A Cryptic Challenge: Banking Virtual Currencies

Tom Keatinge and Kayla Izenman

Banks, guardians of the integrity of the financial system, cannot hide from the risks posed by cryptocurrencies; they must learn to move on from a poor strategy of avoidance and de-risking.

Cryptocurrencies and their use and potential abuse are rarely out of the headlines. In 2017, the rapid and steep rise in the price of cryptocurrencies such as Bitcoin – at one point reaching a value of $19,783 before crashing to $6,000 just three months later – drew wide public and media attention. There has been a regular diet of press coverage more recently, with stories ranging from the plans announced by Facebook to create a new global currency powered by blockchain technology; to the reported 'widespread and increasingly sophisticated' cyberattacks launched by North Korea to steal cryptocurrency from exchanges, platforms via which users are able to hold their coins in online (and offline) wallets as well as transfer funds from cryptocurrency to fiat currency, and vice versa; to the nascent use of cryptocurrencies by terrorists and extremists. Over the past two years, recognising that cryptocurrencies are here to stay, regulators, led by the Financial Crimes Enforcement Network (FinCEN), the financial intelligence unit in the US – and, more recently, the Financial Action Task Force (FATF) – have begun to grapple with the challenge of managing and controlling their use.

The extent to which cryptocurrencies, and their features that enable privacy and anonymity, attract criminal actors has become ever more apparent. Those interested in the use of cryptocurrencies span the breadth of illicit actors, regardless of political affiliation or motivation. For example, right-wing extremists and neo-Nazi organisations have been known to utilise cryptocurrencies, but so have jihadi terrorist groups. In addition, organised crime groups, dark web users, money launderers and human traffickers have all shown interest in the technology. As Europol has observed, the criminal use of cryptocurrencies is growing, with Bitcoin remaining the coin most frequently encountered by law enforcement.

A Range of Illicit Activity

Along with the cryptocurrencies themselves, adjacent third-party platforms are equally abused and exploited by criminals. In this regard, one of the technologies most subject to abuse are cryptocurrency exchanges. Centralised exchanges – trusted third-parties that complete cryptocurrency transactions by identifying and matching buyers and sellers – are by far the easiest way to transact in cryptocurrencies, making them a natural target for exploitation by money launderers and other illicit actors.

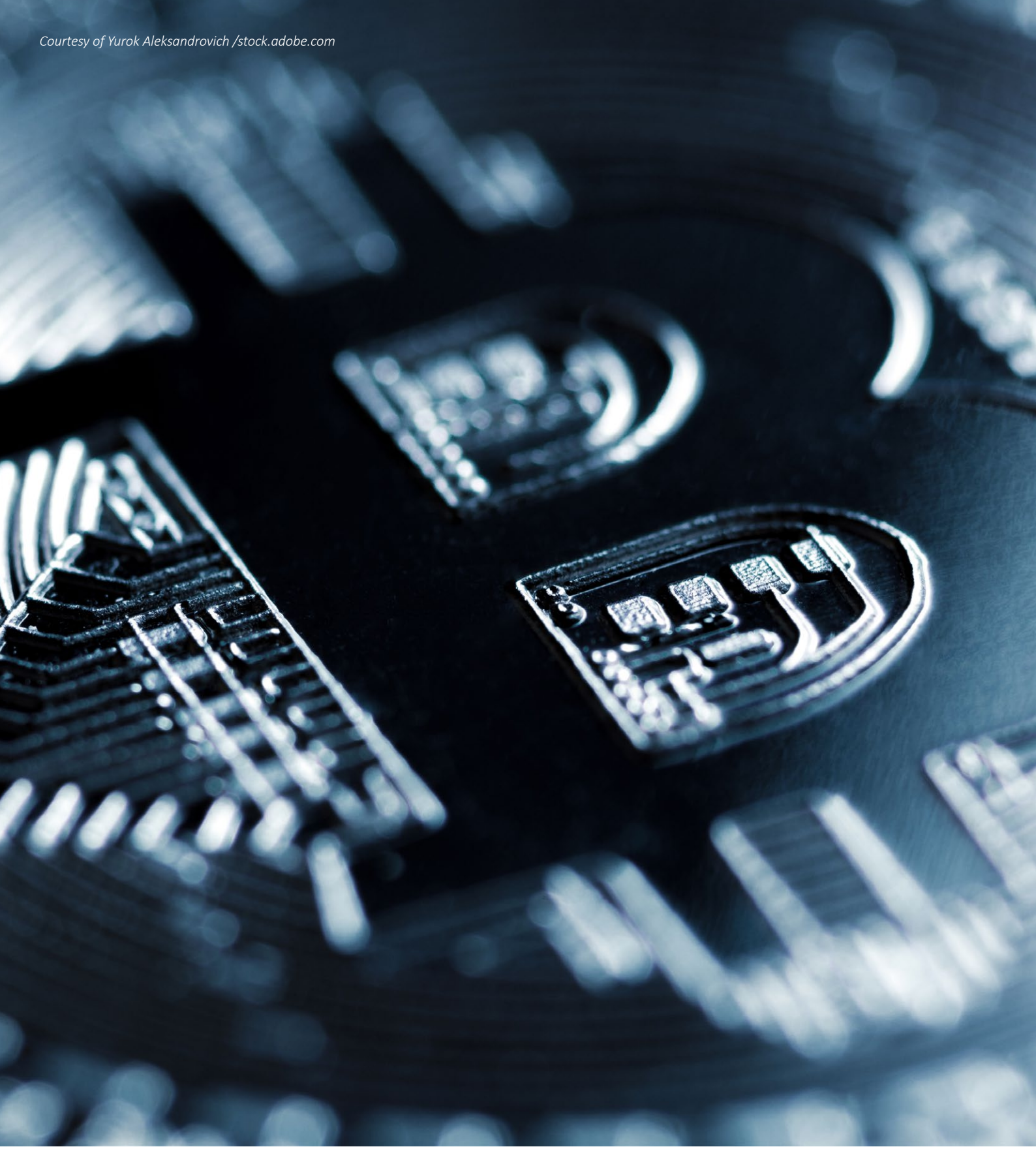
Cryptocurrency exchanges have found themselves increasingly subject to the online equivalent of a bank heist

However, as well as being used by criminal actors and those seeking to operate beyond the law, cryptocurrency exchanges have found themselves increasingly subject to the online equivalent of a bank heist. Many exchanges hold users' funds – at least partially – in 'hot' cryptocurrency wallets, which are hosted online and connected to the internet in some way. This may allow access for hackers who would not have been able to access 'cold' wallets, which are stored offline. These hacks are increasingly frequent, with eight reported large-scale hacks so far in 2019, including thefts from Cryptopia, Coinmama, DragonEx, CoinBene, Bithumb, Binance, Bitrue and BITPoint, ranging in value from $5 million to $100 million. Experts estimate that $227 million had been stolen in the first half of 2019, appearing to continue the trend of the $950 million estimated to have been stolen in 2018.

The Mt. Gox hack is undoubtedly the most well-known exchange hack. The Japanese exchange has been hacked twice, once in 2011 and then again in 2014, leading to the eventual bankruptcy of the company. At the time of the second hack, Mt. Gox was handling 70% of all Bitcoin transactions worldwide and stated that 850,000 bitcoins (around $480 million at the time) had been lost in the hack.

Indeed, Mt. Gox is not the only hack of this scale, and not even the largest, although it is the largest involving Bitcoin. In January 2018, hackers stole 500 million NEM (a lesser-known cryptocurrency launched in 2015, equivalent to approximately $533 million) from Coincheck, another Japanese cryptocurrency exchange.

Beyond criminals, countries seeking to operate financial and trade relations outside the reach of economic sanctions, such as those



Courtesy of Yurok Aleksandrovich /stock.adobe.com

imposed multilaterally by the UN or unilaterally by the US. Employing the benefits of cryptocurrencies and blockchain technology can free actors from the restrictions and risks created by sanctions regimes. Furthermore, deploying cybercrime capabilities can also boost otherwise restricted fundraising activities for sanctioned actors. For example, North Korea was famously responsible for the 2017 WannaCry ransomware attack, which generated an estimated £109,000 in Bitcoin, and was also reliably attributed as the perpetrator of multiple exchange hacks.

Returning to Reality: Real-World Risks for Bankers

While much of this illicit activity occurs in cyberspace, beyond the reach of existing regulatory and law enforcement intervention, at some point cryptocurrencies will need to be

exchanged into fiat currency or used to purchase goods and services.

For banks, tasked with ensuring the integrity of the formal financial system, the wide-ranging use of cryptocurrencies and the difficulties faced in determining their source (in terms of how the value was earned and from whom it came) appears extremely challenging. At first glance, the policies and procedures banks employ to ensure the integrity of the business they facilitate seem ill-equipped to tackle the complexities posed by cryptocurrencies. So, how do cryptocurrencies pose risks to bankers? And how can these risks be mitigated?

How do cryptocurrencies pose risks to bankers? And how can these risks be mitigated?

The Basel Committee on Banking Supervision warned in March 2019 that cryptocurrency growth may pose a number of risks to global financial stability, and banks specifically. The committee painted a challenging picture, stating that, '[cryptocurrencies] present a number of risks for banks, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering and terrorist financing risk; and legal and reputation risks'. To understand the risk for banks as relates to cryptocurrency abuse by illicit actors, it is key to understand a selection of these threats.

Providing services to exchanges or clients using cryptocurrency is generally viewed as risky in the banking sector – many opt to end existing relationships with exchanges or refuse to set up accounts in the first place. One widely publicised example saw Wells Fargo cut ties with the exchange Bitfinex in 2017. Others reject or block clients' cryptocurrency-related transactions on credit cards. And even those that were initially willing to open accounts, such as Barclays for Coinbase, have reportedly recently reversed their originally welcoming position.

As the banking sector has come to terms with the risks posed by cryptocurrencies, formal financial crime compliance policies have been developed. In early 2019, both J.P. Morgan and Bank of America listed cryptocurrencies as a risk factor for their companies. Bank of America specifically cited concerns regarding the potential for cryptocurrency to 'make it more difficult for the bank to comply with regulations by impairing its ability to track the movement of customer funds' thus inhibiting its know-your-customer (KYC) and other anti-money-laundering (AML) checks. This threat is certainly the most obvious – banks have a responsibility to identify and monitor their clients, and cryptocurrencies may prohibit or restrict banks' capacity to fulfil this regulatory requirement. Cryptocurrency is generally viewed (often erroneously) as an entirely anonymous means of exchanging value, leading many to believe that user identification is impossible.

Banks face the added risk of having to manage a threat that is largely misunderstood by governments that deploy highly varied, and mostly unhelpful, regulatory approaches.

Banks face the added risk of having to manage a threat that is largely misunderstood by governments that deploy highly varied, and mostly unhelpful, regulatory approaches. These range from outright bans to openly courting business from exchanges and other cryptocurrency-related activities such as initial coin offerings, where investors in business start-ups are rewarded for their investment with a form of cryptocurrency rather than ownership shares.

Same, Same; Not Different

While the 'virtual' nature of these risks may look unfamiliar, in many ways they actually mirror risks that banks have been dealing with for years. For example, dealing with the increased KYC and AML risks posed by servicing exchanges, as well as customers using cryptocurrency, are not the impossible tasks they may seem to be. The key to mitigating these perceived threats lies in the relationship between traditional financial institutions and cryptocurrency-related businesses. A steep 99% of cryptocurrency transactions currently pass through centralised exchanges – meaning exchanges have the potential to facilitate, rather than hinder, KYC and customer due diligence processes. If customers wishing to open accounts at a centralised exchange are required to present appropriate identification, along with evidence of the source of their funds if they are exchanging fiat currency for cryptocurrency, banks providing services to those exchanges would actually have an extra layer of protection, rather than an increased risk. Similarly, exchanges and other virtual asset service providers (VASPs, the term adopted by the FATF for businesses or persons that conduct a range of activities connected with cryptocurrencies) will ideally face the same obligations as financial institutions to file suspicious transaction reports, thus operating within the existing anti-financial crime architecture.

The key to mitigating these perceived threats lies in the relationship between traditional financial institutions and cryptocurrency-related businesses

For many years, banks have been using client screening and transaction monitoring tools to support their financial crime compliance activity. Part of increasing protection while dealing with cryptocurrencies requires supplementing existing tools with specialist

transaction-monitoring tools, particularly blockchain-tracing capabilities.

Blockchain tracing helps identify patterns of illegal activity as well as monitor for red flags or further information on suspicious customers or transactions. Given Bitcoin's transparent nature, all transactions can be viewed and analysed on the blockchain. An exchange (or a bank or any third-party) has full access to these tools for the accounts held on or related to their platform. It is worth noting that some newer cryptocurrencies, such as Monero, do not provide this level of transparency, but given that Bitcoin still accounts for over two-thirds of the total cryptocurrency market – and many purchases of privacy coins like Monero are still made with Bitcoin – blockchain tracing is certainly a good place to begin. Blockchain tracing companies such as Elliptic and Chainalysis have already worked with law enforcement and the private sector to create enhanced monitoring tools for the cryptocurrency space. These tools can peel back some – although not all – of the layers of opacity that concern banks and other actors required to police the real-world financial system.

Partnership and Understanding are Key

But all of this is only possible with open and positive relationships, not only between banks and exchanges, but also with the public sector. Governments have the responsibility to standardise monitoring and reporting requirements in their jurisdiction, a realisation that has come to the fore in the past year. The one-year US presidency of the FATF, which ended on 30 June, had aimed to 'prioritize clarifying how the FATF standards apply to virtual currency providers and related businesses', specifically focusing on how 'the FATF standards apply to virtual currency providers and related businesses, including for customer due diligence, funds transfers, supervision, and enforcement'. The result of this initial move by the international community towards implementing universally applicable standards was the publication in June 2019 of guidance for a risk-based approach. This document endeavours 'to help both national authorities in understanding and developing regulatory and supervisory responses to [virtual asset] activities and VASPs, and to help private sector entities seeking to engage in [virtual asset] activities, in understanding their AML/CFT obligations and how they can effectively comply with these requirements'.

In providing this guidance, the FATF cites Italy, Norway, Sweden, Finland, Mexico, Japan and the US as examples of countries effectively regulating the AML/CFT risks associated with cryptocurrencies. Consistent with its desire to avoid catalysing de-risking (which describes the wholesale exclusion of sectors such as charities and remittance companies from the financial system) the FATF explicitly states that, 'it is important that [financial institutions] apply the risk-based approach properly and do not resort to the wholesale termination or exclusion of customer relationships within the VASP sector without a proper risk assessment'. Displacement of virtual risk – as in the real world – does not dispense with the threat, it merely moves it into less visible channels, forcing VASPs into relationships with financial service providers that perhaps do not apply the same level of due diligence, thus merely increasing the scope of the financial crime problem.

Cryptocurrencies, in one form or another, are here to stay; banks cannot avoid exposure to the risks they pose by attempting to ignore their existence

The need for risk assessment is not novel in the financial sector. Indeed, it has been central to the development of the anti-financial crime system over the past 30 years. And cryptocurrencies, while certainly providing a new means by which financial crime can be committed, do not actually require a whole new way of thinking about risk, nor do their interactions with banks require the complete restructuring of the financial system.

Getting Coordinated

The vulnerabilities currently posed to banks by cryptocurrencies stem from a lack of understanding and coordination across all key parties. VASPs, especially exchanges, should be requiring increased KYC and due diligence information from customers, and banks can and should require this level of due diligence if choosing to onboard these businesses. This interface between VASPs and the banking system is the key systemic risk. Exchanges rely on some access to the traditional financial system if they hope to convert cryptocurrency to fiat currency in any manner, and banks should not feel threatened, but rather view this as an opportunity. Cryptocurrency usage is only growing, but its expansion is marred by the public perception that the technology is exclusively a tool for criminals or speculative investors. Many banks have chosen to compensate for their ignorance by avoiding the cryptocurrency universe entirely. But these two worlds are inevitably connected and can enjoy a mutually beneficial relationship if they are able to assess and mitigate risks in a comprehensive manner, bringing additional business to financial institutions as well as strengthening regulatory mechanisms surrounding cryptocurrency usage.

Cryptocurrencies, in one form or another, are here to stay; banks cannot avoid exposure to the risks they pose by attempting to ignore their existence. Better to learn to understand the risks associated with cryptocurrencies and develop policies that embrace their responsible use.

Tom Keatinge is the Director of RUSI's Centre for Financial Crime and Security Studies.

Kayla Izenman is a Research Analyst in RUSI's Centre for Financial Crime and Security Studies.

The views expressed in this article are the authors', and do not represent those of RUSI or any other institution.