GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

# Crypto, crime and control

## Cryptocurrencies as an enabler of organized crime

John Collins

June 2022

**Acknowledgements**

The author would like to thank all the reviewers and colleagues who provided feedback for this report, in particular Mark Shaw, Tuesday Reitano, Michael Levi, Jay Albanese, Catalina Uribe Burcher and Crispin Yuen. Thanks also to Nicole Kalczynski for her support with fact checking and proofing.

**About the author**

John Collins is director of academic engagement at the Global Initiative Against Transnational Organized Crime. He is also a Fellow at the Centre for Criminology, University of Hong Kong, and editor in chief of the Journal of Illicit Economies and Development, LSE Press. His research interests include the political economy of national and multilateral drug control, cryptocurrencies and outlaw motorcycle clubs. He recently published a book titled *Legalizing the Drug Wars: A Regulatory History of UN Drug Control* with Cambridge University Press (2021). John holds a PhD in international history from the London School of Economics and Political Science.



Cover: © *Da-kuk/iStock via Getty Images Plus*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

# CONTENTS

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **AML/CTF** | Anti-money laundering/counter-terrorism financing |
| **CBDC** | Central bank digital currency |
| **DAO** | Decentralized autonomous organization |
| **DeFi** | Decentralized finance |
| **DLT** | Distributed ledger technology |
| **FATF** | Financial Action Task Force |
| **ICO** | Initial coin offering |
| **IMF** | International Monetary Fund |
| **IRS** | US Internal Revenue Service |
| **NFT** | Non-fungible token |
| **VA** | Virtual asset |
| **VASP** | Virtual asset service provider |

# EXECUTIVE SUMMARY

Classical economics views money as a functional tool of real economic activity. It facilitates transactions, provides a measure for comparative valuation, a store of wealth and a means of deferred payment. In the licit sphere, money is widely viewed by economists as a 'veil', representing no real long-run economic activity in itself. However, in the underworld of illicit economies and organized crime, money is a facilitator of underlying enterprises – drug trafficking, trafficking in human beings, wildlife trafficking, illegal mining and a number of other criminal activities. Money is part of the process of washing illicit gains into seemingly licit assets and activities, while access to fungible money becomes a scarce commodity. Into this fray emerged cryptocurrencies: a mixture of technological innovation, libertarian pseudo-economics and a mechanism to enable transactions to escape from the regulated financial economy.

Global finance is undergoing a period of great technological disruption. Much of this stems from the innovations sparked by blockchain technologies, in particular Bitcoin. This is driven by the push for decentralization, changes in payment processing and a potential new role for central banks. Blockchain technologies have facilitated the promise of decentralized finance (known as DeFi) and the proliferation of cryptocurrencies and virtual assets.

The payments-processing industry currently generates US$1.5 trillion in annual revenue, and this could rise to US$3 trillion by 2030.[1] Moreover, with roughly 2 billion people unbanked worldwide, financial innovations bring the tantalizing prospect of enabling more people to gain access to mainstream finance.[2] Financial inclusion has witnessed a marked improvement in recent decades, driven by technological forces including mobile-phone technology and fintech. According to the 2017 Global Findex Database, 1.2 billion people gained access to bank accounts between 2011 and 2017.[3] However, with innovation and change comes risk, particularly for enabling crime, corruption, sanctions avoidance, money laundering, terrorist financing and the emergence of financial-market systemic risk.

This report aims to provide a broad overview of cryptocurrencies and organized crime. It is meant for readers that may have an expertise in one, both or neither, as a means to better understand the challenges posed by emerging blockchain technologies and decentralized finance. The paper argues that blockchain technologies and their derivatives are a significant technological innovation, but one that has unclear use cases and outcomes. Potential use cases are currently speculative and surrounded by uncertainty, hype and, in many cases, fraud and Ponzi schemes.[4]

The paper points to central bank digital currencies (CBDCs) as a key global innovation with perhaps the most significant transformative outcomes of blockchain technologies, despite not being based on


**The New York Stock Exchange displays BITO, the first Bitcoin-linked exchange-traded fund in the US. As of June 2022, BITO is priced at US$13.96, down 66.69% over the past year.** *Photo: Spencer Platt/ Getty Images*

such technology. It also points to the regulatory changes underway in response to these emerging technologies and calls for a continued roll-out in regulatory and law enforcement capabilities to limit the risks and challenges posed by these technologies.

Such a focus is timely, understudied and widely misunderstood. A 2022 report by Europol highlighted that the scale of illicit activities enabled by cryptocurrencies is increasing. Their role in facilitating transactions is rising, although it remains relatively low compared with cash and other forms of illicit transactions. Cryptocurrencies facilitate large-scale money laundering and enable an online trade in illicit goods and services, including child sexual abuse material, due to the supposed anonymity – or pseudonymity – they provide.[5] The scale of trade in child sexual abuse material enabled by Bitcoin is unparalleled. One case alone, in South Korea, is considered the largest archive of child sexual abuse material ever captured.[6]

A number of realities seem clear. First, blockchain has had a significant disruptive impact on traditional finance and systems of payment and money. It has driven financial intermediaries and central banks further into the digital age, partly out of fear of being left behind. It has forced regulators to come to terms with an array of previously unimagined technological and transnational coordination issues. Vast amounts of criminal and fraudulent activities have been enabled by these currencies and technologies, and it is likely that the scale of criminal innovation will continue to grow at a rapid pace.

Meanwhile, decentralized finance will almost certainly have further disruptive impacts on the operations of global finance, while proponents of Web3 (an internet based on blockchain technology) suggest its impact will prove nothing short of revolutionary. These disruptions will undoubtedly fuel new opportunities for frauds and predatory hype artists (those who manipulate public expectations in order to artificially inflate virtual asset prices); new platforms and tools for organized criminals and corrupt actors;[7] and new challenges for global regulators enforcing anti-money laundering/counter-terrorism financing (AML/CTF) regulations. There are also the geopolitical changes that these technologies will drive, and which member states and international institutions must come to terms with, including the disruption to global trading and financial infrastructure caused by their adoption.

Alongside these risks, there are significant opportunities that come with financial innovation. The cost–benefit, risk–reward calculations vary by cryptocurrency and DeFi system, driven by design,

regulation, utilization and a number of other factors. The most likely outcome will be an integration within and evolution of traditional finance, rather than a revolutionary change in money and global economic systems. Just as the US and China will find new competitive terrains in CBDCs and European countries will fixate on decentralized finance's contribution to the climate crisis, innovations will continue to become subservient to mainstream economic and geopolitical phenomena.

Blockchain may well prove revolutionary in its impact, but global regulators and institutions have shown a resolve and capability to ensure the changes it enables will occur within traditional state-regulated financial and institutional structures. Tackling organized crime, scams and AML/CTF, whether deriving from or enabled by these technologies, will need to remain a key focus for policymakers, particularly when the dust on the current 'cryptomania' settles – whenever that will be.

## Key findings

- The technological breakthrough of Bitcoin's pseudonymous creator Satoshi Nakamoto, marked by the publication of their 2008 paper,[8] is potentially revolutionary.
- It is likely that the implications of blockchain technology and its offshoots will remain unclear and obscured. Technical, regulatory and environmental challenges continue to be an existential hurdle.
- Cryptocurrencies could potentially help 2 billion people access licit finance, bringing their assets and identities within the global financial system. The realization of this goal is largely speculative and something that other forms of financial innovation and technology are already improving.
- Many of the supposed use cases for cryptocurrency technologies are based on speculative notions, anarcho-utopian goals, flawed economic thinking and unrealistic assessments of the capabilities of public policy. This creates an enabling environment for fraud and Ponzi schemes.
- Celebrities and CEOs have been accused of publicly manipulating cryptocurrencies for financial gain, while the continued development of 'crypto communities' has been plausibly likened to cults.[9]
- Central bank digital currencies are gaining traction and it is likely that they will play a significant role in future counter-crime efforts as well as being a probable avenue of geopolitical and economic competition.
- For an ostensibly radically decentralized project, centralization has rapidly occurred for on-ramp and off-ramp activities – i.e. the transition points between fiat currencies[10] and cryptocurrencies, where investors add or withdraw funds. As governments move to clarify regulatory rules, exchanges and products are becoming strictly regulated as the means to prevent abuse. This, in turn, may ultimately remove one of the core use cases of blockchain technologies – their decentralization.
- Public policies are moving in the right direction to counter the unregulated nature of crypto markets. More needs to be done with dynamic policy frameworks that can evolve and keep up with the pace of technological and financial innovation within the crypto sphere. These regulations could sound a death knell to the current generation of crypto industries.
- Regulators and law enforcement need to become more technologically adept to meet these growing challenges.

# THE CURRENT LANDSCAPE OF CRYPTO, CRIME AND REGULATION

At their most basic level, blockchain technologies – the underpinning of cryptocurrencies and decentralized finance – are deceptively simple. Blockchains essentially enable a decentralized ledger system that maintains an incorruptible, append-only system of records. In other words, it is an accounting system where records can only be added and never changed. With the launch of Bitcoin in 2009 and its many successors, blockchains appeared to overcome previous technological impediments to financial decentralization, including peer-to-peer transactions, self-executing contracts and decentralized organizations.

Yet the technology is deeply polarizing. It is admired as a formidable technological breakthrough, idealized as a panacea for the apparent ills of financial centralization and fiat currency, loathed as a facilitator of criminal activity, and viewed as a Ponzi scheme and financial lunacy on par with the Tulip mania of the 17th century.[11] To some, it is a store of value and hedge against inflation; to others, a highly volatile speculative asset class in which even its most prominent coin, Bitcoin, can fall 50 per cent in value in a three-month period and acts in near perfect correlation with inflation-risk assets such as speculative technology stocks.[12]

However, mainstream companies continue to adopt cryptocurrencies as a means of payment. PayPal is examining its own stablecoin (a cryptocurrency that seeks to peg its value to some external reference, for example the US dollar);[13] in April 2022 Mastercard created a joint venture with crypto lender Nexo to create the first 'crypto backed' payment card;[14] and Visa is conducting a pilot with Crypto.com.[15] In 2021, crypto venture-capital deals reached US$25 billion, a 500 per cent increase on 2020.[16] In November 2021, the total value of crypto assets in the world was roughly US$3 trillion, before more than halving to US$1.27 trillion in May 2022.[17] But other ventures are failing: formerly known as Facebook, Meta's plans for a stablecoin ultimately folded under US regulatory pressure.[18]

In 2021 alone, one analysis suggests total transaction volumes of cryptocurrencies rose 567 per cent on 2020 levels to US$15.8 trillion.[19] Given that rapid growth, the share of confirmed illicit activity conducted through cryptocurrencies actually shrank, growing at 79 per cent.[20] But law enforcement authorities and regulators would be hard pressed to find upside in a sector enabling a near doubling of confirmed illicit activities from US$7.8 billion in 2020 to 14 billion in 2021.[21] The authors of the report

also highlight that their previous years' estimates doubled upon discovering more illicit addresses utilizing the currency.[22] Extrapolating a similar outcome to 2021 would see the total figure reach almost US$32 billion. Moreover, these estimates may understate the share of illicit activities through intelligence gaps that overlook off-chain illicit activities (those occurring in the non-crypto world), including widespread fraud, money laundering and other obscured activities.[23]

In parallel to the crypto hype, the core innovation surrounding the technology may derive not from decentralized communities of users and web developers, but central banks. The emergence of a burgeoning field of CBDCs in over 90 countries and with more than 100 million users could perhaps offer the most long-term disruption of the technology. However, CBDCs largely shun the core block-chain technologies that underpin decentralized finance and cryptocurrencies, instead opting for more traditional centralized 'permissioned' ledgers (those that can only be edited by selected parties), a trend that seems set to continue.

Meanwhile, national regulatory bodies fret and position for some control over the market. As the US Securities and Exchange Commission Chair Gary Gensler said: 'At this time, it's more like the Wild West. This asset class is rife with fraud, scams and abuse … In many cases, investors aren't able to get rigorous, balanced and complete information. If we don't address these issues, I worry a lot of people will be hurt.'[24]

Others strike a more optimistic tone, suggesting that the long-term potential outweighs the short-term risks. As *The Economist* argued, decentralized finance 'has the potential to rewire how the financial system works, with all the promise and perils that entails'.[25] Others even suggest crypto will wipe out traditional finance, national fiat currencies and perhaps even economic inequality and hardship. For example, Bitcoin evangelist and president of El Salvador Nayib Bukele has made his country the first to accept Bitcoin as legal tender and has undertaken to invest in Bitcoin assets with national finances, purportedly through his mobile phone. His gamble has thus far produced disastrous results undermining the fiscal stability of the country and seeing tens of millions of national wealth wiped out.[26]

International institutions tasked with global financial stability fret over the consequences of cryptocurrencies' more mainstream adoption, relatively limited though it remains.[27] While the

Facebook executive David Marcus testifies during a hearing in Washington DC, July 2019. The company's plans to launch a dollar-backed stablecoin was obstructed by lawmakers. *Photo: Alex Wong/Getty Images*

use cases of blockchain technologies, cryptocurrencies and their derivative industries are unclear, financial regulators have increasingly sought to step into the void. Ironically, they do so in contravention of the libertarian goals of blockchain, which aimed to make the intermediated financial system irrelevant.

As of late 2021, according to research by the Law Library of Congress, nine countries, including China, Egypt, Morocco, Algeria, Tunisia, Bangladesh, Iraq and Qatar, have completely banned cryptocurrencies, while dozens of others have implicitly banned them through banking restrictions. The number of countries with severe restrictions has doubled since 2018.[28] Some do so for reasons of political and capital controls, while other pariah governments actively use them to enable geopolitical goals or to circumvent external capital controls.[29]

Most national governments point to criminal and consumer risks as reasons to prohibit these markets or bring them under stricter regulatory control.[30] Both outcomes challenge the fundamental anarcho-decentralization precepts that underpinned the early adoption of blockchain technologies – state control and regulation was not supposed to be possible. This challenge fuels the growing division within the crypto–decentralized finance world between those who maintain a revolutionary decentralized economic purism, and those who see mainstream institutional adoption as key to their scalability and embrace regulation to encourage adoption by traditional financial institutions.

Undoubtedly, many retail crypto investors are the victims of mis-selling, Ponzi schemes, ignorance and a number of other risks that favour unscrupulous actors in this under-regulated market. Possibly, the big cryptocurrencies will turn out to be Ponzi schemes in and of themselves.[31] Meanwhile, crypto has long been associated with facilitating criminal activities and a major source of organized criminal financing, money laundering and, to a lesser degree, terrorist financing.[32] Complete bans, however, would be wildly unpopular and hard to enforce in the major democratic countries, leading many states, such as the US, to try and regulate them instead.

# BLOCKCHAIN TECHNOLOGIES EXPLAINED

The crypto revolution began in October 2008 with the publication of an article by Satoshi Nakamoto. A still unknown cryptographer, they offered a solution to the paradoxes of peer-to-peer electronic cash systems that would negate the need for traditional commercial banks or central banks.[33]

Over centuries, systems of accounting and auditing have evolved to verify transactions, ledgers, ownership and distribution of economic goods. These systems are costly and ultimately duplicative but essential to modern economies and finance. To circumvent these centralized systems, blockchains look to overcome a key problem known as 'distributed consensus'. This problem centres on how multiple, independent computers can agree a common data set in the presence of faults and fraud.[34]

How can numerous actors agree on transactions, balances or overall ledgers when some will be accidentally or maliciously wrong, assigning value or assets to the wrong actors or duplicating transactions? For example, what if one actor tricks the system to send multiple payments to the same fraudulent processor for a good or service? A distributed consensus network ensures a consensus of data among computers and overcomes these problems.[35]

Bitcoin's distributed consensus algorithm derives from transaction validators, or 'miners', freely joining and competing to win rewards of bitcoin. The technological breakthrough is the application of a 'proof of work' function, which imposes computational costs on those mining for rewards. Miners collect a list of outstanding transactions, known as a 'block', while simultaneously competing to find a randomly chosen string of numbers and letters (a secure hash algorithm). The more miners competing, the harder the computational puzzle will be. When a miner solves the puzzle, they broadcast it along with the block, to the broader Bitcoin network and claim their reward. Rewards come from newly minted bitcoins (plus any fees that users have attached).[36]

The network then validates the block through consensus, verifying that transactions are legitimate and no double spending has occurred.[37] Then, competition for the next block begins, mathematically building on the preceding chain of blocks that computationally trace all the way to the origin Bitcoin block. The proof of work consensus mechanism makes it near mathematically impossible that a malicious actor can alter the blockchain without controlling 51 per cent of nodes within the network.[38] The value of Bitcoin is the incentive for miners to continue the process of validating transactions and maintaining the blockchain of transaction histories.[39]

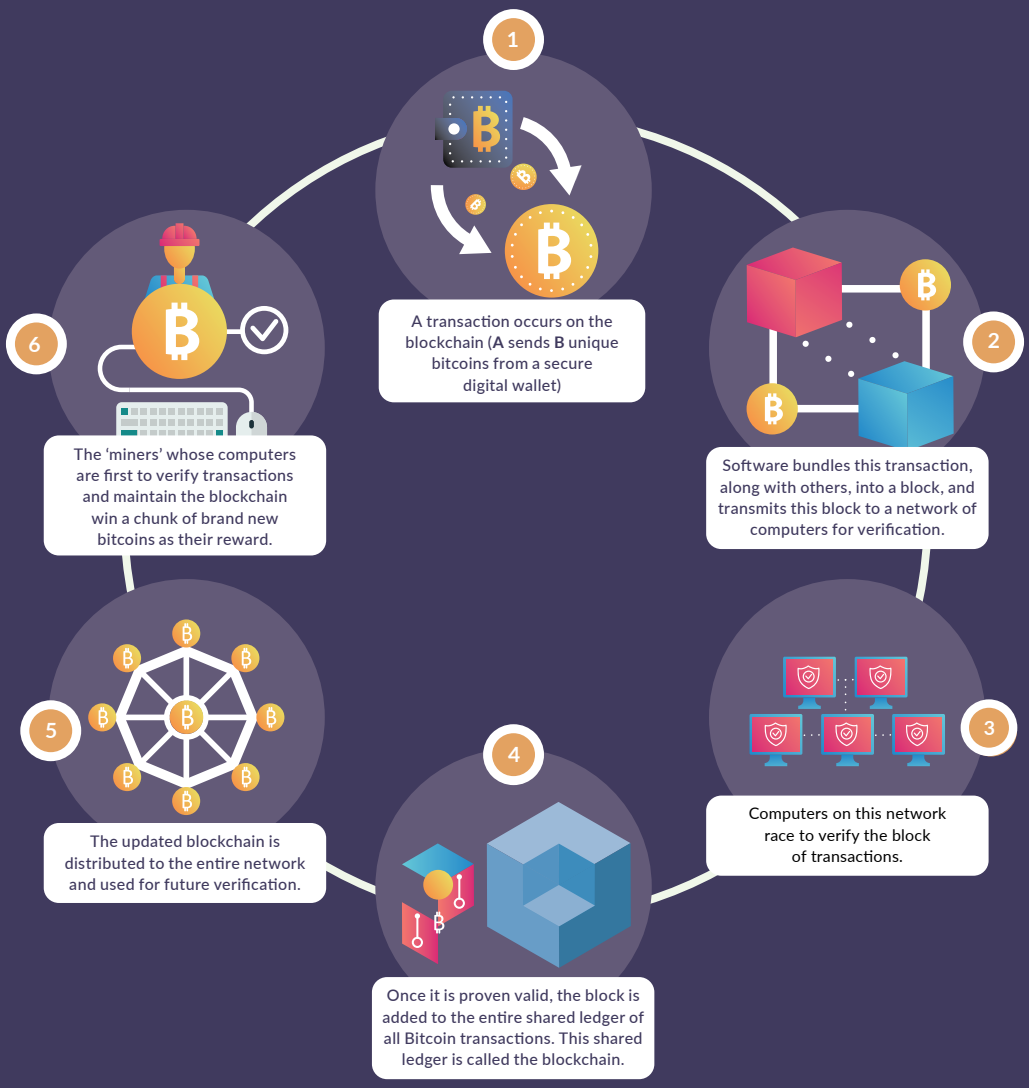


**FIGURE 1** The Bitcoin 'mining' process.

SOURCE: Adapted from Cameron McLain, A brief history of blockchain: An investor's perspective, Medium, July 2017.

Many point to weaknesses within this proof of work model, particularly its slow and limited transaction processing and its massive energy consumption. The more competition, the more computational power that is required. Consequently, Bitcoin mining now utilizes more energy than entire countries. Regulators in Europe are even pushing cryptocurrencies away from proof of work towards proof of stake, with some suggesting a possible ban on the former.[40] Proof of stake only allows miners to validate blocks if they have provided a 'stake' or security deposit, motivating them to confirm legitimate transactions and prevent a 'fork', or split, in the blockchain, as they would lose their stake. The more coins they have to put up as stake combined with the amount of time they have been mining, the higher their capacity to mine and validate blocks will be. Miners are then chosen randomly for each transaction through a weighted algorithm that takes these factors into account. This method seeks to address perceived weaknesses in proof of work, including its energy usage, environmental impact, speed and scalability.[41] However, many view it as a less secure, fair and stable form of mining.[42]

Bitcoin operates on public-key cryptography, which consists of publicly available keys and privately held keys by transacting parties. To make a Bitcoin transaction, the sender first encodes their payment using the receiver's public key. Following this, they use their own private key to authorize the transfer of funds. Upon receipt, the receiver decodes the payment with their private key. Consequently, both parties can in theory remain pseudonymous, identifiable only by their public keys.[43] Further, users can

only retrieve funds by possessing their private keys; a public key alone cannot retrieve funds, meaning that if a private key is compromised or lost, the currency can never be regained. Meanwhile, if the public key is ever matched to a user, then transactions associated with that key can be traced to them given Bitcoin's publicly available database. As such, Bitcoin is not fully anonymous but pseudonymous.

Other technologies have developed to help further increase anonymity such as tumblers and mixing services that obscure the origins of transactions. For example, instead of sending funds to a receiver, leaving a history of transactions between public keys, the sender can transfer the funds to a tumbler that mixes the balance of various senders together and resends part of them to the intended recipient thereby breaking the chain of ownership. Another protocol allows senders to send bitcoins to an escrow account where they mint a secondary temporary currency called 'zerocoin' for the same amount. The zerocoin balance is then sent to the receiver, masking the initial sender from the Bitcoin blockchain. The receiver then redeems the zerocoin for the bitcoins in the escrow account. A number of alternative cryptocurrencies, such as Dash and Monero, have emerged to further enable anonymizing of transactions.[44]

Bitcoin ultimately inaugurated the cryptocurrency industry, which decentralized finance, smart contracts, NFTs, decentralized autonomous organizations (DAOs) and numerous other projects are part of. Bitcoin enabled the operation of decentralized money, but it has more limited capabilities for enabling financial services. Filling that gap, Ethereum was launched in 2015 as an advancement of blockchain technologies, enabling financial services – including lending, borrowing, trading and derivatives. It became a preferred platform for developers given its Turing complete programming language solidity.[45] Further, Ethereum's ERC20 standard for creating new tokens enables developers to build token applications that are interoperable with other products and services.[46]

Since Bitcoin's genesis, many government and private sector initiatives are using variations of blockchain technology in more closed environments and without the presence of in-protocol currencies, such as bitcoins or ethereum. These are referred to as 'permissioned' blockchains, which limit the entities (nodes) that are allowed to add to the blockchain. As this type of permissioned database technology is far from new, many choose not to refer to it as 'blockchain' and instead use the term 'distributed ledger technology' (DLT). However, the expanded use of DLT, alongside central bank digital currencies, is clearly attributable to Bitcoin's disruptive impact. Despite the technology not necessarily being new, the use cases often are, for example, removing the need for individual databases and expensive reconciliation procedures, shifting some organizations towards shared common, auditable databases.[47]

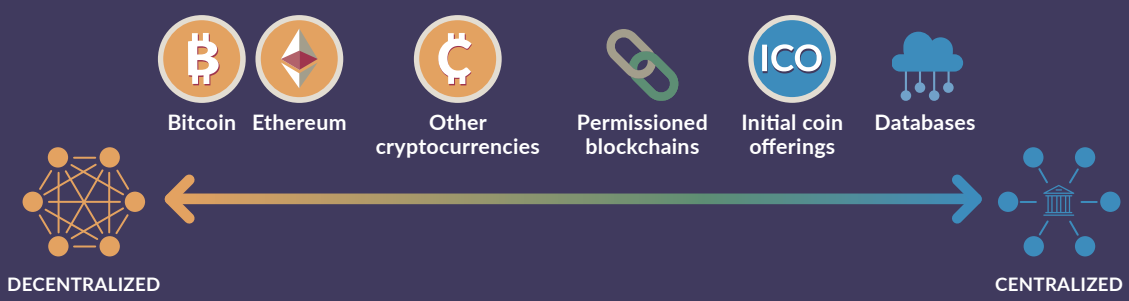


**FIGURE 2** The spectrum of decentralization.

SOURCE: Adapted from Michael Casey et al., *The Impact of Blockchain Technology on Finance: A Catalyst for Change*, Geneva Reports on the World Economy 21 (Geneva: ICMB International Center for Monetary and Banking Studies, 2018).

## Smart contracts and decentralized finance

Aside from being a ledger of transactions and transfers, blockchains can also record other time-sequenced data. This enables blockchains to process so-called 'smart' contracts, which can digitally facilitate and execute transfers and other actions based on pre-programmed contractual conditions.[48] Once live, a smart contract cannot be altered and must run as programmed. For example, it could automatically disburse funds to a recipient account upon receipt of a pre-agreed digital signature confirming the delivery of goods. This removes the need for a trusted third party – such as an intermediary, trustee or escrow agent – as the blockchain network automatically enforces the execution of the contract on its own.[49]

Although Bitcoin enables only a small set of smart contracts, other platforms – most notably Ethereum, Binance Coin, Cardano and Solana, to name a few – enable full-featured smart contracts, i.e they are programmable, on top of core transaction enabling functionality.[50] They allow the creation of distributed applications that, together with smart contracts, enable individuals and organizations to enter into pre-agreed and pre-programmed arrangements executed and operated without the need for human input, management structures or other processes that typify traditional business or organizational structures. As Ethereum's website claims, 'Ethereum is for more than payments. It's a marketplace of financial services, games and apps that can't steal your data or censor you.'[51]

For many, Ethereum has become synonymous with the possibilities of decentralized finance. In early 2020, Ethereum settled the equivalent of US$116 billion worth of transactions. By mid 2021, that figure had reached US$2.5 trillion, roughly the equivalent payment processes of Visa.[52] The arguments in favour of Ethereum range from its cheap operating costs, instant processing capabilities, lack of room for human error and risk reduction, for example by pre-requiring collateral to reduce default risk.[53] Ethereum also allows the creation of tokens, which confer ownership rights and revenue streams to those stipulated within the blockchain. Moreover, the low barriers to entry are a boon for innovation.

However, the downside risks to decentralized finance are substantial. There is no 'real' economy underpinning it – merely a theoretical one, such as the possibility of DeFi currencies replacing traditional ones.[54] Although a real economy could emerge on top of decentralized finance and as a result of it, the likelihood is far from clear. Critics also caution that smart contracts can become another vehicle for fraud and scams, with 'rug pulls' (where developers disappear with investors' funds) and other misconfigurations baked into an otherwise seemingly valid contract.[55] In 2021, US$2.8 billion in crypto-based scams came from rug pulls.[56] The case for decentralized finance, while beguiling, is by no means assured. As one *Financial Times* commentator noted:

> There are only two groups of people prepared to go to costly lengths to decentralize a service which is already available (in what is often a much higher quality form) in a centralised or conventional hierarchal state. One group is criminals and fraudsters. The other is ideologues and cultists. The first sees the additional cost/effort as worthwhile due to the un-censorable utility of these systems. The second consumes it simply as a luxury or cultured good.[57]

# DeFi products

## Non-fungible tokens

Non-fungible tokens (NFTs) are tokens of ownership for things such as digital outputs, art, collectibles and, potentially, tangibles such as real estate. They are created through smart contracts that assign ownership and manage their transferability. NFTs can only have one official owner at any given time and they are immutably stored on a blockchain, meaning that just as with a cryptocurrency, no one can modify a past record of ownership or resell the same NFT to different owners at the same time. A key innovation is that content creators can pre-programme royalties into NFTs, so that they receive a share of payment every time the asset is sold.[58]

## Decentralized autonomous organizations

Decentralized autonomous organizations (DAOs) operate as businesses that are collectively owned and managed by members with rules established through smart contracts. For example, they have pre-programmed treasuries that restrict access without group approval. Decisions, meanwhile, are governed by voting according to pre-programmed statutes and rules, negating the need for a chief executive or financial officer.[59] This, its proponents claim, opens new opportunities for 'collaboration and coordination'.[60] DAOs can operate for a variety of purposes. For example, they can be used to purchase art collectively, as with the November 2021 failed attempt to purchase a rare copy of the US constitution.[61] In 2021, BitDAO became the world's biggest DAO, raising US$2.5 billion, including with large contributions from major tech investors.[62]

## Tokens and initial coin offerings

Cryptocurrencies and tokens are often confused, but they are significantly different. For example, cryptocurrencies are always generated by their own blockchains. Meanwhile, tokens are usually issued within a smart contract run on a blockchain network such as Ethereum.

Most cryptocurrencies were created through the mining process. Tokens, meanwhile, can be sold to investors through initial coin offerings (ICOs) to finance the development of an application or other blockchain projects. However, there is some overlap. Ethereum initially had a rudimentary coin offering of ether, but since then it has relied on mining to issue new coins.[63] The tokens and ICO space is replete with frauds, scams and abuse by criminal actors.[64]


**Sothesby's auction house, New York. In November 2019, a decentralized autonomous organization attempted and failed to purchase a rare copy of the US constitution using cryptocurrencies.** *Photo by Yuki Iwamura/AFP via Getty Images*

# CRYPTO, CRIME AND CONTROL

Blockchain technology in theory could transform the operation of financial markets, with potentially large economic, social and political benefits, such as bringing the financial system closer to those currently without access to it. However, this can only occur if key issues around cost of trust, criminal penetration and utilization, and appropriate governance structures are resolved.[65]

Law enforcement agencies fear the industry will serve to enable criminal activity and financial regulators are concerned about the crypto economy, which poses growing financial systemic risk as crypto assets and derivative products become embedded and disbursed through mainstream finance.[66] To many, it is reminiscent of sub-prime mortgages in the 2000s, where derivative products enabled toxic assets and debt to be catastrophically masked and spread through the financial system precipitating its near collapse in 2008.[67]

Although many governments point to the industry's immense environmental impact as a reason to regulate, the issues of consumer predation, crime, money laundering and terrorist financing present the most immediate impetus for regulators to come to grips with the technology. There are a number of cases of cryptocurrencies being used for crime, including the commissioning of murder, human trafficking and child exploitation.[68] Decentralized finance has spawned a vast world of financial engineering, which has been shadowed by organized crime and malicious actors. Fraud, scams, 'pump and dump' (a fraudulent practice of encouraging new investors to buy crypto assets to artificially inflate the price, selling the shares at their peak and leaving new investors 'holding the bag' when the price collapses),[69] Ponzi schemes,[70] embezzlement, ransomware attacks and phishing, to name a few, seem nearly ubiquitous in the crypto world. In just some examples, perpetrators of Ponzi schemes convince victims to buy non-existent crypto funds or crypto-backed securities.[71]

In May 2021, the crypto market lost 47 per cent of its value in a week due to China's ban on crypto trading and mining, as well as a surreal imbroglio involving a well-known electric car company and Bitcoin.[72] And cases of embezzlement are rife. For example, QuadrigaCX was at one time believed to be Canada's largest crypto exchange. It collapsed after it emerged that the exchange manager had suddenly died, taking all digital wallet passwords with him, and that he had used investor funds for travel and other luxury items. Questions remain about whether the funds had ever actually purchased cryptocurrencies.[73]

Crypto exchanges have emerged as a particularly contentious issue. They provide means towards more widespread adoption of blockchain products but also a mismatch with Bitcoin's anarcho-utopian foundations. Exchanges are a new form of transaction intermediation, helping overcome the transactional and technological limitations of permission-less, decentralized, blockchains. Centralized crypto exchanges tend


**Many cryptocurrency exchange companies locate in tax havens to avoid regulations and oversight. Here, Binance's headquarters in the Cayman Islands.** *Photo: Askarim/Shutterstock*

to go beyond traditional market exchanges, directly matching agents, counterparties and custodians of asset classes. As one *Financial Times* writer argued, 'cryptocurrency trading platforms have a little secret: they masquerade as "exchanges" but, most of the time, they're actually brokers'.[74]

This has led to accusations of conflict of interest, exchanges front-running clients (a generally illegal practice in securities trading where brokers use insider knowledge of client transactions to pre-trade on price changes that planned client activity will produce, for example buying a stock knowing that the client's purchase will drive the price up) and other consumer–investor protection issues. Cases of fraud have been well documented, such as the CoinUp exchange in South Korea, which operated as a Ponzi scheme and defrauded investors of US$384 million. Ultimately, the CEO was sentenced to 16 years in prison, and a range of prison sentences was given to other executives at the firm.[75]

The exchange sector has skyrocketed due to high fees, regulatory arbitrage and market volatility, all of which have driven enormous profits. Many exchanges choose to locate in tax havens to avoid regulations and oversight,[76] leading to high-profile disputes with national regulators. For example, Binance, based in the Cayman Islands, was banned by UK regulators in 2021 from conducting 'any regulated activity' in the UK.[77] Others explicitly seek to bring their activities within regulatory tents, believing it to be the most sustainable approach.

Regardless, the profitability of the sector draws enormous investor interest: Binance is estimated to have made US$1 billion in profits in 2021[78] and Coinbase, as of May 2022, boasts a market cap of US$16.72 billion – down roughly 80 per cent from its peak in 2021, which at one point stood at US$80 billion making it the seventh biggest new listing on the US stock market of all time. (Adjusting for inflation, it was 25 per cent larger than Goldman Sachs, which listed in 1999.)[79] Ultimately, competition and aggressive moves on regulatory oversight are putting downward pressure on exchanges, but questions of their value, security and role in the crypto economy remain.[80]

Decentralized exchanges, on the other hand, are a closer approximation to Bitcoin's peer-to-peer goals, providing only a matching-agent function. However, they represent a relatively small part of the market, although Uniswap, the largest decentralized exchange, recently saw its lifetime trading volume exceed US$1 trillion.[81] Many highlight the lack of consumer protections around decentralized exchanges, other than warning 'buyer beware' – a concept in commercial law originating from the Latin *caveat emptor*, which suggests that the buyer purchases at their own risk.[82]

Meanwhile, phishing attacks thrive on crypto's lack of backdoor entry, i.e. absence of way to gain access without the original password, to user accounts, meaning that gaining control of a users' password can

provide irrevocable access to crypto funds. Another key mechanism is ransomware, whereby hackers take over computer systems and sell access back only upon payment of ransom through Bitcoin or other cryptocurrencies to avoid detection.[83]

The development of anonymity-enhanced cryptocurrencies, mixers and tumblers, decentralized exchanges, privacy wallets and a host of anti-censorship platforms serve to further obscure and reduce transparency. In combination with the proliferation of DeFi activities, these provide high AML/CTF risks.[84] Market manipulation is also seemingly endemic. The tech bubble and crypto boom of the COVID era is a new extreme evolution of this, with billionaires and celebrities taking to TV to 'pump' preferred tokens, many of which saw thousands of per cent gains and losses in short periods.[85] For example, Dogecoin gained 12 000 per cent in a four-month period in 2021, before collapsing over 90 per cent over the next 12 months.[86] Most of the major price changes occurred over a matter of days.

Meanwhile, a number of companies have sought to develop stablecoins to take advantage of the crypto trend. As these digital assets or tokens tend to be pegged to a certain value, they are seen as a less volatile option than other cryptocurrencies. The most prominent and controversial example is Tether, which sells its coins for US$1 and promises to redeem them for US$1, meaning the coins have an equal, or stable, value relative to the dollar.[87] There have been widespread accusations against stablecoins, with significant questions raised about their capital backing. Tether is frequently highlighted as relying excessively on commercial paper, short-term unsecured promissory notes that are issued by commercial entities as a promise to repay a loaned amount. This commercial paper could prove far less liquid in cases of financial distress and raise questions about how redeemable they are, meaning that Tether could potentially be viewed as unable to meet its redemption obligations, resulting in a 'run on the bank' where customers withdraw their funds from the stablecoin all at once, producing a collapse. Others suggest the use of stablecoins is a route to artificially inflate cryptocurrency prices and facilitate market manipulation.[88]

The issues surrounding stablecoins came into stark relief in May 2022 when one of the most prominent US dollar-backed stablecoins, terraUSD and its sister token luna, collapsed in a matter of days, wiping out tens of billions of dollars in investors' money. The episode had all of the hallmarks of a Ponzi scheme, with 'pump and dump' and misplaced technological hubris, coinciding with gullible investors seeking high returns from a financial instrument most could not understand. At its peak, luna had a market cap of US$60 billion. Reports of suicides and complete financial loss for retail investors were matched by reports of large institutional holders cashing out prior to the collapse.[89]

## The crime–crypto nexus

The relationship between cash money and crime is complex. Acclaimed Harvard economist Kenneth Rogoff, for example, called for the elimination of large denomination cash to help reduce criminal activity and tax evasion.[90] Former US Treasury Secretary Lawrence Summers made a similar argument, suggesting the US 'kill the $100 bill'.[91] In Europe, a number of countries limit cash transactions and have reduced the size of their available currency denominations, while the European Central Bank stopped producing €500 notes in 2018.[92]

However, for these initiatives to be successful, countries would also need to ban cash money substitutes, including cryptocurrencies (although how close a substitute they are is a point of heated debate).[93] Many countries have already seen a steady decline in cash payments, such as Sweden, where rates of cash usage fell by 47 per cent from 2009 to 2017.[94] Further, Sweden has one of the most advanced CBDC projects, inspired by cryptocurrencies but using a more centralized and traditional database system.

## Central bank digital currencies

Labelled by *The Economist* as potentially 'the most revolutionary' aspect of crypto-driven financial innovation,[95] CBDCs are a centralized alternative to cryptocurrencies. As seen above, cryptocurrencies are broadly issued by private individuals and based on decentralized consensus validation mechanisms. With a CBDC, the central bank issues a digital currency that, similar to paper money, is guaranteed to be redeemable with the central bank. These have little in common with the blockchain technologies underpinning cryptocurrencies.

Central banks suggest potential upsides to increased use of CBDCs, such as reduced transaction costs and frictions, particularly across borders, and the possibility of reaching the unbanked. There are also many potential downsides, some systemic. For example, concerns over privacy and compliance with AML/CFT given the sidestepping of commercial banks/financial intermediaries who traditionally are tasked with implementing these regulations. Others include the economic risk of disintermediation, for example removing customers as a source of liquidity, credit creation and leverage for banks and the economy more broadly.[96] These innovations may further leave behind marginalized groups who are already excluded from technology, for example in societies where women and other groups are excluded from many forms of technology and economic activity.[97]

Other risks are geopolitical. The Chinese digital renminbi is the most advanced and widely adopted CBDC available. By late 2021, the People's Bank of China boasted 140 million individual digital yuan accounts, 10 million corporate accounts and 150 million transactions, totalling US$9.7 billion.[98] The digital renminbi is viewed as part of a push by the Chinese state to wrest control of payments markets back from its tech giants as well as offer an alternative to US dollar hegemony in global trading markets. It provides an additional possibility for expanded Chinese leverage within trading relationships, for example should the government mandate certain transactions take place in their digital currency. The director of the UK's signals intelligence agency, the Government Communications Headquarters, has raised concerns that it provides the means for China, or other countries, to 'surveil transactions'.[99] This echoes concerns raised by the head of the UK's Secret Intelligence Service that China could 'harvest' such data and use it as a means to 'distort public discourse and political decision-making' beyond its borders.[100]

In January 2022, the US Federal Reserve escalated its CBDC scoping exercises. This is alongside an effort by the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology to create a prototype US CBDC. In February, the military government in Myanmar announced intentions to launch their own digital currency as an ostensible means to counteract economic stagnation. This came not long after supporters of jailed leader Aung San Suu Kyi adopted stablecoin Tether as their official currency to raise funds to fight the regime.[101] ■

A 2022 Europol report highlighted that the role of cryptocurrencies in facilitating criminal transactions is increasing but remains a limited share of the overall criminal economy compared to cash and other transaction forms. Money laundering is an area where utilization and complexity is increasing, with money laundering specialists now using cryptocurrencies and offering them as part of their service. However, Europol finds that the use of cryptocurrencies for terrorist financing is relatively limited. Overall, money laundering, the online trade in illicit goods and services, and fraud are the main criminal uses of cryptocurrencies. The technology is particularly used in transacting for-profit child sexual abuse material.[102]

According to Chainalysis, a cryptocurrency tracing company, in 2021 scammers stole US$14 billion in cryptocurrencies, with losses from crypto-related crime rising 79 per cent on 2020 levels. For example, in late 2021, Israeli cybersecurity firm Check Point Research found numerous events whereby a search engine phishing campaign targeted crypto wallet users with fake URLs in order to steal passwords and up to half a million US dollars.[103]

In 2021, scamming was the leading form of crypto-based crime, followed by theft, largely from hacking crypto businesses.[104] Decentralized finance is increasingly seen as the focal point for crypto crime. According to Chainalysis, DeFi transaction volume grew 912 per cent in 2021.[105] Much of this derives from coding vulnerabilities within new DeFi platforms, with as much as 21 per cent of hacks resulting from these weaknesses. Similarly, DeFi was responsible for

a large part of the 512 per cent rise in crypto thefts between 2020 and 2021. Of the US$3.2 billion of crypto stolen, 72 per cent came from DeFi protocols.[106]

Chainalysis points out that crypto-related crime is growing slower than the crypto market. Only 0.15 per cent of the US$15.8 trillion in crypto trade volume in 2021 derived from illicit addresses – or those confirmed to be related to illicit activity. This is a 79 per cent increase from 2020 but a fraction of the overall increase in the size of the crypto trading market, which expanded 550 per cent.[107] In other words, the share of the market that illicit activities control more than halved from 0.34 per cent in 2020. This dataset places it on par with credit and debit cards, which have a fraud rate in the US of 0.13 per cent.[108]

Critics highlight that these datasets miss vast amounts of criminal activity as the figures are solely based on activity confirmed to be linked to illicit transactions. However, unless money laundering explicitly originates online, it will not be captured by the data. When crimes occur off the blockchain but the funds are washed or 'layered' through crypto transactions, the analysis fails to account for this as money laundering related to crypto. As one analyst said, 'it is reasonable to assume that these reports do not account for a significant "dark figure of crime", which has either not been detected or not been reported so far'.[109]

Some academic assessments place the illicit share at 23 per cent of transactions.[110] In 2019, a report estimated that 'around $76 billion of illegal activity per year involve bitcoin (46% of bitcoin transactions), which is close to the scale of the U.S. and European markets for illegal drugs'.[111] The authors acknowledged that market share declines as Bitcoin increases mainstream societal adoption, but the scale remains enormous.

Despite disagreements on the figures, cryptocurrencies are increasing their role in illicit activities, while the share of illicit activities to the overall scale of the crypto market is decreasing.[112] According to the Chainalysis dataset, by January 2022, US$10 billion in cryptocurrency was held by illicit addresses.[113]

Although law enforcement bodies and regulators have shown greater capabilities at managing crypto-related crime and recovering stolen assets, decentralized finance poses rapidly evolving challenges.[114] For example, the total value of US dollars locked in decentralized finance has risen from roughly US$34 billion in January 2021 to roughly US$90 billion in January 2022, before falling

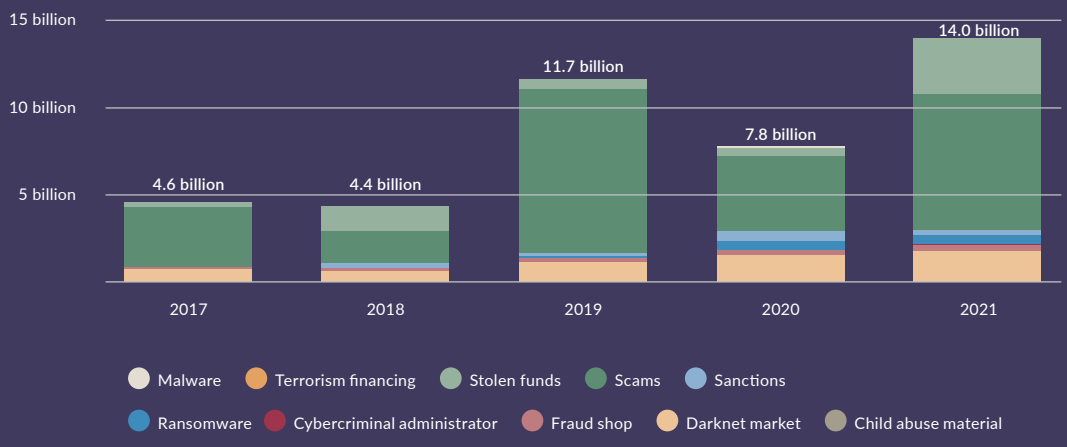


**FIGURE 3** Confirmed illicit cryptocurrency activities, 2017–2021.

NOTE: Values in US dollars.
SOURCE: Chainalysis, Crypto crime trends for 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/

back to US$54 billion in May 2022.[115] Volatility is intense, particularly when broken into component parts of lending, assets, decentralized exchanges, derivatives and payments.[116] In 2021, decentralized finance witnessed roughly US$2.2 billion of funds stolen, up 1 330 per cent from 2020.[117] Nevertheless, new forms of public–private partnerships[118] are also evolving to respond to these challenges, as seen by the collaboration between firms such as Chainalysis, the UK's National Crime Agency and other international law enforcement bodies.[119]

Crypto also facilitates credit card theft. As one article highlights, "hundreds of millions of payment card details have been stolen from online retailers, banks and payments companies before being sold for cryptocurrency on online marketplaces such as UniCC".[120] The stolen card details are used for large purchases of goods or gift cards that can then be resold for cash, known as 'carding'. Estimates put the scale of the carding market at US$1.4 billion annually.[121] In January 2022, UniCC, then the biggest dark web marketplace for stolen credit and debit cards, announced it was closing down. One estimate suggests its operators earned US$358 million in purchases since 2013, transactions that were paid using a number of cryptocurrencies including Bitcoin, Litecoin, Ethereum and Dash.[122] Exactly one year before, in January 2021, the previous market leader, Joker's Stash, closed with sales of stolen card data totalling US$400 million.[123]

It is likely that the voluntary closure of these trading platforms is in part a reflection of risk, with some cases of successful seizure by law enforcement. For example, in mid-2021, Slilpp, a stolen credentials market, was seized by the FBI following support by European and other policing agencies. Slilpp had earned an estimated US$22 million in Bitcoin during its operation.[124]

## Conflict and sanctions avoidance

A number of countries maintain a complex relationship with cryptocurrencies due to their purported ability to facilitate sanctions avoidance and other criminal activities. North Korea allegedly stole up to US$400 million in digital assets in 2021 and, according to a UN report, used the proceeds to fund its missile programmes.[125] Chainalysis, whose research forms the basis for much reporting on North Korea, stated that from 2020 to 2021 'the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%'.[126]

In Russia, estimates before the invasion of Ukraine suggested that roughly US$92 billion were held in crypto assets, spread across 17 million crypto wallets.[127] Russia is the third largest Bitcoin-mining country in the world, behind the US and Kazakhstan (although Kazakhstan may struggle to retain that role given increasing unrest in the country).[128] As of August 2021, Russia accounted for roughly 11 per cent of global 'hashrate', or computing power within the Bitcoin network.[129]

However, Russia has ostensibly opposed cryptocurrencies because of their role in money laundering and terrorist financing. The government gave it legal status in 2020 but instituted a ban on crypto as a means of payment.[130] In December 2021, the country's central bank prohibited mutual funds from investing in cryptocurrencies.[131] And in January 2022, the bank issued a report calling for a complete ban on crypto trading and mining, citing their volatility, potential as Ponzi schemes, their role in illegal transactions and risk for enabling capital flight from emerging markets.[132]

The move suggested an effort to crack down on crypto privacy, seen as a potential boon to opposition groups within Russia.[133] Further, with the central bank planning its own digital rouble, concerns that crypto could serve to weaken monetary policy tools at a time of rising inflation added to the incentive for crypto controls.[134] The Russian parliament had indicated crypto regulation as a priority in its spring 2022 session, although with less support for banning mining given its contribution to the economy.[135] Moreover, the Central Bank's call for a ban on crypto was echoed by the Federal Security Service, which viewed it as a means to fund opposition parties and media outlets deemed 'foreign agents'.[136]

Russia's invasion of Ukraine magnified these dynamics and created new ones. Prior to the war, President Vladimir Putin supported a 'tax and regulate' approach rather than a ban.[137] Following the invasion, cryptocurrencies received significant international attention as a means to fund and support Ukrainian resistance – by mid March, Ukraine had received US$64 million from 120 000 individuals.[138] In the face of tens of billions of dollars in aid to Ukraine, the amount pales significantly, but has been seen as an important public relations element of the war and one which the government has sought to capitalize on, including through wartime legislation to formalize Ukrainian cryptocurrency regulations.[139]

Concerns about how cryptocurrencies could blunt the effectiveness of sanctions have also abounded, and most analyses highlight that both sides potentially benefitted from cryptocurrencies.[140] However, as with the relative size of donations to Ukraine, scale matters. As one analysis highlights, 'total crypto trading volumes on all exchanges worldwide averaged about $24 billion in February, compared to the $5 trillion per day in transactions over SWIFT, the financial messaging system from which major Russian banks are now banned'.[141]

In April 2022, Russia's Central Bank doubled down on efforts to decouple from US- and European-dominated global financial infrastructure and create its own mechanisms, including launching its digital rouble in 2023, which would be capable of making and receiving international payments. They also committed to expand the list of countries that would be willing and able to accept their alternative to Visa and Mastercard, MIR, a banking card issued by the bank.[142]

Meanwhile, Binance – initially reticent about nation-level bans[143] – announced it would deactivate the account of all Russian nationals and registered companies with holdings in excess of €10 000, in line with the fifth round of EU sanctions.[144] Further, US sanctions in April 2022 specifically targeted a Russian Bitcoin-mining firm, BitRiver, to prevent Russia from circumventing earlier sanctions. BitRiver is effectively banned from interacting with US crypto exchanges or purchasing mining equipment.[145]

While the long-term implications of cryptocurrencies in this conflict are by no means clear, a number of tentative themes emerge. First, governments have made progress in linking cryptocurrencies into sanctions packages and it is likely that this will further demonstrate that cryptocurrencies can be regulated as a part of mainstream finance rather than operating as an alternate or parallel system. Second, the scale of cryptocurrency transactions pales into insignificance when compared to more traditional methods of payment and funding in modern war economies. Third, it is likely that the geopolitical role of CBDCs will continue to grow, and there are important and currently unanswerable questions about if and how they will potentially challenge or upend Western-led sanctions against Russia or future sanctions making, or busting, capabilities.


A Bitcoin cryptocurrency exchange shop in Kyiv, February 2022. Following Russia's invasion of Ukraine, governments have made progress in linking cryptocurrencies into sanctions packages. *Photo: Ethan Swope/Bloomberg via Getty Images*

# Cryptocurrencies in Latin America

## Venezuela's *petromoneda*

Venezuela has had an ambivalent relationship with cryptocurrencies. Initially, as the economy went into freefall and hyperinflation destroyed the national currency, many Venezuelans turned to Bitcoin and other digital currencies as a way to counteract government financial controls and protect against inflation.[146]

Nicolás Maduro's regime initially saw it as a threat, before recognizing its potential.[147] In 2018, his government launched a cryptocurrency known as the *petromoneda* (or 'petro'), which many viewed as an attempt to circumvent US sanctions. In March 2018, President Trump issued an executive order banning all transactions within the US or by US nationals with digital currencies issued by the Venezuelan government.[148]

Despite widespread public distaste and mistrust for the currency, the petro is backed by the country's oil reserves and has seen repeated attempts by the government to mandate its use, for example decreeing that all airlines operating in Venezuela pay for their fuel with petro.[149]

## El Salvador: empowerment or fraud?

In September 2021, El Salvador became the world's first country to adopt Bitcoin as a legal tender. President Nayib Bukele promised it would transform the country, although some commentators have referred to his efforts as a 'con artist's grift' that has turned sour.[150]

The International Monetary Fund (IMF) echoes these concerns. In 2021, it described El Salvador's experiment with Bitcoin as providing a possibility for more efficient payments, but at the risk of high price volatility and 'significant risks to consumer protection, financial integrity, and financial stability' as well as 'fiscal contingent liabilities'. The IMF concluded that Bitcoin 'should not be used as a legal tender'. They called for a 'narrowing' of the law and a strengthening of consumer safeguards within the national e-wallet, Chivo, with a greater protection, segregation and ring fencing of reserve assets, and more regulatory oversight of the payment system with a particular focus on AML/CFT.[151]

The reality has been a president using national finances to speculate on Bitcoin, describing himself as trading the currency on his phone on behalf of the country.[152] Although underpinned by secrecy, estimates suggest – based on Bukele's own admissions – that he has purchased 1 801 bitcoins at an estimated average price of US$50 000 for a total of US$90 million. Bukele claimed to continue to 'buy the dip' (purchase more based on the speculative notion that all price declines are transitory, therefore simply 'dips') as Bitcoin's prices tumbled through December 2021 and January 2022.[153]


A protest against President Nayib Bukele and Bitcoin, San Salvador, September 2021. That year, El Salvador became the world's first country to adopt Bitcoin as a legal tender. *Photo: Camilo Freedman/ Bloomberg via Getty Images*

By late January 2022, those state-owned assets were worth around US$65 million, a loss to El Salvador's government of roughly US$20–US$25 million.[154] By May 2022, the losses had reached almost US$40 million, or 35 per cent negative return on the 2 301 state-owned bitcoins.[155] On 26 January 2022, the IMF's Executive Board called on El Salvador to remove Bitcoin as a form of legal tender, warning its status could prevent the country receiving future loans from the organization, including a long sought US$1.3 billion loan currently stalled due to concerns over Bitcoin.[156] Bukele's efforts to circumvent traditional markets by issuing a US$1 billion Bitcoin bond stalled due to ongoing crypto market volatility and domestic political gridlock, while the country faces a US$800 million bond repayment in January 2023, sparking concerns that default is increasingly likely.[157] Far from financial freedom and development, it appears the president's hype experiment with Bitcoin may yet bankrupt the country as its credit rating is now junk status and its dollar bonds trade at record-low values.[158] ■

# INTERNATIONAL REGULATIONS

The Financial Action Task Force (FATF) is an independent inter-governmental body that works to prevent money laundering, terrorist financing and the financing of weapons of mass destruction, and provides the global standard for AML and CFT regulations. The FATF first substantially engaged cryptocurrencies in 2014 with a preliminary assessment, followed by its 'Guidance for a risk-based approach to virtual currencies' in 2015.[159] In 2018, the FATF clarified that its recommendations applied to all financial activities involving 'virtual assets' and updated its glossary to include two new terms: 'virtual assets' (VAs) and 'virtual asset service providers' (VASPs). Under the recommendations, VASPs were to be regulated for AML/CFT, should be licensed or registered, and subject to monitoring and supervision systems.[160]

In 2021, the FATF issued an updated guidance that highlighted key elements that qualify an entity as a VASP, which were 'acting as a business or on behalf of another person and providing or actively facilitating VA-related activities'.[161] As one crypto news site described it, the regulatory guidance 'appears designed to corral much of the nascent industry into the existing regulatory framework for banks'.[162]

The FATF, with strong support from the US and the G20 more broadly,[163] clarified that although CBDCs are not defined as VAs, they are nevertheless bound by FATF standards as fiat currencies. This created a level playing field for all VASPs and traditional financial institutions with regard to AML/CFT obligations,[164] despite extensive criticisms and lobbying against such regulations by the cryptocurrency sector.[165] Former US Treasury Secretary Mnuchin praised this approach in 2019, stating: 'We will not allow cryptocurrency to become the equivalent of secret numbered accounts. We will allow for proper use, but we will not tolerate the continued use for illicit activities.'[166]

The subsequent 2019 guidelines established the 'travel rule' for VASPs, meaning they needed to transmit detailed information from the sending customer and the beneficiary, such as their name and account details, among other data.[167] A collection of crypto industry leaders grouped together to form the Joint Working Group for InterVASP Messaging Standards and in 2020 released IVMS101, a messaging standard that provides a uniform model for datasets sent between VASPs under the travel rule.[168] Meanwhile, the FATF issued a separate report to the G20 on the regulation of stablecoins.[169]

The 2021 FATF guidance focused particularly on decentralized exchanges as well as trying to create regulatory frameworks around rapidly emerging fintech sectors.[170] In October 2021, the FATF updated the guidance to provide narrower definitions of VAs and VASPs, making clear that 'there should not be a case where a relevant financial asset is not covered by the FATF standard'.[171] It also


**The Financial Action Task Force is focusing on creating regulatory frameworks around rapidly emerging fintech sectors.** *Photo: Social media*

offered guidance on how to apply FATF standards to stablecoins as well as additional clarification on the travel rule.[172]

National efforts to comply with the FATF's guidance have raised concerns that countries will move towards bans on decentralized finance and other forms of crackdowns.[173] In one such case, Estonia, one of the first countries to begin issuing cryptocurrency licences in 2017, has embarked on a broad regulatory crackdown in recent years, escalating further since the October 2021 FATF guidance. Simultaneously, the country seeks to reassure crypto investors and holders[174] while also warning that money-laundering and terrorist-funding risks are significant.[175]

Crypto companies licensed in Estonia have 4.5 million customers overall, overseeing €20 billion in transaction flows from August 2020 to August 2021. The country has 381 licensed crypto companies, although 15 account for the majority of transactions. Initially, the country issued thousands of licences, but revoked 2 000 of these over the past few years, with two-thirds of companies at one point registered at just four addresses in Tallin. Moreover, regulators point to the high proportion of transactions with higher-risk countries, with a number of transactions facilitated by the 15 companies ending up in Luxembourg, Syria, Pakistan, Greece, Montenegro, Serbia and Belize. This risk is compounded by the fact that assets often originate from Russia, Japan, Switzerland and North and South America.[176] The Estonian National Financial Intelligence Unit reports a rapidly growing set of queries from authorities abroad, with roughly 100 requests surrounding scams and serious financial crime suspicions in 2021 alone.[177]

Despite concerns within the fintech sector, the clarification of AML/CFT regulations predated a massive influx of more traditional financial-sector funding into the virtual space. As one commentator noted: 'Complying with financial regulation takes time and money, and businesses that have historically invested in compliance resources will have a significant head start … Banks looking to enter the virtual asset space have been eager for greater regulatory clarity, and the FATF is giving them a huge boost in that regard.'[178]

## The policy horizon

Policymakers have a number of goals when regulating markets. First, they look to ensure some level of fairness, efficiency and contractual certainty. Second, they try to instil more consumer and investor protection, particularly in markets with high information or power asymmetries and customers who are at risk of predation. Third, they seek to ensure a level of systemic financial stability. Since the

2008 financial crisis, regulators have been clear that interconnected risk within global financial markets means that no large financial market – however anarchic or libertarian its creators envisioned – can be independent.[179] Lastly, governments and regulators aim to prevent tax evasion, money laundering and terrorist financing.

The year 2021 represented the solidification of regulatory trends already underway. In the US, for instance, decentralized finance is now firmly in the regulatory agenda.[180] In just one example, in late 2021 the US Commodity Futures Trading Commission filed charges against 14 crypto entities for either failing to properly register or making false and misleading claims regarding their registration or organizational membership.[181] Similarly, demonstrating international regulatory reach, the US sanctioned a number of major Russian cryptocurrency exchanges and actors believed to be implicated in money laundering.[182]

The trend continues around the world. In January 2022, Singapore's financial regulator instructed companies to avoid advertising crypto services to the public and instead limit themselves to promotion through their websites and apps.[183] The same month, Spain announced its own controls on crypto advertising.[184] In February, the UK's Her Majesty's Revenue and Customs (HMRC) updated its crypto assets tax guide to specifically include staking and decentralized finance,[185] and seized its first ever NFT, valued at £1.4 million, saying that it served 'as a warning to anyone who thinks they can use crypto assets to hide money from HMRC'.[186] This followed a move by a UK watchdog to restrict crypto advertisements to only the wealthy and experienced Investors.[187]

Cryptocurrencies and decentralized finance face a multifront regulatory push that challenges many of its anarcho-libertarian or criminal uses. AML/CFT regulations effectively treat virtual assets and VASPs as other financial products. National regulatory agencies are pushing for greater oversight and are working to shoehorn crypto and DeFi markets into existing regulatory structures. The environmental challenges of proof of work mining are bringing the currencies squarely into conflict with EU member states, while religious concerns have rendered the currencies haram among many Islamic groups due to their speculative nature, lack of an underpinning commodity (such as gold), and their not fulfilling the criteria for a medium of exchange under Islamic law.[188]

Law enforcement is also getting more effective at tackling crypto-related crime. In one notable case, US law enforcement agencies managed to force a major ransomware operation offline by effectively hacking it.[189] The US Internal Revenue Service (IRS) has also become ruthlessly effective at recouping illicit funds. It seized US$3.5 billion in cryptocurrencies during the 2021 fiscal year, accounting for 93 per cent of all the assets seized in that period.[190] In early 2022, the IRS seized US$3.6 billion from a couple accused of engaging in money laundering and fraud, despite their extensive obfuscation and anonymization techniques.[191] According to the IRS, its Criminal Investigation has 'prioritized training and the deployment of cryptocurrency, blockchain and open-source intelligence technologies to unravel complex cyber-financial criminal schemes'.[192]

The geopolitical consequences of cryptocurrencies appear to run counter to the goals of a rules-based international order. As discussed, pariah regimes seek to utilize the technologies to bypass sanctions, fund military activities and enable an obfuscation of state actions at the international level. Governments and international regulators are right to balk at the risk these currencies and technologies pose if under-regulated and left to unfettered criminal and exploitative forces. Whether they continue to offer any real value added or novel use cases when regulated in the same manner as traditional financial institutions and services remains to be seen.

# CONCLUSION

Cryptocurrencies, blockchain technologies and decentralized finance are a significant financial innovation in and of themselves. However, whether the industry that emerged from that innovation translates into true societal benefit – with actual use cases beyond a technology elite or organized criminal actors – and whether they will outweigh the costs of a financial market reckoning and regulatory crackdown is yet to be seen.

The use cases for cryptocurrencies are largely speculative and unproven. Consumer and investor risk are extreme but masked by a predatory promotional industry built on hype, con, cultism, pseudo-economics and market manipulation. The experience of past speculative manias do not give cause for excessive optimism. As such, regulators are right to clamp down on the worst excesses within these markets and limit their potential for criminal activities or geopolitical conflicts. Investors and consumers should be aware that whatever irrationalities persist in the short to medium run, markets will eventually force rationality on crypto speculation in the longer term. Should it indeed prove to be an immense Ponzi scheme, it is likely that the scale of wealth destruction will be unprecedented in human history.

Regulators must continue to expand their control and law enforcement must keep adapting to ensure that criminals are not the key beneficiaries of these markets. How DeFi engineering will evolve to enable scams, frauds, theft and money laundering to go undetected seems unclear. However, law enforcement is getting more effective at tackling crypto-related crime, as evidenced by repeated seizures of stolen assets and ever more complex methods of tracking criminal activity on blockchains. Moreover, the regulatory net is also tightening. Countries' main financial and AML regulators are moving to tackle what they label as 'mountains of fraud' attached to cryptocurrencies, NFTs and decentralized finance more broadly.[193]

The environmental impacts of crypto are a pressing issue, drawing recent ire from US lawmakers,[194] persistent threats from European governments and criticism from regulators around the world. In 2020 alone, Bitcoin generated 60 million tonnes of CO2, which would require almost 300 million trees to reabsorb.[195] Estimates suggest Bitcoin and Ethereum at their peak used twice as much energy as the country of Sweden. The Cambridge Bitcoin Electricity Consumption Index estimates the energy consumption of Bitcoin alone at 0.18 per cent of global energy consumption.[196] In November 2021, Sweden's financial regulator argued that crypto assets were 'a threat to the climate transition' and that energy-intensive mining 'should be banned'.[197] Their estimates placed the carbon footprint of crypto assets at the equivalent of 100 million round-trip flights from Sweden to Thailand.[198]

A number of technical challenges surrounding blockchain technologies remain, including transaction processing speeds, costs, scalability, interoperability and governance.[199] There are also no barriers to governments adopting blockchain technology as a means to compete with Bitcoin and others.[200] The fact that early experiments with permission-less blockchain systems have led to permissioned systems, and that CBDCs have shunned Nakamoto-style blockchain technology in favour of more traditional ledger systems, suggests a fundamental problem in scalability – i.e. reaching sufficient size. Moreover, the decentralized vision of blockchain, Bitcoin and web3 has given way to the emergence of centralization and individual or institutional gatekeepers. Cryptocurrencies have been 'forked', NFTs have been removed from digital marketplaces and vast transactions rely on centralized exchanges rather than peer-to-peer ones. As Twitter founder Jack Dorsey argued, 'You don't own web 3. [Venture capital] and their [limited partners] do.'[201]

Crypto is a small but significant fraction of global finance. The total assets of the largest banks in the world were roughly US$128 trillion as of 2020, while global GDP was approximately US$84.5 trillion.[202] At the time of writing, the total cryptocurrency market cap is US$1.31 trillion, having fallen from a November 2021 peak of roughly US$3 trillion.[203] Ignoring its extreme volatility, the cryptocurrency industry represents around 1 per cent of global financial assets. For a sector that is under-regulated, an enabler of crime and illicit activities, and replete with examples of fraud and potentialities for systemic risk, regulators should be thankful that the share is not larger. The future path for blockchain technologies seems set towards further regulation, centralization, de-anonymization, policing and development of basic financial infrastructure to limit volatility and the risks of financial contagion or economic collapse. This would be a positive trend for cryptocurrencies, financial markets and efforts to tackle transnational organized crime.

## Notes

1 Boston Consulting Group, Payments revenue pool on track to nearly double by 2030, 11 October 2021, https://www.bcg.com/press/11october2021-payments-revenue-pool-track-to-nearly-double-by-2030.

2 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

3 See The Global Findex Database 2017: https://globalfindex.worldbank.org/#:~:text=The%202017%20Global%20Findex%20database,62%20percent%20to%2069%20percent.

4 A Ponzi scheme is a type of investment fraud that uses funds generated from new investors to pay existing investors. Organizers often promise high investment returns with minimal risk. However, many schemes do not make any investments at all, instead using new investors' inflows as a means to provide a fake return to existing investors. Ponzi schemes therefore require constant flows of new money to continue, and collapse once new investors become scarce or existing investors seek to cash out. See US Securities and Exchange Commission, Ponzi Scheme: https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme.

5 Europol, Cryptocurrencies: Tracing the Evolution of criminal finances, January 2022, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.

6 Internal Revenue Service, South Korean national and hundreds of others charged worldwide in the takedown of the largest darknet child pornography website, which was funded by Bitcoin, 16 October 2019, https://www.irs.gov/compliance/criminal-investigation/south-korean-national-and-hundreds-of-others-charged-worldwide-in-the-takedown-of-the-largest-darknet-child-pornography-website-which-was-funded-by-bitcoin; Andy Greenberg, Inside the Bitcoin bust that took down the web's biggest child abuse site, Wired, 7 April 2022, https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/.

7 For example, see Ciupa Katarzyna, Cryptocurrencies: Opportunities, risks and challenges for anti-corruption compliance systems, Organisation for Economic Co-operation and Development, 2019, https://www.oecd.org/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf.

8 Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf.

9 Siddharth Venkataramakrishnan and Robin Wigglesworth, Inside the cult of crypto, *Financial Times*, 10 September 2021, https://www.ft.com/content/9e787670-6aa7-4479-934f-f4a9fedf4829.

10 Fiat currency is government-issued money made legal tender by government decree, or 'fiat'. It is created by a central bank that holds a legal monopoly on currency creation. It has no commodity underpinning and its value is based on various factors such as supply, demand and future expectations.

11 From 1634 to 1637, speculation around tulip flower bulbs in the Netherlands led to a financial frenzy as novice investors bid up prices to exorbitant levels. It eventually ended with a collapse in prices and widespread losses.

12 Joumanna Bercetche, Twitter, 1 June 2021, https://twitter.com/CNBCJou/status/1399658399453827074.

13 Mark Gurman and Jennifer Surane, PayPal explores launch of own stablecoin in crypto push, Bloomberg, 7 January 2022, https://www.bloomberg.com/news/articles/2022-01-07/paypal-is-exploring-launch-of-own-stablecoin-in-crypto-push.

14 Reuters, Nexo and Mastercard Launch 'world first' crypto-backed payment card, 13 April 2022, https://www.reuters.com/technology/nexo-mastercard-launch-world-first-crypto-backed-payment-card-2022-04-13/.

15 Dikla Barda et al, Scammers are creating new fraudulent crypto tokens and misconfiguring smart contracts to steal funds, Check Point Research, 24 January 2022, https://research.checkpoint.com/2022/scammers-are-creating-new-fraudulent-crypto-tokens-and-misconfiguring-smart-contracts-to-steal-funds/.

16 *The Economist*, Will Web3 reinvent the internet business?, 24 January 2022, https://www.economist.com/business/2022/01/29/will-web3-reinvent-the-internet-business.

17 See Global cryptocurrency market charts, CoinMarketCap, https://coinmarketcap.com/charts/.

18 Liana Baker, Jesse Hamilton and Olga Kharif, Mark Zuckerberg's stablecoin ambitions unravel with Diem sale talks, Bloomberg, 26 January 2022, https://www.bloomberg.com/news/articles/2022-01-25/zuckerberg-s-stablecoin-ambitions-unravel-with-diem-sale-talks.

19 Chainalysis, Crypto crime trends for 2022: Illicit Transaction activity reaches all-time high in value, all-time low in share of all cryptocurrency activity, 6 January 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

20 Ibid.

21 Ibid.

22 Ibid.

23 Europol, Cryptocurrencies: Tracing the Evolution of criminal finances, January 2022, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.

24 Gary Gensler, Remarks before the Aspen Security Forum, US Securities and Exchange Commission, 3 August 2021, https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

25 *The Economist*, The beguiling promise of decentralised finance, 18 September 2021, https://www.economist.com/leaders/2021/09/18/the-beguiling-promise-of-decentralised-finance.

26 Oluwapelumi Adejumo, Nouriel Roubini advises El Salvador legislators to impeach President Bukele, 24 January 2022, https://www.fxempire.com/news/article/foremost-economist-nouriel-roubini-advises-el-salvador-legislators-to-impeach-president-bukele-875553.

27 International Monetary Fund, El Salvador: Staff concluding statement of the 2021 Article IV Mission, 22 November 2021, https://www.imf.org/en/News/Articles/2021/11/22/mcs-el-salvador-staff-concluding-statement-of-the-2021-article-iv-mission.

28 Marco Quiroz-Gutierrez, Crypto is fully banned in China and 8 other countries, Fortune, 4 January 2022, https://fortune.com/2022/01/04/crypto-banned-china-other-countries/.

29 France 24, Maduro bids to revive Venezuela's 'petro' cryptocurrency, 15 January 2020, https://www.france24.com/en/20200114-maduro-bids-to-revive-venezuela-s-petro-cryptocurrency.

30 Central Bank, **中国互联网金融协会 中国银行业协会 中国支付清算协会关于防范虚拟货币交易炒作风险的公告**, 18 May 2021, https://finance.sina.com.cn/money/bank/bank_yhfg/2021-05-18/doc-ikmyaawc6082415.shtml.

31 Sohale Andrus Mortazavi, Cryptocurrency is a giant Ponzi scheme, Jacobin, 21 January 2022, https://jacobinmag.com/2022/01/cryptocurrency-scam-blockchain-bitcoin-economy-decentralization.

32 Paul Marrinan, Crypto-crime & caveats, Thomson Reuters Institute, 29 March 2021, https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/crypto-crime-caveats/.

33 Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, https://bitcoin.org/bitcoin.pdf.

34 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

35 Vic, From distributed consensus algorithms to the blockchain consensus mechanism, Alibaba Cloud Community, 30 August 2019, https://www.alibabacloud.com/blog/from-distributed-consensus-algorithms-to-the-blockchain-consensus-mechanism_595315.

36 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

37 Alexandru Stanciu, Blockchain based distributed control system for edge computing, 2017 21st International Conference on Control Systems and Computer Science, 2017, https://doi.org/10.1109/CSCS.2017.102.

38 Hany F. Atlam et al, Blockchain with Internet of Things: Benefits, challenges, and future directions, International Journal of Intelligent Systems and Applications, 10(6), 2018, https://doi.org/10.5815/ijisa.2018.06.05.

39 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

40 Tom Bateman, Norway could back Bitcoin mining ban on environmental grounds, Euronews, 17 November 2021, https://www.euronews.com/next/2021/11/17/norway-could-back-european-bitcoin-mining-ban-as-minister-calls-energy-use-difficult-to-ju.

41 Amandra Reaume, Proof of work vs. proof of stake: Explained, Seeking Alpha, 22 November 2021, https://seekingalpha.com/article/4468656-proof-of-work-vs-proof-of-stake.

42 Simon Chandler, Proof of stake vs. proof of work: Key differences between these methods of verifying cryptocurrency transactions', Business Insider, 22 December 2021, https://www.businessinsider.com/personal-finance/proof-of-stake-vs-proof-of-work.

43 Joshua R. Hendrickson and William J. Luther, Cash, crime, and cryptocurrencies, The Quarterly Review of Economics and Finance, 27 January 2021, 3, https://doi.org/10.1016/j.qref.2021.01.004.

44 Ibid.

45 Turing completeness refers to a universal language that allows any machine to solve a complex mathematical problem provided it has enough memory and instructions to do so. Bitcoin can only compute linear computational problems, which limits its algorithmic capabilities and means it is not Turing complete. Most new cryptocurrencies claim to be Turing complete, meaning that it is possible to programme on top of the underlying blockchain.

46 See: ERC-20 Token Standard, https://ethereum.org.

47 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

48 Some sceptics refer to these as 'dumb' contracts, pointing to their simplicity and inability to incorporate useful legal obscurity around low probability outcomes, which traditionally facilitates agreement. In other words, over specificity and rigidity of contract can be a cost. MIT OpenCourseWare, 6. Smart Contracts and DApps, 2020, https://www.youtube.com/watch?v=JPkgJwJHYSc.

49 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

50 See: Top smart contract platform coins by market capitalization, CoinGecko, https://www.coingecko.com/en/categories/smart-contract-platform.

51 See: What is Ethereum?', https://ethereum.org/en/what-is-ethereum/.

52 Alice Fulwood, Decentralised finance is booming, but it has yet to find its purpose, *The Economist*, 8 November 2021, https://www.economist.com/the-world-ahead/2021/11/08/decentralised-finance-is-booming-but-it-has-yet-to-find-its-purpose.

53 Ibid.

54 Ibid.

55 Charlie Osborne, Hackers hijack smart contracts in cryptocurrency token 'rug pull' exit scams, ZDNet, 24 January 2022, https://www.zdnet.com/article/hackers-hijack-smart-contracts-in-new-cryptocurrency-token-rug-pull-scams/.

56 MacKenzie Sigalos, Crypto scammers took a record $14 billion in 2021, CNBC, 6 January 2022, https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html.

57 Izabella Kaminska, It's not just a Ponzi, it's a 'smart' Ponzi', *Financial Times*, 1 June 2017, https://www.ft.com/content/5f1ee3fa-b5df-3747-b373-dcaca7292162.

58 See: Non-fungible tokens, https://ethereum.org/en/nft/.

59 See: Decentralized autonomous organizations, https://ethereum.org/en/dao/.

60 Ibid.

61 BBC, Crypto US constitution bidder refunds hit by high fees, 24 November 2021, https://www.bbc.com/news/technology-59392827.

62 Liam J Kelly and Stacy Elliott, 11 most interesting DAOs of 2021, Decrypt, 21 December 2021, https://decrypt.co/88894/11-most-interesting-daos-of-2021.

63 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

64 Klaus Grobys, Did you fall for it? 13 ICO scams that fooled thousands, Cointelegraph, 6 December 2020, https://cointelegraph.com/news/did-you-fall-for-it-13-ico-scams-that-fooled-thousands.

65 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

66 Gary Gensler, Remarks before the Aspen Security Forum, US Securities and Exchange Commission, 3 August 2021, https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

67 Ironically, it was this crisis that spurred Nakamoto to publish their groundbreaking paper. As Nakamoto framed it, Bitcoin would be the answer to excessive financial centralization, institutional predation, and the apparent rigging of the system by governments and central banks in favour of financial intermediaries. It was a means to disintermediate transactions and empower individuals to engage in an economy based on peer-to-peer transactions.

68 Dan Sullivan, Tampa woman pleads guilty in dark web, bitcoin murder-for-hire case, *Tampa Bay Times*, 19 January 2022, https://www.tampabay.com/news/crime/2022/01/19/tampa-woman-pleads-guilty-in-dark-web-bitcoin-murder-for-hire-case/; Robert Gavin, Utah man charged with murder-for-hire plot in hoosick falls appears in court, *Times Union*, 7 February 2022, https://www.timesunion.com/news/article/Utah-man-charged-with-murder-for-hire-plot-in-16839056.php.

69 J. T. Hamrick et al, An examination of the cryptocurrency pump-and-dump ecosystem, *Information Processing & Management* 58(4), 2021, https://doi.org/10.1016/j.ipm.2021.102506.

70 Massimo Bartoletti et al, Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact, *Future Generation Computer Systems* 102, 2020, https://doi.org/10.1016/j.future.2019.08.014.

71 American Institute of Certified Public Accountants, cyber criminals are finding ways to steal your digital dollars, 19 March 2020, https://blog.aicpa.org/2020/05/cyber-criminals-are-finding-ways-to-steal-your-digital-dollars.html#sthash.1IlGwpxq.dpbs.

72 *The Economist*, Why have prices of cryptocurrencies, such as bitcoin, fallen – again?, 6 December 2021, https://www.economist.com/the-economist-explains/2021/12/06/why-have-prices-of-cryptocurrencies-such-as-bitcoin-fallen-again.

73 Enza Uda and Joan Webber, A death in Cryptoland: The story of Gerald Cotten and QuadrigaCX', 25 May 2021, https://newsinteractives.cbc.ca/longform/bitcoin-gerald-cotten-quadriga-cx-death.

74 Eva Szalay, Crypto exchanges' multiple roles raise conflict worries, *Financial Times*, 15 November 2021, https://www.ft.com/content/8b8e6d72-b1d2-435c-88c1-4611e3a98da5.

75 David Canellis, This cryptocurrency exchange was actually a $384 million Ponzi scheme, The Next Web, 13 November 2019, https://thenextweb.com/news/south-korea-coinup-cryptocurrency-exchange-ponzi-pyramid-scheme-fraud-ceo-jail.

76 Robert Stevens, Top 7 crypto companies based in tax havens, Decrypt, 13 February 2020, https://decrypt.co/19204/top-7-crypto-companies-based-in-tax-havens.

77 Ryan Browne, Binance, the world's largest cryptocurrency exchange, gets banned by UK regulator, CNBC, 28 June 2021, https://www.cnbc.com/2021/06/28/cryptocurrency-exchange-binance-banned-by-uk-regulator.html.

78 Eva Szalay, Crypto exchanges are booming, for now, *Financial Times*, 24 August 2021, https://www.ft.com/content/d09adf75-9ee9-4c47-9595-69c02113febe.

79 Shawn Tully, Coinbase seals its rank as the 7th biggest new U.S. listing of all time, Fortune, 14 April 2021, https://fortune.com/2021/04/14/coinbase-ipo-direct-listing-stock-coin-shares-7th-biggest-all-time-nasdaq/.

80 Eva Szalay, Crypto exchanges are booming, for now, *Financial Times*, 24 August 2021, https://www.ft.com/content/d09adf75-9ee9-4c47-9595-69c02113febe.

81 Cameron Thompson, DeFi trading hub Uniswap surpasses $1T in lifetime volume, 24 May 2022, https://www.coindesk.com/business/2022/05/24/defi-trading-hub-uniswap-surpasses-1t-in-lifetime-volume/.

82 Megan DeMatteo, Scammers stole $14 Billion in crypto in 2021. Here's how investors can protect their coins, *Time*, 6 January 2022, https://time.com/nextadvisor/investing/cryptocurrency/common-crypto-scams/.

83 American Institute of Certified Public Accountants, cyber criminals are finding ways to steal your digital dollars, 19 March 2020, https://blog.aicpa.org/2020/05/cyber-criminals-are-finding-ways-to-steal-your-digital-dollars.html#sthash.1IlGwpxq.dpbs.

84 FATF, Updated guidance for a risk-based approach: Virtual Assets and virtual asset service providers, October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

85 Virginia Heffernan, My partner, the Dogecoin mogul, *The Economist*, *23 July 2021*, *https://www.economist.com/1843/2021/07/23/my-partner-the-dogecoin-mogul*.

86 Nicolas Vega, Dogecoin up 12,000% since January — Here's How much money you'd have if you invested $1,000 at the beginning of 2021, CNBC, 5 May 2021, https://www.cnbc.com/2021/05/05/how-much-a-1000-dollar-investment-in-dogecoin-is-worth.html.

87 Liana Baker, Jesse Hamilton and Olga Kharif, Why Yellen, Powell cast a wary eye on stablecoins, Bloomberg, 20 July 2021, https://www.bloomberg.com/news/articles/2021-07-20/why-yellen-powell-cast-a-wary-eye-on-stablecoins-quicktake.

88 Sohale Andrus Mortazavi, Cryptocurrency is a giant Ponzi scheme, *Jacobin*, 21 January 2022, https://jacobinmag.com/2022/01/cryptocurrency-scam-blockchain-bitcoin-economy-decentralization.

89 MacKenzie Sigalos, Some investors got rich before a popular stablecoin imploded, erasing $60 Billion in value, CNBC, 29 May 2022, https://www.cnbc.com/2022/05/29/who-got-rich-before-terra-stablecoin-collapsed.html.

90 Kenneth S. Rogoff, *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*, *The Curse of Cash*. Princeton University Press, 2017, https://doi.org/10.1515/9781400888726.

91 Lawrence Summers, It's time to kill the $100 bill', *Washington Post*, 16 February 2016, https://www.washingtonpost.com/news/wonk/wp/2016/02/16/its-time-to-kill-the-100-bill/.

92 European Central Bank, ECB ends production and issuance of €500 banknote, 4 May 2016, https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html.

93 Joshua R. Hendrickson and William J. Luther, Cash, crime, and cryptocurrencies, *The Quarterly Review of Economics and Finance*, 27 January 2021, 3, https://doi.org/10.1016/j.qref.2021.01.004.

94 Ibid.

95 *The Economist*, The digital currencies that matter, 8 May 2021, https://www.economist.com/leaders/2021/05/08/the-digital-currencies-that-matter.

96 Jonnelle Marte, Fed kicks off debate on issuing its own digital currency with new white paper, Reuters, 21 January 2022, https://www.reuters.com/business/fed-lays-out-risks-benefits-cbdc-paper-takes-no-policy-stance-2022-01-20/.

97 I am indebted to Catalina Uribe Burcher for highlighting this point.

98 Bloomberg, China's PBOC says digital yuan users have surged to 140 million, 3 November 2021, https://www.

bloomberg.com/news/articles/2021-11-03/china-s-pboc-says-digital-yuan-users-have-surged-to-140-million.

99 Roula Khalaf and Helen Warrell, UK spy chief raises fears over China's digital renminbi, *Financial Times*, 11 December 2021, https://www.ft.com/content/128d7139-15d6-4f4d-a247-fc9228a53ebd.

100 Helen Warrell, MI6 chief warns of security threat from China 'miscalculation', *Financial Times*, 30 November 2021, https://www.ft.com/content/eb8afc08-70ea-433c-8f2d-c0c1357461e3.

101 Khine Lin Kyaw, Myanmar plans its own digital currency this year to lift economy, Bloomberg, 4 February 2022, https://www.bloomberg.com/news/articles/2022-02-04/myanmar-plans-its-own-digital-currency-this-year-to-lift-economy.

102 Europol, Cryptocurrencies: Tracing the Evolution of criminal finances, January 2022, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.

103 Dikla Barda, Roman Zaikin and Oded Vanunu, CPR alerts crypto wallet users of massive search engine phishing campaign that has resulted in at least half a million dollars being stolen', Check Point Research, 4 November 2021, https://research.checkpoint.com/2021/cpr-alerts-crypto-wallet-users-of-massive-search-engine-phishing-campaign-that-has-resulted-in-at-least-half-a-million-dollars-being-stolen/.

104 MacKenzie Sigalos, Crypto scammers took a record $14 billion in 2021, CNBC, 6 January 2022, https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html.

105 Ibid.

106 Ibid.

107 Eva Szalay, Record $14bn flowed into crime-linked crypto wallets in 2021, *Financial Times*, 6 January 2022, https://www.ft.com/content/3c171512-7c58-4dc9-950f-28e2f75b03d9.

108 US Federal Reserve, Federal Reserve payments study finds U.S. payments fraud a small but growing fraction of overall payments, Board of Governors of the Federal Reserve System, https://www.federalreserve.gov/newsevents/pressreleases/other20181016a.htm.

109 Paul Marrinan, Crypto-crime & caveats, Thomson Reuters Institute, 29 March 2021, https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/crypto-crime-caveats/.

110 'Cryptocurrencies', 4.

111 Sean Foley, Jonathan R Karlsen, and Tālis J Putniņš, 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', *The Review of Financial Studies* 32, no. 5 (1 May 2019): 1798–1853, https://doi.org/10.1093/rfs/hhz015.

112 Europol, Cryptocurrencies: Tracing the Evolution of criminal finances, January 2022, https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.

113 Eva Szalay, Record $14bn flowed into crime-linked crypto wallets in 2021, *Financial Times*, 6 January 2022, https://www.ft.com/content/3c171512-7c58-4dc9-950f-28e2f75b03d9.

114 Steven Melendez, Stolen Bitcoin is hard to get back, but the FBI says it just did it, Fast Company, 7 June 2021, https://www.fastcompany.com/90644461/stolen-bitcoin-is-hard-to-get-back-but-the-fbi-says-it-just-did-it.

115 See: DeFi Pulse – The decentralized finance leaderboard, https://defipulse.com.

116 Ibid.

117 Eva Szalay, Record $14bn flowed into crime-linked crypto wallets in 2021, *Financial Times*, 6 January 2022, https://www.ft.com/content/3c171512-7c58-4dc9-950f-28e2f75b03d9.

118 I am indebted to Crispen Yuen for highlighting this point.

119 Andy Greenberg, Inside the Bitcoin bust that took down the web's biggest child abuse site, *Wired*, 7 April 2022, https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/.

120 Elliptic Threat Intel, UniCC – the largest dark web vendor of stolen credit cards – retires after raking in $358 million in crypto, 12 January 2022, https://www.elliptic.co/blog/unicc-the-largest-dark-web-vendor-of-stolen-credit-cards-retires-after-raking-in-358-million-in-crypto.

121 Ibid.

122 Ravie Lakshmanan, Dark web's largest marketplace for stolen credit cards is shutting down, The Hacker News, 17 January 2022, https://thehackernews.com/2022/01/dark-webs-largest-marketplace-for.html.

123 Elliptic Threat Intel, UniCC – the largest dark web vendor of stolen credit cards – retires after raking in $358 million in crypto, 12 January 2022, https://www.elliptic.co/blog/unicc-the-largest-dark-web-vendor-of-stolen-credit-cards-retires-after-raking-in-358-million-in-crypto.

124 Ibid.

125 BBC, North Korea: Missile programme funded through stolen crypto, UN report says, 6 February 2022, https://www.bbc.com/news/world-asia-60281129.

126 Chainalysis, North Korean hackers have prolific year as their unlaundered cryptocurrency holdings reach all-time high, Chainalysis, 13 January 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

127 Evgenia Pismennaya and Andrey Biryukov, 'Bank of Russia seeks to outlaw mining and trading of crypto, Bloomberg, 20 January 2022, https://www.bloomberg.com/news/articles/2022-01-20/russia-s-fsb-tells-nabiullina-to-ban-crypto-to-defund-opposition.

128 Tom Wilson, Kazakhstan's Bitcoin 'paradise' may be losing its lustre, Reuters, 17 January 2022, https://www.reuters.

com/technology/kazakhstans-bitcoin-paradise-may-be-losing-its-lustre-2022-01-14/.

129 See: Cambridge Bitcoin Electricity Consumption Index, https://ccaf.io/cbeci/mining_map.

130 Elena Fabrichnaya and Alexander Marrow, Russia proposes ban on use and mining of cryptocurrencies, Reuters, 21 January 2022, https://www.reuters.com/business/finance/russian-cbank-proposes-banning-cryptocurrencies-crypto-mining-2022-01-20/.

131 CBR, Расширяются Инвестиционные Возможности ПИФ | Банк России, 13 December 2021, https://cbr.ru/press/event/?id=12526.

132 Prashant Jha, Russian central bank proposes blanket ban on crypto mining and trading, Cointelegraph, 20 January 2022, https://cointelegraph.com/news/russian-central-bank-proposes-blanket-ban-on-crypto-mining-and-trading.

133 Ibid.

134 Elena Fabrichnaya and Alexander Marrow, Russia proposes ban on use and mining of cryptocurrencies, Reuters, 21 January 2022, https://www.reuters.com/business/finance/russian-cbank-proposes-banning-cryptocurrencies-crypto-mining-2022-01-20/.

135 Evgenia Pismennaya and Andrey Biryukov, 'Bank of Russia seeks to outlaw mining and trading of crypto, Bloomberg, 20 January 2022, https://www.bloomberg.com/news/articles/2022-01-20/russia-s-fsb-tells-nabiullina-to-ban-crypto-to-defund-opposition.

136 Ibid.

137 Evgenia Pismennaya, Putin backs crypto mining despite Bank of Russia's hard line, Bloomberg, 27 January 2022, https://www.bloomberg.com/news/articles/2022-01-27/putin-backs-crypto-mining-despite-bank-of-russia-s-hard-line.

138 Daren Fonda, The Russia–Ukraine war is bringing out the good, bad, and ugly of cryptocurrencies, *Barron's*, 18 March 2022, https://www.barrons.com/articles/russia-ukraine-war-cryptocurrencies-51647548970.

139 Eliza Gkritsi, Ukraine's Zelenskyy signs virtual assets bill into law, legalizing crypto, CoinDesk,16 March 2022, https://www.coindesk.com/policy/2022/03/16/ukraines-zelensky-signs-virtual-assets-bill-into-law-legalizing-crypto/.

140 Emily Stewart, War in the time of crypto, Vox, 1 March 2022, https://www.vox.com/recode/22955381/russia-ukraine-bitcoin-donation-war-crypto.

141 Aidan Arasasingham and Gerard DiPippo, Cryptocurrency's role in the Russia-Ukraine crisis, Center for Strategic & International Studies, 15 March 2022, https://www.csis.org/analysis/cryptocurrencys-role-russia-ukraine-crisis.

142 Reuters, Russia makes 'digital' rouble, home-grown credit card push, *Reuters*, 21 April 2022, https://www.reuters.com/business/finance/russia-makes-digital-rouble-home-grown-credit-card-push-2022-04-21/. As of April 2022, only MIR and China's Union Pay are available for Russians to make payments overseas due to global sanctions.

143 Joanna Partridge, Crypto exchange boss resists calls for ban on all Russia transactions, *The Guardian*, 2 March 2022, https://www.theguardian.com/technology/2022/mar/02/crypto-exchange-boss-changpeng-zhao-binance-resists-calls-for-ban-on-all-russia-transactions.

144 Reuters, Russia makes 'digital' rouble, home-grown credit card push, *Reuters*, 21 April 2022, https://www.reuters.com/business/finance/russia-makes-digital-rouble-home-grown-credit-card-push-2022-04-21/.

145 Ryan Browne, Sanctions threaten to cripple Russia's multibillion-dollar crypto industry, CNBC, 22 April 2022, https://www.cnbc.com/2022/04/22/sanctions-could-hurt-russias-multibillion-dollar-crypto-industry.html.

146 Carlos Hernández, Bitcoin has saved my family, *The New York Times*, 23 February 2019, https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html.

147 Nathaniel Popper and Ana Vanessa Herrero, The coder and the dictator, *The New York Times*, 20 March 2020, https://www.nytimes.com/2020/03/20/technology/venezuela-petro-cryptocurrency.html.

148 Rajiv Biswas, Combating terrorism and organized crime: Cryptocurrencies and cybercrime, in *Emerging Markets Megatrends*, ed. Rajiv Biswas. Cham: Springer International Publishing, 2018, https://doi.org/10.1007/978-3-319-78123-5_13.

149 France 24, Maduro bids to revive Venezuela's 'petro' cryptocurrency, 15 January 2020, https://www.france24.com/en/20200114-maduro-bids-to-revive-venezuela-s-petro-cryptocurrency.

150 David Gerard, Bitcoin failed in El Salvador. The president says the answer is more Bitcoin, *Foreign Policy*, 6 December 2021, https://foreignpolicy.com/2021/12/06/bitcoin-city-el-salvador-nayib-bukele/.

151 International Monetary Fund, El Salvador: Staff concluding statement of the 2021 Article IV Mission, 22 November 2021, https://www.imf.org/en/News/Articles/2021/11/22/mcs-el-salvador-staff-concluding-statement-of-the-2021-article-iv-mission.

152 Nayib Bukele, Twitter, 5 December 2021, https://twitter.com/nayibbukele/status/1467333081505976323.

153 Nathan Crooks, El Salvador president says Bitcoin 'really cheap' amid dip, Bloomberg, 22 January 2022, https://www.bloomberg.com/news/articles/2022-01-21/el-salvador-president-says-bitcoin-really-cheap-amid-dip.

154 Eric Martin, Ditch Bitcoin: IMF urges El Salvador to rethink crypto, Bloomberg, 25 January 2022, https://www.bloomberg.com/news/articles/2022-01-25/imf-board-urges-el-salvador-to-ditch-bitcoin-as-legal-tender.

155 Michael McDonald, Bitcoin is costing El Salvador but President Bukele isn't stressed, Bloomberg, 24 May 2022, https://www.

bloomberg.com/news/newsletters/2022-05-24/el-salvador-is-losing-on-bitcoin-btc-but-president-bukele-says-it-s-cool.

156 Eric Martin, Ditch Bitcoin: IMF urges El Salvador to rethink crypto, Bloomberg, 25 January 2022, https://www.bloomberg.com/news/articles/2022-01-25/imf-board-urges-el-salvador-to-ditch-bitcoin-as-legal-tender.

157 Michael McDonald, Bitcoin-bond sale flop deepens debt market rout in El Salvador, Bloomberg, 29 April 2022, https://www.bloomberg.com/news/articles/2022-04-29/bitcoin-bond-sale-flop-deepens-debt-market-rout-in-el-salvador.

158 Michael McDonald, Bitcoin is costing El Salvador but President Bukele isn't stressed, Bloomberg, 24 May 2022, https://www.bloomberg.com/news/newsletters/2022-05-24/el-salvador-is-losing-on-bitcoin-btc-but-president-bukele-says-it-s-cool.

159 FATF, Guidance for a risk-based approach to virtual currencies, June 2015, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

160 FATF, Updated guidance for a risk-based approach: Virtual Assets and virtual asset service providers, October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

161 Ibid.

162 Ian Allison, FATF crypto guidance looks to bring industry in line with banks, CoinDesk, 28 October 2021, https://www.coindesk.com/policy/2021/10/28/fatf-crypto-guidance-looks-to-bring-industry-in-line-with-banks/.

163 Daniel Palmer, G20 reaffirms it will apply expected tough new FATF rules on crypto, 10 June 2019, https://www.coindesk.com/markets/2019/06/10/g20-reaffirms-it-will-apply-expected-tough-new-fatf-rules-on-crypto/.

164 US Department of the Treasury, Remarks of Secretary Steven T. Mnuchin FATF Plenary Session, Orlando, Florida, 21 June 2019, https://home.treasury.gov/news/press-releases/sm713.

165 Nikhilesh De, 'Onerous' FATF recommendations harmful for crypto transparency: Chainalysis, CoinDesk, 12 April 2019, https://www.coindesk.com/markets/2019/04/12/onerous-fatf-recommendations-harmful-for-crypto-transparency-chainalysis/.

166 US Department of the Treasury, Remarks of Secretary Steven T. Mnuchin FATF Plenary Session, Orlando, Florida, 21 June 2019, https://home.treasury.gov/news/press-releases/sm713.

167 Nikhilesh De and Anna Baydakova, All global crypto exchanges must now share customer data, FATF rules, CoinDesk, 21 June 2019, https://www.coindesk.com/markets/2019/06/21/all-global-crypto-exchanges-must-now-share-customer-data-fatf-rules/.

168 See: InterVASP messaging – A new standard for VASPs, https://intervasp.org/; Ian Allison, Crypto firms establish messaging standard to deal with FATF travel rule, 7 May 2020, https://www.coindesk.com/policy/2020/05/07/crypto-firms-establish-messaging-standard-to-deal-with-fatf-travel-rule/.

169 FATF, FATF Report to the G20 finance ministers and central bank governors on so-called stablecoins', June 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.

170 Eva Szalay et al, Global regulators target blockchain-based 'decentralised finance, *Financial Times*, 28 October 2021, https://www.ft.com/content/126ecd7a-0b02-4d9f-97f7-ffa2b24894a2.

171 FATF, Updated guidance for a risk-based approach: Virtual Assets and virtual asset service providers, October 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

172 Ibid.

173 Arnold Kirimi, Estonia's new AML laws set to clamp down on crypto industry, 31 December 2021, https://cointelegraph.com/news/estonia-s-new-aml-laws-set-to-clamp-down-on-crypto-industry.

174 Ott Tammik and Aaron Eglitis, Estonia moves to reassure crypto sector as new rules weighed, Bloomberg, 3 January 2022, https://www.bloomberg.com/news/articles/2022-01-03/estonia-moves-to-reassure-crypto-sector-amid-new-rules.

175 Ott Tamik, Estonia's crypto market vulnerable to crime, regulator says, Bloomberg, 6 January 2022, https://www.bloomberg.com/news/articles/2022-01-06/estonian-crypto-market-vulnerable-to-crime-says-regulator.

176 Ibid.

177 Ibid.

178 Ian Allison, FATF crypto guidance looks to bring industry in line with banks, CoinDesk, 28 October 2021, https://www.coindesk.com/policy/2021/10/28/fatf-crypto-guidance-looks-to-bring-industry-in-line-with-banks/.

179 In February 2022, the Financial Stability Board, an international monitoring and advisory body, warned: 'Crypto-asset markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system.'

180 In 2021, US Commodity Futures Trading Commission commissioner Dan Berkovitz suggested that many DeFi apps could be illegal, while US Securities and Exchange Commission (SEC) chair Gary Gensler continued his push to extend regulations into the sector, suggesting regulatory equivalence with many financial products covered under existing SEC mandates. See Martin Young, CFTC commissioner calls for crackdown on 'illegal' DeFi, 9 June 2021, https://finance.yahoo.com/news/cftc-commissioner-calls-crackdown-illegal-061340094.html; Kevin Helms, SEC working with CFTC on crypto regulation, says Chairman Gensler, Bitcoin News, 12 February 2022, https://news.bitcoin.com/sec-working-with-cftc-crypto-regulation-chairman-gensler/.

181 Commodity Futures Trading Commission, CFTC charges 14 entities for failing to register as FCMs or falsely claiming to

be registered, 29 September 2021, https://www.cftc.gov/PressRoom/PressReleases/8434-21.

182 Chainalysis, Chainalysis in Action: OFAC sanctions Russian cryptocurrency OTC Suex that received over $160 million from ransomware attackers, scammers, and darknet markets, Chainalysis, 22 September 2021, https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021/; Chainalysis, P2P cryptocurrency exchange Chatex and two Russian nationals indicted and sanctioned for roles in ransomware operations, 8 November 2021, https://blog.chainalysis.com/reports/ofac-sanction-chatex-revil-sodinokibi-november-2021/.

183 Chanyaporn Chanjaroen, Singapore asks crypto firms not to market services to public, Bloomberg, 17 January 2022, https://www.bloomberg.com/news/articles/2022-01-17/singapore-tells-crypto-firms-not-to-market-services-to-public.

184 Clara Hernanz Lizarraga, Spain clamps down on crypto advertising with order to flag risks, Bloomberg, 17 January 2022, https://www.bloomberg.com/news/articles/2022-01-17/spain-clamps-down-on-crypto-advertising-with-order-to-flag-risks.

185 See HMRC Cryptoassets manual, https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto61214.

186 BBC, HMRC seizes NFT for first time in £1.4m fraud case, 13 February 2022, https://www.bbc.com/news/business-60369879.

187 Tom Metcalf, U.K. watchdog to restrict crypto ads to wealthiest investors, Bloomberg, 19 January 2022, https://www.bloomberg.com/news/articles/2022-01-19/u-k-watchdog-to-restrict-crypto-ads-to-wealthiest-investors.

188 Prashant Jha, Indonesian Islamic organization issues new fatwa against crypto use, Cointelegraph, 20 January 2022, https://cointelegraph.com/news/indonesian-islamic-organization-issues-new-fatwa-against-crypto-use.

189 Joseph Menn and Christopher Bing, Governments turn tables on ransomware gang REvil by pushing it offline, Reuters, 21 October 2021, https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

190 Laura Davison and Allyson Vesprille, IRS sees crypto seizures worth billions of dollars next year, Bloomberg, 18 November 2021, https://www.bloomberg.com/news/articles/2021-11-18/irs-sees-crypto-seizures-totaling-billions-of-dollars-next-year.

191 Andy Greenberg, The DOJ's $3.6B seizure shows how hard it is to launder crypto, *Wired*, accessed 14 February 2022, https://www.wired.com/story/bitcoin-seizure-record-doj-crypto-tracing-monero/.

192 Internal Revenue Service, Annual Report 2021, https://www.irs.gov/pub/irs-pdf/p3583.pdf.

193 Allyson Versprille, Crypto, NFTs are rife with 'mountains' of fraud, IRS says', Bloomberg, 26 January 2022, https://www.bloomberg.com/news/articles/2022-01-26/irs-seeing-mountains-and-mountains-of-fraud-with-crypto-nfts.

194 Josh Saul and Allyson Versprille, Bitcoin mining's hearing in U.S. House questions power usage, Bloomberg, 20 January 2022, https://www.bloomberg.com/news/articles/2022-01-20/bitcoin-mining-s-hearing-in-u-s-house-questions-its-power-usage.

195 See: Global impact of crypto trading, Forex Suggest, https://forexsuggest.com/global-impact-of-crypto-trading/.

196 See: Cambridge Bitcoin Electricity Consumption Index, https://ccaf.io/cbeci/index/comparisons.

197 Finansinspektionen, Crypto-assets are a threat to the climate transition – energy-intensive mining should be banned, 5 November 2021, https://www.fi.se/en/published/presentations/2021/crypto-assets-are-a-threat-to-the-climate-transition--energy-intensive-mining-should-be-banned/.

198 Ibid.

199 Michael Casey et al, The impact of blockchain technology on finance: A catalyst for change, International Center for Monetary and Banking Studies, 2018, https://voxeu.org/content/impact-blockchain-technology-finance-catalyst-change.

200 Kenneth S. Rogoff, *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*, *The Curse of Cash*. Princeton University Press, 2017, https://doi.org/10.1515/9781400888726.

201 *The Economist*, Will Web3 reinvent the internet business?, 24 January 2022, https://www.economist.com/business/2022/01/29/will-web3-reinvent-the-internet-business.

202 *The Economist*, A future with fewer banks, 6 May 2021, https://www.economist.com/special-report/2021/05/06/a-future-with-fewer-banks.

203 See Global cryptocurrency market charts, CoinMarketCap, https://coinmarketcap.com/charts/.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

## ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 500 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

**www.globalinitiative.net**