugia, S., Ellul, J. and Azzopardi, G. (2020), "Detection of illicit accounts over the Ethereum blockchain", *Expert Systems with Applications*, Vol. 150, p. 113318, doi: 10.1016/j.eswa.2020.113318.

Ferwerda, J., van Saase, A., Unger, B. and Getzner, M. (2020), "Estimating money laundering flows with a gravity model-based simulation", *Scientific Reports*, Vol. 10 No. 1, pp. 1-11, doi: 10.1038/s41598-020-75653-x.

Financial Action Task Force (2014), "Virtual currencies – key definitions and potential AML/CFT risks", available at: www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Financial Action Task Force (2016), "Anti-money laundering and counter-terrorist financing measures – Canada", available at: www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf

Financial Transactions and Reports Analysis Centre of Canada (2021), "Notice on forthcoming regulatory amendments and flexibility", Financial Transactions and Reports Analysis Centre of Canada", available at: www.fintrac-canafe.gc.ca/covid19/flexible-measures-eng

Foley, S., Karlsen, J.R. and Putniņš, T.J. (2019), "Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", *The Review of Financial Studies*, Vol. 32 No. 5, doi: 10.1093/rfs/hhz015.

German, P.M. (2018), "Dirty money: an independent review of money laundering in lower mainland casinos conducted for the attorney general of British Columbia", available at: https://news.gov.bc.ca/files/Gaming_Final_Report.pdf

German, P.M. (2019), "), turning the tide – an independent review of money laundering in B.C. Real estate, luxury vehicle sales and horse racing", available at: https://cullencommission.ca/files/Dirty_Money_Report_Part_2.pdf

Greenberg, A. (2018), "The dark web's favorite currency is less untraceable than it seems", *Wired*, available at: www.wired.com/story/monero-privacy/

Greenberg, A. (2022), "Inside the bitcoin bust that took down the web's biggest child abuse site", *Wired*, available at: www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

Hayes, A. (2019), "The socio-technological lives of bitcoin", *Theory, Culture and Society*, Vol. 36 No. 4, doi: 10.1177/0263276419826218.

Hudson, R. (2005), *Economic Geographies: Circuits, Flows and Spaces*, Sage, London.

Hudson, R. (2013), "Thinking through the relationships between legal and illegal activities and economies: spaces, flows and pathways", *Journal of Economic Geography*, Vol. 14 No. 4, pp. 775-795.

Hudson, R. (2019), "Economic geographies of the (il)legal and the (il)licit", *A Research Agenda for Global Crime*, Edward Elgar Publishing, Cheltenham, pp. 1-27, doi: 10.4337/9781786438676.00007.

Hughes, S.J. (2019), "Gatekeepers' are vital participants in anti-money-laundering laws and enforcement regimes as permission-less blockchain-based transactions pose challenges to current means to 'follow the money'", *SSRN Electronic Journal*, Vol. 408, doi: 10.2139/ssrn.3436098.

Kethineni, S. and Ying, C. (2020), "The rise in popularity of cryptocurrency and associated criminal activity", *International Criminal Justice Review*, Vol. 30 No. 3, pp. 325-344, doi: 10.1177/1057567719827051.

Kim, H.M. Lee, J. and Paik, R. (2022), "North Korean cryptocurrency operations: an alternative revenue stream", Belfer Center for Science and International Affairs, available at: www.belfercenter.org/sites/default/files/files/publication/North%20Korean%20Cryptocurrency%20Operations%20-%20An%20Alternative%20Revenue%20Stream.pdf

Kumru, C. (2021), "2021 in review: El Salvador's bitcoin experiment", *Australian Institute of International Affairs*, available at: www.internationalaffairs.org.au/australianoutlook/el-salvadors-bitcoin-experiment/

Legrand, T. and Leuprecht, C. (2021), "Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy", *Policy and Society*, Vol. 40 No. 4, pp. 565-586, doi: 10.1080/14494035.2021.1975216.

Leuprecht, C., Cockfield, A., Simpson, P. and Haseeb, M. (2019), "Tracking transnational terrorist resourcing nodes and networks", *Tracking Transnational Terrorist Resourcing Nodes and Networks*, Vol. 46 No. 2, pp. 289-344, available at: https://qspace.library.queensu.ca/handle/1974/29837

Leuprecht, C., Walther, O., Skillicorn, D. and Ryde-Collins, H. (2017), "Hezbollah's global tentacles: a relational approach to convergence with transnational organized crime", *Terrorism and Political Violence*, Vol. 29 No. 5, pp. 902-921, doi: 10.1080/09546553.2015.1089863.

Mabunda, S. (2018), "Cryptocurrency: the new face of cyber money laundering", *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (ICABCD)*.

Mancini, N. (2016), "Bitcoin: Risks and regulatory problems", *Banca Impresa Societa*, Vol. 35 No. 1, pp. 111-140, doi: http://dx.doi.org.proxy.queensu.ca/10.1435/83801.

Maume, P. and Fromberger, M. (2019), "Regulation of initial coin offerings: reconciling U.S. and E.U. securities laws", *Chicago Journal of International Law I*, pp. 548-586.

Neagu, O.M. (2019), "The cryptocurrency as a recent facilitator for money laundering", *Vision 2025: Education Excellence and Management of Innovations through Sustainable Economic Competitive Advantage*, pp. 1537-1542.

Ogunbadewa, A. (2014), "The bitcoin virtual currency: a safe haven for money launderers?", *SSRN Electronic Journal*, doi: 10.2139/ssrn.2402632.

Parkin, J. (2020), "Pandora's blocks", *Money Code Space: Hidden Power in Bitcoin, Blockchain, and Decentralisation*, Oxford University Press, New York, NY, pp. 12-30, doi: 10.1093/oso/9780197515075.001.0001.1

Payments Canada, Bank of Canada, and R3 (2017), "Jasper: a Canadian experiment with distributed ledger technology for domestic interbank payments settlement", pp. 1-66, available at: www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf

Proceeds of Crime (Money Laundering) and Terrorist Financing Act c. 17 (2000), available at: https://lois-laws.justice.gc.ca/eng/acts/P-24.501/

Ryner, J.M. (2006), "International political economy: beyond the poststructuralist/historical materialist dichotomy", in De Goede, M. (Ed.), *International Political Economy and Poststructural Politics*, Palgrave Macmillan, London, pp. 139-156.

Sanchez, E.G. (2017), "Crypto-currencies: the 21st century's money laundering and tax havens", *University of Florida Journal of Law and Public Policy*, Vol. 28, pp. 167-192.

Shovkhalov, S. and Idrisov, H. (2021), "Economic and legal analysis of cryptocurrency: scientific views from Russia and the Muslim world", *Laws*, Vol. 10 No. 2, pp. 32-48, doi: 10.3390/laws10020032.

The High-Level Panel on International Financial Accountability Transparency and Integrity for Achieving the 2030 Agenda (2020), "FACTI Panel Interim Report", available at: https://uploads-ssl.webflow.com/5e0bd9edab846816e263d633/5f6b91b197c6c0d8904089c2_FACTI_Interim_Report_ExecutiveSummary.pdf

Trzcionka, M. (2019), "The bitcoin – democratic money in a neoliberal economy", *Ad American*, Vol. 19, pp. 155-173, doi: 10.12797/adamericam.19.2018.19.11.

Turpin, J.B. (2014), "Bitcoin: the economic case for a global, virtual currency operating in an unexplored legal framework", *Indiana Journal of Global Legal Studies*, Vol. 21 No. 1, pp. 335-368, doi: 10.1353/gls.2014.0004.

World Economic Forum (2015), "State of the illicit economy briefing papers", available at: www3.weforum.org/docs/WEF_State_of_the_Illicit_Economy_2015_2.pdf

Further reading

Barsan, I.M. (2019), "Public blockchains: the privacy-transparency conundrum", *Doctrine*, Vol. 2, pp. 44-53.

Bergström, M. (2018), "Legal perspectives on money laundering", in Mitsilegas, V., Hufnagel, S. and Moiseienko, A. (Eds), *Research Handbook on Transnational Crime*, Edward Elgar Publishing, Cheltenham, pp. 98-111.

Chu, D. (2018), "Broker-dealers for virtual currency: regulating cryptocurrency wallets and exchanges", *Columbia Law Review*, Vol. 118 No. 8, pp. 2323-2360.

Custers, B., Pool, R.L.D. and Cornelisse, R. (2019), "Banking malware and the laundering of its profits", *European Journal of Criminology*, Vol. 16 No. 6, pp. 728-745, doi: 10.1177/1477370818788007.

Dostov, V. and Shust, P. (2014), "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?", *Journal of Financial Crime*, Vol. 21 No. 3, pp., pp. 249-263, doi: 10.1108/JFC-06-2013-0043.

Maleta, N. and Stipanovic, I. (2018), "Difficulties in procedure of obtaining evidence on money laundering through cryptocurrencies as a possible threat to the market stability", *Economic and Social Development: Book of Proceedings*, pp. 589-598.

Maloney, M., Somerville, T. and Unger, B. (2019), "Combatting money laundering in BC Real Estate Combatting Money Laundering Report", available at: https://cullencommission.ca/files/Combatting_Money_Laundering_Report.pdf

Miladinovic, J.S. (2018), "Bitcoin – its condition and tendencies", *Ekonomika*, Vol. 64 No. 4, pp. 109-120, doi: 10.5937/ekonomika1804107S.

Novak, M. (2020), "Crypto-friendliness: understanding blockchain public policy", *Journal of Entrepreneurship and Public Policy*, Vol. 9 No. 2, pp. 165-184, doi: 10.1108/JEPP-03-2019-0014.

O'Sullivan, A. (2018), "Ungoverned or anti-governance? How bitcoin threatens the future of Western institutions", *Journal of International Affairs*, Vol. 71 No. 2, pp. 90-102.

Teichmann, F.M. and Falker, M.C. (2020), "Money laundering via underground currency exchange networks", *Journal of Financial Regulation and Compliance*, Vol. 29 No. 1, pp. 1-14, doi: 10.1108/JFRC-01-2020-0003.

Wronka, C. (2021), "Money laundering through cryptocurrencies-analysis of the phenomenon and appropriate prevention measures", *Journal of Money Laundering Control*, Vol. 25 No. 1, doi: 10.1108/JMLC-02-2021-0017.

Appendix

Table A1.
Cases from sample

Case	Jurisdiction	Year
People v. Western Express Inc	USA	2012
USA v. Ulbricht	USA	2014
USA v. Liberty Reserve *et al.*	USA	2013
USA v. Jones *et al.*.	USA	2020
USA v. Stoica *et al.*	USA	2018
USA v. 113 Virtual Accounts	USA	2020
USA v. Vinnik	USA, France	2017
USA v. Ponle	USA, United Arab Emirates	2020
USA v. Karlsson	USA	2020
USA v. Faiella and Shrem	USA	2014
USA v. Hyok *et al.*	USA	2020
Commodity Futures Trading Commission v. Reynolds *et al.*	USA	2019

Corresponding author
Christian Leuprecht can be contacted at: christian.leuprecht@queensu.ca