RUSI
Royal United Services Institute
for Defence and Security Studies

Emerging Insights

Virtual Asset Mining: Typologies, Risks and Responses

Allison Owen and Aaron Arnold

August 2023

EXECUTIVE SUMMARY

The rise in digital assets' popularity over the last decade has attracted its fair share of illicit actors. Prized for their ease of use and perceived relative anonymity, digital assets such as Bitcoin have become targets for sanctions evaders, criminal enterprises, narcotraffickers and terrorist networks. North Korea, for example, has stolen billions of dollars' worth of cryptocurrency in the past five years, in part to fund its WMD programme. Consequently, regulatory, monitoring and enforcement agencies have had to set their sights on addressing the often overlooked space between traditional finance and cryptocurrency. Despite modest progress addressing key vulnerabilities that cryptocurrency creates for global finance, the dynamic and rapidly changing nature of digital assets requires new thought about risk and sources of risk.

One increasingly difficult problem for regulatory and monitoring authorities is how to address and mitigate risks associated with cryptocurrency mining (the processes used to verify transactions). Unlike traditional cryptocurrency exchanges, mining typically falls outside the scope of anti-money-laundering (AML) regulatory authorities and can provide illicit actors with a stream of nearly anonymous – and possibly unlimited – revenue. Unfortunately, discussions on how to best mitigate these risks is largely absent from broader policy discussions on regulating and monitoring digital assets.

This paper, intended for policymakers and those with compliance obligations, seeks to broaden the discussions of risk around cryptocurrency by providing a typology of risks related to cryptocurrency mining. The objective is not to provide an all-encompassing snapshot of cryptocurrency mining activities, but to offer a general framework for policymakers to consider and mitigate a range of risks that may not be immediately apparent. The paper also places the described typologies within the context of recent or emerging regulatory and enforcement actions, to highlight gaps and challenges.

The paper concludes with a series of recommendations aimed at mitigating risks and addressing regulatory and monitoring shortfalls in relation to cryptocurrency mining, consistent with global AML standards. These include, for example, modifying registration requirements for commercial and remote mining enterprises so that they fall under the purview of regulatory frameworks, despite outstanding questions over custody of cryptocurrency.

It is abundantly clear that illicit actors have focused in on the usefulness of cryptocurrency, and it is quite likely that cryptocurrency will feature in financial crime for decades to come. Given the uniqueness, novelty and rapidly evolving nature of the digital assets industry, however, it is critically important that policymakers continue to think outside the box, re-examine previously held assumptions about the nature of risks associated with cryptocurrency – including mining – and continuously adapt regulatory and monitoring frameworks in response to emerging risks.

INTRODUCTION

What was once considered a fringe, novel technology, virtual assets – that is, cryptocurrencies such as Bitcoin – now have a global market capitalisation of more than $1 trillion.[1] The sheer scale and scope of the cryptocurrency industry, paired with regulation and monitoring challenges, have created, over the past decade, opportunities for illicit state and non-state actors to facilitate financial crimes, including sanctions evasion, money laundering and terrorist financing, among others, using cryptocurrencies.

In 2018, the Financial Action Task Force (FATF), the international organisation responsible for setting anti-money-laundering (AML) and counterterrorist-finance (CTF) standards, set about addressing threats posed by digital assets to the international financial system. However, despite the introduction of several new requirements, including a requirement for virtual asset service providers (VASPs) to be 'regulated for (anti-money laundering and countering the financing of terrorism) AML/CTF purposes, and licensed or registered, and subject to effective systems for monitoring … or supervision',[2] key vulnerabilities and gaps remain.

One of these gaps is cryptocurrency mining, which is generally not covered by AML rules and regulations. Mining cryptocurrency is the process by which users verify the accuracy of transactions on a blockchain and are subsequently rewarded for their efforts with newly minted cryptocurrency. Due to the fundamental design of this decentralised process, little in the way of information is available to national authorities on who has 'mined' cryptocurrency.[3]

1. For more information on the global virtual asset market capitalisation, see CoinMarketCap, 'Today's Cryptocurrency Prices by Market Cap', <https://coinmarketcap.com/>, accessed 4 August 2023; Billy Bambrough, '"The Sky's the Limit" – Crypto Now Braced for a Multi-Trillion Wall Street Earthquake After Bitcoin, Ethereum, BNB, XRP, Cardano, Dogecoin, Litecoin, Solana, Tron and Polygon Price Boom', *Forbes*, 25 July 2023, <https://www.forbes.com/sites/digital-assets/2023/07/25/the-skys-the-limit-crypto-now-braced-for-a-multi-trillion-wall-street-earthquake-after-bitcoin-ethereum-bnb-xrp-cardano-dogecoin-litecoin-solana-tron-and-polygon-price-boom/?sh=74cff3d9f520>, accessed 7 August 2023.
2. Financial Action Task Force (FATF), 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', updated February 2023, p. 17, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 4 August 2023.
3. Identifying the scale of cryptocurrency mining within a country is often limited to inferential methods. For example, those based on energy consumption or aggregating IP addresses from cryptocurrency mining pools. For more information on how this information is collected, see University of Cambridge Judge Business School, Cambridge Centre for Alternative Finance, 'Cambridge

Because there is very little in the way of transparency on miners, mining has attracted illicit actors ranging from narcotics traffickers to sanctions evaders such as North Korea. In 2019, for example, a report by the UN Panel of Experts on North Korea found that the country engaged in mining cryptocurrencies to generate revenue for its military programmes.[4]

This paper offers jurisdictions a typology of laundering through cryptocurrency mining. The objective is to increase overall awareness of money-laundering and proliferation-finance risks posed by mining, as well as guidance on how to best address these threats from a legal and regulatory perspective. Although this paper is not meant to be comprehensive, it aims to expand on these identified threats so that jurisdictions can detect vulnerabilities in their financial systems and form risk mitigation strategies.

Mining has attracted illicit actors ranging from narcotics traffickers to sanctions evaders

The paper first outlines general financial crime risks associated with cryptocurrency mining that have occurred since Bitcoin's start. Next, it presents a typology of cryptocurrency mining risks, designed to illustrate how illicit actors can take advantage of existing and emerging mining to facilitate money laundering and proliferation financing. Finally, the paper concludes with an analysis of the legal and regulatory challenges to responding to mining risks, and their implications.

METHODOLOGY

The typologies outlined in this paper are based on a series of semi-structured interviews with public and private stakeholders, including representatives of VASPs, blockchain analytics companies, compliance specialists and academics.[5]

These interviews, along with a review of relevant news articles, guidance released by international organisations and other law enforcement and regulatory actions, have helped to inform case studies and risk mitigation strategies.

Bitcoin Electricity Consumption Index Methodology', <https://ccaf.io/cbnsi/cbeci/mining_map/methodology>, accessed 7 July 2023.

4. UN Security Council, 'UNSC Report S/2019/691', 30 August 2019, p. 26, <https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports>, accessed 22 April 2022.
5. Six semi-structured interviews were conducted online between February and August 2022 to further identify areas at risk of proliferation financing. As miners themselves would not be able to provide information about the risk of financial crime, which is the focus of this paper, they were not interviewed for this research. Experts interviewed are based in the US, Europe and Asia.

UNDERSTANDING CRYPTOCURRENCY MINING RISKS

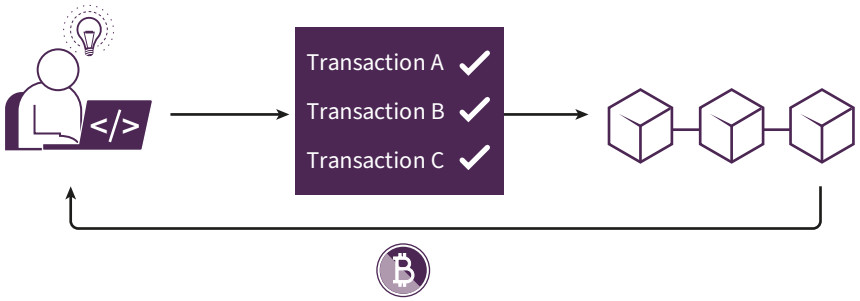
The FATF defines virtual assets as 'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'.[6] Bitcoin, for example, one of the most recognised and earliest virtual assets, was first conceptualised in 2008 as a decentralised currency – that is, free of a central monetary authority.

A decentralised digital currency, however, faces a significant hurdle: without a central authority, how can users be assured that the record of transactions is complete and accurate? To solve this problem, Bitcoin and other similar types of cryptocurrencies use a 'proof-of-work' model to validate and record transactions on a blockchain.

The blockchain, or ledger, consists of blocks of transactions linked together. In a proof-of-work model, a user, referred to as a cryptocurrency miner, employs computer processing power (or 'work') to solve a computationally complex mathematical problem that effectively ensures transactions are accurate and in the correct order – that is, that each new block is linked to the previous one.

This work, however, is not free. To incentivise users to keep the ledger accurate, miners are rewarded with cryptocurrency (such as Bitcoin). Miners compete against other miners to be the first to solve the complex problem and the first miner to do so is permitted to record the next block of transactions. Figure 1 illustrates how new blocks of transactions are added to a given blockchain that uses a 'proof-of-work' model.

Figure 1: Proof-of-Work Model



Source: Author generated.

Note: An individual uses their computer processing power to solve complex mathematical problems, resulting in transaction verification on the blockchain.

6. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation', p. 135. This paper uses the terms 'virtual asset', 'digital asset' and 'cryptocurrency' interchangeably.

Importantly, mining increases the overall supply of cryptocurrency. Minting new cryptocurrency through mining, however, creates several pernicious problems from a financial crime perspective. Namely, newly minted cryptocurrency is not easily linked to an individual. Because of this, mining cryptocurrency is an attractive target for enterprising criminal organisations, sanctions evaders and those looking to avoid law enforcement and intelligence agencies.

In 2019, for example, an investigation by Brazil's Department of Narcotics uncovered a cryptocurrency mining operation as part of a drug enforcement investigation, shining a light on how criminal organisations are adapting to digital currencies.[7] Similarly, in Argentina, there have been reports of crime associated with illicitly obtaining cryptocurrency mining equipment, either to launder funds or to make money from reselling the equipment at a lower price.[8]

North Korea's brazen cyber attacks against cryptocurrency businesses and applications, which have netted the country billions of dollars in cryptocurrency, are now well known. According to a 2019 UN report, North Korea has also been involved in mining cryptocurrency since at least May 2017.[9] In February 2020, a cyber-security firm found that North Korea's mining activity had increased at least tenfold since May 2019, based on an analysis of a North Korea-linked IP address.[10]

While converting stolen cryptocurrency to fiat currency requires a multi-step laundering process that runs the risk of detection, mining, on the other hand, has the potential to generate a nearly anonymous revenue stream. The ability to generate practically decoupled revenue is an enticing lure

7. Intsights Defend Forward, 'The Dark Side of Latin America: Cryptocurrency, Cartels, Carding, and the Rise of Cybercrime', <https://intsights.com/resources/the-dark-side-of-latin-america-cryptocurrency-cartels-carding-and-the-rise-of-cybercrime>, accessed 24 February 2022; Juan Camilo Jaramillo, 'Latin America Lacks Regional Strategy to Halt Bitcoin Money Laundering', InSight Crime, 7 May 2019, <https://insightcrime.org/news/brief/latin-america-lacks-regional-strategy-Bitcoin-money-laundering/>, accessed 4 August 2023.
8. Federico Fahsbender and Pilar Safatle, 'Las placas para minería de criptomonedas son el nuevo objeto de deseo de los ladrones porteños' ['Cryptocurrency Mining Boards are the New Object of Desire of Buenos Aires Thieves'], *Infobae*, 4 May 2022, <https://www.infobae.com/sociedad/policiales/2022/05/04/las-placas-para-mineria-de-criptomonedas-son-el-nuevo-objeto-de-deseo-de-los-ladrones-portenos/>, accessed 30 March 2023.
9. UN Security Council, 'UNSC Report S/2019/691', p. 28; Priscilla Moriuchi, 'North Korea's Ruling Elite Adapt Internet Behaviour to Foreign Scrutiny', Recorded Future, 25 April 2018, <https://www.recordedfuture.com/north-korea-internet-behavior>, accessed 23 November 2022.
10. Insikt Group, 'How North Korea Revolutionized the Internet as a Tool for Rogue Regimes', Recorded Future, 9 February 2020, <https://www.recordedfuture.com/north-korea-internet-tool>, accessed 4 August 2023. Since 2020, however, little research has been carried out on North Korea's crypto-mining activities.

to illicit activity. Indeed, as illustrated in the next section, there has been a significant increase in the scale and scope of illicit activity targeting the cryptocurrency mining process.

The mining industry, however, is not static. Much like virtual currency, mining encompasses rapidly changing and dynamic technologies. To better understand how illicit actors can exploit mining, the next section provides a series of typologies and case studies.

KEY CRYPTOCURRENCY MINING TYPOLOGIES

This section describes a range of available cryptocurrency mining typologies, which includes cryptojacking and remote mining. These methods pose a challenge to law enforcement and regulatory authorities because they involve an individual receiving newly minted cryptocurrency that is not tied to previous transactions, thus making user identification more difficult. Such coins can then be converted to fiat currency without detection of a criminal link on the blockchain. The fourth typology in this section focuses on cryptocurrencies that use a 'proof-of-stake' transaction verification model. Although this model does not provide a viable laundering mechanism, it is a method that illicit actors can use to generate revenue.

TYPOLOGY 1: CRYPTOJACKING

Due to the steep costs of specialised equipment, or sometimes a lack of access to stable internet or power grids, criminals have turned to cryptojacking – the process of hijacking another user's computer processing power to mine cryptocurrency without their knowledge.

In 2014, for example, a researcher used supercomputers funded by the US National Science Foundation (NSF – an independent federal government agency) to mine Bitcoin, resulting in his suspension from working with the US government. According to an audit report, '[t]he researcher misused over $150,000 in NSF-supported computer usage at two universities to generate Bitcoins valued between $8,000 and $10,000'.[11] Later, from 2017 to 2021, this illicit revenue generation method grew in popularity as demand and price for cryptocurrency increased.

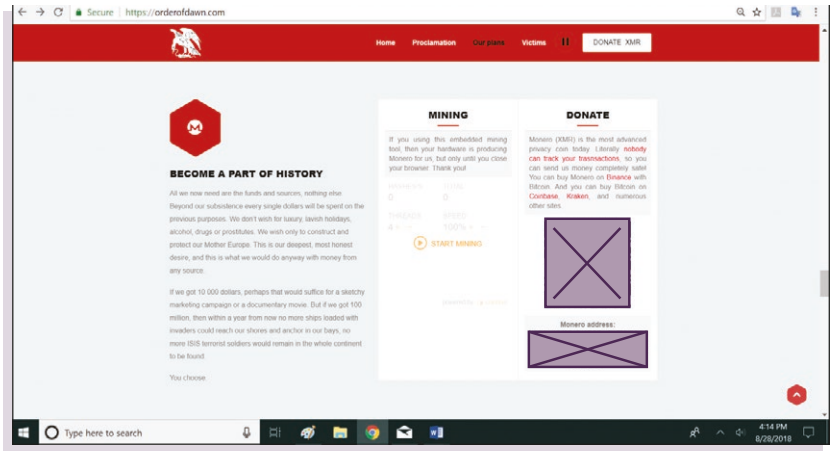
Browser-based cryptojacking, or 'drive-by mining', likewise grew in popularity. The process involves embedding malicious code in a website, which allows the website owner to use visitors' computer processing power to mine cryptocurrency.[12] While there are legitimate reasons a website owner may

11. Office of Inspector General, National Science Foundation, 'Semiannual Report to Congress', March 2014, pp. 29–30, <https://www.nsf.gov/pubs/2014/oig14002/oig14002.pdf>, accessed 30 November 2022.
12. Jérôme Segura, 'A Look into the Global "Drive-by Cryptocurrency Mining" Phenomenon', Malwarebytes, October 2017, <https://go.malwarebytes.com/rs/805-USG-300/images/Drive-by_Mining_FINAL.pdf>, accessed 22 April 2022.

include web-based mining on a website – such as generating revenue for a charity – criminal enterprises, extremists or even sanctions evaders can exploit the same method to generate revenue.

In 2018, for example, a neo-Nazi militant group known as the Order of Dawn allowed supporters to mine Monero to generate revenue for its volunteer army. The group's website is shown in Figure 2.[13]

Figure 2: Order of Dawn and Cryptocurrency Mining



Source: Counter Extremism Project, 'Far-Right European Terrorist Group Crowdfunding Cryptocurrency', 28 April 2018, <https://www.counterextremism.com/blog/far-right-european-terrorist-group-crowdfunding-cryptocurrency>, accessed 7 July 2023.

Cryptojacking can also occur on a larger scale by rerouting unwitting users' computer processing power to a mining 'pool', which functions as an aggregator for computer processing power. This method has the potential to create a nearly anonymous revenue stream for an illicit actor. Alternatively, it is also possible to target and hijack resources from cryptocurrency mining pools. In 2014, a hacker gained access to a Canadian internet provider and rerouted traffic from a legitimate pool to a malicious pool, which netted nearly US$84,000 worth of Bitcoin.[14]

Cryptojacking has similarly caught the attention of North Korea. One of the first reported cases of North Korea-linked criminal activity associated with cryptojacking occurred in 2017, when cyber-criminals hacked a South

13. David Carlisle, 'Preventing Financial Crime in Cryptoassets: The Definitive Practical Guide for Governance, Risk and Compliance Professionals', Typologies Report 2022, Elliptic, 20 March 2022, <https://www.elliptic.co/resources/typologies-report-2022>, accessed 7 July 2023.
14. Tom Brewster, 'Hacker Makes $84k Hijacking Bitcoin Mining Pool', *The Guardian*, 7 August 2014, <https://www.theguardian.com/technology/2014/aug/07/hacker-bitcoin-mining-pool-internet-service-providers-canada-dell>, accessed 20 April 2022.

Korean company's server to illicitly mine Monero.[15] North Korea was able to mine nearly 70 Monero coins, worth approximately $25,000 at the time.[16]

North Korea is also alleged to have employed malware to infect computers to mine Monero. According to a 2019 UN report, analysts were able to trace the mined Monero back to servers located at Kim Il Sung University.[17]

TYPOLOGY 2: COMMERCIAL MINING FACILITIES

Large-scale mining operations have become a lucrative business in recent years, and although the exact number of commercial mining facilities worldwide is unknown, the scale and scope of the industry can be estimated by the demand that such facilities place on power grids. A 2022 report by the US Office of Science and Technology Policy, which coordinates interagency science and technology policy efforts, found that commercial mining facilities are on the rise, estimating that the 'total global estimated electricity usage for blockchains that support crypto-assets in 2022 falls into a range of 120 to 240 billion kWh per year'.[18] While such estimates can fluctuate considerably according to demand within cryptocurrency markets, this nonetheless highlights the sheer magnitude of such operations, which at times has accounted for nearly 1% of global energy consumption.[19]

Mining facilities also have the capability to provide illicit actors with a substantial and relatively anonymous revenue stream. Mined cryptocurrency can be moved across jurisdictions through peer-to-peer transactions and potentially converted to fiat currency at cryptocurrency businesses worldwide.

The capital costs of such ventures can, however, be high. Specialised equipment, such as application-specific integrated circuits (ASICs), can cost anywhere from thousands to tens of thousands of US dollars. In at least one

15. Sam Kim, 'North Korean Hackers Hijack Computers to Mine Cryptocurrencies', *Bloomberg*, 2 January 2018, <https://www.bloomberg.com/news/articles/2018-01-02/north-korean-hackers-hijack-computers-to-mine-cryptocurrencies>, accessed 22 April 2022.
16. *Ibid*.; UN Security Council, 'UNSC Report S/2019/691', p. 111.
17. UN Security Council, 'UNSC Report S/2019/691', p. 29.
18. The White House, 'Climate and Energy Implications of Crypto-Assets in the United States', September 2022, p.14, <https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-atCrypto-Assets-and-Climate-Report.pdf>, accessed 4 August 2023.
19. Tom Robinson, 'How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil', Elliptic, 21 May 2021, <https://www.elliptic.co/blog/how-iran-uses-Bitcoin-mining-to-evade-sanctions>, accessed 16 November 2022; Kim Grauer, Will Kueshner and Henry Updegrave, 'The 2022 Crypto Crime Report', Chainalysis, February 2022, <https://go.chainalysis.com/2022-crypto-crime-report.html>, accessed 16 November 2022.

case, illicit actors have used the crypto-mining process to launder other ill-gotten gains, as shown in the following case study.

Box 1: Case Study: Bitcoin Mining Centres and Crime

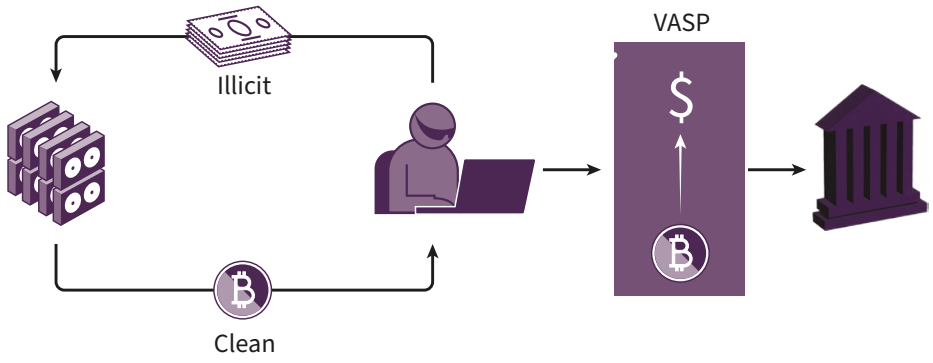
In 2016, Spanish police and tax authorities arrested 30 individuals suspected of laundering illicit proceeds via Bitcoin mining centres. The authorities seized Bitcoin mining centres that they suspected were being used by a large criminal network to launder funds. The amount of funds laundered through the operation is unknown.

Sources: Dev Odedra and Chris Gschwend, 'On the Periphery: Financial Crime Risks in Cryptocurrency Mining', KYC360, 13 July 2020, <https://kyc360.riskscreen.com/article/on-the-periphery-financial-crime-risks-in-cryptocurrency-mining/>, accessed 24 January 2022; *Reuters*, 'Spain Arrests 30 Suspected of Laundering Money in Bitcoin Centres', 25 May 2016.

State actors have also focused on large-scale mining facilities

Figure 3 provides a notional summary of how criminal networks could feasibly invest in mining equipment that can ultimately provide revenue that is decoupled from any illicit activity.

Figure 3: Mining as a Laundry Service



Source: Author generated.
Note: A criminal uses illicit funds to purchase or rent a mining 'rig'. In return, they receive clean cryptocurrency and can transfer funds across jurisdictions or convert them to fiat currency at exchanges with limited detection. By contrast, on regulated cryptocurrency exchanges, the criminal in question would still face the need to surpass controls during the customer onboarding procedure.

In addition to criminal networks, state actors have also focused on large-scale mining facilities, requesting that the proceeds be sold to a central bank. Iran, for example, used this technique to generate revenue while under sanctions, according to several blockchain analytics firms.[20] Furthermore, the head of

20. Tom Robinson, 'How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil', Elliptic, 21 May 2021, <https://www.elliptic.co/blog/how-iran-uses-Bitcoin-mining-to-evade-sanctions>, accessed 16 November 2022;

Iran's Trade Promotion Organization has said that the country's central bank had made a proposal for how Iran can 'use the cryptocurrencies produced internally or cryptocurrencies purchased by companies such as the private sector' for the import of goods.[21] Similarly, although the full extent of North Korea's mining operations is unknown, its 2020 efforts to mine Monero demonstrate, at a minimum, an interest in conducting mining operations on a larger scale.

Of course, there are several elements necessary for a successful commercial operation and, therefore, the extent of this financial crime risk will vary among jurisdictions. First and foremost is whether there is access to stable and cheap power. According to the Cambridge Centre for Alternative Finance, mining farm operators generally choose locations with lower electricity costs to optimise profit.[22] In addition to cheap power, commercial facilities also require stable access to the internet that can accommodate transferring data at high speeds. Climate can also play a role. Mining is preferred in regions with low temperatures, which can help operators avoid substantial cooling costs.

As demand for cryptocurrency has increased, many states have considered and enacted policies to attract the crypto-mining industry. One such example is Transnistria, an unrecognised republic situated between Ukraine and Moldova. The unrecognised breakaway state adopted legislation in 2018 to legalise cryptocurrency mining and created incentives to attract parts of the industry. In addition to offering cheap, stable energy, Transnistria also allows entrepreneurs to set up a mining facility without needing to register as a local company.[23]

Chainalysis, 'The 2022 Crypto Crime Report', February 2022, <https://go.chainalysis.com/2022-crypto-crime-report.html>, accessed 16 November 2022.

21. *Mehr News*, 'Cryptocurrencies in International Trade for the Next Two Weeks', 10 January 2021, <https://www.mehrnews.com/news/5396149>, accessed 28 January 2022.
22. Garrick Hileman and Michel Rauchs, 'Global Cryptocurrency Benchmarking Study', Cambridge Centre for Alternative Finance, 2017, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf>, accessed 19 July 2022.
23. Lubomir Tassev, 'Another Post-Soviet Jurisdiction Welcomes Crypto Miners', *Bitcoin News*, 2 February 2018, <https://news.Bitcoin.com/another-post-soviet-jurisdiction-welcomes-crypto-miners/>, accessed 27 July 2022; Supreme Council of the Pridnestrovian Moldavian Republic, 'О развиьии информационных блокчеий-технологий в Приднестровской Молдавской Республике' ['Law of the Pridnestrovian Moldavian Republic "On the Development of Information Blockchain Technologies in the Pridnestrovian Moldavian Republic"'], updated 16 June 2021, <http://www.vspmr.org/legislation/laws/zakonodateljnie-akti-pridnestrovskoy-moldavskoy-respubliki-v-sfere-konstitutsionnogo-stroya-osnov-pravoporyadka-a-takje-deyateljnosti-organov-gosudarstvennoy-vlasti-i-upravleniya/zakon-pridnestrovskoy-moldavskoy-

TYPOLOGY 3: REMOTE MINING

The rising costs of specialised mining equipment, as well as the need for cheap power and stable internet infrastructure, have prompted the formation of businesses that host mining equipment on behalf of customers.

Remote mining presents a particularly thorny problem when it comes to combating financial crime. Operators of remote mining services may be unaware of their client's identity or whether they are acting on behalf of a third party, as they are often located in different jurisdictions. This could mean that a remote mining service could unwittingly facilitate sanctions evasion or other types of illicit activity.

Host mining facilities, for example, allow remote customers to purchase mining rigs hosted on their property. The overhead costs for a hosting service typically comprise electricity and maintenance costs, including the setup of the mining equipment. Once the rig is operating, all earnings are directly transferred to the wallet that the customer has listed – whether their own or a third party's.

One host mining facility, Bitriver, fell onto the US sanctions list in 2022. BitRiver and its subsidiaries were alleged to have aided Russia in monetising its natural resources by leveraging the country's cheap energy to mine cryptocurrency.[24] Prior to unilateral sanctions, BitRiver created a cryptocurrency known as the BTR Token. Holders of the coin receive an equivalent amount of electricity power for their hosted mining equipment and can submit tokens once a month to pay up to 10% of the bill.[25]

In a similar manner, host mining facilities typically allow a portion of the electricity costs to be paid in cryptocurrency, which could provide avenues for criminal organisations and sanctions evaders to launder the proceeds of crime. It would be quite feasible for a representative operating on behalf of a sanctioned country to pay for electricity costs with illicit funds, and in return receive mined cryptocurrency decoupled from any criminal link.[26] Notably, if traceable cryptocurrency is used to pay for a portion of the mining fees, investigators can still track the funds to the business that accepted

---

respubliki-o-razvitii-informatsionnih-blokcheyn-tehnologiy-v-pridnestrovskoy-moldavskoy-respublike-.html>, accessed 27 July 2022.

24. US Department of Treasury, 'U.S. Treasury Designates Facilitators of Russian Sanctions Evasion', 20 April 2022, <https://home.treasury.gov/news/press-releases/jy0731>, accessed 16 November 2022.
25. BitRiver, 'About', 15 May 2023, <https://bitriver.farm/en/about>, accessed 15 May 2023.
26. Dev Odedra and Chris Gschwend, 'On the Periphery: Financial Crime Risks in Cryptocurrency Mining', KYC360, 13 July 2020, <https://kyc360.riskscreen.com/article/on-the-periphery-financial-crime-risks-in-cryptocurrency-mining/>, accessed 23 June 2022.

the illicit funds. However, the facility may be based in a jurisdiction that is not cooperative.

Some commercial mining facilities also offer cloud-based mining services, whereby users can lease equipment and computer time. Some of the primary cloud-based mining services allow payment in cryptocurrency and for the receiving cryptocurrency address to be changed after purchase. The benefit of using such services is that it can help reduce long-term costs, including investments in expensive equipment, as well as provide a solution to those in jurisdictions with geographic, energy, legal or other limitations on mining. Like host mining, the user does not need to be physically located in the jurisdiction to reap the rewards of mining.

If information is needed, it is likely that the cloud-based mining service would keep a database of cryptocurrency addresses used by the customer. However, depending on whether the service obtains custody of the funds, it can be unclear to investigators where the funds then move to, when looking at on-chain activity. This form of laundering is outlined in the following case study of a North Korea-linked cyber group.

The user does not need to be in the jurisdiction to reap the rewards

Box 2: Case Study: North Korea and Cloud Mining Services

In March 2023, Mandiant, a US cyber security firm, released a report on the cryptocurrency laundering methods of APT43, a North Korea-linked cyber group. According to Mandiant, APT43 likely uses hash rental (the rental of a set amount of computing power to mine cryptocurrency) and cloud-based mining services as a method of laundering funds. The process of laundering via hash rental and cloud-based mining services allows for the buyer's original payments and the mined cryptocurrency to be decoupled.

Source: Fred Plan et al., 'APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations', Mandiant, 29 March 2023, p. 7, <https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage>, accessed 30 March 2023.

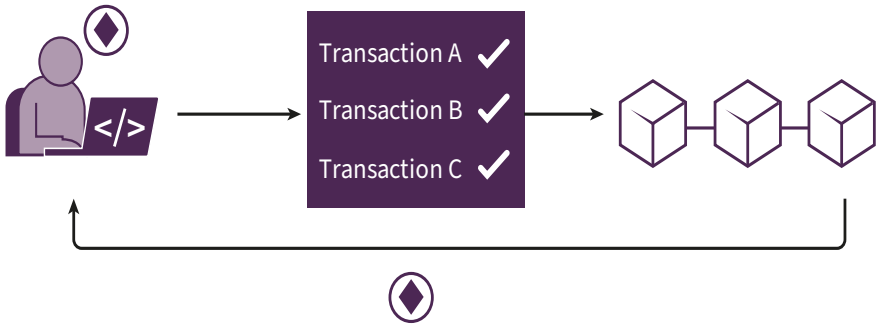
Another cloud mining model involves peer-to-peer marketplaces that allow payments in cryptocurrency. For these services, the buyer can mine using the seller's computer processing power. Of course, this can also create problems – especially from a transparency perspective.[27] Operators of cloud mining services such as these generally have, for example, no insights into their users' activities.[28]

27. Due to the lack of custody of client funds, the operator of the mining farm generally does not fall under the FATF definition of a VASP and is thus not required to implement compliance measures to counteract money laundering, terrorist financing and proliferation financing.
28. ByBit Learn, 'What is Cloud Mining and How Does it Work?', 25 May 2021, <https://learn.bybit.com/crypto/what-is-cloud-mining/>, accessed 21 April 2022.

TYPOLOGY 4: PROOF-OF-STAKE MODEL

Whereas a proof-of-work model requires miners to solve computationally complex problems to verify the accuracy of a blockchain and record new transactions, the proof-of-stake model requires validators to 'stake' their own cryptocurrency as collateral to verify transactions. To confirm a transaction, the blockchain network randomly selects a validator based on the number of coins the user has staked.[29]

Figure 4: Proof-of-Stake Model



Source: Author generated.
Note: An individual stakes their own funds and, when chosen, will verify transactions on the blockchain.

Overall, proof-of-stake mining is less energy- and resource-intensive than a proof-of-work model. For these reasons, it may be more attractive to illicit actors. North Korea, for example, has a large stock of cryptocurrency from its various hacks over the past five years that the country could feasibly stake – effectively allowing it to 'earn interest' on its illicit hacking operations.

Recently, Ethereum, a blockchain-enabled platform that allows smart contracts,[30] shifted its economic model from proof-of-work to proof-of-stake to reduce environmental impact.[31] For many illicit actors, this move could prove a boost to revenue generation. A recent report by Harvard University's Belfer Center for Science and International Affairs noted that while North

29. E Napoletano and Benjamin Curry, 'Proof of Stake Explained', *Forbes*, 8 April 2022, <https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake/>, accessed 22 July 2022.
30. Smart contracts are 'contracts' that are coded and stored on the blockchain. They automate transactions between the creator and recipients without the involvement of a third party.
31. Amy Castor, 'Why Ethereum is Switching to Proof of Stake and How it will Work', *MIT Technology Review*, 4 March 2022, <https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/>, accessed 16 April 2022; Ethereum, 'The Merge', 25 July 2022, <https://ethereum.org/en/upgrades/merge/>, 27 July 2022.

Korea has not previously mined Ether, the shift to a proof-of-stake model may prove more attractive for revenue generation.[32]

Staking coins, along with cryptojacking, commercial mining facilities and remote mining, represent avenues for criminals to circumvent regulations or take advantage of a lack of oversight. Despite the difficulty of identifying users behind the transaction verification process, the public and private sectors can take steps to mitigate potential risks.

REGULATORY RESPONSE, IMPLICATIONS AND SOLUTIONS

The preceding analysis of key crypto-mining typologies – cryptojacking, commercial mining, remote mining and staking – shows that, despite global interest in regulating digital assets, significant risks to the global financial system remain. In most cases, crypto mining does not fall within the purview of financial supervisors or AML frameworks. The following section addresses some of these legal and regulatory challenges, as well as their implications.

Currently, only a handful of countries have addressed cryptocurrency mining within their sectoral risk assessments. Moreover, of those that have attempted to tackle mining, regulatory approaches have varied considerably. In some jurisdictions, for example, legislation explicitly states that cryptocurrency mining activity is outside the scope of AML rules and regulations, while in other jurisdictions, miners are subject to licensing and registration requirements.

REGULATORY APPROACHES

Among the many challenges is the fact that cryptocurrency mining businesses do not generally retain custody of the mined cryptocurrency. This means they do not generally fit into the category of financial institutions that fall under the purview of the FATF.

From the perspective of the FATF, 'natural or legal persons that solely engage in the operation of a VA [virtual assets] network and do not engage in or facilitate any of the activities or operations of a VASP on behalf of their customers … are not VASPs', even if those activities are undertaken as part of

32. Heeu Millie Kim, June Lee and Rachel Paik, 'North Korean Cryptocurrency Operations: An Alternative Revenue Stream', North Korea Cyber Working Group Policy Memo No. 1, Belfer Center, May 2022, <https://www.belfercenter.org/sites/default/files/files/publication/North%20Korean%20Cryptocurrency%20Operations%20-%20An%20Alternative%20Revenue%20Stream.pdf>, accessed 16 November 2022.

their business.[33] Examples provided by the FATF of activities that would not in themselves qualify an entity to be considered a VASP include:

- Offering customers internet network services and infrastructure.
- Providing computing resources ('cloud services and creating, validating, and broadcasting blocks of transactions').[34]

Similarly, the report notes that those that do not fall under the definition of a VASP include '[v]alidators … whose functions are only validating transactions [and] cloud service providers whose functions are only offering the operation of infrastructure'.[35]

To provide further clarification on these requirements, countries have taken steps to release guidance on crypto mining. However, in the US, for example, little has been done in the way of modernising AML rules and regulations related to crypto mining. Current guidance, put forward by the Financial Crimes Enforcement Network (FinCEN), the key agency responsible for countering money laundering in the US, is now nearly a decade old.[36]

China banned mining outright in 2021

This guidance, unfortunately, does not take into account crypto-mining businesses, noting that '[t]o the extent that a user mines Bitcoin and uses the Bitcoin solely for the user's own purposes and not for the benefit of another, the user is ***not*** an MSB [money service business] under FinCEN's regulations'.[37] Thus, a crypto-mining company is typically not considered an MSB, and as such is not required to implement AML rules and regulations, such as know-your-customer procedures and record-keeping requirements, which are commonplace at banks.[38]

Some countries have taken drastically different approaches. China, for example, banned mining outright in 2021. Prior to the ban, nearly 50% of global Bitcoin mining occurred in China.[39] In response to the new restrictions, cryptocurrency mining companies relocated to other jurisdictions, including

33. FATF, 'Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', October 2021, p. 32, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>, accessed 7 April 2023.
34. *Ibid*.
35. *Ibid*., p. 35.
36. Department of the Treasury, Financial Crimes Enforcement Network, 'Application of FinCEN's Regulations to Virtual Currency Mining Operations', FIN-2014-R001, 30 January 2014, <https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R001.pdf>, accessed 20 July 2022.
37. *Ibid*. Emphasis in original.
38. *Ibid*.
39. Cambridge Centre for Alternative Finance, 'Bitcoin Mining Map', 2022, <https://ccaf.io/cbnsi/cbeci/mining_map>, accessed 18 April 2022.

Russia, Kazakhstan, Iran and the US.[40] Despite the ban, however, an analysis of hash rates, which can be a proxy for measuring total levels of mining, indicate that there are still mining operations in mainland China.[41]

The following subsections offer recommendations that countries should consider to restrict abuse of this type of activity.

Consider the Risk

The overall lack of rules around businesses that offer crypto-mining services poses a problem for securing the international financial system against illicit actors. The typologies outlined in this paper detail various methods that criminal networks and sanctions evaders can exploit to generate relatively 'clean' streams of revenue – that is, revenue not linked to a specific criminal group or individual or prohibited activity.

Given the risks posed to the international financial system, states should, at a minimum, consider their relative risk exposure to crypto mining from a cyber security standpoint, and identify associated risk with businesses within the industry. This includes understanding the scale and scope of mining-centric businesses within their jurisdiction, which is not always straightforward – especially if there are no registration or licensing requirements. At a minimum, countries should include their crypto-mining industries within national risk assessments.[42] To aid with understanding risk and mitigation strategies, operators of crypto-mining enterprises should be included in domestic public–private partnerships centred on cryptocurrency.

Jurisdictions should be especially concerned if sanctions evasion or other types of illicit financial activity have previously been associated with their jurisdiction. It is important to note that countries have an obligation to implement and enforce international sanctions. In the case of North Korea, for example, states are required to prevent the provision of financial services or economic resources to North Korea. While crypto-mining services may not fit neatly within the definition of a 'financial service', they are nonetheless an economic resource that North Korea could exploit to support its nuclear weapons and ballistic missile programme.

---

40. It is also worth noting that China, as of 2019, acted as one of the main producers of cryptocurrency mining equipment. See, for example, Andrey Sergeenkov, 'China Crypto Bans: A Complete History', CoinDesk, 9 March 2022, <https://www.coindesk.com/learn/china-crypto-bans-a-complete-history/>, accessed 12 July 2022.
41. Cambridge Centre for Alternative Finance, 'Bitcoin Mining Map'.
42. FATF members are required to conduct a national money-laundering, terrorist-financing and proliferation-financing national risk assessment. For more information, see FATF, 'FATF Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', October 2021, <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html>, accessed 7 April 2023.

Understand Regional Risk

Another factor countries should consider is regional risk exposure. There could be negative spillover effects from neighbouring jurisdictions that incentivise crypto-mining businesses, such as by offering cheap energy or establishing free trade zones with favourable crypto-mining laws. For example, a country with little or no crypto-mining activity but active cryptocurrency exchanges may face significant risks from illicit actors mining in one region and cashing out in another.

Collect and Verify Beneficial Ownership Information

Countries need to identify and verify individuals who have ownership and control of crypto-mining facilities located in their jurisdictions.[43] As shown in the second section, illicit actors can exploit such facilities for laundering or sanctions evasion purposes, so it is critical to identify who is behind operations.

The FATF outlines that countries should take measures to prevent the misuse of corporate vehicles for criminal purposes by:

- Understanding the risk associated with legal arrangements.
- Making legal persons and legal arrangements sufficiently transparent.
- Requiring corporate vehicles to provide accurate and up-to-date basic and beneficial ownership information to competent authorities in a timely fashion.[44]

Furthermore, to detect large-scale mining facilities that are not registered as businesses, law enforcement can look at spikes in energy consumption, as the proof-of-work mining process requires a substantial amount of energy.

Require Customer Identification and Verification

Countries should also consider modifying registration requirements for commercial and remote mining enterprises. At a minimum, regulatory authorities should require these companies to retain customer identifying information for law enforcement purposes.

---

43. Countries should register legal entities. However, it is critical to also have a robust process in place to collect, verify and share beneficial ownership information. As of April 2022, the FATF reported that only 9% of countries were meeting the effectiveness requirement for collecting and sharing beneficial ownership. For more information, see FATF, 'Report on the State of Effectiveness and Compliance with the FATF Standards', April 2022, p. 6, <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html>, accessed 7 July 2022.
44. FATF, 'Beneficial Ownership of Legal Persons', March 2023, pp. 10, 21, 38, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html>, accessed 7 April 2023.

While most types of crypto-mining activities would not meet the definition of a VASP, and thus not be subject to AML rules and regulations, collection of customer information by remote crypto-mining businesses is highly recommended. By undertaking the following checks on remote clients when establishing business relations these facilities can ensure sanctions compliance:

- Recording the full name, date of birth, nationality and address of the customer.
- Verifying the information provided to ensure the use of official government identification documents.
- Keeping a record of cryptocurrency addresses used by the customer to receive generated funds.

If illicitly obtained funds are linked to the remote crypto-mining business, holding this customer information will aid in law enforcement investigations. Furthermore, these facilities need to ensure they do not accept funds from sanctioned entities by screening customer information against relevant sanctions lists.

CONCLUSION

Criminal networks and state actors have both used crypto mining to generate nearly anonymous streams of revenue. While the scale and scope of these illicit operations is largely unknown, the risk posed to the international financial system is clear.

In a rapidly evolving industry, new innovations also bring new opportunities for illicit actors to exploit, and governments are failing to recognise risks associated with mining. To mitigate the risks that mining can generate, it will be important for governments to think outside traditional AML frameworks. Defining a crypto-mining company as an MSB, for example, may be akin to trying to place a square peg in a round hole. Instead, identification of beneficial ownership and recording client information will likely prove more useful for identifying illicit activity.

ABOUT THE AUTHORS

Allison Owen is an Associate Fellow at RUSI's Centre for Financial Crime and Security Studies. Her primary research projects focus on the policy and security dimensions of cryptocurrency and new payment methods. Allison leads RUSI's work on cryptocurrency and counter-proliferation finance, focusing on North Korea's use of crypto to evade sanctions, and provides guidance for the private and public sector to understand and mitigate associated threats. She holds an MA in Nonproliferation and Terrorism Studies from the Middlebury Institute of International Studies, Monterey, an MA in International Affairs from MGIMO University, Moscow, and a BSc in

Electrical Engineering from the University of Kansas. Allison is also a Certified Anti-Money Laundering Specialist.

Aaron Arnold is a Senior Associate Fellow in the Centre for Financial Crime and Security Studies at RUSI, where his work focuses on sanctions and proliferation financing. Prior to joining RUSI, Aaron served as the finance and economics expert on the UN Panel of Experts for North Korea sanctions, where he monitored global sanctions implementation and investigated instances of sanctions violations. Before joining the Panel of Experts, Aaron was a fellow with the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center, where he published work on the extraterritorial use of sanctions and the efficacy of WMD trade controls. He also previously worked as a counter-proliferation subject matter expert in the US Department of Defense and the US Justice Department, where he specialised in WMD counter-proliferation investigations and operations. Aaron holds a PhD and an MPP in public policy and national security from George Mason University and a BA in political science from Virginia Tech.

About RUSI

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

The views expressed in this publication are those of the author(s), and do not necessarily reflect the views of RUSI or any other institution.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)