12-2021

Contactless, Crypto, and Cash: Laundering Illicit Profits in the Age of COVID-19

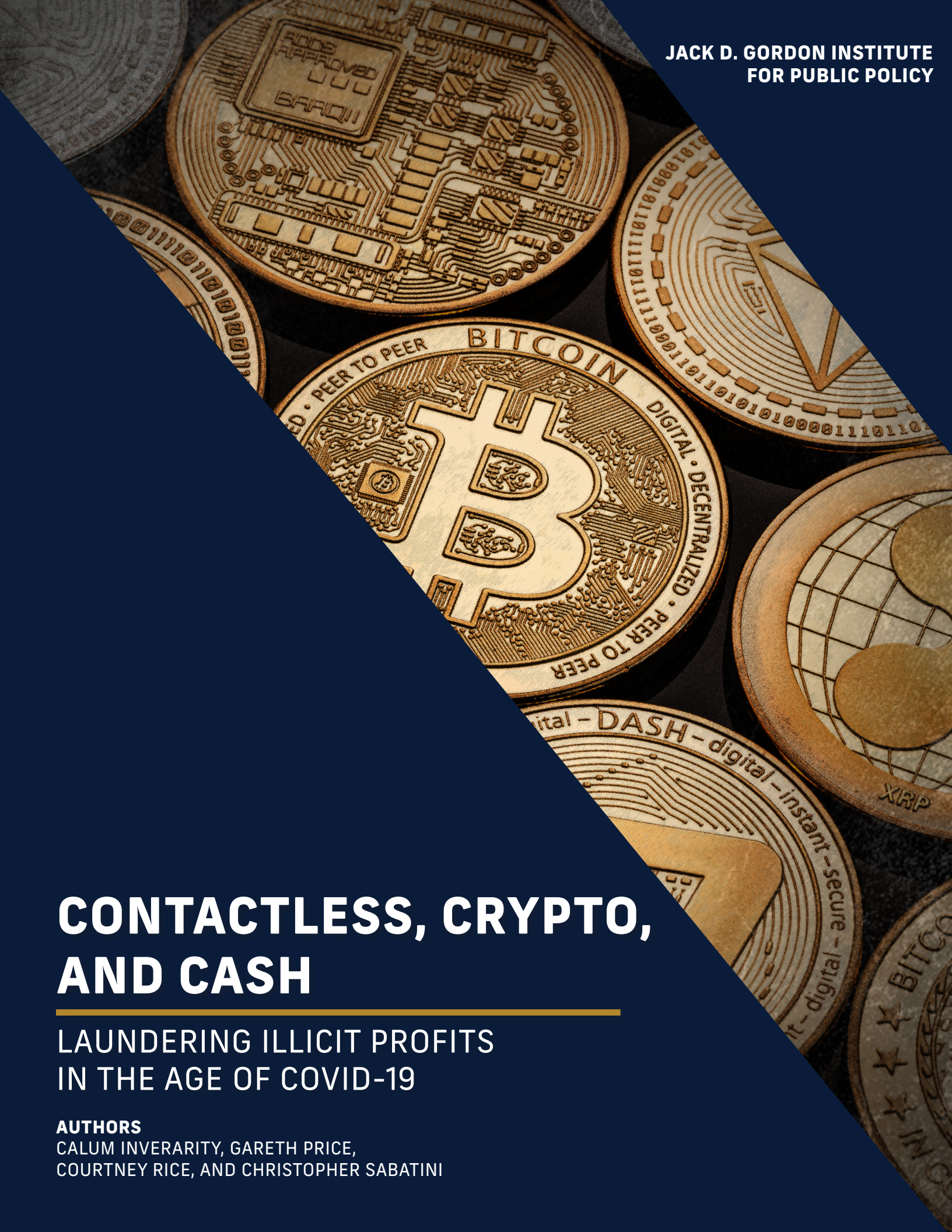
Calum Inverarity

Gareth Price

Courtney Rice

Christopher Sabatini

JACK D. GORDON INSTITUTE
FOR PUBLIC POLICY



CONTACTLESS, CRYPTO, AND CASH

LAUNDERING ILLICIT PROFITS IN THE AGE OF COVID-19

AUTHORS
CALUM INVERARITY, GARETH PRICE,
COURTNEY RICE, AND CHRISTOPHER SABATINI

DECEMBER 2021

The Jack D. Gordon Institute for Public Policy, part of FIU's Steven J. Green School for International & Public Affairs was founded in 1985 to establish, promote, and advance the study of public policy and national security studies. The Gordon Institute serves as the forefront of public policy discourse by leading, integrating, and delivering exceptional multidisciplinary education and research while improving the competitiveness and diversity of students and professionals entering the workforce. The Gordon Institute is centered on four pillars: Academics, Professional Education, Research, and Community Outreach, each serving the mission of shaping public policy and national security solutions in the 21st century.

This publication is in partnership with

CHATHAM HOUSE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Travel restrictions and lockdowns have forced changes to the traditional means illicit groups have used to launder their ill-gotten profits. This paper explores whether COVID-19 may have affected these processes through three main channels:

1. Increased reliance on cryptocurrencies to move and launder funds tied to illicit activity;
2. The expanded use of the internet through e-commerce sites to continue and expand trade mispricing practices to move illicit funds; and,
3. The use of FinTech and peer-to-peer payment services to transfer illicit funds.

For now, at least, the pandemic's impact on money laundering appears to have been more balanced. Despite many traditional means of laundering money—such as through casinos or high cash turnover businesses—being closed to criminals, there has not yet been a detectable, significant jump in the use of cryptocurrencies or FinTech in money laundering.

Where there is more evidence of an increase in likely illicit activity is in e-commerce. Trade mispricing in person-to-person transactions is a commonly used technique. Increasingly, however, that has moved to online commerce, a trend that has increased under COVID-19 as global trade and supply chains were disrupted by the pandemic and economic contraction.

Nevertheless, the implications of the COVID-19 pandemic on the global economy, markets, commercial relations, global supply chain, and daily life of citizens will be felt for years to come. The same is true of the virus's effects on illicit markets and money laundering. Changes in the structure of global financial markets had already started before the pandemic but have been accelerated by the events of 2020. For these reasons, there a number of areas that governments and anti-money laundering groups will need to focus on in the coming years.

Continue to monitor new trends in virtual and electronic markets and finance.

Given the accelerated growth of online commerce and peer-to-peer finance in daily life, these innovations and tools will likely influence criminal transactions. In short, it will be necessary when monitoring and prosecuting illicit activity not to assume that it will be business as usual following 2021.

Update and tighten the regulation and monitoring of FinTech and Cryptocurrencies.

While Bitcoin and the other cryptocurrencies have not translated into as large and central a market as many imagined for illicit transactions before COVID-19, the need to push financial transactions and money laundering to virtual means or hold on to cash indicate the move toward these platforms may just be beginning.

In cryptocurrency markets, focus on known over the counter brokers.

As researchers and law enforcement officials identify the owners of cryptocurrency wallets used by criminals, they should share that information through international law enforcement and financial agencies such as Interpol, Europol, and the Financial Action Task Force (FATF). Such an effort could create an alert system, similar to Interpol's red list for wanted international criminals, but dedicated to known wallets and brokers engaging in illicit transactions.

Upgrade government capacity to track and understand the cryptocurrency world.

Anti-money laundering software that helps officials identify potential sites and transactions related to money laundering—based on tested high-risk areas, transactions, and wallets—can help track and capture or at least shut down bad actors in the rapidly-changing cryptocurrency ecosystem.

Work with China to identify and shut down money-laundering operations.

Given China's growing global network and footprint commercially and financially, a desire to project itself as a legitimate economic actor will work to the advantage of regulators and law enforcement agencies that combat money laundering.

INTRODUCTION

Successful international criminal groups are innovative and highly adaptable. Smuggling routes and methods adjust according to circumstances—tightened security on one border crossing will encourage the exploration of alternative routes or new methods altogether. Criminal organizations are adept at finding and exploiting the weakest link to achieve their means, adapting to the latest developments, and identifying opportunities that law-abiding citizens may never have considered possible.

These characteristics apply equally to money laundering, the process by which proceeds from illicit activities are "cleaned" and made available for use in legitimate society. Criminal groups launder funds through various means and methods, assessing simplicity, speed, cost, and risk. Clearly, this varies in each situation and from country to country, according to the legal framework and the country's capacity to police it. However, as a guiding principle, the tightening of one loophole encourages criminals to find alternative means of cleaning their illicit profits.

The COVID-19 pandemic and the associated response by governments have led to potential shifts in criminal behavior, including money laundering. The closure of small businesses and borders and disruptions of trade flows during national lockdowns has presented a challenge for criminal entities in many better-policed jurisdictions, forcing some to warehouse rather than launder cash, putting them at greater risk.

Others have attempted to launder funds through the purchase and sale of high-value goods, such as real estate or precious gems. These options are not without risk at the best of times, particularly as traditional means to launder money and how to spot and counter them are well known by law enforcement agencies the world over. However, during the COVID-19 pandemic, and following the introduction of the associated policies intended to contain its spread, the risks to these criminal groups were potentially reduced since the drastic and rapid change to working practices may have reduced the capacity of law enforcement and regulators assigned to monitor, investigate, and prosecute potential money-laundering activity.[1]

In addition to the impact on day-to-day activities, the pandemic may well have exacerbated or expedited pre-existing trends whereby criminal organizations were seeking to exploit e-commerce businesses and use cryptocurrencies to launder funds. With restrictions on physical movement in place, it is probable that greater attention has shifted to this method.

This Chatham House paper provides a comparison of the likely trends used by criminal groups to launder their illicit profits in light of the COVID-19 pandemic by drawing on publicly available information and firsthand interviews. The pages that follow examine the availability and use of cryptocurrencies for money laundering, including whether their role is a viable medium to transfer and launder monies for and from illicit commerce. The paper also explores the potential and use of virtual marketplaces, especially shared-economy and peer-to-peer commercial and financial platforms, as a means for laundering illicit profits and the potential role of peer-to-peer and contactless systems through FinTech for illicit transactions. Lastly, the paper returns to the more traditional means of shadow banks and trade-based money laundering and whether COVID-19 and other tech options have shifted those patterns of use. In doing so, we examine trends globally and provide policy recommendations for U.S. and Latin American policymakers.

Based on these new and traditional tools and platforms for money laundering and changes in their use, the paper concludes with a series of recommendations, including ways that national and international judicial and security organizations can better understand and track emerging and older trends in money laundering. The paper also discusses the implications for better tightening regulations on cryptocurrency transactions by national and international author-

ities, improving oversight of e-commerce and trade mispricing, and understanding and interrupting shadow banking networks organized around Chinese commerce.

BACKGROUND

There are several ways that COVID-19 has raised the risk for illicit activity. The pandemic presented new criminal opportunities relating to the provision of medical equipment and numerous scams and cyberattacks.[2] For instance, the increased number of remotely performed transactions coupled with a rising number of inexperienced users, such as the elderly, resulted in a rapid escalation in online financial fraud.[3] Government responses such as bailouts have also presented opportunities for fraud and theft, possibly helped by the work-from-home regimes that may have made money-laundering tracking activities more difficult. That large numbers of individuals are working from home has also presented new opportunities relating to the increased use of internet shopping and banking.[4] At the same time, the global economic slowdown and the spike in unemployment—especially in Latin America and the Caribbean—may have resulted in a greater propensity for criminal activity to compensate for economic insecurity and loss of income. Previously legitimate businesses struggling because of the pandemic may, for instance, be tempted to receive payment for moving funds through their accounts. Some criminal groups also appear to have targeted elderly individuals who are out of work to act as "money mules," laundering money through their accounts for a small fee.[5]

Changing behavior in the population at large may also have facilitated criminal behavior. For example, a dramatic shift toward contactless payments to avoid viral transmission may well have made it more difficult to distinguish between legitimate and illegitimate activity. The pandemic appears to have expedited a pre-existing trend in the general economy whereby criminals may accept card payments for illicit goods.

But other impacts of the pandemic have been negative for criminals and forced them to adopt riskier behaviors. Travel restrictions have forced changes to smuggling methods, preventing the use of drug mules. They have also made it harder to physically move cash overseas. In line with national lockdowns, the temporary closure of numerous legitimate businesses previously used to launder cash—restaurants, sports clubs, and other cash-dominated businesses, as well as casinos—has forced criminal groups to warehouse cash or launder funds through purchasing high-value items such as jewelry, precious metals, boats and vehicles, and real estate, evidenced through the increased quantity and volume of cash seizures.[6]

The question is, to what extent have these processes been altered by the COVID-19 pandemic and the associated response by governments? As typically defined, money laundering is comprised by a three-step process:

- **Placement** of illicit profits into the banking system or, more generally, moving funds away from their original cash source into another form (includes purchasing of luxury goods such as valuable artwork and antiques, bonds, lottery tickets, etc.).
- **Layering,** to disguise the funds from the original source. In this instance, launderers move funds between accounts to hinder the audit trail. This step is often repeated multiple times to further obscure attempts to locate the source of the illicit profits.
- **Integration,** in which illegal proceeds are reintegrated into the legitimate financial system for assimilation with other assets in the system and reunited with the launderer.

We hypothesize that COVID-19 may have affected these processes through three main channels:

- Increased reliance on cryptocurrencies to move and launder funds tied to illicit activity;[7]
- The expanded use of the internet through e-commerce sites to continue and expand trade mispricing practices to move illicit funds;[8] and
- The use of FinTech and peer-to-peer payment services to transfer funds.[9]

The logic for the increased use of more impersonal internet and mobile systems for illegal activities that don't involve face-to-face exchange, including but not limited to money laundering, certainly exists given the limited economic activity and restrictions on personal contact and travel associated with COVID-19. These restrictions would have limited the opportunities to move and launder cash through more traditional means, such as trade mispricing, retail operations, or through casinos, "money mules," and shell companies.

In the years leading up to the COVID-19 pandemic, user sharing economies and markets (such as eBay, Airbnb, and others), cashless payment methods and peer-to-peer payment systems (such as Venmo), and the spread of the number and use of cryptocurrencies had grown. A 2017 Brookings Institution study concluded that, by 2025, the sharing economy would grow to US$335 billion.[10] At the same time, cashless payments had already increased. According to a late 2021 YouGov survey in 21 countries, 74 percent of citizens in Sweden had already turned away from cash to digital means of payment before the pandemic. While Swedish consumers are the most plugged into FinTech, 60 percent of Chinese individuals polled report that they too rely on the internet and virtual platforms for commerce and financial transactions, as do 59 percent of those in Denmark, and 46 percent in the United States.[11]

Some of these platforms were exploited for illicit activities and money laundering even before the pandemic.[12] The emergence, expansion of options, and increased use of cryptocurrencies have also provided a virtual means of conducting illicit commerce and laundering money. While the scope of the use of cryptocurrencies for large-scale, massive money laundering outside the dark web has been disputed, the general opinion is that cryptocurrencies and different means of hiding the identity of those conducting the transactions have provided a new potent vehicle for illicit financial transactions.[13] As the Global Financial Action Task Force of Latin America (GAFILAT) states, "the use of virtual currencies such as Bitcoin have made detecting the illegal transfer of money ever more difficult. Moreover, the use of proxy servers and anonymizing software makes the third component of money laundering—integration—almost impossible to detect, as money can be transferred or withdrawn leaving little or no trace of an IP [Internet Protocol] address."[14] Some of this, as discussed below, is debatable, as is the scope of the illicit activities relative to other more legitimate investors and investments.

At least it was until the COVID-19 pandemic. Despite the advances in internet access and reliability, the e-economy, FinTech, and cryptocurrencies—cash and the U.S. dollar in particular—remained central to the black market and criminal economies. According to the American Institute for Economic Research, "more than a third of all U.S. currency in circulation is used by criminals and tax cheats."[15]

In the first quarter of 2020, as we witnessed the start of the lockdowns globally, cash withdrawals rose as individuals prepared for the unexpected. According to the FATF, the periods approaching potential lockdowns saw spikes in the withdrawal of cash from accounts.[16] While the vast majority of those withdrawals were for legitimate reasons, the sudden jump of cash in circulation provides several options for money laundering. For example, at the start of COVID-19, the FATF warned that "When financial markets stabilize, large movements to redeposit funds could provide cover to efforts at laundering illicit funds, including banknotes."[17] Similarly, the FATF speculated that "[b]anknotes can be used to purchase safe-haven assets (e.g., gold), which are less easily traceable."[18] The report continues that later, customers involved in illicit withdrawal or transitions of cash could mask those by citing them as COVID-19 related activities.

Nevertheless, according to the YouGov survey, COVID-19 accelerated the global shift to more cashless societies.[19] In a chart titled, "The pandemic speeds up the decline of cash globally," YouGov details the steep drop in the use of cash in 21 countries in favor of electronic payments, adding to the base of those who were already primarily relying on these means. For example, 50 percent of those surveyed in the United Kingdom said they had curtailed their use of cash since the onset of the COVID-19 pandemic, "while 37% already mostly paid digitally."[20] Certainly, the closure of retail banks and the increased reliance by retailers and vendors on cashless payments accelerated the trend.

For these reasons, the FATF issued a set of warnings in mid-2020 concerning the impact of COVID-19 on financial regulation and anti-money laundering. Several of them directly addressed the risks associated with the internet, cashless transactions, and cryptocurrencies. The FATF raised red flags on the following issues:

- "With global trade volumes in decline and individual travel at a near standstill, conventional transnational organised crime schemes that take advantage of global supply chains and the traditional illicit revenue schemes of organised crime groups are impacted by COVID-19." [21]
- "Reporting indicates significant changes in financial behaviours and patterns in light of COVID-19. Many bank offices and branches are closed due to public health and 'lockdown' measures. Customers are therefore carrying out more transactions remotely. Over the medium to long-term, an economic downturn could further alter financial activities and result in individuals seeking financing outside the formal economy."[22]
- "Increased remote transactions: FATF and FSRB [FATF-Style Regional Bodies] members report that some banks have closed their physical branches, reduced opening hours or restricted the services available in-person. Members also report increased online banking activities, including customer on-boarding and identity verification. Some supervisors have clarified that, in line with a risk-based approach, banks can postpone certain elements of customer identity verification during confinement periods. However, FATF and FSRB members note that some financial institutions may not be equipped to verify customers' identity remotely."[23]

The FATF also mentioned the case of one individual who used virtual assets to launder proceeds earned from selling fraudulent COVID-19 medicine.[24] These risks were compounded by the restrictions on in-person and in-office work. According to the FATF:

- The COVID-19 pandemic is also impacting government and private sector abilities to implement anti-money laundering and counterterrorist financing obligations from supervision, regulation, and policy reform to suspicious transaction reporting and international cooperation.
- These threats and vulnerabilities represent emerging money laundering and terrorist financing risks. Such risks could result in:
    - Criminals finding ways to bypass customer due diligence measures;
    - Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
    - Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;
    - Increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;
    - Misuse and misappropriation of domestic and international financial aid and emergency funding; and
    - Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.[25]

Now, more than 20 months since the threat of COVID-19 became a public concern, how many of these warnings have come to pass? The short answer is that it is still too early to tell. This is due, in part, to the gaps in administration, research, and reporting mentioned above that have made tracking and reporting difficult. It is also too soon to draw conclusions about any emerging patterns, especially since any picture of the flow of illicit goods and services against which to compare expectations of financial transactions and laundering is incomplete. According to several incomplete studies, while drug use may have shifted in terms of the type of drug, it did not decline significantly. While social distancing and lockdowns complicated illic-

it drug trafficking and the street sale of drugs, the consumption of stimulating and "socializing or party" drugs likely declined, though the use of psychoactive or other drugs may have increased.[26] These data and reporting gaps also complicate the ability to project COVID-19 linked trends to the future.

Despite these limitations, it is still possible to infer some trends and possible impacts that can lead to several limited recommendations. As discussed in the concluding section, the uniqueness and novelty of the convergence of these new financial technologies with the human, commercial, financial, and economic impact of the COVID-19 pandemic present a growing number of challenges that will require greater international collaboration to overcome. Among them are the proliferation and use of "mixers" or "tumblers" to hide the identity of those using of cryptocurrencies for illegal activities and the increasing use of online or shared economy commercial platforms for trade-based money laundering.

ARE CRYPTOCURRENCIES A SIGNIFICANT VEHICLE FOR MONEY LAUNDERING OR IS CASH STILL KING? THE TECHNICAL ACADEMIC AND POLICY DEBATES

The extent to which cryptocurrencies, from the better-known Bitcoin and Ethereum to other lesser-known and circulated cryptoassets,[27] are and can be used to facilitate illicit transactions has been hotly debated by policymakers, financial analysts, law enforcement officials, and scholars. Of these cryptocurrencies (also known as virtual assets), Bitcoin is the dominant player. It was the first significant cryptocurrency of its type and, in 2018, accounted for 66 percent of the more than 2,000 cryptocurrencies.[28]

Certainly, Bitcoin and other cryptocurrencies have received their fair share of attention and accusations from policymakers and journalists, including in July 2018 when Federal Reserve Chairman Jerome Powell told the U.S. Congress that such virtual assets are "great" for money laundering.[29] Many of them have properties that would lend them to becoming the preferred source of asset for illicit transactions, including money laundering. While traditional transfers that must pass through a trusted third-party institution—such as a bank—can be slow and cumbersome (made so, in part, because of national and international regulations intended to alert authorities of cash flow suspected to be linked to terrorism and illicit commerce), transfers via cryptocurrency can be made anytime. Transactions are, on average, approved every 10 minutes, according to tech entrepreneur and author Andreas Antonopoulos,[30] and the fees are relatively cheap, especially compared to transfer fees charged by traditional banks. Without a third-party broker, cryptocurrency transactions are decentralized and conducted through self-enrolled participants by creating one's own key pair, a combination of a public key used to encrypt data and a private key used to decrypt it. The decentralized system allows transactions to be conducted with a certain degree of anonymity outside the rules and oversight of financial institutions subject to anti-money laundering regulations and law enforcement, including know-your-customer requirements and the automatic investigation into transfers over certain thresholds.[31]

Despite the decentralized structure for transfers, Bitcoin and most major cryptocurrencies have not turned out as anonymous as initially thought. For this reason, Bitcoin and other cryptocurrencies are increasingly referred to as pseudonymous rather than anonymous. User passkey information required for transactions needs to be registered, and the digital wallets involved in transfers can be identified by "tracing wallet ownership, token provenance, source IP addresses, and user identification."[32] According to Anton Moiseienko and Kayla Izenman, 99 percent of the currency transactions in the years before COVID-19 were performed through centralized exchanges that were "subject to AML/CFT [Anti-money laundering/counterterrorist financing] regulation similar to traditional banks or exchanges."[33]

Because of the pseudonymous nature of standard Bitcoin transactions, criminal elements began turning to the dark web to hide the identity of the users. Drawing on U.S. Drug Enforcement Administration (DEA) data, Camila Russo calculated that approximately 90 percent of Bitcoin

transactions in 2013 were related to criminal activities.[34] Increasingly, that occurred through means, such as Tor, Freenet, and I2P, to access the dark web anonymously.[35] The creation of privacy coins, such as Zcash and Monero, also offered a hidden means for illicit activity—although one analysis of Monero could trace the parties in the transactions in 88 percent of the cases. According to Erik Silfversten, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, and Adrian Salas, most criminals who use cryptocurrencies continue to rely on Bitcoin because of its dominance and relative stature.[36]

Criminals have also turned to "tumblers" or "mixers" that pass cryptocurrencies and transactions across chains and through unregulated exchanges to hide their identities. Those processes pool cryptocurrency deposits and spread them across wallets; after they have been washed, they redeposit them with customers. According to one source, "[m]ixers have consistently processed about a quarter of incoming illicit Bitcoins per year," although their unreliability has been a constraint on their full adoption.[37] The attractiveness of cryptocurrencies to criminals has also been dampened by the rise of cryptocurrency intelligence companies that track transactions to assist law enforcement and other parties.[38]

Despite these advances, until 2020, cryptocurrencies as a means to transfer and launder illicit funds remained underused. According to a 2020 Chainalysis study, in 2019, approximately US$11.5 billion of cryptocurrency was spent on illicit activity. In all, this totaled a mere 1.1 percent of the total activities of cryptocurrencies. In 2015, Europol declared that cash was still the preferred means for criminals to conduct transactions and launder money.[39]

This is not to say cryptocurrencies do not have a role or that these analyses capture all the criminal activities that occur or are laundered through them. Because of the legal transaction costs, cryptocurrencies are easily used for "smurfing" or transferring small amounts of money to avoid detection by authorities or bank regulators—something that is often prohibitively expensive because of transfer fees in established financial institutions.

China has played a disproportionate role within the cryptocurrency world in the growth and use of those currencies for licit and illicit purposes. According to a 2021 report published by Chainalysis, Inc., Chinese over-the-counter brokers "have played an outsized role in facilitating money laundering for those involved in cryptocurrency-based crime."[40] According to the same report, between "April 2019 and June 2021, Chinese [crypto wallet] addresses have sent over US$2.2 billion worth of cryptocurrency to [crypto wallet] addresses associated with illicit activity such as scams and dark web market operations and received over US$2.0 billion." The bulk of this period spans the 15 months when the world was in the throes of the COVID-19 pandemic and its associated social distancing and lockdown policies.

At an official countrywide level, El Salvador has curiously moved toward adopting Bitcoin with uncertain consequences, not just for the country's economy and citizens' access to cash, but also for the broader global anti-money laundering and law enforcement community. The September 2021 adoption by El Salvadoran President Nayib Bukele of Bitcoin as the country's national currency has raised suspicion of ulterior motives, in part because around 30 percent of the population is unbanked, complicating their ability to access their accounts. While the 40-year-old president hailed the move as a way to reduce the cost of remittances being sent by friends and family to El Salvador—remittances represent 20 percent of the country's gross domestic product (GDP)[41]—there has been speculation that the unexpected shift could obscure criminal activities and funds. Allegations of ties between those close to the president to criminal networks have sustained those concerns.[42]

Individuals who are fortunate enough not to see their incomes negatively affected by COVID-19-related policies and the economic contraction have watched their savings grow. At the same time, news and attention on cryptocurrencies have generated new engagement.[43] As a result, investment in cryptocurrencies has ballooned and diversified, making markets and transactions more complex and potentially making it easier to hide illicit transactions.[44]

Cryptomania: A Real or Virtual Money Laundering Threat?

Newspapers and blogs regularly publish news of the use of cryptocurrencies, and Bitcoin in particular, as the new vehicle for money laundering. Recently the non-profit journalism and investigative organization *InSight Crime* published a report with the eye-catching title, "The Digital Gold Rush: 5 Ways Bitcoin Helps Organized Crime."[45] But when it came to money laundering, the article only mentioned two cases, which appeared relatively small in scope. In one case, the funds from an extortion racket in Brazil were laundered, and, in another, Bitcoin was used to deposit small amounts of a cartel's ill-gotten gains to hide their provenance (the "smurfing" of funds mentioned earlier on page 15 of this report). Similarly, another article on the same site ran a story under the flashy headline "Bitcoin Cryptocurrency Adds to Venezuela Money Laundering Risks," but notes that Bitcoin is not the greatest risk.[46] Instead, it said that the more significant threats are the dark web and other, more hidden, cryptocurrencies described earlier in this paper. Even then, citing a Chainalysis report (referenced earlier in this report) and a report by the Consortium of Investigative Journalists and *Buzzfeed* News, the article concluded that "the vast majority of illicit gains are still laundered through the traditional banking system, not cryptocurrency."[47]

The DEA 2020 National Drug Threat Assessment raised concerns about cryptocurrency being used to move and launder funds during COVID-19. As a result of border restrictions stemming from the COVID-19 pandemic, the report says that "large amount of U.S. currency are being held along the U.S. side, awaiting transport to Mexico."[48] The report argues that money laundering organizations use "virtual currency automated teller machines (ATMs) to aid in the movement of illicit bulk currency" without providing specific examples or cases.[49] Later, as this report describes, virtual currency is increasingly used for traditional trade-based money laundering, although there are few specifics.

There are other reasons to remain vigilant about cryptocurrencies with regard to money laundering. For one, cryptocurrencies and, in particular, privacy functions, through either coin, such as Monero, or through tumblers and mixers, will continue to evolve as monitoring and law enforcement capacities improve. Second is the apparent rise of China as a market for illicit cryptocurrency transactions. Kim Grauer and Henry Updegrave argue that "China also stands out for receiving a disproportionate share of funds sent from addresses associated with stolen funds and ransomware. Some of this may come from cryptocurrency theft and ransomware activity associated with the Lazarus Group, a cybercriminal syndicate linked to the North Korean government."[50] In recent years, a pattern has emerged of reliance on over-the-counter brokers in China that specialize in money laundering. These brokers, of which they focus on the 270 most active deposit addresses, appear to be developing money laundering as a "key part of the business model."[51] This may, in fact, make them easier to track for law enforcement officials, especially since many of them come from exchanges at high risk for illicit activity, including those in high-risk jurisdictions where regulation and enforcement is lax or non-existent and from identifiable sources, such as mixers or gambling platforms. One such example, as detailed by Schoenberg, was Binance, the Cayman Islands incorporated but Singapore-based cryptocurrency exchange, which federal agents determined handled more illicit funds than any other exchange, including funds tied to a fentanyl trafficking ring.[52]

The last reason it will be important to monitor cryptocurrencies for a potential uptick in money laundering activities is that it is still too early to tell the long-term effects of COVID-19 on illicit activities in the sector. As detailed above, several studies and investigations have detected increased activity specifically focused on China in one instance and accounts and brokers in another. At the same time, despite early predictions of the eventual irrelevance of cryptocurrencies,[53] Bitcoin and other cryptocurrencies appear to be with us to stay, and even expand in the public discussion, if not in their use. As the market evolves, if there is demand from criminal elements, their needs will produce adaptations, especially as the trend toward cashless economies accelerates. In addition, given that

tracing illicit cryptocurrency activity involves a substantial degree of retrospective attribution, it may take several years before we have a clear picture of the significance of any trends in the use of cryptocurrencies for money laundering during COVID-19.

China's Ban on Cryptocurrencies: Beyond the Babble

China's recent ban on cryptocurrencies has received a lot of coverage, as well as mockery, given that it has already done so 18 times before.[54] Much has also been written on the motivations behind the Chinese government taking this step. There is the more benevolent narrative that encouraging or even permitting the mining of cryptocurrencies runs counter to the Chinese leadership's determination to become carbon neutral by 2060.[55] While undoubtedly a factor that would have been taken into consideration, it is more likely this move was taken due to the government's discomfort toward the presence and usage of a decentralized, non-sovereign currency.[56] This line of reasoning gains greater credence when considering that plans for the digital Yuan continue to move toward becoming a reality, which, if successful, would see the release of the world's first state-backed digital currency.

In this approach, it appears China will stand alone, however, as it is unlikely the United States and governments of Europe would make any similar moves. In response to questions on whether the United States would consider a China-like prohibition, U.S. Securities and Exchange Commission Chair Gary Gensler recently reaffirmed that the U.S. approach ensures the cryptocurrency industry adheres to investor and consumer protection rules, anti-money laundering regulations, and tax laws.[57] Similarly, the recent strengthening of EU regulations on cryptocurrencies echoes the transatlantic sentiment that an outright ban is unlikely.[58]

Despite this divergence in approaches, law enforcement agencies in the United States and Europe could do worse than pay attention to trends that unfold in China in the wake of the ban. Particularly when considering how the use of cryptocurrencies for money-laundering purposes has permeated criminal activity in China,[59] this test case of prohibition could provide valuable insights that might better inform efforts at regulation elsewhere.

This is particularly relevant if policymakers intend to avoid unwittingly incentivizing criminals into seeking out more obscure and harder to trace methods for trading cryptocurrencies and, therefore, potentially obfuscating money-laundering trails. One immediate observation in the case of China's cryptocurrency ban is that problematic over-the-counter trading, identified as a significant problem by Chainalysis,[60] will likely persist, and an increased number of Chinese traders and miners will use virtual private networks (VPNs)[61] to avoid detection.[62]

Perhaps of greater relevance to the conversation on money laundering is the suggestion that the Chinese clampdown on the more established exchanges could push traders to use decentralized finance (DeFi) platforms, such as Uniswap. Eleanor Olcott has noted that the use of such platforms, which don't have the same "know your client" (KYC) obligations as the conventional exchanges, have been growing in China in the past year amid the banning of cryptocurrencies. In fact, from January to June 2021, US$256bn in cryptocurrency was traded through such DeFi platforms in China.[63] Therefore, banning conventional, regulated exchanges appears to have pushed traders—both legal and illicit—toward the use of infrastructure that is darker and less traceable. Until now, DeFi has had a relatively patchy record.[64] However, with such voluminous transactions now taking place on these unregulated platforms, there now runs the risk they become established mainstays of the cryptotrading infrastructure, which would be an appealing development for those looking to layer their ill-gotten proceeds.

In terms of immediate recommendations in light of the experience of the Chinese prohibition of cryptocurrencies, it would be wise to consider added scrutiny of DeFi when developing regulations surrounding cryptocurrencies—particularly pushing for the necessity of KYC protocols for these to operate. Another recommendation borne out of this example is that DeFi is now moving into the mainstream.

Those who choose regulation over prohibition, such as the United States and Europe, would be wise to explore what types of monitoring tools are available or possible for decentralized systems.

FINTECH AND E-COMMERCE: PEER-TO-PEER FINANCE AND COMMERCE

For many of the same reasons explained above with cryptocurrencies, it may be too early to tell the extent to which COVID-19 has incentivized the integration of FinTech and peer-to-peer finance into illicit transactions and money-laundering schemes. A joint study by the World Bank Group and the University of Cambridge notes a strong uptick in the use of FinTech during the pandemic.[65] Based on surveys of 118 central bank and financial regulators between June and August 2020, the study reveals that digital payments and remittances increased 60 percent, digital banking services expanded by 22 percent, and digital savings and deposits through FinTech grew by 19 percent.

Yet along with this rise in digital transactions during the pandemic, social distancing and lockdown measures became a hindrance to regulators. The report states that the regulators surveyed noted challenges in performing core regulatory functions such as on-site inspection of firms (49 percent overall and 65 percent in advanced economies), difficulties in external communications (43 percent), and coordination with domestic agencies (43 percent).[66]

While challenges exist in assessing what impact COVID-19 has had on the adoption of modern FinTech and peer-to-peer platforms by criminal elements, we do know from the above that use spiked at a time when regulators were not operating at full capacity. While many FinTechs are generally more coherently regulated than cryptocurrencies with an institutional third-party guaranteeing transactions, the relative ease and low costs of transactions and their impersonal nature may well have made them a platform for illicit activity.

There is more evidence of an increase in likely illicit activity in e-commerce. Trade mispricing in person-to-person transactions is a heavily used technique. Increasingly, however, that has moved to online commerce, a trend that has increased under COVID-19 as global trade and supply chains were disrupted by the pandemic and the economic contraction.

The patterns were already taking shape before 2020. According to Christoph Wronka, "money launderers have over the years mastered the art of using e-commerce websites to take advantage of this vulnerability and proceed with their illegal activities. These types of money laundering activities are referred to as transaction laundering." [67] While they reportedly occur on e-commerce platforms like eBay and Pinduoduo on a large scale, they also happen on a smaller scale at a frequency that makes them a useful means for criminals to launder money, with lower levels of potential detection. In one case in 2018, an author found their identity had been assumed on Amazon, and their books were being sold at vastly inflated prices.[68] They speculated that stolen credit cards could have been used to repeat purchase the book, with the author pocketing the 60 percent commission from Amazon. But the basic means of buying overpriced goods, which may even be worthless, as a means of transferring funds elsewhere is common. In the case of Amazon, when the overpriced book scam was brought to its attention, it started withdrawing several other books; however the adaptability of criminals suggests they would migrate to other products and platforms.

As with FinTech, the e-commerce sector saw a large surge in usage due to COVID-19. A *Forbes* article concluded that COVID-19 accelerated the adoption and integration of e-commerce by four to six years.[69] According to a UN Conference on Trade and Development report, online retail sales grew from 16 percent to 18 percent of global retail.[70] However, the number as an aggregate amount is deceptive; it includes online travel and service retailers severely hurt by social distancing and lockdown measures. For example, Expedia's sales shrunk by 65.9 percent in the same period, Booking Holdings contracted by 63.3 percent, and Airbnb by 37.1 percent. In contrast, Alibaba grew by 20 percent, Amazon by 38 percent, Pinduoduo by 65.9 percent, and Shopify by 95.6 percent. The biggest gains were

in business-to-business e-commerce through online market platforms and electronic data interchange transactions.

The increased volume of traffic and money exchanged via e-commerce provided a much-expanded avenue for transaction laundering of funds that would typically have been washed through casinos pre-pandemic, a medium widely used in Asia and the Americas alike for money laundering. Prior to the pandemic, several casinos in Australia and Canada (British Colombia, in particular) had been investigated for non-compliance with money-laundering regulations. In Sydney in May 2021, casinos agreed to ban the use of cash, requiring card payments. Several countries reported a rise in online gambling at times when casinos and gambling venues were closed during the pandemic.[71]

There are various ways to use casinos to launder money, most simply by buying casino chips and subsequently claiming them back as winnings, validated by a check or receipt. While similar tactics can be used in online gambling, using cash in physical casinos provides an obvious advantage over online gambling. In September 2020, the *Financial Times* reported that in China, money launderers used leading online shopping sites to transfer billions of dollars to offshore gambling sites.[72] People seeking to evade China's capital controls placed fake orders on various shopping sites and received credit to their gambling accounts. According to Chinese police, around US$2 billion was laundered through phony e-commerce purchases.

The *Financial Times* similarly reported that in one prominent case, police in the eastern city of Wuxi found 600 million fake packages had been inserted into courier firms' tracking systems by company insiders to complete false e-commerce transactions. Many of those same package tracking numbers appeared in money-laundering cases in two other Chinese cities where more than RMB7bn was allegedly funneled to offshore gambling sites.

According to one of the affected e-commerce sites, "gambling syndicates operating under false pretenses on e[-]commerce platforms is an industry-wide problem."[73] Australia's largest casino operator, Crown Resorts, is accused of accepting deposits over the AUS$10,000 threshold at its Perth location, dating back to 2014. Possibly hundreds of millions of dollars were processed through this scheme. The set-up was reportedly linked to Chinese organized crime (the Crown group had pulled out of Macau in 2017 after facing an investigation from Beijing).

The pattern follows an already well-worn path for money launderers established before the COVID-19 pandemic in a network of shadow banking and mis-priced trade. Traditionally, criminals from China, India, and Pakistan would use their respective alternative banking systems (hui k'uan, hawala, and hundi, respectively). However, based on trust and policed through fear of ostracization, these systems were closed to those outside the community.

Over the past few years, a new means of transferring funds has emerged using the official Chinese banking system and is open to criminals from any community. The system uses Chinese businesses in the respective countries and is predicated on having bank accounts in their country of residence and in China.

For example, to transfer the profits of drugs sales from the United States to Mexico, the funds would be passed to a Chinese business operating in the United States. This business would then transfer an equivalent sum in Yuan from its Chinese bank account to the Chinese bank account of a Chinese firm operating in Mexico. This business would then pass the funds in pesos to the intended recipient in Mexico. Alternatively, instances of trade-based money laundering have also been found, with goods—often clothing or footwear—being purchased in China and sold in Mexico, with the proceeds passed to the cartel. Either way, the funds have been transferred outside the remit of Western law enforcement agencies. *Reuters* has detailed how the process unfolds in several stages:

Step One: A Mexican criminal syndicate wants to bring proceeds from U.S. drug sales back to Mexico. It contacts Chinese money brokers operating in Mexico to see who offers the cheapest rates.

Step Two: The parties agree on a commission and the amount to be laundered, for example $150,000.

Step Three: The Chinese broker, using encrypted phone messages, would send the cartel three things:

1. A code word
2. The number of a US burner phone
3. Unique serial number of an authentic $1 bill

Step Four: The Mexican crime group shares those details with a drug dealer in the United States, who calls the burner phone and identifies himself by using the code word. He arranges to meet a US-based money courier working for the Chinese broker.

Step Five: The drug dealer and the money courier meet in public. The courier hands over a $1 bill with the unique serial number. When that that is validated, the dealer hands over the cash, keeping the bill as a "receipt."

Step Six: The courier takes the $150,000 to a US-based Chinese merchant who has a bank account in China. The merchant then performs a currency swap known as a "mirror transaction." They take possession of the US cash and then transfers $150,000 worth of Chinese yuan from their Chinese bank account to the money broker's Chinese account, using an account number provided to them by the courier.

Step Seven: The cartel's drug cash is now sitting in a Chinese bank, outside the view of US law enforcement. The broker has two options to send it on to Mexico to the drug cartel.

Step Eight: Option 1 is to do another 'mirror transaction.' The $150,000 worth of yuan is now transferred from the money broker's Chinese account to the Chinese bank account of a Mexico-based businessperson. That Mexico-based businessperson then provides $150,000 worth of pesos to the money broker in Mexico, who delivers that cash to the cartel.Under option 2, the Chinese money broker buys $150,000 worth of consumer products in China, such as clothing, and exports them to Mexico. The goods are then sold, and the proceeds delivered to the cartell.[74]

One of the major challenges for underground banking systems arises if there is an imbalance in the demand for currencies; the system works better when the demand is roughly balanced. For example, capital flight from the Philippines in the 1990s was generally equivalent to inward remittances from overseas workers.[75] Flows of drug money between Hong Kong and Thailand, however, were more one-sided, with three times the funds flowing into Hong Kong compared with Thailand. This requires regular compensation to balance the accounts.

In the case of Chinese banking systems in the Americas, the system works because there is a rough balance between the demand and supply of dollars. Drug dealers in the United States offer a supply of dollars (to be converted into local currency), while Chinese expatriate communities demand dollars to circumvent Chinese capital controls.

These patterns may well have been updated and will continue to develop. What we will not know, except with more time, is to what extent money laundering via e-commerce kept pace or even grew disproportionately during the COVID-19 pandemic with consumer and business transactions shifting online. As a recent *Global Financial Integrity* article describes, trade-based money laundering is one of the "weakest links in the fight against corruption."[76] For drug cartels in Mexico and Colombia, the article says this means of money laundering is "low risk and high reward," largely due to the corruption of public officials—customs officials in particular—and the lack of political will. Questions remain whether and how the COVID-19 pandemic and e-commerce boom that accompanied it have changed this in the short and long term. Chinese e-commerce sites used to launder money show there is a wide scope for retailers to facilitate that process unwittingly. There's also another potential upside, however. While mispricing in real-world traditional trade is often facilitated by corrupt customs officials far from the businesses originally engaged in the trans-

action, e-commerce may open an avenue for more effective monitoring and tracking of illicit processes by independent transnational bodies and regulators.

The Need for International Collaboration: Tax Havens and the Case of the Pandora Papers

The existence of tax havens, jurisdictions with low tax regimes that, more importantly, fail to disclose financial information with other jurisdictions, provide a potential opening to launder illicit funds. Tax havens operate on the basis that they can accept money without reporting it to the country in which it originated. According to U.S. economist Gabriel Zucman, 8 percent of the world's wealth –US$7.6 trillion—is held in tax havens.[77]

In recent years, several data leaks from tax havens have revealed the extent to which companies and wealthy individuals seek to minimize their tax payments, along with instances of the use of tax havens for money laundering. The most recent leak—the Pandora Papers—is the largest thus far, but the data does not yet reveal whether offshore banking has been used for tax avoidance, tax evasion, or money laundering. Earlier leaks included the 2019 FinCEN Leaks, the 2017 Paradise Papers, focusing on the records of law firm Appleby, based in Bermuda, the Singapore-based Asiaciti Trust, and the 2016 Panama Papers, which disclosed the records of Panama-based law firm, Mossack Fonseca. HSBC Jersey's account holders were leaked in 2012 and HSBC Geneva's in 2009. While several legal actions are ongoing concerning Mossack Fonseca, cursory checks on identity coupled with an unwillingness to pry too deeply into the source of wealth provided potential opportunities for money laundering. According to the International Consortium of Investigative Journalists, two months after its records were breached, Mossack Fonseca could not identify the owners of more than 70 percent of 28,500 active companies in the British Virgin Islands and 75 percent of 10,500 active shell companies in Panama.[78]

While some moves have attempted to make tax havens more transparent, progress is slow, and steps made in one jurisdiction shift business to less transparent jurisdictions. Furthermore, as successive leaks have shown, many of those in charge of running financial systems are using loopholes provided by tax havens. This creates an environment conducive for illegal activities to take place alongside legal tax avoidance schemes.

CONCLUSION

Criminals are highly innovative and adaptable. The emergence of new technologies and ways of conducting business have provided unique opportunities to commit crimes and launder funds. The emergence of cryptocurrencies over the last decade has provided a new means to launder and transfer funds anonymously, with regulators slow to respond to the latest challenges. Even the COVID-19 pandemic presented new opportunities to make money illegally.

For now, at least, the pandemic's impact on money laundering appears to have been more balanced. Despite many traditional means of laundering money—such as through casinos or high cash turnover businesses like restaurants—being closed off because of government-imposed lockdowns, there has not yet been a significant detectable jump in the use of cryptocurrencies or FinTech in money laundering. In many cases, criminals were forced to warehouse cash, raising the risk of discovery. Meanwhile, the same government COVID-related restrictions hindered those seeking to tackle money laundering.

Nevertheless, it may be too early to tell. The increasing sophistication of financial products, coupled with the secrecy surrounding numerous jurisdictions, facilitates money laundering. Financial institutions are developing increasingly sophisticated tools, including through artificial intelligence, to identify money laundering, but opportunistic criminals are often quick to adapt and develop new means of avoiding scrutiny. Better and faster data-sharing at both the national and international level would help identify the proceeds of crime, as would an enhanced capacity of law enforcement agencies to analyze suspicious activity reports.

There is growing evidence that larger transnational criminal groups are becoming increasingly cooperative rather than competitive. This may well enable them to increase their profits, but it makes them more vulnerable to detection and harder to stay under the radar. At the same time, organized crime presents a threat to stability, and the sums involved threaten to capture states. The threat is not confined to drug-producing countries but also affects important distribution hubs, from Central America to Europe. The recent decision to place the Dutch Prime Minister, Mark Rutte, under police protection because of an ongoing trial relating to cocaine smuggling demonstrates the scale of the threat.[79]

To successfully counter money laundering would require a concerted international approach. While one tax haven is willing to undercut another to attract unscrupulous business, actions taken in other jurisdictions simply displace the problem to the benefit of less scrupulous countries. The situation is further exacerbated by the existence of a few narco-states in which the scale of criminality—narcotic production or transit—provides safe havens for criminals. These countries act as magnets and undermine global efforts.

In addition, countries such as China and Russia appear ambivalent about the challenges facing Western countries. While China has taken steps to tackle the misuse of cryptocurrencies, the emergence of its domestic banking system as a new means to launder and transfer funds between, for example, the United States and Mexico, provides a particular challenge for Western law enforcement agencies.

There is also a distinct challenge for technology firms. While law enforcement agencies recognize that criminals will misuse new technologies, technology companies appear more reactive, focused more on the positive uses for their technology. Overpricing goods on digital marketplaces, for instance, provides a new and relatively easy means of laundering money. Unless companies can easily identify overvalued products or ensure that those using their services are easily identifiable, this will remain a challenge.

These challenges in tracking and understanding the effects of COVID-19 and related government measures point to the need for regulators, state security, and financial sector officials to reflect on the past near-two years. Despite the current lack of data on how the global pandemic has affected the tools and tactics in the movement of illicit profits, there are potential areas of collaboration that investigators and researchers should focus on in their anti-money laundering efforts. Some of those are outlined below.

RECOMMENDATIONS

The implications of the COVID-19 pandemic on the global economy, markets, commercial relations, global supply chain, and daily life of citizens will be felt for years to come. The same is true of the virus's effects on illicit markets and money laundering. Changes in the structure of global financial markets had already started before the COVID-19 pandemic but have been accelerated by the events of 2020. The recommendations that follow respond to both those pre-existing trends as well as likely impacts stemming from COVID-19 and its associated effects on markets and finance.

Continue to monitor new trends in virtual and electronic markets and finance

It is difficult to understand all the impacts of COVID-19 on human behavior and markets in the near-two years of experience we have had. Patterns and trends will take longer to discern and address. But just as we are already witnessing a spectrum of effects on everything from increased integration of work-from-home schedules to urban design to the integration of e-commerce as a regular part of our consumer habits—there will be an impact on the organization and operation of criminal syndicates. Given the accelerated growth of online commerce and peer-to-peer finance in daily life, these innovations and tools will likely affect criminal transactions. In short, it will be necessary when monitoring and prosecuting illicit activity not to assume it will be business as usual from 2021 and beyond.

Update and tighten regulation and monitoring of FinTech and cryptocurrencies

While Bitcoin and other cryptocurrencies have not translated into as large and central a market as many imagined for illicit transactions pre-COVID-19, the need to push financial transactions and money laundering to either virtual means or to hold on to cash indicates that the move toward these platforms may just be beginning. This may be particularly true as many criminal groups will have warehoused cash during the periods of lockdown that they could not launder through more traditional means. In the early days of the pandemic, the FATF outlined a series of policy responses to address AML and CTF to respond to COVID-19-related threats. They remain valid absent the COVID-19 pandemic and include:

- Domestic coordination to assess the impact of COVID-19 on AML/CTF risks and systems;
- Strengthened communication with the private sector; and
- Encouraging the full use of a risk-based approach to customer due diligence.[80]

In all these cases, special attention should be paid to peer-to-peer financial platforms and e-commerce.

In cryptocurrency markets, focus on known over-the-counter brokers

Recent research indicates that rather than a widespread phenomenon of using cryptocurrencies for money laundering, illicit activities—including money laundering—tend to be conducted through anonymous exchanges, using the mixers and tumblers described above. Better monitoring and enforcement of money laundering laws on those brokers will help choke off the primary illicit practice in the cryptocurrency ecosystem. Along the same lines, as researchers and law enforcement officials identify the owners of wallets used by criminals, they should share that information through international law enforcement and financial agencies such as Interpol, Europol, and the FATF. Such an effort could create an alert system similar to Interpol's red list for wanted international criminals but dedicated to known wallets and brokers engaging in illicit transactions.

Upgrade government capacity to track and understand the cryptocurrency world

As criminals and the cryptocurrency world evolved and adapted to new opportunities in money laundering, so has the software to detect it. Money laundering software that helps officials identify potential sites and operations related to money laundering based on tested high-risk areas, transactions, and wallets can help track and capture or at least shut down bad actors in the rapidly changing cryptocurrency ecosystem. This will also require training and staffing government regulatory bodies. According to one scholar, "relatively few current government employees have the skills to use this technology to its full potential."[81]

Work with China to identify and shut down money laundering operations

While research has identified various China-based operations actively laundering money through cryptocurrency markets, e-commerce, or shadow banks, Beijing has also demonstrated a willingness to take on these bad actors. One of the founders of several of the cryptocurrency brokers mentioned earlier, Zhao Dong, pled guilty in May 2021 to money laundering charges, and other arrests have continued with up to 1,100 individuals arrested because of the Chinese Communist Party's crackdown on money laundering.[82] According to one report, the reasons stem in part from a desire to reduce capital flight and a crackdown on illegal money transactions. While in the case of the Chinese e-vendor Pinduoduo, they had not knowingly engaged in the money laundering scheme that used its platform. Given China's growing global network and footprint commercially and financially, a desire to project itself as a legitimate economic actor will work to the advantage of regulators and law enforcement agencies that combat money laundering.

BIBLIOGRAPHY

Agence France-Presse. "China's vast bitcoin mining empire risks derailing its climate targets, says study." *The Guardian*. April 7, 2021. https://www.theguardian.com/technology/2021/apr/07/china-bitcoin-mining-climate-targets-nature-study.

Alba, Ricardo M. "Evolution of methods of money laundering in Latin America." *Journal of Financial Crime* Vol. 10 No. 2 (December 31, 2002): 137-140. https://doi.org/10.1108/13590790310808718.

Americas Quarterly. "Guess who's having a good pandemic: How COVID-19 is changing organized crime." Volume 15, issue 1 (2021). https://americasquarterly.org/wp-content/uploads/2021/01/AQTransnationalOrganizedCrime.pdf.

Antonopoulos, Andreas M. *Mastering Bitcoin, 2nd Edition*. Sebastopol, California: O'Reilly Media, Inc., 2017.

Associated Press. "Sixty charged with running US meth lab which allegedly sold drugs in Australia." *Nine News*. June 30, 2021. https://www.9news.com.au/world/60-charged-with-running-california-meth-lab-which-allegedly-created-drugs-sold-in-australia/66668c4c-d28f-423e-a78e-0db2dcab093e?ocid=Social-9News.

Ávalos, Silva. "El Salvador's Nayib Bukele Tainted by Money Laundering Allegations." Analysis. *InSight Crime*. September 24, 2019. https://insightcrime.org/news/analysis/el-salvadors-nayib-bukele-tainted-money-laundering-allegations/.

Bambrough, Billy. "The U.S. Treasury Secretary Made a Dire Warning Over the Future of Bitcoin." *Forbes*. July 27, 2019. https://www.forbes.com/sites/billybambrough/2019/07/27/the-u-s-treasury-secretary-made-a-dire-warning-over-the-future-of-bitcoin/?sh=735778242c93.

Bain, Benjamin. "SEC Chief Says the U.S. Won't Ban Cryptocurrencies." *Bloomberg*. October 5, 2021. https://www.bloomberg.com/news/articles/2021-10-05/sec-chief-signals-crypto-ban-like-china-s-won-t-happen-in-u-s.

Barysevich, Andrei, and Alexandr Solad. "Litecoin Emerges as the Next Dominant Dark Web Currency." Recorded Future, Insikt Group. February 8, 2018. https://www.recordedfuture.com/dark-web-currency/.

Baydakova, Anna. "Indian Crypto Firms Suggest Policy Ideas to Government Ahead of Possible Ban." *Coindesk*. March 30, 2021. https://www.coindesk.com/indian-crypto-firms-suggest-policy-ideas-to-government-ahead-of-possible-ban.

Biggs, John. "FBI Seizes Popular Dark Market Search Site DeepDotWeb for Money Laundering." *Coindesk*. May 7, 2019. https://www.coindesk.com/fbi-seizes-popular-dark-market-search-site-deepdotweb-for-money-laundering.

Blandin, Apolline, Ana Sofie Cloots, Hatim Hussain, Michel Rauchs, Rasheed Saleuddin, Jason Grant Allen, Bryan Zhang, and Katherine Cloud. "Global Cryptoasset Regulatory Landscape Study." Cambridge: University of Cambridge, 2019. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf.

Bonar, Hugo, and Andrada Filip. "COVID-19-related Trafficking of Medical Products as a Threat to Public Health." Research Brief. United Nations Office on Drugs and Crime. July 6, 2020. https://www.unodc.org/documents/data-and-analysis/covid/COVID-19_research_brief_trafficking_medical_products.pdf.

Brown, Rick, and Amelia Hickman, "Changes in online gambling during the COVID-19 pandemic: April update." Canberra: Australian Institute of Criminology, 2020. https://www.aic.gov.au/sites/default/files/2020-06/sb27_changes_in_online_gambling-during_the_covid-19_pandemic_april_update.pdf.

Business Insider Nordic. "Bank robberies decline as Sweden ditches cash — but more people are turning to black market crime instead." June 18, 2018. https://www.businessinsider.com/swedens-reduced-cash-circulation-means-black-market-crimes-increase-2018-6?r=US&IR=T.

Carney, Mark. "The Future of Money." Speech, Bank of England. March 2, 2018. https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418.

Chainalysis. "Cryptocurrency and China: Analyzing China's Historic Cryptocurrency Activity Amidst Government Crackdowns." *Chainalysis*. September 23, 2021. https://go.chainalysis.com/rs/503-FAP-074/images/China%20report%20final.pdf.

Charles, Brooke Satti. "It All Comes Out in the Wash: The Most Popular Money Laundering Methods in Cybercrime." *SecurityIntelligence*. May 11, 2016. https://securityintelligence.com/it-all-comes-out-in-the-wash-the-most-popular-money-laundering-methods-in-cybercrime/.

Chatham House. "Russian dirty money: What would it take to shut down the London laundromat?" Chatham House Research Event. Event Recording. February 24, 2021. https://www.chathamhouse.org/events/all/research-event/russian-dirty-money-what-would-it-take-shut-down-london-laundromat?utm_medium=email&utm_source=Chatham%20House.

Chaum, David. "Blind Signatures for Untraceable Payments." *Advances in Cryptology*. 1983. https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

CIFAS. "Latest fraud statistics reveal middle-aged mules targeted by online money laundering gangs." CIFAS. June 3, 2021. https://www.cifas.org.uk/newsroom/middle-aged-mules.

CIFAS. "Money mule recruiters use fake online job adverts to target 'Generation Covid'." Newsroom. March 11, 2021. https://www.cifas.org.uk/newsroom/money-mules-target-generation-covid.

Coinmarketcap. "Cryptocurrency Market Capitalizations." Coinmarketcap. 2019. https://coinmarketcap.com/.

Council of Europe. "Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, MONEYVAL: Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID-19 crisis." Strasbourg: Council of Europe, September 2, 2020. https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3.

Crawley, Jamie. "UK Crypto Companies Now Have to Submit to Financial Crime Reports." *Coindesk*. March 31, 2021. https://www.coindesk.com/uk-crypto-companies-now-have-to-submit-financial-crime-reports.

Crawley, Jamie. "Japan to Adopt FATF Travel Rule for Crypto." *Coindesk*. April 1, 2021. https://www.coindesk.com/japan-to-adopt-fatf-travel-rule-for-crypto.

CYFOR. "EncroChat: What is it and why did criminals use it?" CYFOR. Undated. https://cyfor.co.uk/encrochat-what-is-it-and-why-did-criminals-use-it/.

Dalby, Chris. "How Chinese Criminals Secretly Move Millions for Mexico Cartels." *InSight Crime*. May 12, 2021. https://insightcrime.org/news/chinese-money-launderers-mexico-cartels-move-millions-secret/.

De, Nikhilesh. "DEA Report: Bitcoin Used for Trade-Based Money Laundering." *Coindesk*. October 25, 2017. https://www.coindesk.com/dea-report-bitcoin-used-trade-based-money-laundering.

Desmond, Dennis B., David Lacey, and Paul Salmon. "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review." *Journal of Money Laundering Control*, vol. 22 issue 3 (July 2, 2019). https://doi.org/10.1108/JMLC-10-2018-0063.

Desmond, Dennis B., Paul Salmon, and David Lacey. "Functional systems within cryptolaundering processes: a work domain analysis model of cryptolaundering activities." *Journal of Cyber Policy*. (July 5, 2021): 155-176. https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1948088.

The Economist. "How the digital surge will reshape finance." *The Economist*. October 10, 2020. https://www.economist.com/finance-and-economics/2020/10/08/how-the-digital-surge-will-reshape-finance.

European Commission. "Director of the European Parliament and of the Council: amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC." Strasbourg: European Commission, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1512664006207&uri=CELEX-:52016PC0450.

European Commission. "Strengthened EU Rules to Prevent Money Laundering and Terrorist Financing." Strasbourg: European Commission, 2018. https://ec.europa.eu/newsroom/just/items/610991.

Faux, Zeke. "Anyone Seen Tether's Billions?" *Bloomberg*. October 7, 2021. https://www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether.

Financial Action Task Force. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations." Paris: FATF, 2020. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

Financial Action Task Force. "COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses." Paris: FATF, May 2020. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf.

Fitzgibbon, Will. "New Panama Papers Leak Reveals Firm's Chaotic Scramble to Identify Clients, Save Business Amid Global Fallout." *International Consortium of Investigative Journalists*. June 20, 2018. https://www.icij.org/investigations/panama-papers/new-panama-papers-leak-reveals-mossack-fonsecas-chaotic-scramble/.

Flood, Alison. "Fake books sold on Amazon could be used for money laundering." *The Guardian*. April 27, 2018. https://www.theguardian.com/books/2018/apr/27/fake-books-sold-amazon-money-laundering.

Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniņš. "Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies?" *The Review of Financial Studies* Vol 32, issue 5 (May 2019). https://academic.oup.com/rfs/article/32/5/1798/5427781.

GAFILAT. "GAFILAT statement on Covid-19– and its associated ML and FT risks." Buenos Aires: GAFILAT, April 8, 2020. https://www.gafilat.org/index.php/es/noticias/102-comunicado-del-gafilat-sobre-covid-19-coronavirus.

Gerard, David. "El Salvador's Bitcoin Law Is a Farce." *Foreign Policy*. September 17, 2021. https://foreignpolicy.com/2021/09/17/el-salvador-bitcoin-law-farce/.

Gkritsi, Eliza. "Police in Chain's Zunyi City Bust a $124M Money Laundering Scam." *CoinDesk*. October 13, 2021. https://www.coindesk.com/policy/2021/10/13/police-in-chinas-zunyi-city-bust-a-124m-money-laundering-scam/.

Global Financial Integrity. "Trade Misinvoicing." Undated. https://gfintegrity.org/issue/trade-misinvoicing/.

Global Times. "Latin American crime cartels turn to cryptocurrencies for money laundering." *Global Times*. September 12, 2020. https://www.globaltimes.cn/content/1209499.shtml.

Grauer, Kim, and Henry Updegrave. "The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet markets, and more." *Chainalysis*. https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.

Griffin, Alicia. "Tackling the risks of the FinTech boom – AML considerations." Expert Insights. CharlesRussellSpeechlys. November 18, 2018. https://www.charlesrussellspeechlys.com/en/news-and-insights/insights/financial-services/2018/tackling-the-risks-of-the-fintech-boom---aml-considerations/.

The Guardian. "Met police seize nearly £180m of bitcoin in money laundering investigation." *The Guardian*. July 13, 2021. https://www.theguardian.com/technology/2021/jul/13/met-police-bitcoin-money-laundering-cryptocurrency?CMP=Share_iOSApp_Other.

Hager, Mike. "B.C.'s money laundering commission hears from those who saw dirty money washing through casinos." *The Globe and Mail*. December 9, 2020. https://www.theglobeandmail.com/canada/british-columbia/article-bcs-money-laundering-commission-hears-from-those-who-saw-dirty/.

Harding, Luke. "Mossack Fonseca: inside the firm that helps the super-rich hide their money." Panama Papers: a special investigation. *The Guardian*. April 8, 2016. https://www.theguardian.com/news/2016/apr/08/mossack-fonseca-law-firm-hide-money-panama-papers.

HM Treasury. "Cash and digital payments in the new economy: summary of responses." London: Bank of England, May 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799548/CfE_-_Cash___Digital_Payments_Response_020519_vf_digicomms.pdf.

HM Treasury, Financial Conduct Authority, and Bank of England. "Cryptoassets Taskforce: Final Report." 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.

Hardy, Peter D. "FinCEN Warns Financial Institutions about Economic Stimulus Aid Scams." Ballard Spahr LLP. February 28, 2021. https://www.moneylaunderingnews.com/2021/02/fincen-warns-financial-institutions-about-economic-stimulus-aid-scams/.

InSight Crime. "Venezuela: A Mafia State?"' *InSight Crime*. May 25, 2018. https://insightcrime.org/investigations/venezuela-mafia-state/.

InSight Crime. "Bitcoin Cryptocurrency Adds to Venezuela Money Laundering Risk." Venezuela Investigative Unit. *InSight Crime*. April 7, 2021. https://insightcrime.org/news/bitcoin-cryptocurrency-adds-venezuela-money-laundering-risk/.

Inman, Phillip. "Bitcoin jumps to three-year high as Covid crisis changes investor outlook." *The Guardian*. November 17, 2020. https://www.theguardian.com/technology/2020/nov/17/bitcoin-jumps-to-three-year-high-as-covid-crisis-changes-investor-outlook.

Interpol. "Against Organized Crime: Interpol Trafficking and Counterfeiting Casebook 2014." Lyon: Interpol, 2014. https://www.iipcic.org/documents/LD_INTERACTIVE_INTERPOL_CASEBOOK_EN_FINALE_pages.pdf.

Irrera, Anna. "Criminals getting smarter in use of digital currencies to launder money." *Reuters*. December 9, 2020. https://www.reuters.com/article/crypto-currencies-criminals-idUSKBN28J1IX.

Izquierdo, Pedro. "Seeking Solutions to Trade Misinvoicing in Mexico and Colombia." Global Financial Integrity. September 14, 2021. https://gfintegrity.org/seeking-solutions-to-trade-misinvoicing-in-mexico-and-colombia/.

Jorgic, Drazen. "Factbox: Step by step - How Chinese 'money brokers' launder cash for Mexican drug cartels." *Reuters*. December 3, 2020. https://www.reuters.com/article/uk-mexico-china-cartels-factbox/factbox-step-by-step-how-chinese-money-brokers-launder-cash-for-mexican-drug-cartels-idUKKBN28D1M1.

Jorgic, Drazen. "Special Report: Burner phones and banking apps: Meet the Chinese 'brokers' laundering Mexican drug money." *Reuters*. December 3, 2020. https://www.reuters.com/article/us-mexico-china-cartels-specialreport-idUSKBN28D1M4.

Jones, Huw. "EU to tighten rules on cryptoasset transfers." *Reuters*. July 20, 2021. https://www.reuters.com/technology/eu-tighten-rules-cryptoasset-transfers-2021-07-20/.

Keatinge, Tom, David Carlisle, and Florence Keen. "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses." The Hague: Europol, 2018. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

Keyworth, Marie. "I was a teenage 'money mule'." *BBC News*. April 26, 2018. https://www.bbc.co.uk/news/business-43897614.

Koetsier, John. "COVID-19 Accelerated E-Commerce Growth '4 To 6 Years'." *Forbes*. May 3, 2021. https://www.forbes.com/sites/johnkoetsier/2020/06/12/covid-19-accelerated-e-commerce-growth-4-to-6-years/?sh=-21f3a684600f.

Krebs, Brian. "How Scammers use eBay as a personal ATM." *The Sunday Morning Herald*. November 4, 2015. https://www.smh.com.au/technology/how-scammers-use-ebay-as-a-personal-atm-20151104-gkq3aq.html.

Lagunes, Paul. "Backgrounder on Lava Jato." Center on Global Economic Governance, Columbia University. 2018. https://www.bakerinstitute.org/media/files/files/b49a8c69/lagunes-lava-jato-backgrounder.pdf.

The Law Society. "Legal Sector Affinity Group (LSAG) - Advisory Note: COVID-19 and preventing money laundering/terrorist financing in legal practices." 2020. https://www.lawsociety.org.uk/en/topics/anti-money-laundering/lsag-advisory-note-covid-19-and-preventing-money-laundering.

Luther, William J. "How Much Cash is Used by Criminals and Tax Cheats?" American Institute for Economic Research. February 8, 2017. https://www.aier.org/article/how-much-cash-is-used-by-criminals-and-tax-cheats/.

Lyons, Izzy. "Met's £47m 'dirty cash' swoop as Covid cripples gangs' money-laundering." *The Telegraph*. May 19, 2021. https://www.telegraph.co.uk/news/2021/05/19/mets-47m-dirty-cash-swoop-gangs-money-laundering-hit-covid/.

Mazur, Robert. "Attacking Drug Cartels Through Undercover Money Laundering Operations." Combating Terrorism Centre, West Point. Volume 5, issue 3 (March 2012). https://ctc.usma.edu/attacking-drug-cartels-through-undercover-money-laundering-operations/.

McMorrow, Ryan, and Qianer Liu. "Money-launderers use Chinese online shopping sites to funnel cash offshore." *Financial Times*. September 16, 2020. https://www.ft.com/content/e669a621-b40b-45b0-abc0-9648d10cdd1b.

Me, Angela, Irmgard Zeiler, and Jacqueline Garcia Yi. "COVID-19 and the drug supply chain: from production and trafficking to use." Research Brief. Vienna: United Nations Office on Drugs and Crime, May 7, 2020. https://www.unodc.org/documents/data-and-analysis/covid/Covid-19-and-drug-supply-chain-Mai2020.pdf.

Moiseienko, Anton, and Kayla Izenman. "From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency." Occasional papers. Royal United Services Institute. April 6, 2021. https://rusi.org/explore-our-research/publications/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency.

Morell, Michael, Josh Kirshner, and Thomas Schoenberger. "An Analysis of Bitcoin's Use in Illicit Finance." Crypto Council for Innovation. April 6, 2021. https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf.

Murphy, Hannah. "The rise of crypto laundries: how criminals cash out of bitcoin." *Financial Times*. May 28, 2021. https://www.ft.com/content/4169ea4b-d6d7-4a2e-bc91-480550c2f539.

Nelson, Danny. "DeepDotWeb Operator Pleads Guilty to Laundering $8.4M in Bitcoin Kickbacks." *Coindesk*. March 31, 2021. https://www.coindesk.com/policy/2021/03/31/deepdotweb-operator-pleads-guilty-to-laundering-84m-in-bitcoin-kickbacks/.

Nilsson, Patricia. "Online fraud up by a third in the UK during the pandemic." *Financial Times*. July 15, 2021. https://www.ft.com/content/e820cc8a-090c-4632-95f3-cb295d3d31ad.

Nolsoe, Eir. "How the Coronavirus pandemic impacted the use of cash globally." November 16, 2020. https://yougov.co.uk/topics/economy/articles-reports/2020/11/16/pandemic-accelerates-decline-cash-globally.

Olcott, Eleanor. "Chinese investors flock to the 'wild west in crypto'." *Financial Times*. October 20, 2021. https://www.ft.com/content/fd0579aa-6f3c-434c-9f5d-7e10aa7db70b.

Peachey, Kevin. "Money launderers 'prey on generation Covid'." *BBC News*. March 10, 2021. https://www.bbc.co.uk/news/business-56334862.

Peachey, Kevin. "ATM withdrawals drop by £37bn during year of Covid." *BBC News*. March 17, 2021. https://www.bbc.co.uk/news/business-56413993.

Peltier, Elian. "As Dutch Prime Minister Gets Extra Security, Fears Focus on Drug Gangs." *The New York Times*. September 30, 2021. https://www.nytimes.com/2021/09/30/world/europe/netherlands-prime-minister-threats.html.

Praudins, Arnis. "Money laundering and hybrid threats: Has COVID-19 made it all worse?" Interview by Nicolas Véron. Banking and Capital Markets. Bruegel. February 18, 2021. https://www.bruegel.org/events/money-laundering-and-hybrid-threats-has-covid-19-made-it-all-worse/.

PYMNTS.com. "Former UK Payments Group Chair Found Guilty In Money Laundering Case." 2021. https://www.pymnts.com/pymnts-post/news/security-and-risk/2021/former-united-kingdom-payments-group-chair-found-guilty-money-laundering/?c=international-2/page/Page/page/4.

Reuters. "China arrests over 1,100 suspects in crackdown on crypto-related money laundering." *Reuters*. June 10, 2021. https://www.reuters.com/world/china/china-arrests-over-1100-suspects-crackdown-crypto-related-money-laundering-2021-06-10/.

Rowan, Philip, Margaret Miller, Bryan Zhang, Sharmista Appaya, Sarah Ombija, Aleem Mubarak Tejani, Dea Markova, Daphnée Papiasse, Herman Smit, and Thomas Ward. "The Global Covid-19 FinTech Regulatory Rapid Assessment Study." The World Bank Group and University of Cambridge. Undated. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf.

Russo, Camila. "Bitcoin speculators dominate cryptocurrency use now, but criminals haven't backed away." *Los Angeles Times*. August 7, 2018. https://www.latimes.com/business/la-fi-cryptocurrency-bitcoin-20180807-story.html.

Sands, Peter. "Making It Harder for the Bad Guys: The Case for Eliminating High Denomination Notes." Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government. 2016. https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp52.

Schoenberg, Tom. "Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths." *Bloomberg*. May 13, 2021. https://www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in?sref=M8H6LjUF.

Shah, Saqib. "Airbnb is reportedly being used to launder money." engadget. November 27, 2017. https://www.engadget.com/2017-11-27-airbnb-russian-money-laundering-scam.html.

Shi, Madeline Meng. "Fed Chair: Cryptocurrencies Are 'Great' For Money Laundering." *Coindesk*. July 18, 2018. https://www.coindesk.com/markets/2018/07/18/fed-chair-cryptocurrencies-are-great-for-money-laundering/.

Silfversten, Erik, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, and Adrian Salas. "Exploring the use of Zcash cryptocurrency for illicit or criminal purposes." Research Reports. *RAND Corporation*. 2020. https://doi.org/10.7249/RR4418.

Taylor, Emily. "China's Ban on Cryptocurrencies Isn't Just About Control." *World Politics Review*. October 5, 2021. https://www.worldpoliticsreview.com/articles/30015/with-crypto-china-isn-t-just-worried-about-control.

Tookitaki. "5 Modern Money Laundering Methods That Criminals Use." *Tooktikai.* Undated. https://www.tookitaki.ai/news-views/5-methods-that-modern-money-launderers-use-to-beat-detection/.

Tornaghi, Cecilia. "Q&A: Brazil's Pioneering Fight Against Gang Money Laundering." *Americas Quarterly*. January 26, 2021. https://americasquarterly.org/article/to-fight-organized-crime-in-latin-america-defund-it/.

Traders Magazine. "Is Cryptocurrency Making Money Laundering Easier?" *Traders Magazine.* June 18, 2021. https://www.tradersmagazine.com/am/is-cryptocurrency-making-money-laundering-easier/.

UK Finance. "Criminals exploit Covid-19 pandemic with rise in scams targeting victims online." Press Release. March 25, 2021. https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online#summary.

United Nations Conference on Trade and Development. "COVID-19 has changed online shopping forever, survey shows." October 8, 2020. https://unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows.

United Nations Conference on Trade and Development. "Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales." May 3, 2021. https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales.

U.S. Department of Justice. "Asian Money Movement Methods." *Drug Intelligence Report*. Drug Enforcement Administration. 1994. https://www.ojp.gov/pdffiles1/Digitization/151447NCJRS.pdf.

U.S. Department of Justice, "2020 National Drug Threat Assessment." Drug Enforcement Administration. March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

U.S. Department of Justice. *Joint Law Enforcement Operation Results In Arrests And Federal Drug Trafficking And Money Laundering Charges.* United States Attorney's Office, District of Nevada. July 14, 2021. https://www.justice.gov/usao-nv/pr/joint-law-enforcement-operation-results-arrests-and-federal-drug-trafficking-and-money.

Vermaak, Werner. "What Are Privacy Coins?" *Coin Market Cap.* April 7, 2021. https://coinmarketcap.com/alexandria/article/what-are-privacy-coins.

Villalba, Javier. "Colombia Drug Trafficking Money Laundered Through Modified Gold." *InSight Crime.* June 17, 2021. https://insightcrime.org/news/urabenos-gold-launder-drug-money-colombia/.

Volpicelli, Gian M. "This is why China finally halted its bitcoin boom." *Wired.* September 29, 2021. https://www.wired.co.uk/article/china-ban-bitcoin-cryptocurrencies.

Wainwright, Rob. "Why is Cash Still a King? A Strategic report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering." The Hague: Europol, February 8, 2015. https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering.

Wilson, Mark. "The Digital Gold Rush - 5 Ways Bitcoin Helps Organized Crime." *InSight Crime*. October 1, 2021. https://insightcrime.org/news/digital-gold-rush-how-bitcoin-helps-organized-crime/.

Wolfson, Rachel. "Tracing Illegal Activity Through the Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes." *Forbes.* November 26, 2018. https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/?sh=5d690f8033a9.

The World Bank. "Personal remittances, received (% of GDP) – El Salvador." Data. https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=SV.

The World Bank Group and University of Cambridge. "The Global Covid-19 FinTech Regulatory Rapid Assessment Study." Undated. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf.

Wronka, Christoph. "'Cyber-laundering': the change of money laundering in the digital age." *Journal of Money Laundering Control*. June 25, 2021. https://doi.org/10.1108/JMLC-04-2021-0035.

Yaraghi, Nian, and Shamika Ravi. "The Current and Future State of the Sharing Economy." Brookings Institution. 2017. https://www.brookings.edu/wp-content/uploads/2016/12/sharingeconomy_032017final.pdf.

Zaami, Simona, Enrico Marinelli, and Maria Rosaria Vari. "New Trends of Substance Abuse During COVID-19 Pandemic: An International Perspective." Opinion article. *Frontiers in Psychiatry*. July 16, 2020. https://www.frontiersin.org/articles/10.3389/fpsyt.2020.00700/full.

END NOTES

1. This concern was shared with the researchers in a July 7, 2021, interview by a senior colleague with a financial regulatory body in the United Kingdom on the condition of anonymity.

2. Government of the United Kingdom Press Release, "Criminals exploit Covid-19 pandemic with rise in scams targeting victims online," UK Finance, March 25, 2021, www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online#summary; and Hugo Bonar and Andrada Filip, "COVID-19-related Trafficking of Medical Products as a Threat to Public Health," Research Brief, United Nations Office on Drugs and Crime, July 6, 2020, www.unodc.org/documents/data-and-analysis/covid/COVID-19_research_brief_trafficking_medical_products.pdf.

3. Patricia Nilsson, "Online fraud up by a third in the UK during the pandemic," *Financial Times*, July 15, 2021, www.ft.com/content/e820cc8a-090c-4632-95f3-cb295d3d31ad.

4. "COVID-19 has changed online shopping forever, survey shows," United Nations Conference on Trade and Development, October 8, 2020, unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows.

5. "Money mule recruiters use fake online job adverts to target 'Generation Covid'," Newsroom, CIFAS, March 11, 2021, www.cifas.org.uk/newsroom/money-mules-target-generation-covid.

6. Izzy Lyons, "Met's £47m 'dirty cash' swoop as Covid cripples gangs' money-laundering," *The Telegraph*, May 19, 2021, www.telegraph.co.uk/news/2021/05/19/mets-47m-dirty-cash-swoop-gangs-money-laundering-hit-covid/.

7. Anna Irrera, "Criminals getting smarter in use of digital currencies to launder money," *Reuters*, December 9, 2020, www.reuters.com/article/crypto-currencies-criminals-idUSKBN28J1IX.
8. "Trade Misinvoicing," Issues, Global Financial Integrity, accessed October 14, 2021, gfintegrity.org/issue/trade-misinvoicing/.

9. Alicia Griffin, "Tackling the risks of the FinTech boom – AML considerations," Expert Insights, Charles-RussellSpeechlys, November 18, 2018, www.charlesrussellspeechlys.com/en/news-and-insights/insights/financial-services/2018/tackling-the-risks-of-the-fintech-boom---aml-considerations/.

10. Nian Yaraghi and Shamika Ravi, "The Current and Future State of the Sharing Economy," *Brookings Institution*, 2017, www.brookings.edu/wp-content/uploads/2016/12/sharingeconomy_032017final.pdf.

11. Eir Nolsoe, "How the Coronavirus pandemic impacted the use of cash globally," November 16, 2020, yougov.co.uk/topics/economy/articles-reports/2020/11/16/pandemic-accelerates-decline-cash-globally.

12. For summaries see Brian Krebs, "How Scammers use eBay as a personal ATM," *The Sunday Morning Herald*, November 4, 2015, www.smh.com.au/technology/how-scammers-use-ebay-as-a-personal-atm-20151104-gkq3aq.html; and Saqib Shah, "Airbnb is reportedly being used to launder money," *engadget*, November 27, 2017, www.engadget.com/2017-11-27-airbnb-russian-money-laundering-scam.html.

13. For example, see Hannah Murphy, "The rise of crypto laundries: how criminals cash out of bitcoin," *Financial Times*, May 28, 2021, www.ft.com/content/4169ea4b-d6d7-4a2e-bc91-480550c2f539; and Christoph Wronka, "Cyber-laundering: the change of money laundering in the digital age," *Journal of Money Laundering Control*, Vol. ahead-of-print No. ahead-of-print, June 25, 2021, doi.org/10.1108/JMLC-04-2021-0035.

14. "GAFILAT statement on Covid-19 – and its associated ML and FT risks," GAFILAT, April 8, 2020, www.gafilat.org/index.php/es/noticias/102-comunicado-del-gafilat-sobre-covid-19-coronavirus.

15. William Luther, "How Much Cash is Used by Criminals and Tax Cheats?" American Institute for Economic Research, February 8, 2017, www.aier.org/article/how-much-cash-is-used-by-criminals-and-tax-cheats/.

16. "COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses," FATF, May 2020, www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf.

17. "COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses," FATF: 10.

18. "COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses," FATF, 10.

19. Nolsoe, "How the Coronavirus pandemic impacted the use of cash globally."

20. Nolsoe, "How the Coronavirus pandemic impacted the use of cash globally."

21. FATF, "COVID-19-related Money Laundering and Terrorist Financing," 6.

22. FATF, "COVID-19-related Money Laundering and Terrorist Financing," 8.

23. FATF, "COVID-19-related Money Laundering and Terrorist Financing," 8.

24. FATF, "COVID-19-related Money Laundering and Terrorist Financing," 6.

25. FATF, "COVID-19-related Money Laundering and Terrorist Financing," 4.

26. See Angela Me, Irmgard Zeiler, and Jacqueline Garcia Yi, "COVID-19 and the drug supply chain: from production and trafficking to use," Research Brief, United Nations Office on Drugs and Crime, May 7, 2020, www.unodc.org/documents/data-and-analysis/covid/Covid-19-and-drug-supply-chain-Mai2020.pdf; and Simona Zaami, Enrico Marinelli, and Maria Rosaria Vari, "New Trends of Substance Abuse During COVID-19 Pandemic: An International Perspective," opinion article, *Frontiers in Psychiatry*, July 16, 2020, www.frontiersin.org/articles/10.3389/fpsyt.2020.00700/full.

27. Arguably, except for Bitcoin—recently adopted by El Salvador as its currency—cryptocurrencies are not actually currencies but assets.

28. "Cryptocurrency Market Capitalizations," Coinmarketcap, 2019, coinmarketcap.com/.

29. Madeline Meng Shi, "Fed Chair: Cryptocurrencies Are 'Great' For Money Laundering," *Coindesk*, July 18, 2018, www.coindesk.com/markets/2018/07/18/fed-chair-cryptocurrencies-are-great-for-money-laundering/.

30. Andreas M. Antonopoulos, *Mastering Bitcoin, 2nd Edition* (Sebastopol, California: O'Reilly Media, Inc., 2017), 255

31. Dennis B. Desmond, David Lacey, and Paul Salmon, "Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review," *Journal of Money Laundering Control*, vol. 22 issue 3 (July 2, 2019), doi.org/10.1108/JMLC-10-2018-0063.

32. Dennis Desmond, Paul Salmon, and David Lacey, "Functional systems within cryptolaundering processes: a work domain analysis model of cryptolaundering activities," *Journal of Cyber Policy* (July 5, 2021): 155-176, www.tandfonline.com/doi/full/10.1080/23738871.2021.1948088.

33. Anton Moiseienko and Kayla Izenman, "From Intention to Action: Next Steps in Preventing Criminal Abuse of Cryptocurrency," occasional papers, Royal United Services Institute (April 6, 2019): 8, rusi.org/explore-our-research/publications/occasional-papers/intention-action-next-steps-preventing-criminal-abuse-cryptocurrency.

34. Camila Russo, "Bitcoin speculators dominate cryptocurrency use now, but criminals haven't backed away," *Los Angeles Times*, August 7, 2018, www.latimes.com/business/la-fi-cryptocurrency-bitcoin-20180807-story.html.

35. Tor, Freenet, and I2P are examples of free and open-source internet browsers, readily downloadable for public use that enable anonymous communication and encrypt user data.

36. Erik Silfversten, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, and Adrian Salas, "Exploring the use of Zcash cryptocurrency for illicit or criminal purposes," Research Reports, *RAND* Corporation (2020), doi.org/10.7249/RR4418.

37. Yaya Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows in Digital Currency Systems," Center on Sanctions and Illicit Finance, January 12, 2018, www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf; and Rolf van Wegberg, Jan-Jaap Oerlemans, and Oskar van Deventer, "Bitcoin money laundering: mixed results? An explorative study on money laundering of crybercrime proceeds using bitcoins," *Journal of Financial Crime*, 25(1) (March 2018), doi.org/10.1108/JFC-11-2016-0067.

38. Rachel Wolfson, "Tracing Illegal Activity Through the Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes," *Forbes*, November 26, 2018, www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/?sh=5d690f8033a9.

39. Rob Wainwright, "Why is Cash Still a King? A Strategic report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering," Europol, February 8, 2015, www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering.

40. "Cryptocurrency and China: Analyzing China's Historic Cryptocurrency Activity Amidst Government Crackdowns," *Chainalysis*, September 23, 2021: 3, go.chainalysis.com/rs/503-FAP-074/images/China%20report%20final.pdf.

41. "Personal remittances, received (% of GDP) – El Salvador," Data, The World Bank, data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=SV.

42. See Silva Ávalos, "El Salvador's Nayib Bukele Tainted by Money Laundering Allegations," Analysis, *InSight Crime*, September 24, 2019, insightcrime.org/news/analysis/el-salvadors-nayib-bukele-tainted-money-laundering-allegations/; and David Gerard, "El Salvador's Bitcoin Law Is a Farce," *Foreign* Policy, September 17, 2021, foreignpolicy.com/2021/09/17/el-salvador-bitcoin-law-farce/.

43. Phillip Inman, "Bitcoin jumps to three-year high as Covid crisis changes investor outlook," *The Guardian*, November 17, 2020, www.theguardian.com/technology/2020/nov/17/bitcoin-jumps-to-three-year-high-as-covid-crisis-changes-investor-outlook.

44. Arnis Praudins, "Money laundering and hybrid threats: Has COVID-19 made it all worse?," interview by Nicolas Véron, Banking and Capital Markets, *Bruegel*, February 18, 2021, www.bruegel.org/events/money-laundering-and-hybrid-threats-has-covid-19-made-it-all-worse/.

45. Mark Wilson, "The Digital Gold Rush - 5 Ways Bitcoin Helps Organized Crime," *InSight Crime*, October 1, 2021, insightcrime.org/news/digital-gold-rush-how-bitcoin-helps-organized-crime/.

46. "Bitcoin Cryptocurrency Adds to Venezuela Money Laundering Risk," Venezuela Investigative Unit, *InSight Crime*, April 7, 2021, insightcrime.org/news/bitcoin-cryptocurrency-adds-venezuela-money-laundering-risk/.

47. Chainalysis, "Cryptocurrency and China: Analyzing China's Historic Cryptocurrency Activity Amidst Government Crackdowns."

48. U.S. Department of Justice, Drug Enforcement Administration, "2020 National Drug Threat Assessment," March 2021, 85, www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

49. U.S. Department of Justice, Drug Enforcement Administration, "2020 National Drug Threat Assessment," 89.

50. Kim Grauer and Henry Updegrave, "The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet markets, and more," *Chainalysis*, 12, go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.

51. Grauer and Updegrave, "The 2021 Crypto Crime Report," 18.

52. Tom Schoenberg, "Binance Faces Probe by U.S. Money-Laundering and Tax Sleuths," *Bloomberg*, May 13, 2021, www.bloomberg.com/news/articles/2021-05-13/binance-probed-by-u-s-as-money-laundering-tax-sleuths-bore-in?sref=M8H6LjUF.

53. See, for example, former U.S. Secretary of Treasury Steven Mnuchin's statement that "Bitcoin will not be widely used in ten years' time" in Billy Bambrough, "The U.S. Treasury Secretary Made A Dire Warning Over the Future of Bitcoin," *Forbes*, July 27, 2019, www.forbes.com/sites/billybambrough/2019/07/27/the-u-s-treasury-secretary-made-a-dire-warning-over-the-future-of-bitcoin/?sh=735778242c93.

54. Gian M. Volpicelli, "This is why China finally halted its bitcoin boom," *Wired*, September 29, 2021, www.wired.co.uk/article/china-ban-bitcoin-cryptocurrencies.

55. Agence France-Presse, "China's vast bitcoin mining empire risks derailing its climate targets, says study," *The Guardian*, April 7, 2021, www.theguardian.com/technology/2021/apr/07/china-bitcoin-mining-climate-targets-nature-study.

56. Emily Taylor, "China's Ban on Cryptocurrencies Isn't Just About Control," *World Politics Review*, October 5, 2021, www.worldpoliticsreview.com/articles/30015/with-crypto-china-isn-t-just-worried-about-control.

57. Benjamin Bain, "SEC Chief Says the U.S. Won't Ban Cryptocurrencies," *Bloomberg*, October 5, 2021, www.bloomberg.com/news/articles/2021-10-05/sec-chief-signals-crypto-ban-like-china-s-won-t-happen-in-u-s.

58. Huw Jones, "EU to tighten rules on cryptoasset transfers," *Reuters*, July 20, 2021, www.reuters.com/technology/eu-tighten-rules-cryptoasset-transfers-2021-07-20/.

59. "China arrests over 1,100 suspects in crackdown on crypto-related money laundering," *Reuters*, June 10, 2021, www.reuters.com/world/china/china-arrests-over-1100-suspects-crackdown-crypto-related-money-laundering-2021-06-10/; Zeke Faux, "Anyone Seen Tether's Billions?," *Bloomberg*, October 7, 2021, www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether; and Eliza Gkritsi, "Police in Chain's Zunyi City Bust a $124M Money Laundering Scam," *CoinDesk*, October 13, 2021, www.coindesk.com/policy/2021/10/13/police-in-chinas-zunyi-city-bust-a-124m-money-laundering-scam/.

60. Chainalysis, "Cryptocurrency and China: Analyzing China's Historic Cryptocurrency Activity Amidst Government Crackdowns."

61. A Virtual Private Network or VPN is a piece of software that provides the user with online privacy and anonymity by creating a private network from a public internet connection by masking the internet protocol address to keep online actions private.

62. Volpicelli, "This is why China finally halted its bitcoin boom."

63. Eleanor Olcott, "Chinese investors flock to the 'wild west in crypto'," *Financial Times*, October 20, 2021, www.ft.com/content/fd0579aa-6f3c-434c-9f5d-7e10aa7db70b.

64. Grauer and Updegrave, "The 2021 Crypto Crime Report: Everything you need to know about ransomware, darknet markets, and more."

65. Philip Rowan, Margaret Miller, Bryan Zhang, Sharmista Appaya, Sarah Ombija, Aleem Mubarak Tejani, Dea Markova, Daphnée Papiasse, Herman Smit, and Thomas Ward, "The Global Covid-19 FinTech Regulatory Rapid Assessment Study," The World Bank Group and University of Cambridge, accessed October 14, 2021, www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-report-fintech-regulatory-rapid-assessment.pdf.

66. Rowan, Miller et al, "The Global Covid-19 FinTech Regulatory Rapid Assessment Study."

67. Wronka, "'Cyber-laundering': the change of money laundering in the digital age."

68. Alison Flood, "Fake books sold on Amazon could be used for money laundering," *The Guardian*, April 27, 2018, www.theguardian.com/books/2018/apr/27/fake-books-sold-amazon-money-laundering.

69. John Koetsier, "COVID-19 Accelerated E-Commerce Growth '4 To 6 Years'," *Forbes*, May 3, 2021, www.forbes.com/sites/johnkoetsier/2020/06/12/covid-19-accelerated-e-commerce-growth-4-to-6-years/?sh=21f3a684600f.

70. "Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales," United Nations Conference on Trade and Development, May 3, 2021, unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales.

71. Rick Brown and Amelia Hickman, "Changes in online gambling during the COVID-19 pandemic: April update," Australian Institute of Criminology, 2020, www.aic.gov.au/sites/default/files/2020-06/sb27_changes_in_online_gambling-during_the_covid-19_pandemic_april_update.pdf.

72. Ryan McMorrow and Qianer Liu, "Money-launderers use Chinese online shopping sites to funnel cash offshore," *Financial Times*, September 16, 2020, www.ft.com/content/e669a621-b40b-45b0-abc0-9648d10cdd1b.

73. McMorrow and Liu, "Money-launderers use Chinese online shopping sites to funnel cash offshore."

74. Drazen Jorgic, "Factbox: Step by step - How Chinese 'money brokers' launder cash for Mexican drug cartels," *Reuters*, December 3, 2020, www.reuters.com/article/uk-mexico-china-cartels-factbox/factbox-step-by-step-how-chinese-money-brokers-launder-cash-for-mexican-drug-cartels-idUKKBN28D1M1.

75. U.S Department of Justice, Drug Enforcement Administration, "Asian Money Movement Methods" (1994): 11, www.ojp.gov/pdffiles1/Digitization/151447NCJRS.pdf.

76. Pedro Izquierdo, "Seeking Solutions to Trade Misinvoicing in Mexico and Colombia," *Global Financial Integrity*, September 14, 2021, gfintegrity.org/seeking-solutions-to-trade-misinvoicing-in-mexico-and-colombia/.

77. Luke Harding, "Mossack Fonseca: inside the firm that helps the super-rich hide their money," Panama Papers: a special investigation, *The Guardian*, April 8, 2016, www.theguardian.com/news/2016/apr/08/mossack-fonseca-law-firm-hide-money-panama-papers.

78. Will Fitzgibbon, "New Panama Papers Leak Reveals Firm's Chaotic Scramble to Identify Clients, Save Business Amid Global Fallout," *International Consortium of Investigative Journalists*, June 20, 2018, www.icij.org/investigations/panama-papers/new-panama-papers-leak-reveals-mossack-fonsecas-chaotic-scramble/.

79. Elian Peltier, "As Dutch Prime Minister Gets Extra Security, Fears Focus on Drug Gangs," *The New York Times*, September 30, 2021, www.nytimes.com/2021/09/30/world/europe/netherlands-prime-minister-threats.html.

80. "COVID-19-related Money Laundering and Terrorist Financing," FATF: 4.

81. Michael Morell, Josh Kirshner, and Thomas Schoenberger, "An Analysis of Bitcoin's Use in Illicit Finance," Crypto Council for Innovation (April 6, 2021): 6, cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf.

82. Chainalysis, "Cryptocurrency and China: Analyzing China's Historic Cryptocurrency Activity Amidst Government Crackdowns," 8.

ABOUT THE AUTHORS

CALUM INVERARITY

Calum Inverarity is a senior researcher at the Open Data Institute. He was previously a research associate with the International Security Programme at Chatham House, where he worked across the programme's research portfolio. His work focuses primarily on conflict prevention and resolution, including the role of governance in facilitating these processes. He formerly worked at Bruegel, the Democratic Progress Institute, and UN House, Scotland. Calum holds an M.Sc. in Conflict Resolution and Governance from the University of Amsterdam and a BA in International Development and International Relations from the University of Leeds. As part of his studies, he also spent time at the University of California, San Diego, and the University of Ghana.

GARETH PRICE

Gareth Price is a senior research fellow in the Asia-Pacific Programme at Chatham House, where he has led research on a range of economic and political issues affecting South Asia since 2004. He was also head of the institute's Asia Programme between 2005 and 2011. Previously he worked as an analyst at the Economist Intelligence Unit, focusing on South Asia, and before that was the South Asia analyst at Control Risks Group. He holds a Ph.D. in the politics of northeast India from the University of Bristol.

ABOUT THE AUTHORS

COURTNEY RICE

Courtney Rice is a senior manager in the U.S. and the Americas Programme at Chatham House and is involved in each of the programme's research projects. He has worked across several departments at Chatham House since first joining the institute in 2014. Courtney holds an MA in International Studies and Diplomacy, from SOAS, University of London, and a BA dual honors in International Relations and History from Keele University, Staffordshire.

CHRISTOPHER SABATINI

Christopher Sabatini is a senior fellow for Latin America at Chatham House and was formerly a lecturer in discipline at the School of International and Public Affairs at Columbia University. Chris is also on the advisory boards of Harvard University's Laspau, Human Rights Watch's Americas Division, and the Inter-American Foundation. He is an HFX Fellow at the Halifax International Security Forum. He is a frequent contributor to policy journals and newspapers and appears in the media and on panels on issues related to Latin America and foreign policy. Chris has testified multiple times before the U.S. Senate and the U.S. House of Representatives. He has a Ph.D. in government from the University of Virginia.

FIU | Steven J. Green School of International & Public Affairs
FLORIDA INTERNATIONAL UNIVERSITY

DECEMBER 2021