Financial Authorities Confront Two Cryptocurrency Ecosystems

Yaya J. Fanusie

Within the cryptocurrency space, two separate ecosystems are evolving. This will likely require strategies from financial authorities looking to counter illicit finance threats. One ecosystem is the above-ground, formal sector of cryptocurrency companies that largely accommodate anti–money laundering/know-your-customer (AML/KYC) regulations and are working to promote a business culture of compliance, which this arena mostly lacked in its earliest years. The other ecosystem is underground and consists of actors, platforms, and tokens that are more resistant to the regulatory pressures that undercut anonymity. This underground environment is currently smaller and much less developed than the formal one, but it offers little to no corporate accountability to law enforcement and will likely enable substantial illicit financing should it scale up.

THE ABOVE-GROUND CRYPTOCURRENCY ECOSYSTEM

The conventional banking sector is becoming more comfortable with cryptocurrencies, even establishing formal partnerships with industry actors to facilitate direct purchase of digital currencies through bank accounts.[1] The proliferation of blockchain analysis firms offering tools to assess the AML risk of cryptocurrency users and investigate suspicious transactions is giving cryptocurrency exchanges the ability to identify and deter illicit activity on their platforms.[2] Some business due diligence firms are also helping the cryptocurrency industry use watch-list databases, similar to those used by banks, to vet customers during the identification verification process.[3] These initiatives—although they do not eliminate illicit activity—create a compliance environment that enables self-policing by exchanges and makes law enforcement intervention easier when suspected illegal activity is detected. This essentially makes cryptocurrency exchanges similar to other decades-old money service businesses, such as Western Union or MoneyGram, in which crime and fraud exist but at an acceptable rate, sufficiently addressed by mitigation procedures. The U.S. Department of the Treasury acknowledges these regulatory limitations in its most recent National Money Laundering Risk Assessment, which points out that while AML practices help curb illicit finance, they do not eliminate it.[4]

While AML/KYC standards for cryptocurrency exchanges are not upheld equivalently nor necessarily agreed upon among financial regulators in all countries, progress is being made to address regulatory gaps across jurisdictions. For example, a study of bitcoin transaction data for digital currency exchanges from 2013 to 2016 showed that European exchange services processed a disproportionately large number of transactions from illicit sources such as darknet markets compared to North American exchanges.[5] This is likely because the United States, in 2013, and Canada, in 2014,

issued clear guidance for local cryptocurrency businesses to follow the same AML regulations as other money transmitters while EU authorities did not formally bring European crypto-businesses under AML regulations until the European Commission officially updated its AML directive in late 2017.[6] European cybersecurity officials are aware of the increasing role of cryptocurrencies in crime. Europol in recent years has held annual virtual currency conferences for European law enforcement and cryptocurrency exchange companies to share information and lessons learned.[7]

The Group of Twenty (G20) recently acknowledged the importance of developing global regulatory standards for cryptocurrency use.[8] Although the G20 has not articulated what standards the regulation should entail, the group announced that it will make specific recommendations in October 2018, in consultation with the Financial Action Task Force (FATF).[9] Outlining a global standard can help minimize opportunities for AML arbitrage. At present, illicit actors in regulated jurisdictions can easily access cryptocurrency exchange websites based in poorly regulated locations. Setting international standards will not result in high performance across all jurisdictions, but it would help institutions such as FATF address the growth of the cryptocurrency space as it evaluates nations' AML and combating the financing of terrorism (CFT) capacity. FATF has a notable influence on major cryptocurrency exchanges. In May 2018, South Korea's largest cryptocurrency exchange, Bithumb, announced that it would not serve customers who are citizens of FATF's Non-Cooperating Countries and Territories, designated as such for having insufficient AML measures in place.[10] Furthermore, with the Treasury Department recently announcing that it could begin adding digital currency wallet addresses to its Specially Designated Nationals blacklist, cryptocurrency exchanges will be pressured to take steps to ensure they are not violating sanctions by transacting with designated wallets.[11]

THE UNDERGROUND CRYPTOCURRENCY ECOSYSTEM

While the developments discussed above represent a step in the right direction for establishing an AML-compliant cryptocurrency ecosystem, a countertrend is developing simultaneously, undermining their efficacy: some cryptocurrency developers are pushing for blockchain infrastructure and platforms that operate outside the reach of AML compliance measures. A small part of this trend is reminiscent of the de-risking phenomenon: stricter AML/CFT regulations in the banking sector after the 9/11 terrorist attacks caused banks to reduce their exposure to high-risk populations; this pushed many potential consumers into informal markets, particularly for cross-border money transfers.[12] Discussions about de-risking in the cryptocurrency space are rare and seemingly premature, given that the blockchain industry's formalization is in its infancy. By averting services from high-risk jurisdictions and customers, cryptocurrency businesses can lessen their individual compliance risk; however, doing so will not eliminate the demand for cryptocurrency transactions among high-risk consumers. Workarounds and unregulated exchange platforms will likely capture that demand. For example, several websites currently offer cryptocurrency exchange services with little to no identification verification.[13]

The growth of the noncompliant cryptocurrency ecosystem today is fueled not by the externality of de-risking but by the willful development of anonymous cryptocurrency tokens by some programmers as well as the existence of exchanges that unabashedly advertise their lack of KYC requirements. As cryptocurrency investors and traders discover that blockchain forensics tools make it easier to de-anonymize transactions and compromise the privacy levels of popular cryptocurrencies

such as bitcoin and Ethereum, many users are seeking cryptocurrencies with stronger anonymity features and less traceability, such as Monero and Zcash.[14] This is not surprising because a strong libertarian ethos motivated the rise of bitcoin in the wake of the 2008 financial crisis when cynicism and distrust of the banking sector intensified.

In response to the perceived dwindling of privacy in the cryptocurrency space, some software developers are building decentralized cryptocurrency exchanges that facilitate trading without taking possession of users' tokens and without requiring customer identity verification. These platforms work through software-encoded smart contracts that simply transfer values between addresses of different cryptocurrencies and do not need central servers to store and move tokens, as regular cryptocurrency exchanges do. This trading structure minimizes the risk of hackers attacking servers to steal tokens, but it also eliminates token custodianship. Lacking central servers could encourage some decentralized exchanges to operate with less regard for legal requirements usually attached to jurisdictions. In fact, one decentralized exchange site published a blog post in February 2018 highlighting a critical benefit of its service—that it operates with "no KYC."[15] Criminals tend to be early adopters of new technologies and thus are likely to take advantage of these more anonymous ecosystems, adapting and innovating as opportunities arise to transact outside of regulated spaces.[16] Therefore, ensuring that cryptocurrency exchanges enforce KYC requirements has become all the more important.

RECONCEIVING REGULATORY FRAMEWORKS

The growth of a bifurcated cryptocurrency sphere means that financial authorities will have to address both philosophical questions and tactical challenges in implementing regulatory and enforcement frameworks. One question, for instance, is whether an underground cryptocurrency ecosystem is akin to the underground cash economies that operate in parallel to many formal financial sectors. In the world of fiat currencies, authorities could try to bring the informal sector into the formal economy, but underground economies are unlikely to completely disappear. However, underground fiat money and underground cryptocurrency markets are structurally different.

Large amounts of fiat cash cannot be transported across borders easily. Moving volumes in the billions, or even hundreds of millions, in cash requires planes or caravans of trucks; such movements are inherently conspicuous and need sophisticated schemes to conceal. However, transferring cryptocurrency units across the globe is no more technically difficult when the value is in the millions of dollars than when it is in the hundreds. The only thing likely preventing the widespread movement of illicit funds in untraceable, anonymous cryptocurrencies right now is the relatively low level of capitalization and liquidity of tokens such as Monero. Decentralized exchanges, though growing in number, account for perhaps 1 percent of cryptocurrency trading, according to blockchain technology experts.[17] The underground cryptocurrency ecosystem has not yet scaled to serve as the primary place for transaction.

This bifurcation, while important for conceptual purposes, is not always clear, nor is it static. If a business running a decentralized exchange decides to implement KYC protocols for its users, it would join the above-ground ecosystem. And many experts would argue that centralized exchanges with poor AML practices and elusive owners such as BTC-e—which was notorious for facilitating money laundering before it was shut down by law enforcement in 2017—are underground operations.[18] Still, the differing technical features should not be ignored, as they necessitate different regu-

latory and enforcement approaches. For the most part, the same investigative and enforcement techniques used to go after conventional money transmitters with poor AML practices can be used to address owners of centralized exchanges. However, the greater decentralization and built-in anonymity of the most nascent cryptocurrency innovations make traditional law enforcement methods inadequate. Authorities should be prepared for untraceable coins and no-KYC exchanges to become more prevalent.

Countering illicit activity associated with the underground cryptocurrency system will require innovation. The blockchain forensics tools that work well in analyzing bitcoin transactions are mostly ineffective at tracking Monero, for example. And while law enforcement can easily subpoenas owners of centralized exchanges, compelling them to provide information about customers suspected of illicit transactions, many decentralized exchange platforms keep no records at all of user identities.

Strategies relying on intervention and enforcement by centralized entities are not fit for the underground cryptocurrency ecosystem. Financial regulation authorities should instead consider decentralized approaches. The bitcoin protocol was groundbreaking in developing cryptography and game-theory technology to incentivize disparate actors across the globe to confirm transactions and authenticate a growing, distributed ledger. Enforcement officials should work with blockchain technology experts who share their goal of minimizing illicit finance in the cryptocurrency system. Government and industry experts should explore together how cryptocurrency platforms could be leveraged to support AML aims, whether by making cleaner coins more valuable or by crowdsourcing and validating reports of illicit transactions and actors. Additional, more suitable, strategies will become apparent as the technology evolves and becomes widely adopted, and as traders, investors, and regulators learn more about the cryptocurrency system.

ENDNOTES

1. Lily Katz, "Bittrex Gets Bank Agreement to Help You Buy Bitcoin With Dollars," Bloomberg, May 31, 2018, http://bloomberg.com/news/articles/2018-05-31/bittrex-gets-bank-agreement-to-help-you-buy-bitcoin-with-dollars.
2. Cryptocurrency exchanges are websites that allow users to buy or sell cryptocurrencies. See Annaliese Milano, "Chainalysis Raises $16 Million for Real-Time Crypto Compliance," Coindesk, April 5, 2018, http://coindesk.com/chainalysis-raises-16-million-for-real-time-crypto-compliance; Will Yakowicz, "Startups Helping the FBI Catch Bitcoin Criminals," *Inc.,* January 9, 2018, http://inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html.
3. Michael del Castillo, "$817M Later: LexisNexis Partners With First Institutional Cryptocurrency Exchange," *Forbes*, June 4, 2018, http://forbes.com/sites/michaeldelcastillo/2018/06/04/817m-later-lexisnexis-partners-with-first-institutional-cryptocurrency-exchange/#2ff552ab4ff1.
4. U.S. Department of the Treasury, *National Money Laundering Risk Assessment 2015* (Washington, DC: Government Printing Office, 2015), http://treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.
5. Yaya J. Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows Into Digital Currency Services," Foundation for Defense of Democracies, January 12, 2018, http://defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.
6. Financial Crimes Enforcement Network, "FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities," news release, U.S. Department of the Treasury, March 18, 2013, http://fincen.gov/sites/default/files/news_release/20130318.pdf; Financial Transactions and Reports Analysis Centre of Canada, "FINTRAC Advisory Regarding Money Services Businesses Dealing in Virtual Currency," Government of Canada, July 30, 2014, http://canafe-fintrac.gc.ca/new-neuf/avs/2014-07-30-eng.asp; Presidency of the European Union, "Proposal for a Directive 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," Council of the European Union, December 19, 2017, http://data.consilium.europa.eu/doc/document/ST-15849-2017-INIT/en/pdf.
7. Europol, "Europol Hosted 4th Conference on Virtual Currencies," Europol, July 5, 2017, http://www.europol.europa.eu/newsroom/news/europol-hosted-4th-conference-virtual-currencies.
8. Wolfie Zhao, "G20 Eyes October Deadline for Crypto Anti-Money Laundering Standard," Coindesk, July 23, 2018, http://coindesk.com/g20-eyes-october-deadline-for-crypto-anti-money-laundering-standard.
9. Group of Twenty, "Communiqué," Group of Twenty Finance Ministers and Central Bank Governors Meeting, July 22, 2018, http://g20.org/sites/default/files/media/communique-_fmcbg_july.pdf.
10. William Suberg, "Bithumb Crypto Exchange Bans Accounts From 11 Countries," Coin Telegraph, May 28, 2018, http://cointelegraph.com/news/bithumb-crypto-exchange-bans-accounts-from-11-countries; Joseph Young, "South Korea's Biggest Cryptocurrency Exchange Posts 171x Revenue Spike in 2017," CCN, April 10, 2018, http://ccn.com/south-koreas-biggest-cryptocurrency-exchange-posts-171x-revenue-spike-in-2017.
11. A digital currency address is an alphanumeric string used as a public identifier to send, receive, and store digital currency value, such as bitcoin. A wallet is software that can contain multiple addresses. See Office of Foreign Assets Control, "Questions on Virtual Currency," U.S. Department of the Treasury, March 19, 2018, http://treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs.
12. Matthew Collin et al., *Unintended Consequences of Anti–Money Laundering Policies for Poor Countries* (Washington, DC: Center for Global Development, 2015), http://cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf.
13. Sudhir Khatwani, "7 Altcoin Exchanges to Start Trading On Without KYC & AML," Coinsutra, April 2, 2018, http://coinsutra.com/altcoin-exchanges-without-kyc-aml.
14. Douglas Heaven, "Sitting With the Cyber-Sleuths Who Track Cryptocurrency Criminals," *MIT Technology Review,* April 19, 2018, http://technologyreview.com/s/610807/sitting-with-the-cyber-sleuths-who-track-cryptocurrency-criminals.
15. The Blocknet, "Understanding a Decentralized Exchange," Medium, February 6, 2018, http://medium.com/@theblocknetchannel/understanding-a-decentralized-exchange-eee9e1043f45.
16. Emma Jacobs, "Taking on the Smart Criminals," *Financial Times*, April 9, 2015, http://ft.com/content/806ac8f0-d7ac-11e4-849b-00144feab7de.
17. Nathan Sexer, "State of Decentralized Exchanges, 2018," Medium, January 31, 2018, http://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79.

18. U.S. Attorney's Office, Northern District of California, "Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack of Mt. Gox," U.S. Department of Justice, July 26, 2017, http://justice.gov/usao-ndca/pr/russiannational-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.