Crypto Crime Report

Decoding increasingly sophisticated hacks, darknet markets, and scams

January 2019

CHAINALYSIS

Table of Contents

Summary

Crypto crime increased in 2018, but it made up a smaller slice of a much larger market. Indeed, according to our analysis, illicit transactions comprised less than 1% of all economic bitcoin activity in 2018, down from 7% in 2012.

Even so, crime remains a significant problem in the cryptocurrency ecosystem. Exchange hacks have generated billions of dollars in criminal proceeds, darknet market activities have netted hundreds of millions of dollars in illicit revenues, and scams targeting individuals have stolen tens of millions of dollars. Moreover, criminal use of cryptocurrencies has become far more sophisticated. As a result, in this second edition of our Crypto Crime Report, we go deeper in our analysis to seek out granular insight into three categories of criminal activity.

For instance, we first look at hacks targeting cryptocurrency exchanges, not just in aggregate, but by tracing the movement of hacked funds from the scene of the crime to their exit points. Our analysis uncovers signature patterns in transaction activity in the months after a hack that may eventually assist in identifying and recovering hacked assets.

Then, we examine the surprising resilience of darknet markets as law enforcement takes aggressive action against them. In a report on the “whack-a-mole” problem with the darknet, we look at how transaction activity briefly subsides then quickly reroutes itself to new platforms when major darknet markets are closed down.

We also examine changing trends in Ethereum scams, where individuals are targeted, as last year’s phishing schemes lose their effectiveness and more complex Ponzi and ICO exit scams emerge to make outsized gains.

Finally, we discuss the role of cryptocurrency in the broader context of money laundering and highlight the importance of different types of services that are used to integrate illicit cryptocurrency into the clean economy.

Based on our analysis, we provide a summary of trends and developments that we believe will shape crypto crime activities—and crypto crime prevention—during the year to come.

Key Takeaways

Crime in the cryptocurrency ecosystem is incredibly diverse and fast-changing, with different types of illicit activities taking root in different cryptocurrencies. The most important trends for 2018 are listed below.

Decoding hacks sheds light on two prominent groups and their laundering strategies

The hacking of exchanges is far and away the most costly type of crypto crime, generating around $1 billion in hacking revenues in 2018 alone. We track the two prominent hacking groups responsible for a majority of these stolen funds. Hackers move fast, cashing out the majority of funds within three months of an attack, and create complex patterns of transactions to hide their activity. As other exchanges tend to be the main cash-out point, the industry can chip away at the success of these sophisticated hackers through greater coordination.

Darknet markets demonstrate resilience

After major closures in 2017, darknet market activity nearly doubled throughout 2018, with transaction volume surpassing $600 million, despite falling cryptocurrency prices.

Criminal organizations value the secrecy and convenience of darknet markets; they are not driven by price speculation. Efforts to shut down darknet markets have successfully curbed growth to some degree, although our analysis finds that much of the demand is merely displaced to other markets. Furthermore, sellers and buyers are developing new techniques to communicate, taking advantage of distributed technologies and encrypted messaging apps, such as Telegram and WhatsApp.

Ethereum scams are small in scale but evolving fast

While the absolute amount of revenue stolen by Ethereum scammers nearly doubled between 2017 and 2018, this represents less than 0.01% of all ether value. Furthermore, the cooling hype and more informed user base means that many of the attacks aren’t working as well in 2018 as they did in 2017. The number of scammed victims, as well as the total revenue sent to Ethereum phishing scams is rapidly declining, after a peak in early 2018. The success of phishing scams, in particular, is cyclical, moving with the price. So users should watch out for the more sophisticated ponzi schemes and ICO exits while prices are low, and be prepared for more phishing attacks should prices rise.

DECODING HACKS: Tracking $1 billion in hacked funds

Following the money of two prominent hacking groups

Hacks occur when an individual or group maliciously gains access to computing systems, making it possible to steal money. Some hackers target individuals by sending a phishing email that gives a criminal access to their phone and personal credentials. We'll focus on these types of attacks in the later section on Ethereum scams.

In this section, we focus on hacks that target cryptocurrency organizations such as exchanges. These hacks involve large thefts, often stealing tens or even hundreds of millions of dollars directly from exchanges. Hacking dwarfs all other forms of crypto crime, and it is dominated by two prominent, professional hacking groups. Together, these two groups are responsible for stealing around $1 billion to date, at least 60% of all publicly reported hacks. And given the potential rewards, there's no question hacking will continue; it is the most lucrative of all crypto crimes.

While several surveys have emerged that try to quantify the scale of hacking, no one has yet peeled back the surface to see how hackers cash out. At Chainalysis, we seek to "decode" hacking, that is to gain insight into how and when hackers move assets after the initial crime, how long it takes them to cash out via an exchange, and whether this teaches us anything about who they are.

Understanding how hacked funds move through the cryptocurrency ecosystem is the first step towards figuring out how hacking works and, potentially, identifying hackers and recovering hacked assets. Here is what we found.

> *We seek to "decode" hacking, that is to gain insight into how and when hackers move assets after the initial crime.*

How hacked funds move through the cryptocurrency ecosystem

The hacks we traced from the two prominent hacking groups stole an average of $90 million per hack. The hackers typically move stolen funds through a complex array of wallets and exchanges in an attempt to disguise the funds' criminal origins. On average, the hackers move funds at least 5,000 times.

The hackers then often observe a quiet period of 40 or more days in which they don't move funds, waiting until interest in the theft has died down. Once they feel safe, they move quickly. At least 50% of the hacked funds are cashed out through some conversion service within 112 days, and 75% of the hacked funds have been cashed out within 168 days.

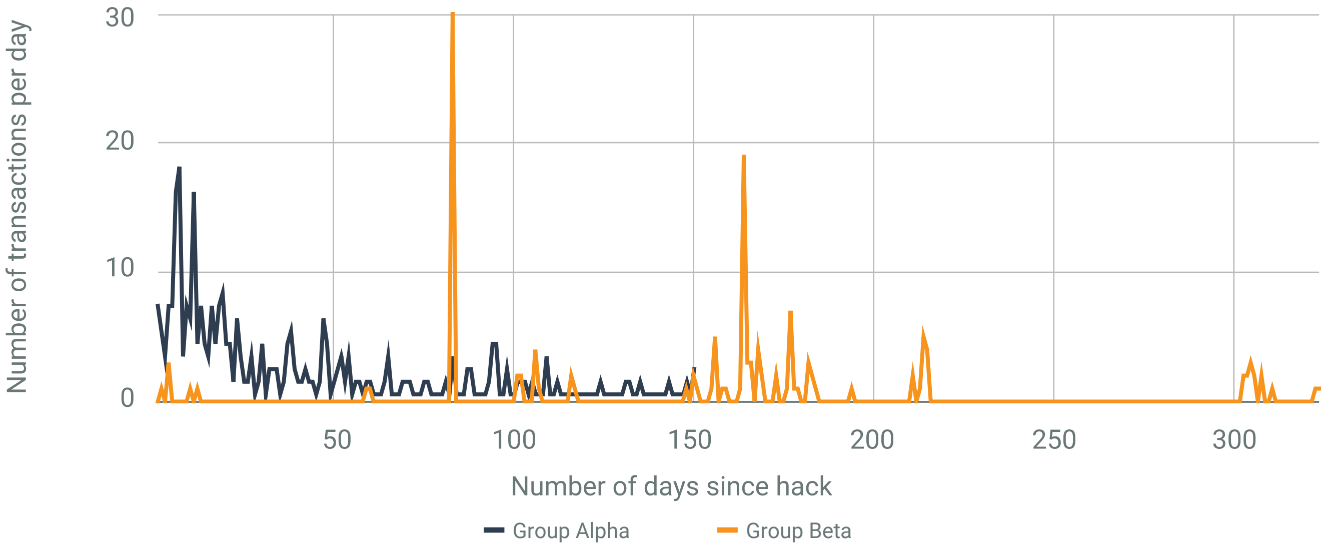
Both hacking groups seek to evade detection between the hack and their exit, but they use different approaches to achieve these ends. For example, we suspect that one of the prominent hacking groups, which we'll refer to as group Alpha, is a giant, tightly controlled organization partly driven by non-monetary goals. They appear as eager to create havoc as to maximize profits. Alpha seems much more sophisticated, expertly shuffling funds around in a way that suggests they want to avoid detection. By contrast the second hacking organization, group Beta, seems to be a less organized and smaller organization absolutely focused on the money. They don't appear to care very much about evading detection, just about getting a clear route to convert illicit assets to clean cash.

By studying these exit strategies, analysts may eventually be able to identify "fingerprint" styles that help catch hackers, though that capability is still in its preliminary stages.

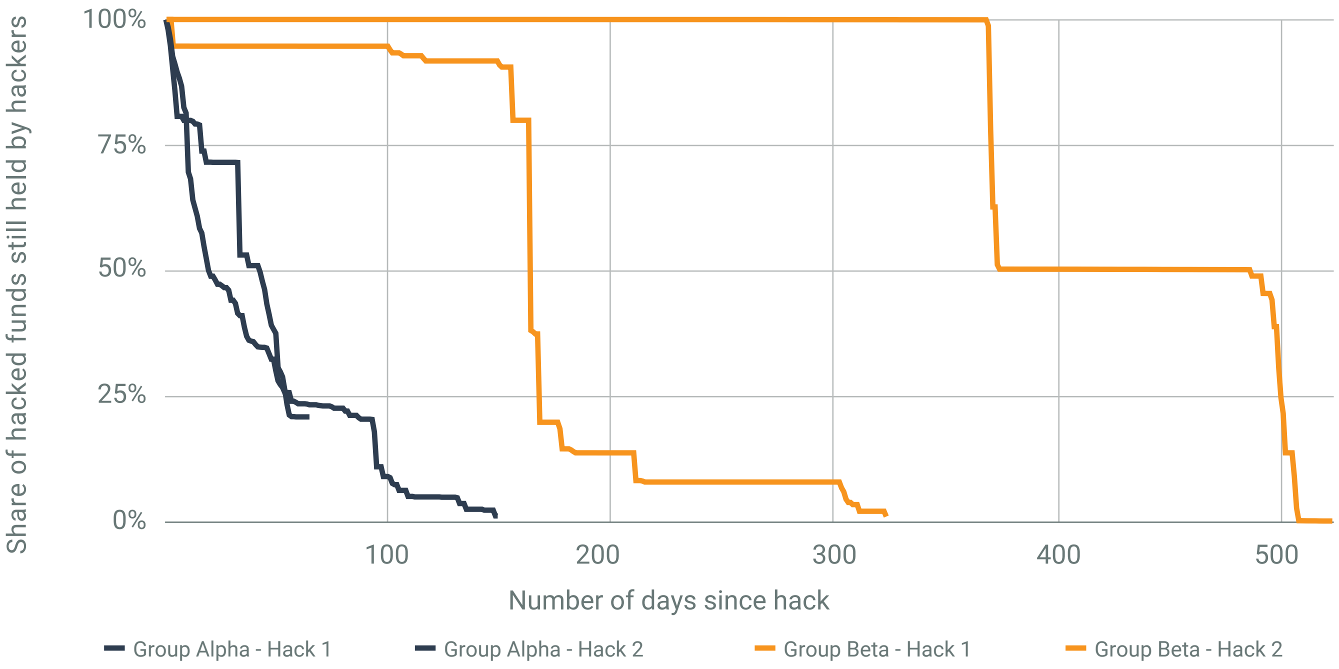
Transaction analysis shows that Alpha typically steals funds and immediately begins to shuffle them around rapidly. Alpha is skilled at moving money around, with an extremely high average number of transfers (up to 15,000 movements in one of the traced hacks). Alpha also moves relatively quickly, converting up to 75% of stolen assets to cash within 30 days.

The other prominent hacking group, Beta, bides its time but does far less to obscure the source of its assets. This group steals funds and then sits on those funds for 6 to 18 months before they cash out. And then, when they feel ready to cash out, they quickly hit one exchange, cashing out over 50% of funds within days, about $32 million in one instance.

Number of transactions per day after hacks



Share of hacked funds cashed out over time



Working together to contain the damage

Until now, exchanges and law enforcement have had limited ability to track hacked funds. Furthermore, exchanges are regularly processing the stolen funds, allowing the hackers to convert the funds to traditional currencies or other cryptocurrencies. From the four hacks analyzed in detail for this report, at least $135 million exited through known exchanges. This is in part because unless you're the exchange that was hacked, these funds look like they have come from legitimate owners (that is, the original entities who were hacked); it is hard to tell which funds have been stolen and which haven't without specialized investigation software.

A working knowledge of how hackers move funds can equip legitimate participants to identify unusual spikes in transactions that may be tied to criminal activity. Cooperation between exchanges also goes a long way to help fight crime in this ecosystem. Neutral intermediaries between exchanges can play an important role in this effort. For instance, one exchange recently experienced a hack, and our analysis indicated that the stolen funds had been moved to another exchange. We worked to verify that deposits made at the second exchange had originated from the hack of the first exchange, allowing them to engage with law enforcement.

Hacking is on the rise partly because it works. It is hard to defend against given the scale of the adversaries. So the stakes are high for exchanges and the cryptocurrency ecosystem more generally. However, decoding the hacks is the first step towards stopping them, and tracking and recovering funds through mutual cooperation may be the best defense.

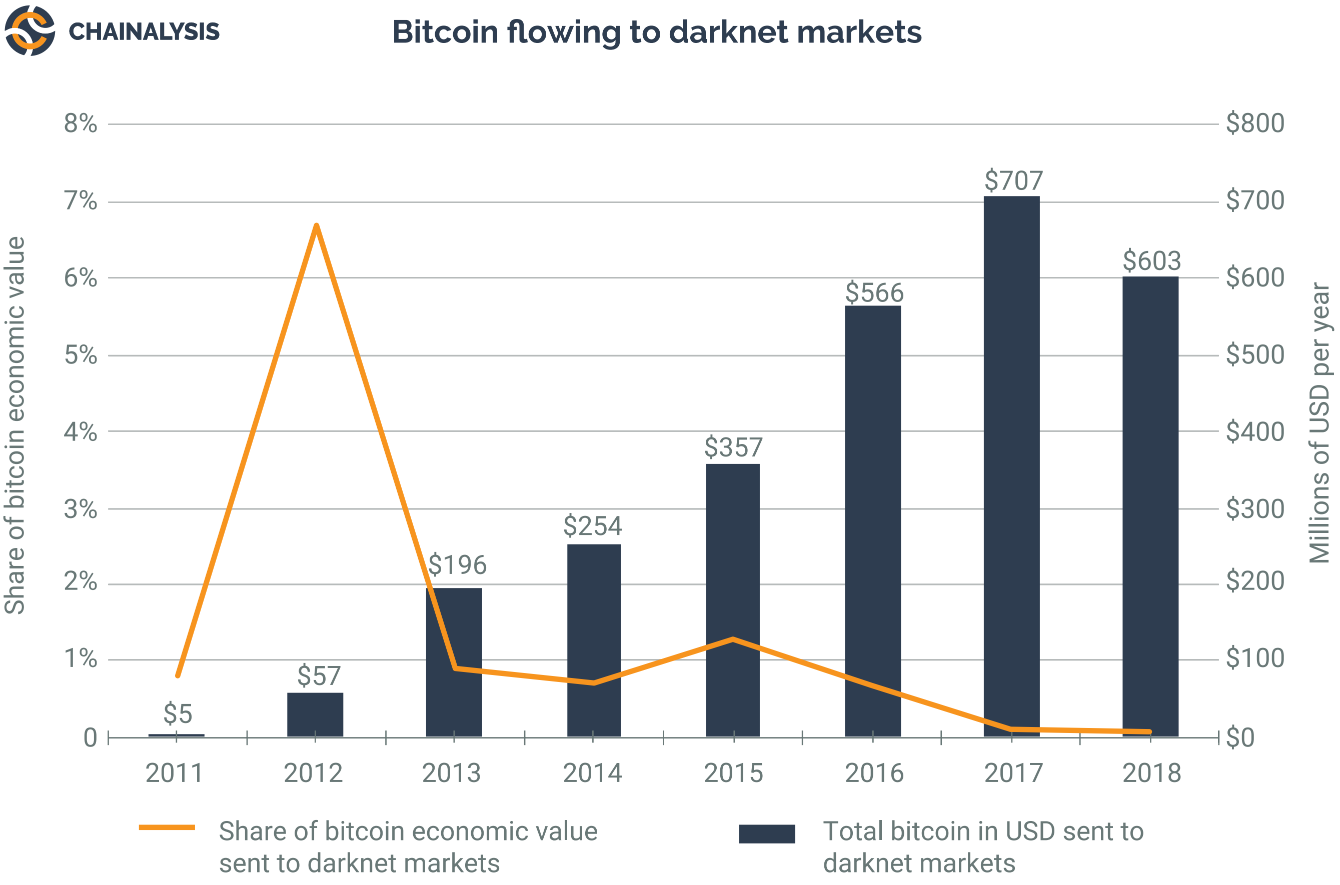
> “ *Cooperation between exchanges also goes a long way to help fight crime in this ecosystem. Neutral intermediaries between exchanges can play an important role in this effort.*

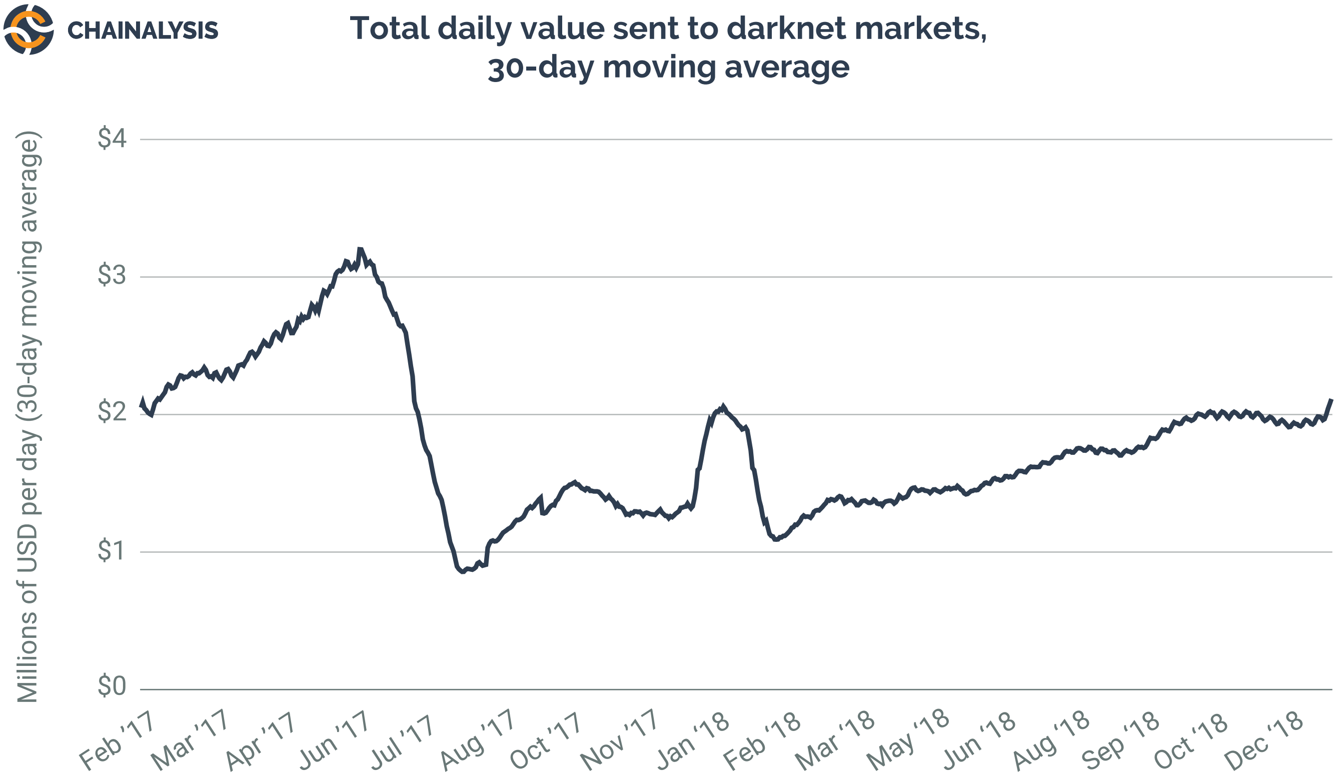
DECODING DARKNET MARKETS: Understanding their resilience

Playing whack-a-mole with darknet markets

Darknet market activity has been remarkably resilient over the last few years, despite continued efforts by law enforcement to shut down illicit activities. When one darknet market closes, others pop up to take its place. Even price movements have limited impact on darknet market participants, who use cryptocurrency to buy illicit goods rather than to speculate.

As the chart below shows, volumes going to identified darknet markets peaked in 2017, hitting over $700 million. Darknet market activity fell by 60% after AlphaBay and Hansa closed in mid-2017, but the slowdown was short-lived.



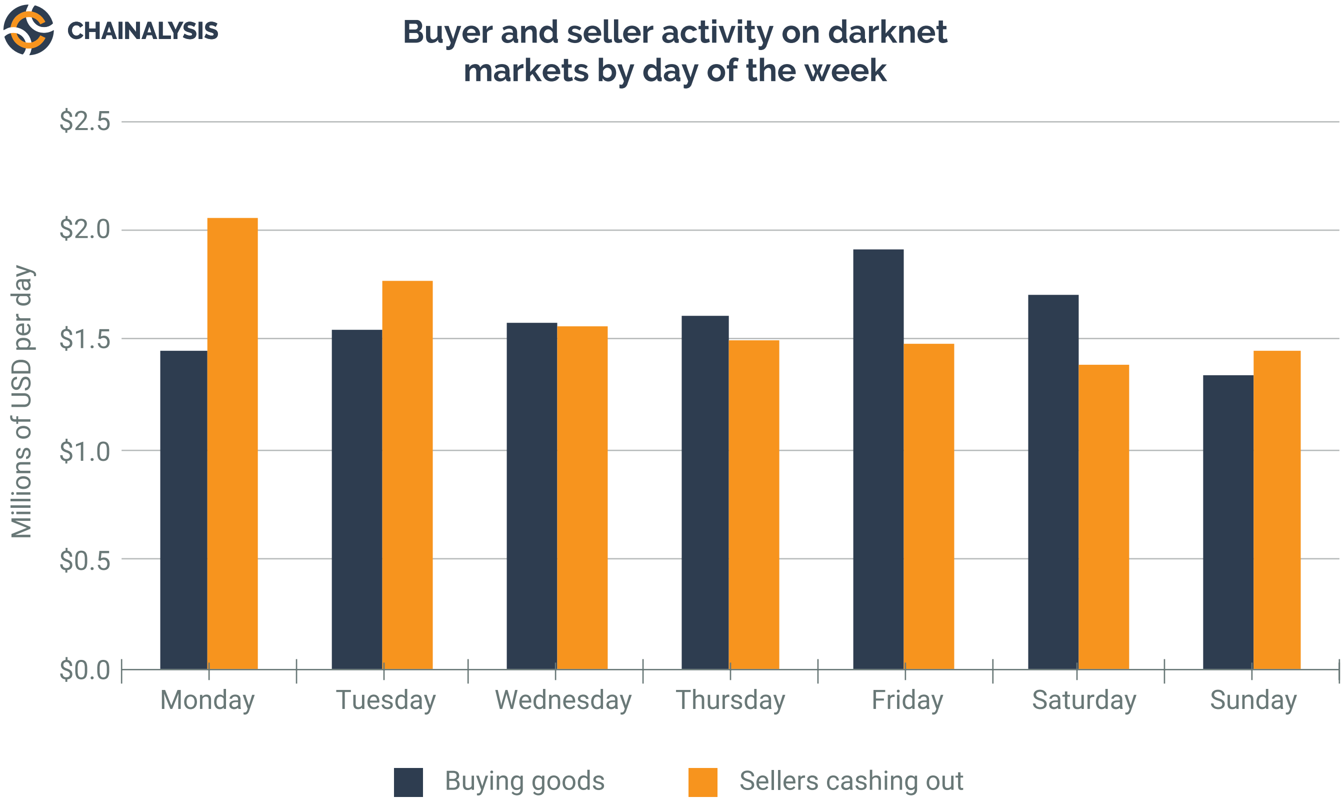


Today, activity flowing to darknet markets is back on the rise, averaging around $2 million worth of bitcoin alone every day. However, this still accounts for less than 1% of economic activity in bitcoin.

Much of the activity that once went to AlphaBay appears to have been redirected to Hydra, a Russian language darknet market that has to date received over $780 million in bitcoin, 14% more than AlphaBay's $690 million. We estimate the closure of AlphaBay could have doubled the flows to Hydra. This brings up a fundamental problem with darknet market activity: closing one darknet market often just leads people to use other platforms.

Price movements don't affect darknet flows

Darknet market activity is relatively price inelastic; that is, you don't see a drop in this type of activity when cryptocurrency prices fall. In fact, in 2018, when Bitcoin volumes dropped by 78%, darknet market activity nearly doubled.


Buyer and seller activity on darknet markets by day of the week

Flows to darknet markets are sensitive to days of the week, however. We see more bitcoin flowing to darknet markets on Fridays and Saturdays, and a spike in cash-outs on Monday. This pattern aligns with what we know about drug trafficking. Individuals purchase drugs at the beginning of the weekend when they have the time and privacy to browse—it's not like sneaking in an Amazon purchase at work!—then drug dealers convert cryptocurrency to cash on Monday.

Darknet markets are shifting and thriving despite law enforcement's best efforts

Law enforcement has been working hard to stop illicit activity on darknet markets, and there have been some notable successes like the closure of AlphaBay. Overall, these markets continue to thrive, however, as participants simply move their business to other platforms and technologies.

For instance, the closure of AlphaBay and Hansa drove a sharp decline in darknet market activity at the end of 2017, and this continued through February of 2018, when activity began to pick up again. Transaction volume has grown steadily since then. So while 2018 had, in aggregate, a lower level of darknet market activity than 2017, volume increased steadily, month by month throughout most of the year.

In fact, as law enforcement gets better at shutting down centralized darknet markets, a new distributed model for darknet market activity has emerged. Top law enforcement officials tell us that criminals are migrating increasingly to encrypted messaging apps including Telegram and WhatsApp to execute illegal transactions. When conducted through these apps, transaction activity is decentralized and person-to-person; there's little risk that law enforcement will shut down the entire network by closing a website. However, to transact via a message app, you have to trust the end user. Darknet market participants take on an additional layer of counterparty risk in this decentralized system.

Darknet markets continue to thrive regardless of cryptocurrency prices or choice of platform. The buying and selling of illicit goods via cryptocurrencies is, in many ways, similar to traditional illicit markets. Understanding the patterns among darknet market buyers and sellers is key for law enforcement to develop effective strategies to combat this type of illicit activity.

> “ *As law enforcement gets better at shutting down centralized darknet markets, a new distributed model for darknet market activity has emerged.*

DECODING ETHEREUM SCAMS: Small in scale but evolving fast

Fewer scams, bigger revenues: a radically changing landscape for Ethereum crime

In 2018, only 0.01%[1] of ether was stolen in scams, worth $36 million, double the $17 million take for 2017. This makes scamming on the Ethereum blockchain one of the lowest-earning types of crypto crime analyzed in this report for 2018. Furthermore, the number of scams declined through 2018, although those that remained were bigger, more sophisticated, and vastly more lucrative.

Why focus on Ethereum scams?

Ether has long been known as the cryptocurrency of choice for scams, for a variety of reasons. The Ethereum smart contract platform created a new phenomenon of decentralized investment via initial coin offerings (ICOs). People grew accustomed to parting with their ether coins in hopes of receiving outsized returns from these ICOs during the crypto hype of late 2017. Scammers took advantage of this new willingness—and of people's fear of missing out—by creating phishing scams involving fake investment pages into which people enter their personal details.

These types of scams are not inherent to Ethereum's smart contract functionality, but since 82%[2] of all ICOs are built on the Ethereum blockchain, it quickly became a go-to favorite for scammers. In addition to phishing scams, other common types of scams include ICO exit scams, hidden among the many genuine ICOs, and ponzi schemes.

[1] The numerator for this figure is from Chainalysis data, while denominator is from Coinmetrics

[2] Source: https://icowatchlist.com/statistics/blockchain

Types of Ethereum scams

Most scamming activity falls into one of three categories:

- **Phishing scams**

  These are the most common type of Ethereum scams. The target receives email or other communication that tricks them into sharing personal financial information that allows access to their Ethereum wallets.

- **Ponzi scams**

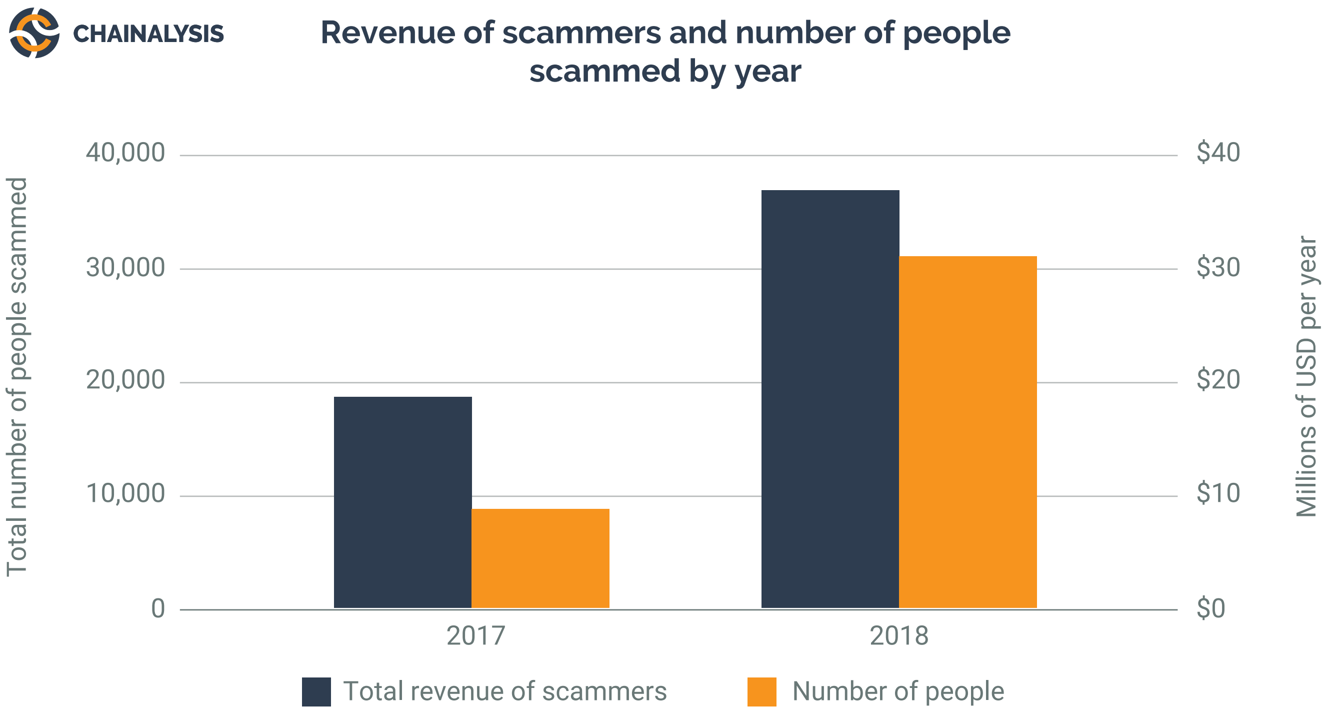
  Cryptocurrency ponzi schemes promise investors very high returns in exchange for an initial investment. Returns are paid out of new investment funds to attract additional investors until the scammers close up their scam and abscond with the proceeds.

- **ICO exit scams**

  In these types of scams, criminals set up fake companies, often with elaborate websites and collateral, then raise capital via unregulated initial coin offerings or ICOs. Once the ICO is completed, they intentionally cash in the proceeds and disappear, leaving funders with nothing to show for their investment.

The rise and fall of scamming activity

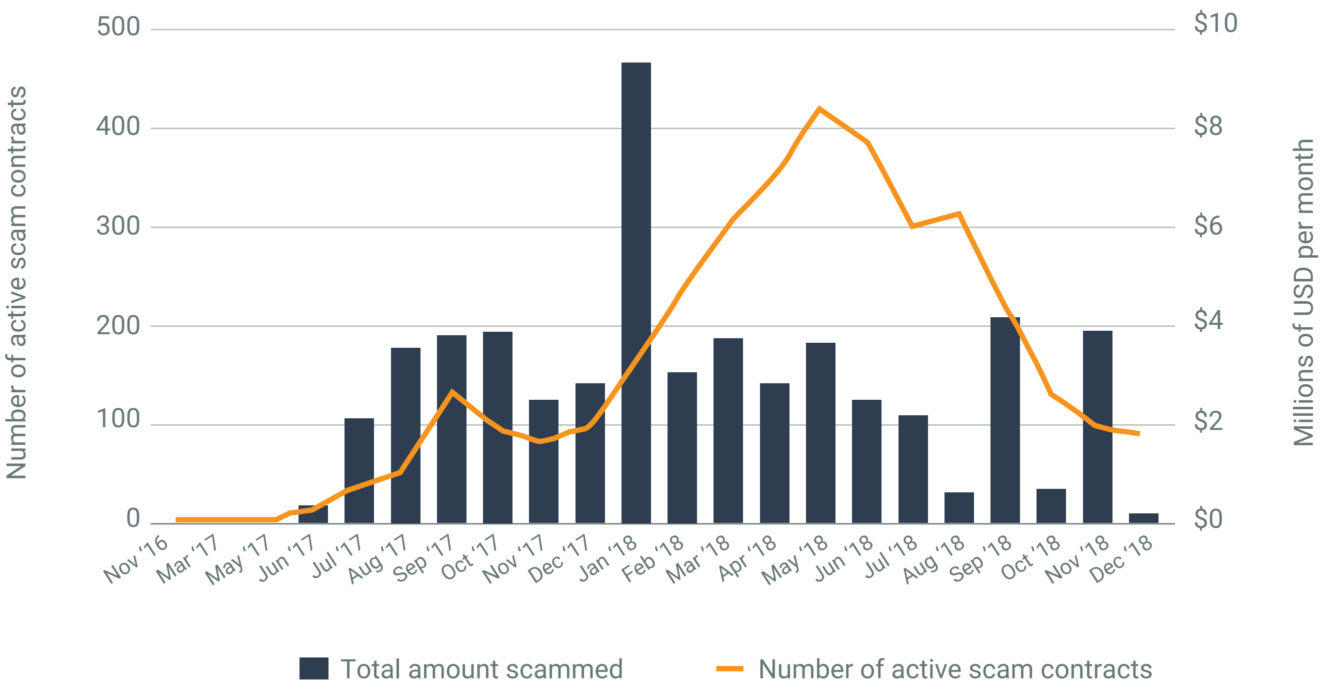
From late 2016 through the end of 2018, Chainalysis has identified over 2,000 scam addresses on Ethereum that have received funds from nearly 40,000 unique users. Scam activity increased dramatically in 2018. Of the total 40,000 users hit by Ethereum scams ever, nearly 75% were scammed in 2018. The number of people scammed increased four times from 2017 to 2018.



But the activity changed radically throughout the year. The first quarter of the year saw scamming activity spike, largely tied to the market hype of late 2017. In fact, nearly 45% of all scammed value occurred in the first quarter of 2018, as shown on the next chart.

CHAINALYSIS

Number of active scam contracts and total revenue per month



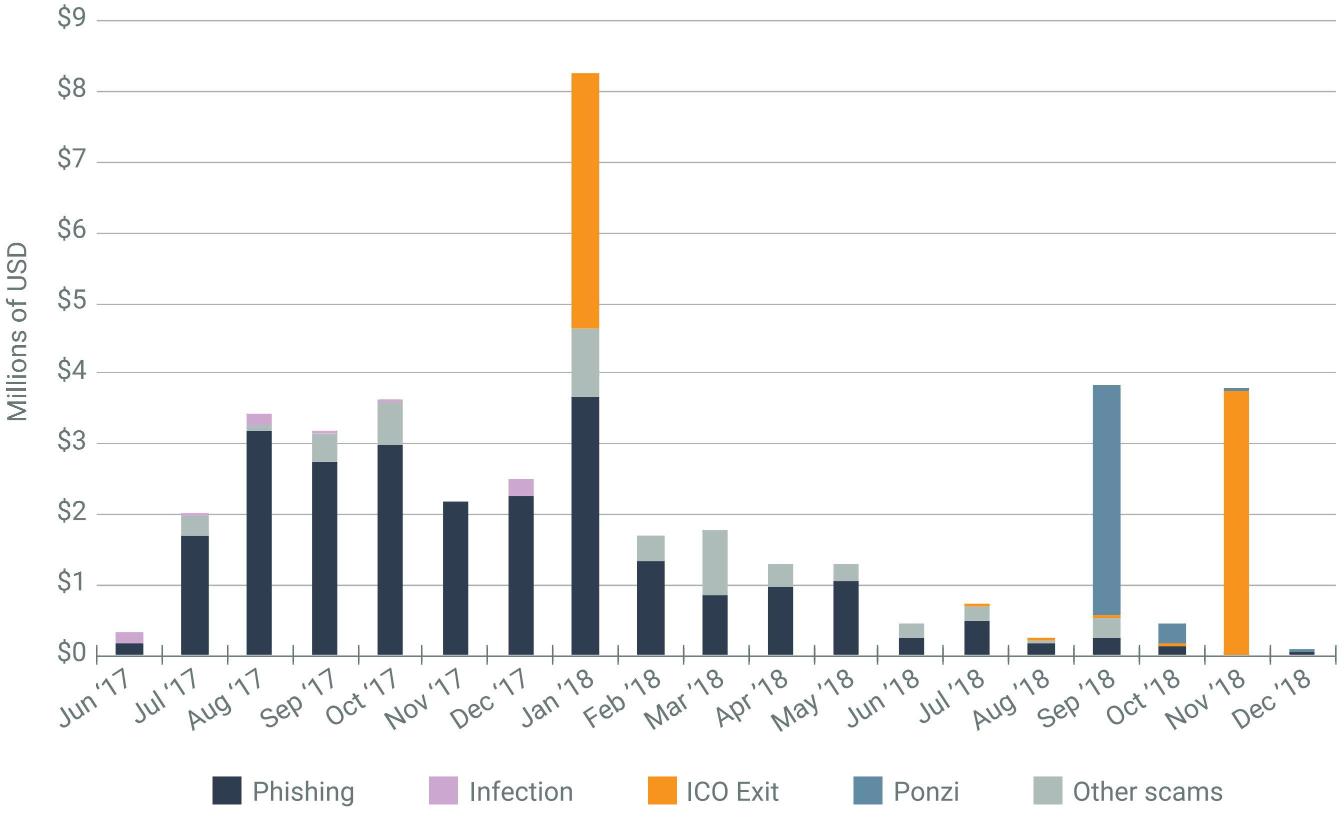
Understanding types of scams

Though phishing, ponzi schemes and ICO exits are the most common scam types, there are additional types of Ethereum scams, such as infection scams. The frequency and success rates of these types of scams has changed over time.

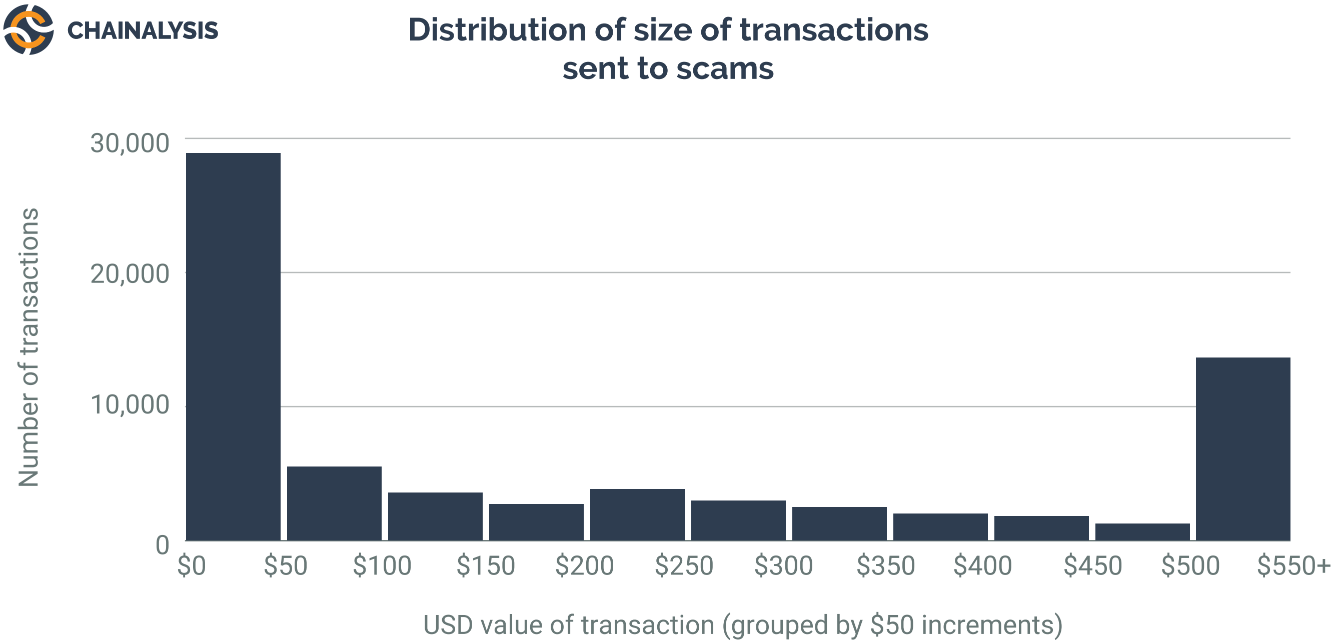
In 2018, scamming activity shifted in two ways. First, after the success of phishing scams in 2017, many more criminals jumped on the bandwagon. They saturated the market with phishing attacks, but fewer users took the hook.

CHAINALYSIS

200 most profitable Ethereum scams by type, 2017-2018



As a result, phishing scams were much less effective than in previous years. In 2018, the median amount sent to a scam was around $94, far less than 2017's median of $144. Furthermore, the median total revenue made by a scammer in 2017 was over $6,500, as opposed to $2,440 in 2018. In 2017, only 49 scams made less than $100, whereas in 2018, that number jumped to 181, of which 65 made less than $10. However, while most Ethereum scams were less lucrative, a few outliers brought in millions.



A smaller group of innovative criminals executed more complex ponzi and ICO exit scams that generated millions of dollars in income. These more sophisticated schemes dominated the second half of the year.

Protecting against changing threats

The good news is that although Ethereum has a reputation for scams, the amount reported stolen represents a very small portion. Moreover, scams decreased after the first quarter as prices dropped. The simplest scams like phishing emails were far less effective in 2018 than previous years.

However, on the negative side, criminals responded by getting creative, developing big, innovative, complex scams that paid huge dividends. Twice as many users lost four times as much in assets in 2018 relative to 2017, because of these outsized scams.

What to do? Users need to protect themselves against different types of scams as market conditions change, looking out for ponzi schemes when prices are low and becoming vigilant against phishing scams when prices are rising. In-depth data analysis can decode these changing threats and arm users with the knowledge to defend themselves.

UNDERSTANDING MONEY LAUNDERING

Understanding money laundering

The crimes analyzed in this report generate proceeds in the billions of dollars, which need to be laundered. Money laundering is hard to quantify, whether in traditional currencies or in cryptocurrency. That's because successful money laundering is essentially invisible; the whole point is to make criminal proceeds look like legitimate funds.

In traditional currencies, analysts can only estimate money laundering activity by working backward from successful prosecutions and making assumptions about how much of the total activity has been detected.

Estimation is also difficult in cryptocurrencies, though the transparency and completeness of cryptocurrency transaction data shows promise in tracking money laundering activity.

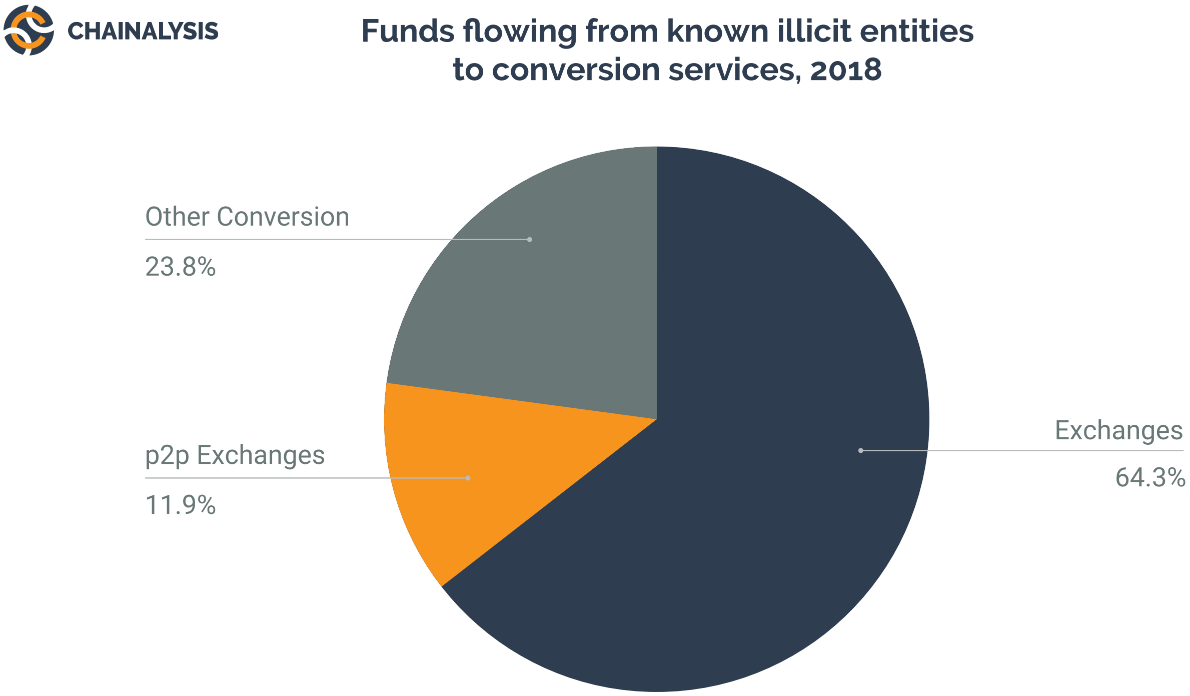
As in traditional currencies, money laundering in cryptocurrencies has three distinct phases:

Placement **Layering** **Integration**

Thus, a successful laundering scheme involves "placing" criminal funds into the financial system, moving them around or "layering" to avoid detection, and then "integrating" those funds into the real economy, usually through a business, to make them look like legitimate profit.

> *Successful money laundering is essentially invisible; the whole point is to make criminal proceeds look like legitimate funds.*

There are two types of software needed to aid in quantifying cryptocurrency money laundering. First, investigative software enables us to estimate funds flowing from illicit entities to conversion services where they can be integrated into the wider economy. A majority of illicit funds actually flow through either exchanges (65%) or peer-to-peer exchanges (12%), with the rest flowing through other conversion services such as mixing services, bitcoin ATM's and gambling sites.



Of course, this analysis only captures part of the problem. A significant amount of criminal activity originates off the blockchain—for instance, when drug cartels use cryptocurrencies to make cross-border payments. To investigate this form of money laundering would require anomaly detection software, the second of the necessary software mentioned. This software flags unusual activity that looks like "layering," for instance spikes in the frequency and size of transactions.

The role of cryptocurrencies in money laundering will continue to evolve as the legal and regulatory environment shifts. However, the greater traceability of cryptocurrency, paired with increasing know-your-customer (KYC) requirements across the cryptocurrency ecosystem means it is not a game-changing new way to launder funds for large criminal organizations. Still, the use of cryptocurrency by smaller players such as local drug dealers is a concern for law enforcement, who will continue to prosecute these crimes.

LOOKING AHEAD TO 2019

Looking ahead to 2019

The price bubble of late 2017 and early 2018 is over, and with it many of the scams devised to take advantage of investment hype, such as phishing scams and ICO exits. Because law enforcement takes time, we will continue to see prosecutions of these types of crimes. However, we believe illicit activity in 2019 will shift away from hype-driven investment fraud and towards the following emerging trends:

▶ A new era of distributed crime

We believe 2019 will be the year of distributed crime, where criminal activity is shifting to new decentralized platforms. This is a major issue for law enforcement. Criminal organizations will shift away from darknet markets towards encrypted apps including Telegram, Signal, and WhatsApp. Telegram, for example, could be attractive to criminals because it offers semi-direct connections and automated chat bots. Some of these distributed apps already have channels for drug traffickers and child pornographers.

▶ Traditional criminals add cryptocurrencies to their toolbox

Cryptocurrency crime is evolving to become part of traditional crime, and we think this trend will continue in 2019. Already many traditional crime organizations use virtual currencies, including bitcoin, to support their businesses. Criminal organizations are bringing in virtual currency experts to advise them on integrating cryptocurrency into fraud, money laundering, and illegal gambling activities. Cartels and other criminal groups are taking over exchanges and bitcoin miners as a source for clean money. These groups are exploring traditional cryptocurrency scams and inventing new ones, and they present a growing challenge for law enforcement.

▶ Giving sanctions back their bite

And finally, we believe that 2019 will force a reckoning with the role that cryptocurrencies play in evading sanctions. Governments will be seeking ways to limit rogue states, state-sponsored hacking groups, and sanctioned officials in their ability to move funds via cryptocurrencies.

Against this backdrop, cryptocurrency networks will continue to grow and evolve. They will likely be more regulated than they are now, providing additional assurances to attract law-abiding investors. Criminals will continue to push the envelope, finding applications for cryptocurrency in everything from street crimes to cyber crimes. Cryptocurrency market participants will need cutting edge technology and investigative analysis to fight back.

RECOMMENDATIONS

What institutional participants can do about crypto crime

Crypto crime represents a small portion of transaction activity, but gives the cryptocurrency ecosystem a bad name. Here are some ways that institutional participants, including businesses, regulators, and law enforcement, can improve the system and make it work for everyone.

Enable Know Your Transaction (KYT) capabilities to identify illicit activity

In the traditional financial system, Know Your Customer (KYC) is the foundation for compliance. It's also becoming the standard in the cryptocurrency ecosystem. We see an opportunity to go beyond this—to Know Your Transaction (KYT).

KYT means cryptocurrency businesses and financial institutions can be informed about illicit activity so they can avoid getting involved in transactions that could harm them or their customers. Automated cryptocurrency transaction monitoring is key to identifying patterns that indicate trouble spots and empower market participants to take action.

Understand the differences between types of crime

Crypto crime trends constantly shift, and so should compliance strategies. For instance, a compliance manager at a cryptocurrency payment processor who knows that darknet market activities increase on Mondays, when drug dealers convert weekend revenue to cash, can adjust their transaction monitoring system to account for this at the beginning of the week. A compliance officer at a cryptocurrency exchange who knows that hackers can take 45 or more days to cash out stolen funds can be alert to large, suspicious bursts of transactions that may be tied to hacks. Trusted experts in the market, like Chainalysis, can help in decoding illicit activity so that companies and exchanges can shape their compliance programs accordingly.

Work with the community to weed out major criminal organizations

Illicit activity in the cryptocurrency ecosystem isn't as common as many people think, but unfortunately, a small number of bad actors has given the space a bad reputation. By sharing information and working together, businesses and financial institutions can make it harder for criminal organizations to operate.

Law enforcement, exchanges, and merchant services are in a unique position to collaborate in identifying criminals as they steal funds and move them around. Where necessary, companies like Chainalysis can serve as an intermediary, linking market participants in a safe, neutral way, so that they can share insights that benefit all. By communicating quickly and across exchanges and other institutions whenever funds are stolen, cryptocurrency businesses can protect themselves and their customers. This ultimately makes the entire ecosystem more approachable and safer for all.

Chainalysis offers cryptocurrency investigation and compliance solutions to global law enforcement agencies, regulators, and businesses as they work together to fight illicit cryptocurrency activity. Backed by Benchmark and other leading names in venture capital, Chainalysis builds trust in blockchains. For more information, visit www.chainalysis.com.

GET IN TOUCH:
info@chainalysis.com

For more content, or to subscribe to receive future reports, visit blog.chainalysis.com.

This document is not intended as legal advice. We recommend you consult your general counsel, chief compliance officer, and/or own compliance policies & procedures for regulatory, legal or compliance-related questions.

CHAINALYSIS