Chainalysis

The Chainalysis Crypto Myth Busting Report

33 Cryptocurrency Myths Refuted

July 2023

Table of Contents

Introduction

From the TerraLUNA crash to the FTX collapse, 2022 went down as a tumultuous year for cryptocurrency. While the shake-ups caused chaos, the cryptocurrency ecosystem has proven to be remarkably resilient. But bad news always leads, and when crypto scandals rise to the fore, so too do long-held myths about digital currency.

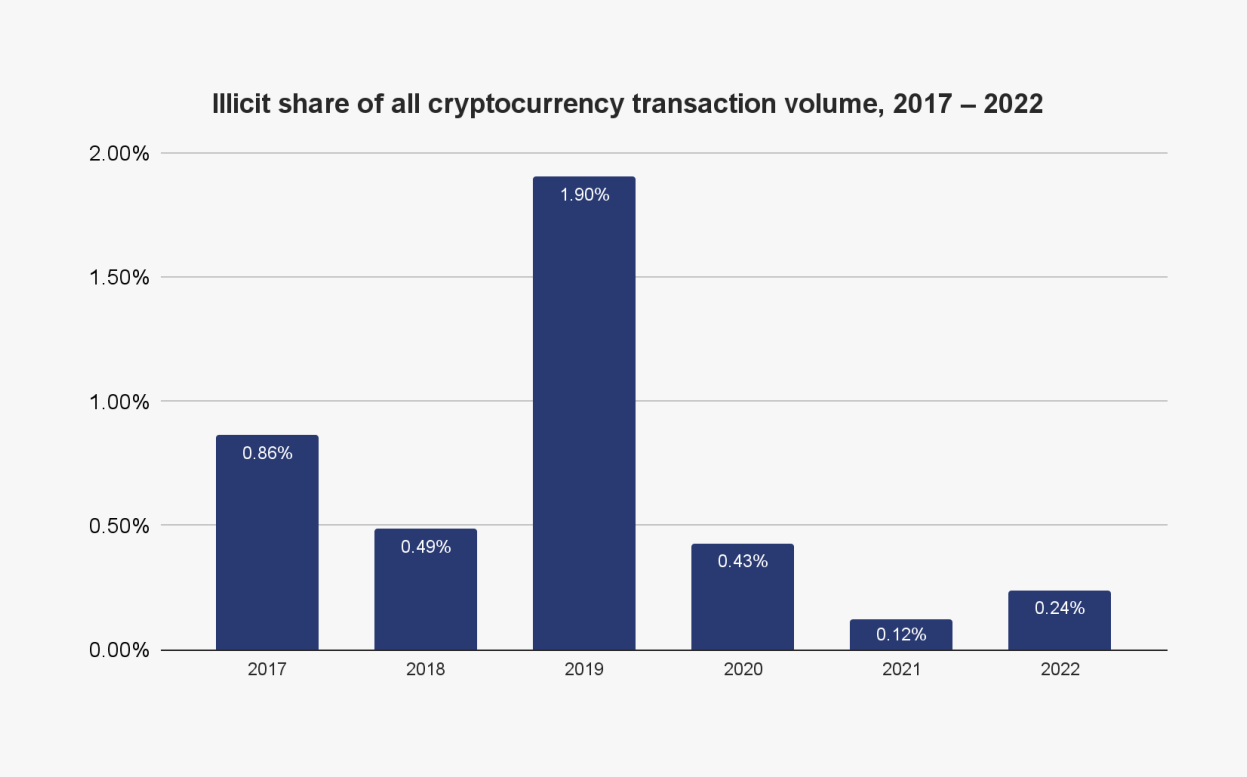
Now, as governments and financial institutions consider how to regulate and integrate cryptocurrency into the global financial system, it's especially important to set the record straight. While there are certainly risks and valid concerns, blockchain technology has enormous potential to democratize finance, increase economic transparency, reduce costs of doing business, and spur innovation. Given that, we want to ensure financial institutions and regulators are focused on the *right* risks — the true, valid concerns — when they evaluate the opportunities posed by cryptocurrency. To that end, in this report, we're going to dispel some misconceptions, and tackle 33 myths related to cryptocurrency's safety, legitimacy, viability, and scalability.

Safety and security

MYTH 01

Crypto is only used by criminals.

In crypto's early days, a much higher share of all transaction volume was associated with crime. One emblematic example of this was Silk Road, the first modern darknet market, which at its peak accounted for nearly 20% of Bitcoin's daily economic activity before being shut down by law enforcement in 2013. In the last decade, increased law enforcement pressure and crypto regulation has helped reduce crypto-related crime, while blockchain analysis tools have also made it easier to investigate and prevent illicit activity. The progress has been impressive, as we estimate that illicit activity represented less than 1% of overall crypto transaction volume in 2022.[1]



MYTH 02

Crypto is completely unregulated.

Particularly over the past four years, we have seen countries steadily move forward to introduce regulations covering cryptocurrency, on topics as diverse as anti-money laundering, consumer protection, market conduct, and prudential requirements. Below, we set out a few examples from across the world.

In 2019, the intergovernmental Financial Action Task Force (FATF) issued detailed global standards for combating illicit finance amongst its many participating countries, and those standards have been periodically updated since. At their core though, these standards call for crypto businesses to be subject to AML/CFT requirements such as customer due diligence and transaction monitoring, as well as the exchange and retention of certain transaction information under what is known as the "Travel Rule".

Regulators globally have been working hard since then to translate FATF's global standards into domestic rules. For instance, Singapore's Monetary Authority of Singapore (MAS) regulates digital payment token (DPT) service providers under the 2019 Payment Services Act (PSA), with AML/CFT requirements stipulated in an accompanying Notice. In South Korea, virtual asset service providers have been regulated for AML/CFT purposes since 2021. Australia requires digital currency exchanges to be registered with AUSTRAC and is currently in the process of updating its AML/CFT rules to further align them with the FATF standards.

In the United States, crypto businesses that qualify as money services businesses (MSBs) are required to comply with anti-money laundering and counter-terrorist financing (AML/CFT) requirements under the Bank Secrecy Act. This means that a broad range of crypto businesses, such as exchanges, ATMs, brokers, custody providers, and more need to register as MSBs with the Financial Crimes Enforcement Network (FinCEN) and implement AML/CFT programs.

The U.S. government's focus on cryptocurrency has also grown beyond AML/CFT in recent years. In March of 2022, for example, President Biden signed an Executive Order on Ensuring Responsible Development of Digital Assets with objectives to expand America's global leadership in the space, ensure financial stability, prevent illicit activity, protect national security, and help the U.S. take the lead on central bank digital currency (CBDC) research and development. Since 2022, the U.S. House of Representatives has been working on legislation that would improve regulatory clarity. The Chairmen of the House Financial Services Committee and House Agriculture Committee have recently released a joint discussion draft of legislation providing a statutory framework for crypto regulation.

In 2022, the United Arab Emirates (UAE) launched its Virtual Asset Regulatory Authority (VARA), a government body dedicated to crypto regulation. Dubai-based VARA has since rolled out a comprehensive set of regulations and rulebooks covering seven types of virtual asset activities.

In April 2023, the EU parliament passed Markets in Crypto-assets (MiCA), the first comprehensive legislation in its region for regulating digital assets. Many other parts of the world are also pursuing crypto regulation. So, while there's still uncertainty surrounding crypto in some parts of the world, these examples show the market is moving towards more regulatory clarity.

MYTH 03

Miners could alter Bitcoin's properties for their own gain.

A blockchain is an immutable database that records transactions on a distributed public ledger. Bitcoin and subsequent blockchains are designed to be decentralized and secure so that the ledger is always synchronized for all users and accurately reflective of users' transactions.

However, a 51% attack presents one case where a blockchain like Bitcoin's can be altered. The term refers to a case in which one person or a group gains more than half of a blockchain's hashing power, meaning the total computing power being used to mine that blockchain's primary asset. In that case, the 51% attacker could stop miners from completing blocks and prevent new blocks from being recorded, as well as change the order in which new transactions are processed. The attacker could even reverse transactions that haven't yet been processed in order to double spend the coins.

Fortunately, 51% attacks are rare and have never occurred on a major blockchain, largely because the consensus mechanisms work as designed. Let's use Bitcoin as our example again: Under Bitcoin's Proof-of-Work (PoW) consensus mechanism, the more widely used Bitcoin is, the more incentive there is to mine it, which means it becomes harder and more cost-prohibitive to amass the hashing power necessary for an attack. Additionally, it would go against most miners' economic interests to launch a 51% attack even if they could, because doing so would destroy investor faith in the compromised network.

MYTH 04

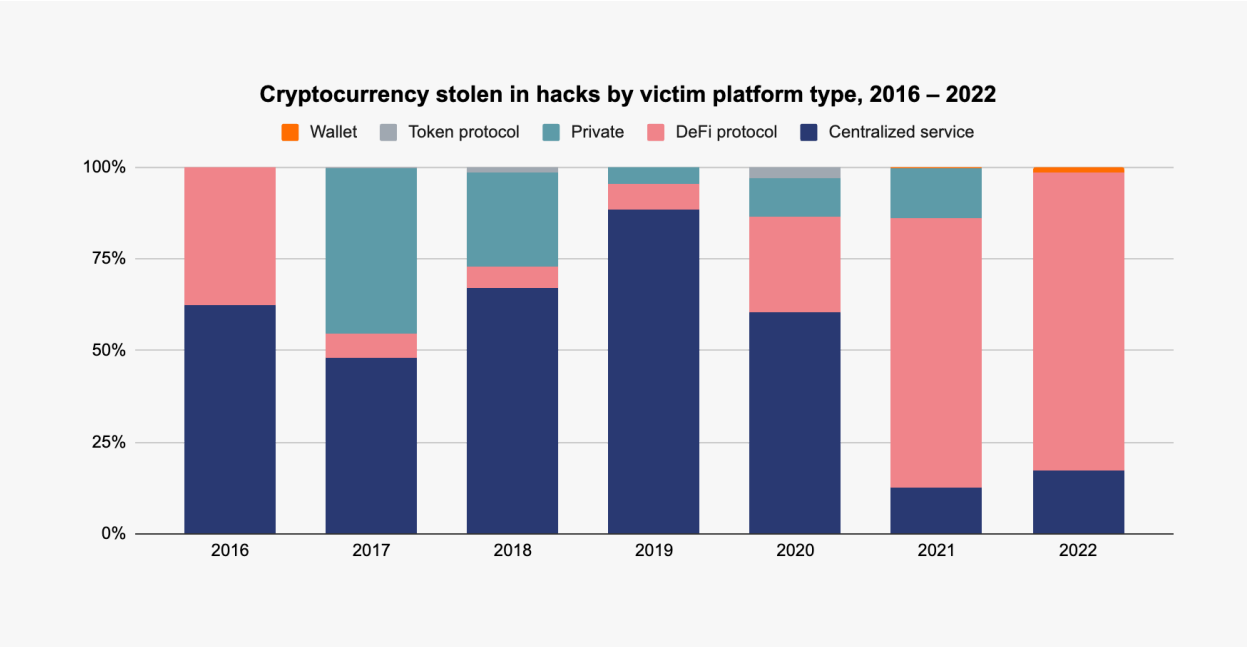
There's no way to guard against hacks.

In the early days of the internet, prevailing wisdom said to never enter your credit card data on a website. Once SSL encryption technology came around and reputable payment gateways were established, e-commerce began to proliferate.

We're seeing a similar dynamic play out in cryptocurrency, where hacking is an issue, but one that is being solved over time.

In the early days of crypto, centralized exchanges emerged as a popular solution for swapping and storing cryptocurrency with a custodian, but security shortcomings led to major hacks such as the one that felled Mt. Gox. In the years since though, centralized exchanges have become a more established sector of the industry, improved their security capabilities, and face fewer hacking incidents.

Now, the hacking problem has shifted to the cutting edge of crypto: DeFi, or decentralized finance. Our 2023 crime report revealed that most hacking incidents last year occurred with decentralized finance (DeFi) protocols.



Within the DeFi segment, 64% of attacks targeted cross-chain bridges, which are protocols that let users port their cryptocurrency from one blockchain to another. We've covered previously why cross-chain bridges are uniquely vulnerable to attacks. Even so, DeFi is responding, with blockchain security firms like Chainalysis partner Halborn providing DeFi code audits to identify and fix vulnerabilities. The bottom line is this: New technologies, especially those born from the internet, often face security challenges in their early days. As adoption grows, industry participants learn from each incident and security improves. We expect this to continue with cryptocurrency.

MYTH 05

There's no way to prevent criminals from using crypto.

As mentioned earlier, crypto exchanges are subject to the same KYC and AML rules as banks under FATF standards. Blockchain analysis tools are key to helping crypto organizations comply with these rules as they provide transaction monitoring services and tools for tracing the movement of illicit funds. Law enforcement usage of these tools has led to several successful investigations of criminals abusing cryptocurrency. Let's look at some examples below.

In 2019, Chainalysis assisted law enforcement in taking down the world's largest child abuse material site, Welcome to Video. Using Chainalysis Reactor, IRS-Criminal Investigations (IRS-CI), Homeland Security Investigations (HSI), and other agencies analyzed blockchain transactions to locate the site's owner, contributors, and users, and collaborated with international law enforcement to make arrests across 12 countries.

In 2022, the U.S. government seized $3.6 billion worth of cryptocurrency connected to the 2016 Bitfinex hack — the largest recovery of assets in the history of law enforcement. Law enforcement also arrested Ilya Lichtenstein and his wife, Heather Morgan for their role in laundering the stolen funds. The same year, another prominent case, Axie Infinity's Ronin Bridge hack, saw law enforcement seize $30 million worth of cryptocurrency stolen by North Korean-linked hackers — the first time funds stolen from a crypto service by North Korean hackers were recovered. In 2022 alone, the IRS Criminal Investigation Unit seized $7 billion worth of digital assets.

In April 2023, a coordinated international law enforcement effort called Operation Cookie Monster shut down fraud shop Genesis Market and resulted in the arrest of hundreds. The following day, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the criminal marketplace. Just weeks later in a separate case, OFAC sanctioned three individuals tied to North Korean money laundering via crypto, and the Department of Justice (DOJ) also charged one of them for his role in money laundering conspiracies.

As evidenced by these examples, when it comes to fighting crypto-based crime, governments are quickly ramping their ability to recover stolen crypto used for illicit purposes.

Notable cryptocurrency seizures, 2013 – 2023

2013

Mt Gox seizure

The U.S. government seized **$2.9 million** from a subsidiary of the Mt. Gox exchange for operating as an unlicensed money transmitting business. Learn more.

2019

Welcome to Video seizure

The U.S. Department of Justice (DOJ) shut down the largest ever child exploitation site by amount of material stored. Authorities seized **over 8 terabytes of data** and arrested the site's owner and operator. Learn more.

2020

Silk Road hack recovery

The U.S. DOJ seized **$1 billion** in cryptocurrency from a wallet tied to a Silk Road hacker known as Individual X. Learn more.

2021

Silk Road hack recovery continued

Law enforcement seized **over $3.36 billion** in cryptocurrency from James Zhong, who stole Bitcoin from the Silk Road darknet marketplace in 2012.
Learn more.

International money laundering operation seizure

In June and July, British police seized a total of **£294 million** in cryptocurrency tied to an international money laundering investigation. Learn more.

International rug pull seizure

The Greater Manchester Police's (GMP) Economic Crime Unit seized **over £16 million** in crypto tied to an investment scam. The following year, the GMP returned **over £4 million** to victims. Learn more.

2022

Bitfinex hack recovery

The IRS Criminal Investigation division, the FBI, and Homeland Security Investigations recovered **$3.6 billion** in crypto (the largest ever recovery of assets from a theft) in connection with the 2016 Bitfinex hack. Learn more.

Ronin Bridge hack recovery

Law enforcement seized **$30 million** in cryptocurrency from North Korean-linked hackers, the first time that crypto stolen by a North Korean hacking group was recovered. Learn more.

2023

Bitzlato seizure

Europol seized **over $19 million** in crypto after the exchange's founder was charged with money laundering. Learn more.

Chipmixer seizure

Supported by Europol, a group of international authorities seized **over €40 million** from this unlicensed cryptocurrency mixer. Learn more.

Hezbollah and Iran Quds Force seizure

In the first Hezbollah-related digital currency seizure, Israeli authorities recovered roughly **$1.7 million** in crypto from Hezbollah, a heavily sanctioned terrorist group based in Lebanon, and from Iran's Quds Force, which funds and works extensively with Hezbollah. Learn more.

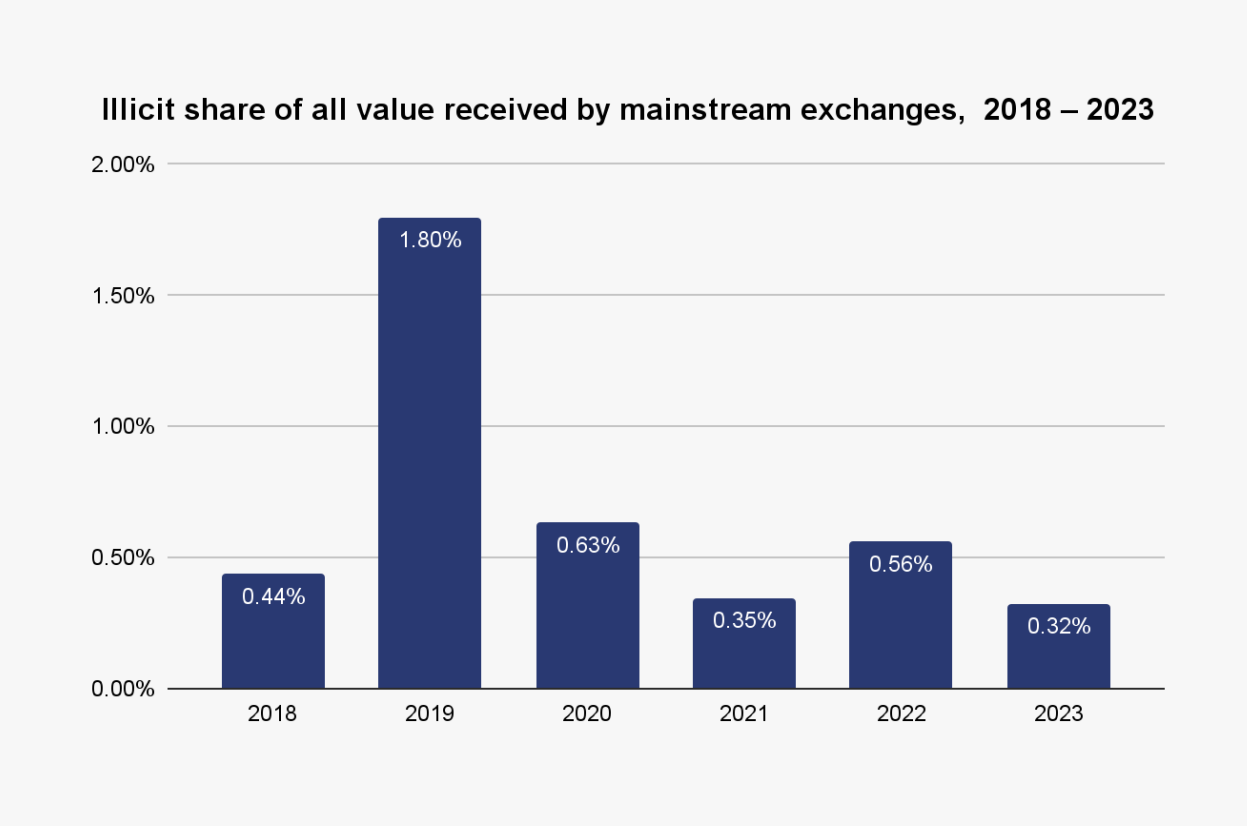
MYTH 06

It's impossible to know what cryptocurrency businesses do with their crypto, and therefore cryptocurrency businesses are too risky for banks to interact with.

Too many institutions regard the cryptocurrency industry as a high-risk monolith when it comes to compliance. In reality, the ecosystem is incredibly diverse. There are direct market participants, infrastructure and data providers, gaming and AI platforms, payment processors, and entirely new organizations that are constructing novel ways of creating, socializing, and transacting. And due to the inherent transparency of blockchains, banks can see all of these companies' crypto transactions in real time. Blockchain analysis tools allow financial institutions to analyze the risk of each platform's transactions as they occur, which means they can support the most promising and innovative industry participants while still meeting their compliance needs.

Imagine if a bank had this kind of transparency with all of its corporate clients' funds. Blockchain analysis builds a picture of a business's biggest counterparties and can flag transactions that may present concerns or risks to its customers. These platforms also help compliance teams benchmark the activity of one cryptocurrency business against its peers. This picture provides an enormous amount of context in the onboarding process. Transaction activity that Chainalysis observes is perhaps the best reflection of the strength of a company's transaction monitoring and AML programs.

It's also worth noting that if we apply blockchain analysis at scale, we can see that cryptocurrency businesses are generally quite safe. The chart below demonstrates that illicit exposure is a very small share of total inflows across mainstream exchanges.[2]



Aside from the anomalous year of 2019, which saw extreme levels of scamming activity, well below 1% of all value entering exchanges since 2018 has come from illicit addresses.

Of course, financial institutions must still remain vigilant. For banks considering cryptocurrency adoption, the key is to acquire the blockchain analysis expertise necessary for a compliance team to interpret the risks posed by blockchain entities — either through training or hiring — and analyze those risks within the framework of their strategy around market risk, KYC, AML/TF, sanctions, financial crimes, and fraud. We lay out some of the steps banks can take to accomplish this in our Crypto Maturity Model.

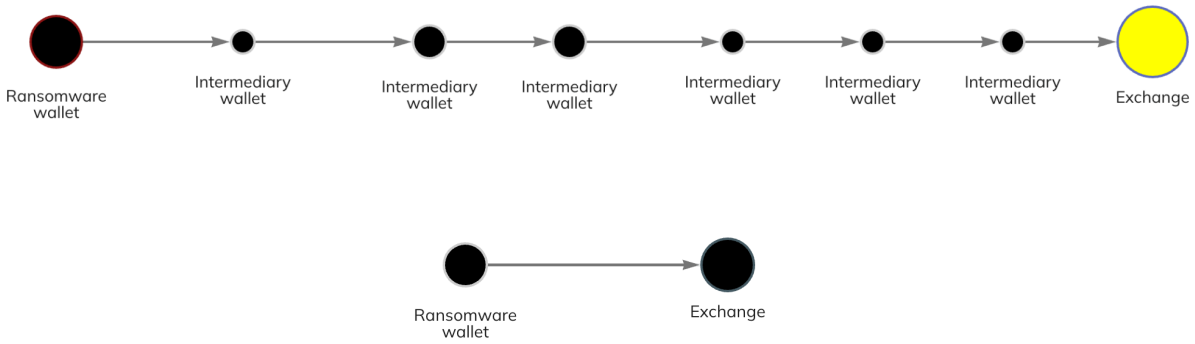
From there, moving into crypto with confidence also requires establishing a risk appetite and compliance procedures, and then, for retail banks, letting customers transact with those crypto businesses that are aligned in terms of risk. It used to be a challenge for banks to accurately assess the landscape, but tools like Kryptos provide in-depth on-chain metrics, which help banks grow exposure to the crypto ecosystem safely. With that foundation, banks can also start taking cryptocurrency businesses as clients, and offer services beyond just business banking, like advising crypto businesses on IPOs and mergers and acquisitions, or providing foreign exchange services.

MYTH 07

In financial crimes compliance, tracing crypto “a few hops back” is sufficient analysis.

Compliance teams and investigators typically assess the risk levels of an address, wallet, or service by looking at its on-chain exposure to entities associated with risky or illicit activity. For example, if a cryptocurrency exchange has received significant cryptocurrency from a wallet associated with a ransomware organization, a bank may decide that exchange is too risky to work with. But what if the exchange didn’t receive those funds *directly* from the ransomware wallet? What if the funds instead passed through an intermediary personal wallet? What if they passed through three intermediary wallets? Or 10? Blockchain analysts generally refer to these intermediaries as “hops,” and many have asked how many hops away from danger a wallet or service must be to be considered safe.

The answer: The relevance of the number of hops will always depend on the scenario at hand. Our clients have investigated cases involving hundreds of hops that occurred over a single day, as well as cases involving two hops that occurred over the course of three years. As the fiat on-ramps for cryptocurrency businesses, exchanges require software for their compliance teams that provides analysis for every scenario to get to the ultimate cash-in and cash-out points.



Both scenarios above would likely require closer analysis from compliance teams.

Consider the two graphs above. The first may appear to present less risk for the exchange, as there are several hops between it and the ransomware wallet. However, in reality, the personal wallets making up those hops could all belong to the ransomware actor. That’s why Chainalysis calculates every blockchain entity’s *indirect exposure* to illicit activity, meaning the funds received from or sent to illicit addresses regardless of the number of non-service addresses in between. That last point is important — if a service sits between two entities, we wouldn’t say they necessarily have exposure to one another, as ownership of assets can change within services in ways that aren’t visible on-chain.

MYTH 08

Banks need a risk score to determine if a crypto business is risky or not.

In an industry as new as cryptocurrency, it can be tempting to think that something like a simple risk score could encompass everything a bank needs to know about any particular business. However, as is always the case with KYC, an assessment of a cryptocurrency counterparty should be guided by the risk-based approach the bank takes with all of its counterparties.

As discussed above, on-chain data from Chainalysis can help banks better understand the risk presented by a given crypto business and its counterparties, but that on-chain data is only one part of a comprehensive risk assessment. Banks leverage several other sources of information to assess the risk of every business they interact with, whether crypto or fiat-based. For instance, much like traditional financial institutions, crypto businesses collect KYC data to tie real-world identities to accounts when users sign up. That process can include checks for connections to sanctioned entities, politically exposed person screenings, and adverse media screenings.

Legitimacy

MYTH 09

All crypto is Bitcoin.

While Bitcoin was the first form of cryptocurrency and is the largest by market capitalization, thousands of other cryptocurrencies have since entered the ecosystem on hundreds of different blockchains. According to CoinMarketCap, there are over 24,000 cryptocurrencies as of this report, traded on over 600 exchanges, and crypto's market capitalization exceeds $1 trillion.

MYTH 10

Cryptocurrency is all scams.

Over the years, we've seen disheartening stories about victims losing cryptocurrency in everything from romance scams to pump and dump token sales. Given the attention on these exploits, those with minimal knowledge of the ecosystem would believe cryptocurrency simply can't be trusted. However, the data shows that scams represent a tiny fraction of all cryptocurrency activity. Mainstream services received inflows of $8.1 trillion worth of cryptocurrency in 2022, while crypto scammers' collective on-chain revenue was just $6 billion on the year.

MYTH 11

Crypto is anonymous and untraceable.

Despite what you may have heard, Bitcoin was never meant to be and has never been untraceable. Satoshi Nakamoto's Bitcoin whitepaper contrasted the potential privacy of Bitcoin with that of bank transactions, while outlining a vision for cryptocurrency's traceability. Cryptocurrency transactions have always been pseudonymous, in that they're tied to a static, publicly visible address, and not anonymous, as many believe. The extension of KYC obligations to cryptocurrency businesses also ensured that other transactions, such as conversions of fiat currency into crypto, wouldn't be anonymous either.

Far from being anonymous, the blockchain has produced the most transparent, democratized financial system the world has seen yet, with all transactions recorded in a public ledger. However, to effectively monitor activity or track down criminals, having the right tools is important, and that's where blockchain analysis platforms come in. Crypto businesses, financial institutions, and law

enforcement agencies have been using these tools to maintain compliance, mitigate risk, and trace criminal activity in order to recover stolen or illicit funds.

MYTH 12

Anyone can produce new crypto, so it's worthless.

For most cryptocurrencies, creating new tokens is done by devoting resources to the blockchain's consensus mechanism, which is the process by which network participants authenticate new transactions and add them to the ledger, thereby perpetuating a single, shared blockchain for all participants.

The two most common consensus mechanisms are Proof-of-Work (PoW) and Proof-of-Stake (PoS). Bitcoin, for instance, is mined through the PoW consensus mechanism. In this model, groups or individuals "mine" new Bitcoin blocks by solving complex, cryptographic puzzles. Whoever solves the puzzle first receives the right to validate new transactions, add them to the blockchain, and receive the associated prize of newly minted Bitcoin, plus fees from the new block's transactions. This work is energy and computing power-intensive. More often than not, miners are offramping large portions of their Bitcoin prizes to pay for operational expenses like electricity.

Under the Proof-of-Stake (PoS) model, on the other hand, validators of new blocks don't have to expend computing power. Instead, they lock up — or stake — some of their cryptocurrency in a smart contract. A validator is randomly chosen to create each new block and receive the associated rewards, and participants can stake as much as they want to increase their odds. Ether, TRON, and Solana are examples of cryptocurrencies using the PoS model.

Regardless of the specific consensus mechanism, mining and staking require enough time, resources, and expertise that it would be inaccurate to say anyone can do it.

Aside from mining and staking, anyone can also build new tokens on top of many smart contract-supporting blockchains such as Ethereum, BNB Chain, Solana, and others. However, that doesn't inherently devalue existing cryptocurrencies. Since Bitcoin launched in 2009, thousands of other cryptocurrencies have launched as well, and Bitcoin's price has continued to appreciate, while none of its price fluctuations appear related to other cryptocurrencies emerging. Any new cryptocurrency can gain traction if it fills an existing market need, but that traction doesn't necessarily come at the expense of existing cryptocurrencies.

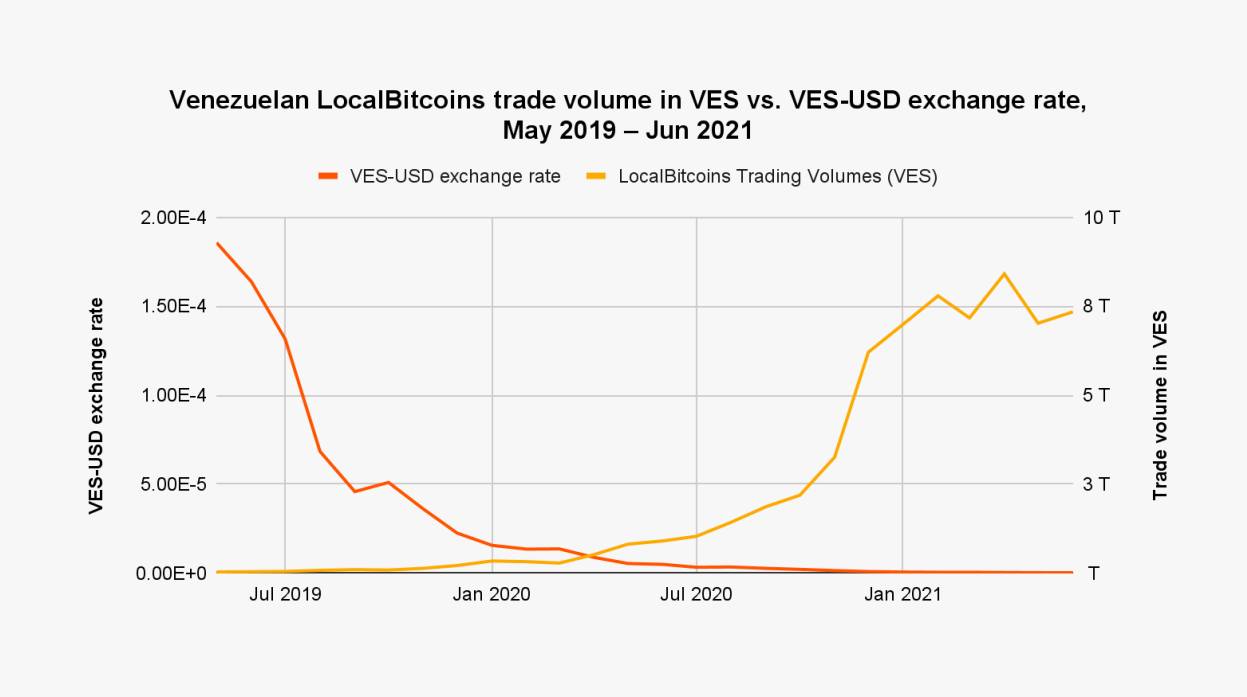
MYTH 13

Crypto has no real-world use case.

Cryptocurrency has several real-world use cases, especially in emerging markets, many of which are leading the way in grassroots crypto adoption. One of those use cases is remittances. In our 2022 Geography of Cryptocurrency Report, we found that international payments for individuals and small business owners are increasingly being carried out in cryptocurrency due to both increased speed and lower costs. Remittances are also enabling charitable giving. For instance, in the year following the outbreak of the Russia-Ukraine War, cryptocurrency users donated over $56 million worth of crypto to war-torn Ukraine. In February 2023, crypto donations again played a significant role in providing relief to victims of the earthquake that rocked Turkey and Syria, with users sending nearly $6 million in the days following.

Additionally, we've also seen cryptocurrency used as an alternative store of value during times of financial instability. Venezuela offers a useful example. The country has suffered from frequent bouts of hyperinflation, and holders of its national currency, the bolivar, have seen their purchasing power and savings drastically decrease. That may be one reason the country has embraced cryptocurrency so much — we estimate Venezuelans received over $37.4 billion worth of crypto in 2022, the sixth most of any Latin American country, despite Venezuela having one of the lowest GDPs per capita in the region.

The data even suggests that at times of high inflation and currency depreciation, Venezuelans have sought to protect themselves by acquiring more cryptocurrency. Check out the chart below, which plots the bolivar-USD exchange rate against bolivar-for-Bitcoin trading volume on P2P exchange LocalBitcoins.



We can see that as the exchange rate fell and the bolivar weakened between 2019 and 2021, Venezuelans moved to acquire more Bitcoin. We've seen similar dynamics in other countries like Argentina, Nigeria, and Kenya during times of currency instability.

Though not yet as prevalent as others, retail purchasing is a growing crypto use case. According to a survey PYMNTS conducted of merchants with annual online sales totaling at least $250 million, 46% of merchants accept crypto as payment. PYMTS also found that "85% of businesses with more than $1 billion in annual online sales say they accept some form of crypto-enabled payment method." Deloitte's 2021 Merchants getting ready for crypto study, which polled 2,000 senior executives at U.S. retail organizations, found that over 75% of merchants reported plans to accept stablecoin and cryptocurrency payments in the next two years.

MYTH 14

It's bad that lost Bitcoin can't be replaced.

In order to access Bitcoin stored in a personal wallet, users must keep track of their private keys, which are long strings of alphanumerics similar to a password that allow users to access the Bitcoin held on their corresponding public keys, also known as addresses. The only difference is that there's no "reset password" option — if the keys are lost, they're lost. Some personal wallets offer workarounds, such as easier-to-remember seed phrases, but these options aren't always widespread. There have been several notable stories of early Bitcoin adopters who subsequently lost

their private keys and lost out on major wealth, such as the Welsh man who accidentally threw a USB drive with 8,000 Bitcoin in the trash in 2013 and has been trying to excavate his local landfill ever since, thus far without success.

Mishaps aside, since most Bitcoin is held for long-term investment, it's hard to quantify how many are lost. We consider Bitcoin lost if it hasn't moved from its current set of addresses in five years or longer and roughly 20% of Bitcoin falls into that category. However, while lost Bitcoin may be frustrating for the owner, it's not a bad thing for the ecosystem. Satoshi Nakamoto said, "Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone." Because Bitcoin is finite and lost coins reduce supply, they raise the value of all other coins.

Another consideration is that a single Bitcoin can be divided into units as small as one one hundred millionth of a Bitcoin (these smallest possible units are known as satoshis). That divisibility means that even if the millions of lost Bitcoin drives the price of the asset sky high, users can simply transact with smaller units. In other words, Bitcoin can remain viable as a means of value transfer even in a deflationary environment.

There are also proven ways to secure Bitcoin (and any other cryptocurrency) to prevent loss. For less experienced investors or those with a small amount of cryptocurrency, storing funds in a custodial exchange is a good place to start as it secures the assets on your behalf. These services also have recovery options if you get locked out of your wallet.

MYTH 15

Early crypto adopters receive disproportionate rewards.

Any time new technology is introduced, there's risk for investors, but also huge potential upside. For instance, Jeff Bezos famously told early Amazon investors there was a 30% chance the company would fail — a reasonable warning given the internet was in its infancy — but those who took on that risk got rich. This is a widely accepted aspect of our financial system, so why should we feel any different when it plays out in cryptocurrency? In crypto's early days, adoption was risky because Bitcoin was unregulated, there weren't many legitimate enterprises accepting cryptocurrency as a form of payment, and most importantly, there was no telling if there would ever be wider demand for it. So, even though Bitcoin's price was low (the initial value was US$0.0008, and didn't hit $1 until February 2011), investors had no way of knowing if they'd be able to spend the cryptocurrency they'd mined or purchased.

MYTH 16

CBDCs will make existing cryptocurrencies obsolete.

Many central banks around the world are exploring the potential of central bank digital currencies (CBDCs) as a way to enhance and broaden access to payment systems. While most CBDC projects are still in the experimental phase, some have speculated that a currency combining the convenience of crypto with the full faith and backing of a central bank would render cryptocurrency obsolete.

In practice, CBDCs are tailored to specific priorities of each country, such as to promote financial inclusion, foster competition in payment systems, or to facilitate the tokenization of finance. Not unlike crypto, a common aspiration of CBDCs is to make finance more widely accessible or less costly.

This doesn't mean that CBDCs and crypto are substitutes for one another. Just as many currencies and payment rails co-exist today, so may crypto and CBDCs in the future. For instance, some countries with active CBDC projects, such as Singapore and Australia, have concurrently highlighted the potential role of stablecoins in making traditional finance more efficient.

Most importantly, while cryptocurrencies like Bitcoin were invented partly in response to some challenges associated with fiat currencies, such as inflation, today their purpose and potential extend beyond the streamlining of finance. Use cases for crypto and blockchain continue to grow, including in the nascent but fast-growing space of Web3.

MYTH 17

All cryptocurrencies are alike.

There are hundreds, if not thousands of different cryptocurrencies seeing significant usage. While many share similarities, there are also key differences in their technical characteristics and, subsequently, the use cases they enable. To illustrate this point, let's compare and contrast three of the most prominent blockchains: Bitcoin, Ethereum, and BNB (also known as Binance Coin).

Bitcoin is the first ever blockchain, and its Proof-of-Work (PoW) consensus mechanism gives it an emphasis on decentralization and security, which along with its purposeful scarcity makes it popular as a store of value and hedge against fiat financial systems. For this reason, Bitcoin has often been compared to "digital gold." However, Bitcoin's relatively small block sizes and ten-minute time for block processing translate into a relatively low number of transactions per second that can be processed. This makes Bitcoin more conducive to large, less time-sensitive transactions as compared to other blockchains.

Ethereum can also function as a store of value, but its smart contract technology gives it many other use cases not possible with Bitcoin. Smart contracts are self-executing contracts whose

functionalities and actions are written into code. This means that developers can build other forms of programmable currency on top of the Ethereum blockchain, as well as decentralized apps for use cases like borrowing, lending, asset exchange (all of which are examples of decentralized finance, or DeFi), provably scarce digital art (in the form of NFTs), and more. Ethereum recently switched its consensus mechanism from PoW to Proof-of-Stake (PoS), making it more environmentally friendly and allowing it to process more transactions per second than Bitcoin.

BNB Chain is a blockchain launched and managed by Binance, the world's largest cryptocurrency exchange. It's similar to Ethereum, but uses a consensus mechanism known as Proof of Staked Authority (PoSA) that allows for lower fees and greater scalability, but with more stringent control over who can participate in staking and validating transactions. Like Ethereum, BNB has smart contract functionality that supports its own DeFi and NFT ecosystem. Perhaps BNB's greatest attribute is its association with Binance, which gives it an enormous built-in user base.

Bitcoin, Ethereum, and BNB have all managed to grow and attract millions of users precisely because they're *not* interchangeable. Each one offers different benefits to both developers and end users, which stem from the choices made in how they were built, and particularly in their tradeoffs between decentralization, scalability, and security.

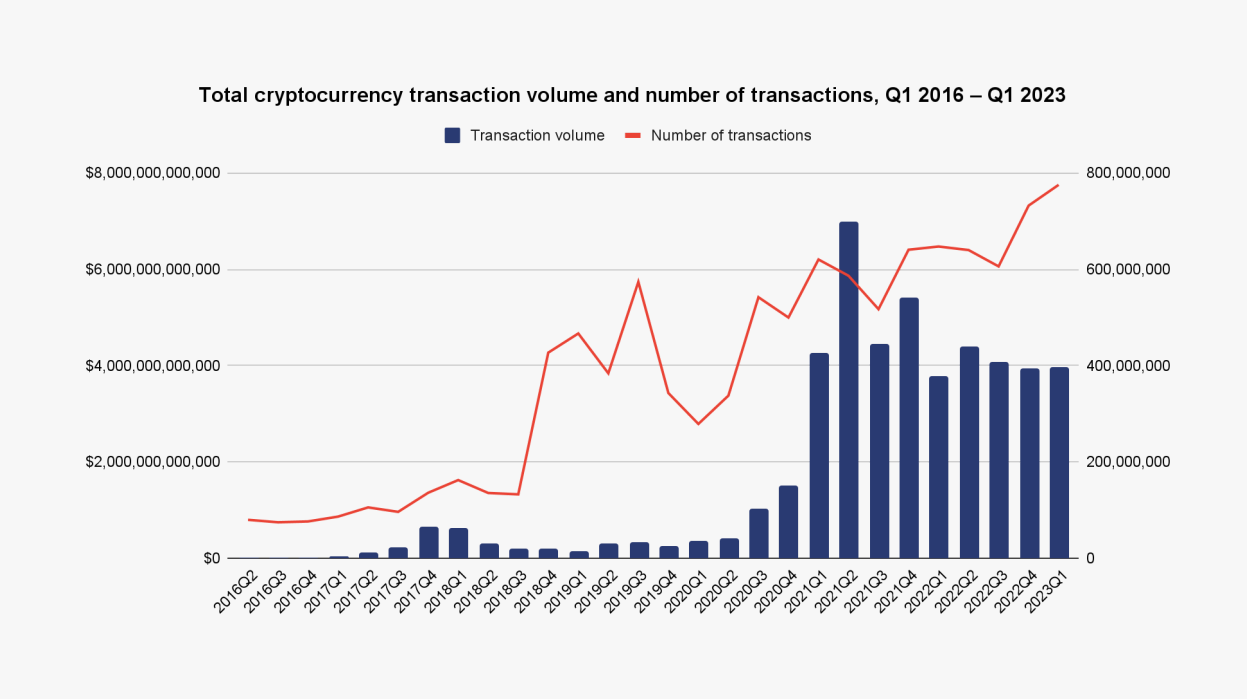
Viability

MYTH 18

Crypto is a fad.

Fifteen years after Satoshi Nakamoto's Bitcoin whitepaper, digital currencies have exploded from the concept of a single digital asset to a thriving ecosystem with a global market cap of $1.18 trillion. Additionally, governments are now implementing or investigating the feasibility of blockchain-based central bank digital currencies (CBDCs), as well as providing regulatory clarity for existing cryptocurrency. Of 45 countries that the Atlantic Council studied, nearly three-quarters are in the process of making substantial changes to their regulatory framework for crypto.

While disruptive events dampened crypto market capitalization and usage in 2022, transaction volume is still much higher than it was in 2019 and 2020, and the raw number of transactions happening is higher than ever. In other words, crypto usage is still rising even if transaction values aren't as high.



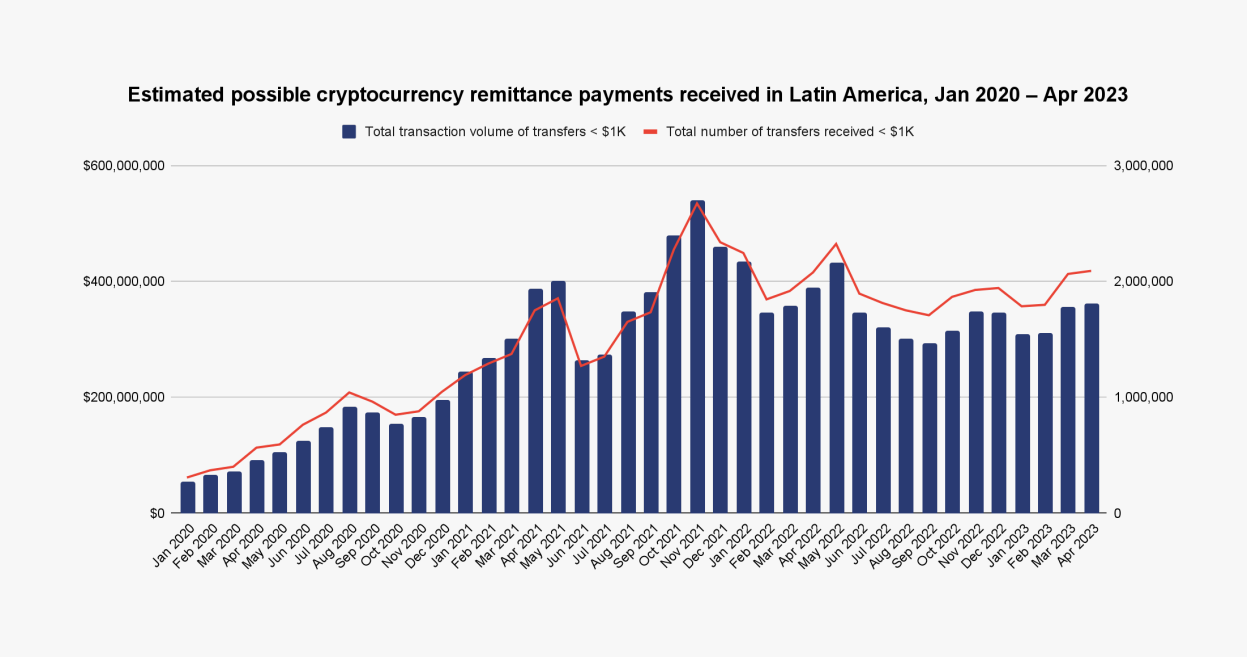
MYTH 19

Investing in crypto is gambling.

There's no denying that speculation drives at least some of the usage of cryptocurrency we see today. But to characterize all of it as gambling denies the existence of other, more societally beneficial use cases we see today, particularly in emerging markets. These include:

- Protection against the effects of currency devaluation
- Use for day-to-day transactions where payment rails are inefficient
- Faster, cheaper cross-border transactions, such as remittances and international purchases

Latin America, for instance, which has a large and growing remittance market, has seen a steady increase in estimated remittance payments received via crypto, based on our analysis of cryptocurrency payments under $1,000 to users in the region.



The "crypto as gambling" myth also closes the door on future innovation. Already, DeFi has shown that smart contracts can enable faster, simpler forms of lending. While most of that lending today is used to acquire other crypto assets, it's not hard to imagine a future where more conventional loans like mortgages can take place on-chain and remove friction from the present-day process. The tokenization of assets — most commonly seen today in the form of digital art through NFTs — also holds promise for simplifying and opening up the markets for mainstream asset classes.

MYTH 20

Crypto's volatility makes it too unreliable to be a store of value.

Many cryptocurrencies are indeed more volatile than many traditional assets. However, this isn't true in every case. We've seen in the past, for instance, that during periods of fiat currency volatility and devaluation, citizens of Colombia and Argentina have responded by acquiring Bitcoin and other cryptocurrencies in order to preserve their savings.

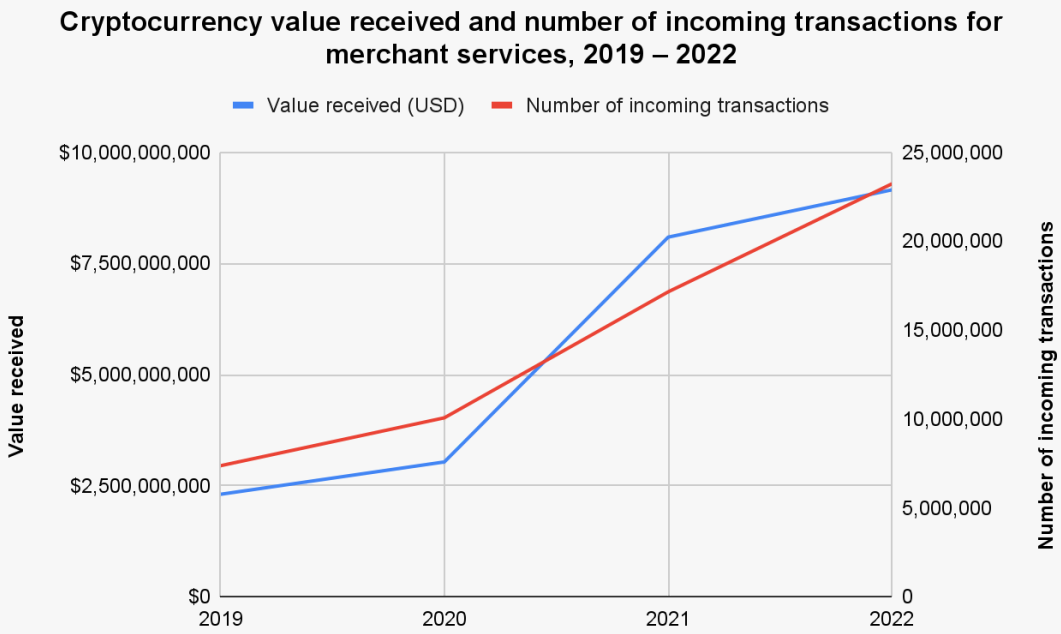
Plus, not all cryptocurrencies are volatile. There's an entire class of cryptocurrencies known as stablecoins that maintain a peg with fiat currencies — usually the U.S. dollar — by backing the stablecoin supply with an equal amount of actual fiat currency or short-term securities like treasury bills and commercial paper. Circle's U.S. Dollar Coin (USDC) and Tether (USDT) are popular examples. They too have become tools for saving and transacting in countries with inflation difficulties.

MYTH 21

Exchange rate volatility makes it impossible for merchants to set prices in crypto.

On the contrary, many merchants can and do set prices in cryptocurrency without having to worry about the volatility. How? As discussed earlier, stablecoins are one solution. Merchants who accept mainstream stablecoins like USDC and USDT are largely spared from any fluctuations in asset value.

But some businesses are even able to accept payments in more volatile cryptocurrencies thanks to innovative merchant services providers, which facilitate crypto payments for businesses while still allowing them to settle in cash.



BitPay is a great example. Merchants using BitPay can cater to the crypto crowd and accept payments even in relatively obscure currencies like Dogecoin or Shiba Inu, without actually being exposed to their volatility, as the payment processor allows for the currency to immediately be converted into cash upon completion of the sale. Merchants don't need to worry about setting prices in each individual cryptocurrency they want to support either. They can just set prices in their fiat currency of choice, and the payment processor handles conversion in real time.

MYTH 22

The principles of crypto are too complicated for consumers to understand.

First, purchasing and trading crypto doesn't require understanding the technology that supports it. After all, most people probably don't know exactly how the SWIFT system works, but no one would object to them making international bank transfers. Additionally, using a trusted service has made it easier than ever for novice investors to buy and sell crypto via secure, guided, and seamless user experiences.

As mentioned earlier, in 2022 we studied global cryptocurrency adoption and found some insightful trends that illustrate how consumers worldwide are embracing crypto. We found that emerging markets demonstrated high levels of grassroots cryptocurrency adoption, with countries like Vietnam and the Philippines leading the charge. It's also worth noting that Vietnam and the Philippines are among the top five countries with the largest unbanked populations. The prominence of crypto adoption in these regions indicates that digital currencies have the power to democratize finance and offer unbanked markets alternative methods of value exchange — far from being too complicated for consumers, crypto is in many cases the best or only option available for meeting basic financial needs those in developed markets take for granted.

Many cryptocurrency platforms have also led with education to onboard new users, thus demonstrating that the principles of cryptocurrency aren't too difficult for most consumers. Binance, for instance, has launched several initiatives to educate potential users in Africa on the benefits of cryptocurrency and how to use it — the success of those efforts shows that consumers are capable of learning crypto, especially when they see how it can improve their lives.

MYTH 23

The fact that there's a finite number of Bitcoin and that coins can be lost could cause a deflationary spiral.

Bitcoin was designed with a hard cap of 21 million coins in large part to avoid the inflation issues that have periodically arisen in fiat currency. No central body can increase the printing of Bitcoin, so there's less danger of an inflationary crisis in which Bitcoin's value drops precipitously. Bitcoin's value comes from the demand for Bitcoin — if that demand disappeared, inflation would be the least of Bitcoin's concerns.

However, some have worried that if Bitcoin were to achieve its goal of widespread usage as a currency and store of value, these characteristics could result in catastrophic deflation. This could lead to a decrease in transaction activity and hoarding of Bitcoin. If Bitcoin were to become truly mainstream, that could mean less economic activity, lower revenue for businesses accepting Bitcoin, and subsequently, wage deflation.

These concerns are a long way off given how nascent Bitcoin is, but there's good reason to believe that they could be easily mitigated. First and foremost, Bitcoin is highly divisible, as each unit of Bitcoin can be divided into 100 million satoshis. So, even if Bitcoin's value were to rise rapidly during a period of deflation, users could continue to make transactions in smaller and smaller fractions of Bitcoin. Secondly, deflation of Bitcoin could simply shift its use case more toward that of digital gold — an asset to be held as a value store rather than transacted with frequently — with other cryptocurrencies stepping in to handle everyday transactions. In that same vein, if necessary, Bitcoin's

developers could always fork the Bitcoin blockchain and create a new version of it with a higher supply. There's precedent for this: In 2017, Bitcoin developers forked Bitcoin due to disagreements over how to handle the increase in transaction fees as Bitcoin's usage exceeded its data storage capabilities. While the original Bitcoin blockchain remains much more popular, Bitcoin Cash still sees significant usage. Looking beyond the specific scenario of a deflationary crisis, the forking possibility highlights cryptocurrencies' general robustness and ability to adapt to changing conditions.

MYTH 24

Only seasoned investors should get involved with crypto.

Many people assume that crypto trading is highly complex, but it can be a small part of an ordinary investor portfolio. In fact, a 2022 NBC News poll revealed that one in five adults has invested in, traded, or used cryptocurrency. It's also worth noting that new asset classes are continually appearing and making their way into the average investor's portfolio. Cryptocurrency exchange-traded funds (ETFs) provide a prime example of what this could look like, as they would allow investors to get exposure to the asset class without having to hold them directly. As with any investment product, what is most important is for investors to have a good understanding of the features and risks of any product, so that they can make an informed decision.

MYTH 25

Crypto enables tax evaders.

There are no per se exemptions from tax for transactions involving virtual currency. In the US, for example, the IRS treats digital assets as property for income tax purposes — that includes (but isn't limited to) convertible virtual currency and cryptocurrency, stablecoins, and non-fungible tokens (NFTs). Investors must report crypto transactions on a tax return and a variety of transaction types may result in taxable gain or loss. Additionally, blockchain transparency and immutability make it difficult to hide transaction activity that can trigger tax events.

MYTH 26

Crypto can't integrate with traditional finance.

We've partnered with financial institutions across the world to help them assess opportunities and manage risk in cryptocurrency. Whether banks are dipping their toes in the water or debating DeFi, it doesn't need to be daunting. The Crypto Maturity Model we've discussed previously is a great place

for banks to start, and the key is determining the right types of products and services to add along the way.

Cryptocurrency's transparency makes the entire process easier. Using blockchain analysis tools, financial institutions can observe how data gets recorded on a public blockchain and how funds move between wallets and services. Aggregating this information will help them decide what crypto services to offer their customers. The final step? Hire crypto experts or partner with crypto-native businesses to create the new offerings.

In October 2022, America's oldest financial institution, BNY Mellon, became the first large bank to custody cryptocurrency. In a global survey BNY Mellon commissioned of institutional asset managers, asset owners, and hedge funds, it found that 88% of institutional investors were still moving ahead with plans to adopt digital assets despite crypto winter, and 72% were seeking providers to support these needs. The market is rife with opportunity for financial institutions willing to invest in cryptocurrency.

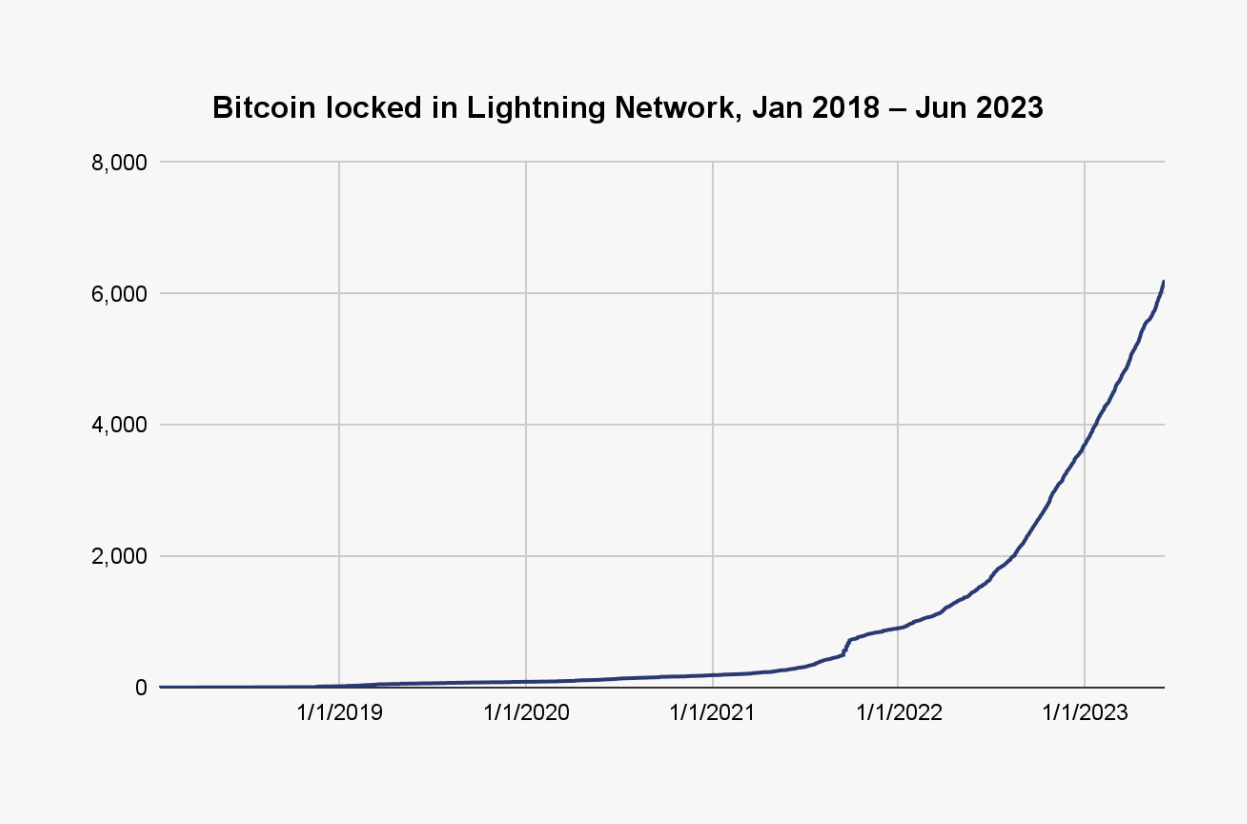
Additionally, some financial institutions are beginning to offer blockchain-supported products or provide integrations with crypto exchanges. For example, in 2020 JP Morgan launched Onyx, a platform that uses blockchain technology to facilitate exchange of value, information, and digital assets for the financial services industry. And since 2016, USAA Federal Savings Bank (FSB), has offered its account holders a Coinbase integration. USAA FSB customers can access their Coinbase accounts from USAA's website where they can view cryptocurrency balances and monitor transactions.

Scalability

MYTH 27

Blockchain doesn’t scale.

Many blockchains have run into issues of scalability, which essentially boil down to their ability to process transactions efficiently as their usage increases. Blockchains like Bitcoin, for example, can only process five to seven transactions per second — much fewer than fiat solutions — and in general when any blockchain becomes congested, transactions slow down and fees go up. However, there are solutions to these problems. In the case of Bitcoin, developers have come up with the Lightning Network, which allows users to lock Bitcoin into payment channels, make many small transactions off-chain, then settle them all at once on-chain later in one big transaction using the initial amount locked.



Similarly, Ethereum and other smart contract-enabled blockchains support layer 2 blockchains — these sit atop the primary blockchain but process transactions themselves, then record them later on the primary blockchain. Others have built entirely new blockchains specifically designed to solve the scalability problem, with varying degrees of success — Solana, Algorand, and Avalanche are three popular examples.

More generally, blockchain is still a young technology. If one believes it can improve on our current financial system and solve real world problems, it follows that incentives are there to attract innovators who can solve scalability problems.

MYTH 28

Blockchains have no business application.

While blockchains are most commonly used to facilitate value exchange, that's not where their usefulness ends. Considering that a blockchain is a permanent, secure, traceable database, the business applications are endless — supply chain management, data management, logistics, healthcare, media, stock trading, auditing, internet of things (IoT), and more. For instance, Sustainable Shrimp Partnership (SSP) is using IBM's Food Trust™ — a blockchain solution for supply chain intelligence — to ensure it produces shrimp sustainably. With tracking and tracing capabilities, SSP can also share information about its product's origins with retailers and customers.

MYTH 29

It's extremely difficult for banks to level up their crypto expertise in order to offer products.

We often hear that developing in-house cryptocurrency expertise is too time-consuming. The breadth of information on cryptocurrency is expansive and, understandably, intimidating. However, there are ways to learn about cryptocurrency that are faster than one might think. Banks contemplating cryptocurrency products or enabling crypto deposits can start by reviewing our Crypto Maturity Model mentioned earlier. It outlines the steps a bank can take to move from no crypto capabilities to provision of custodial services and beyond. Institutions just getting started should designate key stakeholders across multiple functions, as well as an executive, to lead the charge. Additionally, many educational resources are available, from content on the Chainalysis Academy to crypto's large community on social media and platforms like Discord.

MYTH 30

Banks need to see the provenance of every bitcoin.

In evaluating a service or wallet for compliance risk, banks must trace the origins of the cryptocurrency it's received in order to make sure it didn't come from an illicit source. It's critical to limit exposure to addresses tied to illicit activity.

However, there's virtually never any need to trace cryptocurrency back to when it was originally minted. Banks only need to trace cryptocurrency back to the service it most recently came from, because tracing cryptocurrency *through* services is impossible. Why? When cryptocurrency moves to a service such as an exchange, what happens to the cryptocurrency within that service can't be discerned on-chain. Though transactions are still recorded on the ledger, the service moves money around inside the exchange between its own internal addresses as needed, and funds originally deposited by many users are often co-mingled. Think of it like this: When you withdraw $20 from an ATM, you won't receive the same $20 bill you deposited a week ago, right? Of course not! Therefore, banks don't actually need to trace every bit of crypto they want to interact with to its ultimate source.

MYTH 31

There's no way to mitigate crypto's effects on the environment.

It's no secret that cryptocurrency mining – particularly Bitcoin mining — has significant environmental impact. Yet, as discussed earlier, not all crypto is mined in the same way. While Bitcoin's PoW consensus mechanism is quite energy intensive, PoS blockchains like Ethereum require much less.

Given the high energy costs associated with Bitcoin mining, miners are incentivized to seek more affordable, renewable energy sources. For example, one mining company, Marathon Digital, recently moved its operations from a coal-powered facility to one with more sustainable energy options like wind power. Many other miners are following suit. In Q4 2022, the Bitcoin Mining Council estimated that "renewable energy sources accounted for 58.9% of the electricity used to mine bitcoin, a significant improvement compared to 36.8% estimated in Q1 2021."

Leveraging stranded energy is another sustainable method for powering crypto mining operations. For example, when oil companies drill, they sometimes hit natural gas formations. Especially for oil rigs in remote locations, there's no way to effectively transport that natural gas to a populous location, so drillers burn it off in a process called flaring. Recognizing the environmental cost and missed economic opportunity that natural gas flares represent, the founders of Giga Energy engineered a creative solution — they installed generators at oil rigs that convert these flares into electricity. That energy then powers Bitcoin mining machines inside shipping containers also placed

at the oil-drilling site. This type of solution, when compared with flares not converted into energy, cuts CO2-equivalent emissions by roughly 63%.

Bitcoin miners are facilitating energy transition in other ways, too. Because mining isn't dependent on location, companies can set up operations anywhere in the world where power is cheap. Rural areas rely on hydroelectric power plants and often produce more power than is needed for their region. Crypto miners can operate in these locations and use the extra power these plants produce that otherwise can't be consumed. In some cases, Bitcoin mining can even shield hydroelectric companies from economic downturn, as was the case with a plant in Costa Rica. Because it had a surplus power supply during the pandemic, the Costa Rican government stopped buying electricity from a hydroelectric plant that had operated for 30 years. After suffering a 9-month shutdown, the plant began a Bitcoin mining operation using the excess energy it produced.

When it comes to sustainability, it's worth asking why cryptocurrency businesses are subject to so much scrutiny when more established industries with detrimental environmental impact don't face the same interrogation. To fairly judge the merits of any technology, society must balance its setbacks with the advancements it provides. That said, cryptocurrency offers more transparency than any financial system to date and blockchain technology continues to accelerate innovation and economic opportunity worldwide. These advantages must be considered.

What does the future hold for crypto?

MYTH 32

Crypto will replace fiat.

At Chainalysis, we believe that blockchain will revolutionize the exchange of value, much like the internet did for the exchange of information. We are building toward a future when all value is transferred on blockchains, and every company is a blockchain company. But even in that scenario, there would still be a place for fiat currency. Governments still need the ability to exercise some control over their economies and money supplies. Fiat currency is the primary tool for them to do this, and there are plenty of examples of governments enacting successful monetary policies that have improved citizens' lives. Secondly, as a form of legal tender, fiat currency has special standing. Businesses *must* accept fiat currency for all debts public and private, but can choose whether or not to accept crypto — that probably won't change any time soon (unless you count CBDCs). And finally, we have to consider culture and psychology. People have been using fiat currency for centuries, and many of them will never be convinced to give that up. Even the most ardent cryptocurrency enthusiast wouldn't say those people should be shut out from the financial system.

MYTH 33

Blockchain technology solves all problems.

When someone claims they've got the remedy for everything, you know you've entered the red flag zone. And while some enthusiasts go a *tad bit* overboard evangelizing crypto, we get it. At Chainalysis, we believe that blockchain technology can revolutionize so much more than just the financial system, which would be a big deal in its own right. It's hard **not** to get excited about that. So, where does crypto go from here?

Cryptocurrency adoption continues to grow — especially as governments prioritize regulation that makes consumers feel secure. As more financial institutions recognize that crypto can help their customers, they're coming up with innovative, revenue-driving products and initiatives to meet this demand. Lawmakers and government agencies are also analyzing how to best protect consumers and legislation continually evolves. In the meantime, there are proven ways to set yourself up for success when it comes to incorporating crypto into a broader strategy. You just need to move incrementally with the right tools and Chainalysis is here to help when you're ready.

Endnotes

1. Notes on our illicit transaction volume chart:

    - These are lower bound estimates that will likely rise over time as additional illicit activity is discovered.
    - This does not include off-chain criminal activity where proceeds may have been moved into crypto for laundering, though that activity can still be traced.
    - This does not include volumes associated with centralized services that collapsed in 2022, some of which are facing charges of fraud.

2. Similar to our previous statistic on crime as a percentage of all transaction volume, this data is also a lower bound estimate and will most likely grow as we identify new addresses associated with illicit activity.

Chainalysis

Building trust in blockchains

About Chainalysis

Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries. Our data powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Coatue, GIC, Paradigm, Ribbit, and other leading firms in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk. For more information, visit www.chainalysis.com.

FOR MORE INSIGHTS
blog.chainalysis.com

GET IN TOUCH
info@chainalysis.com

FOLLOW US ON TWITTER
@chainalysis

FOLLOW US ON LINKEDIN
linkedin.com/company/chainalysis