GRC World Forums

Chainalysis

Crypto-crime

An introduction to ransomware, darknet markets, money laundering and related illicit activities defining the crypto- crime landscape today.

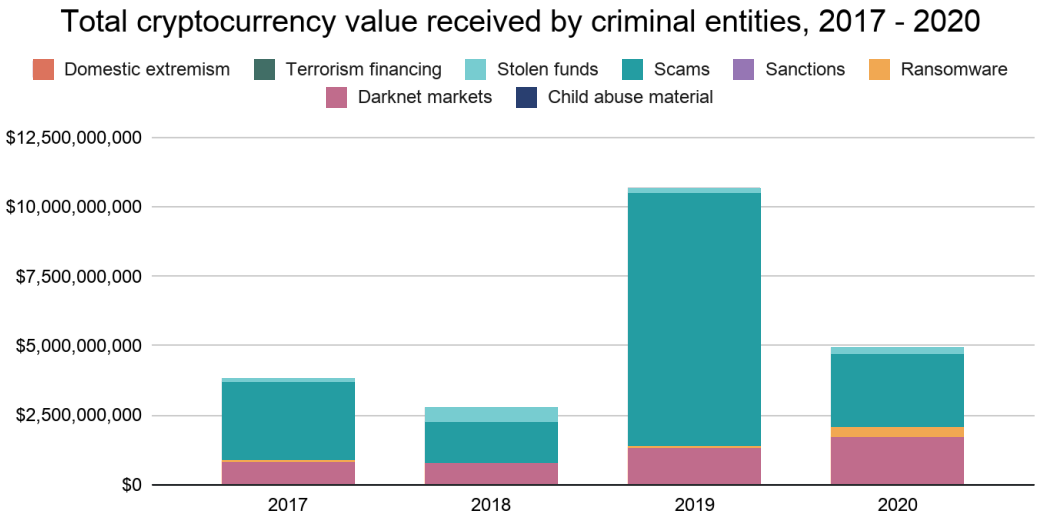
Contents

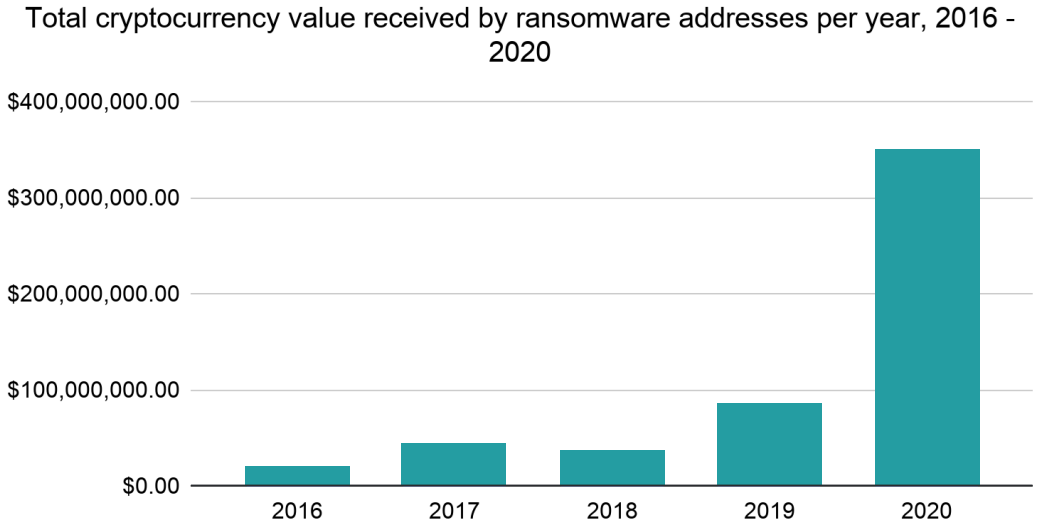
Introduction

Amid the global devastation wrought by the COVD-19 pandemic, 2020 was a transformative year for cryptocurrency.

Nowhere was this shift shown more observable than in the performance of Bitcoin.

Bitcoin shattered previous price records, largely due to increased demand from institutional investors that many in the crypto-community long speculated would drive the digital asset to new value heights.

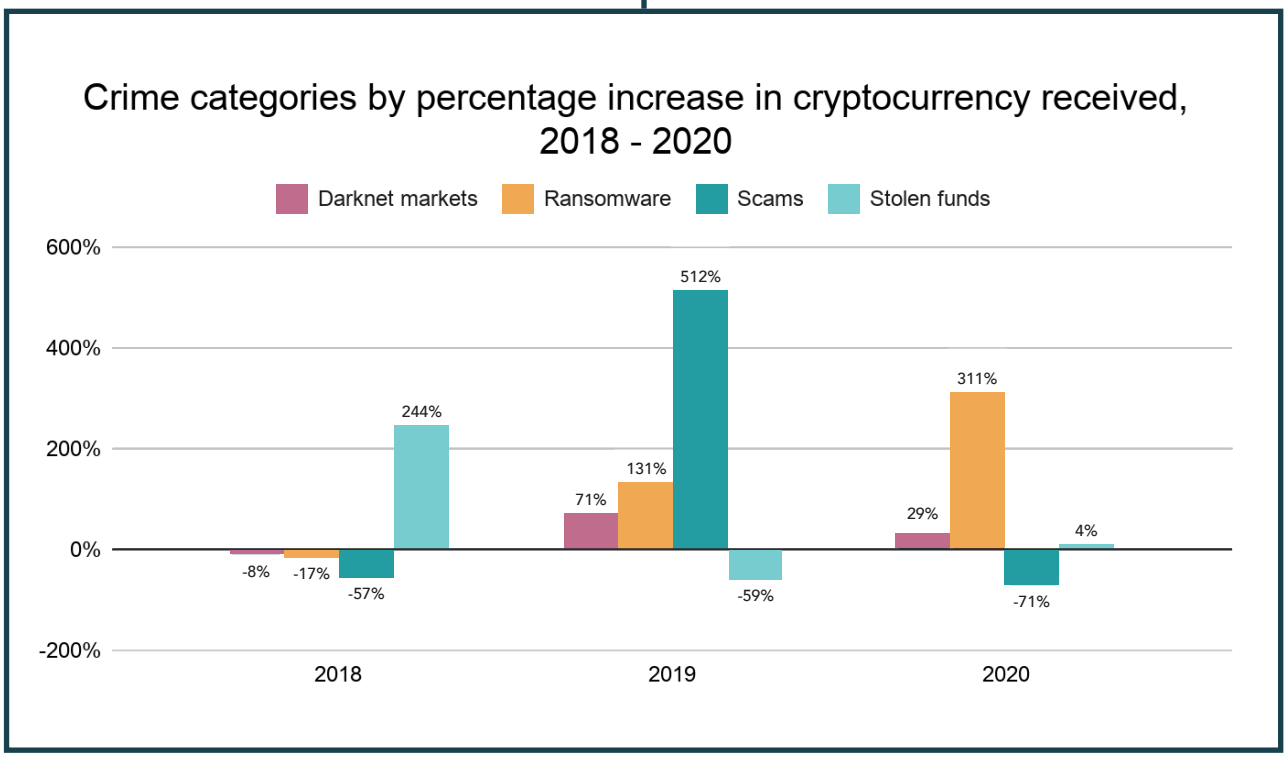




For the criminal world, the pseudonymous nature of cryptocurrency makes it highly appealing for criminals, who can use it to instantly send funds to and from any location in the world.

However, the good news is that cryptocurrency-related crime actually dropped significantly through last year.

Crypto-crime overview



In 2019, criminal activity was responsible for 2.1% of all cryptocurrency transactions that took place, equating to around $21.4 billion.

This figure dropped to $10 billion in 2020, a fall that saw the criminals' market share of cryptocurrency reduce to just 0.34%.

Most of this 0.34% was taken up by scams and darknet market activity, but the growth of ransomware grabbed the headlines, with ransomware payments quadrupling through 2020 to reach almost $350 million in cryptocurrency value.

Generally, cryptocurrency-based crime fell by 54% through 2020, but the year was significant for digital money platforms as a deluge of institutional investment drove Bitcoin and other crypto assets to record levels.

It's important to remember that these numbers are conservative, as underreporting means the true totals may be considerably greater.

Criminals are attracted to the use of cryptocurrency thanks to its pseudonymous nature, whichallows transactions to be made under deep cover instantly anywhere in the world.

Other trends in cryptocurrency-based crime:

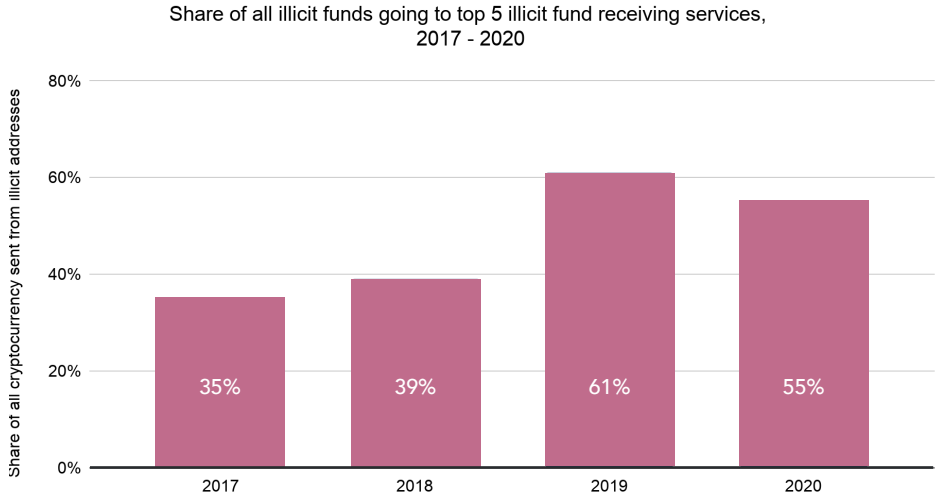
- How a small group of shady cryptocurrency services, mostly operating on top of large exchanges, conduct most of the money laundering that cybercriminals rely on to make cryptocurrency-based crime profitable.
- Decentralized Finance (DeFi) platforms' unique vulnerability to hacking, as well as how cybercriminals such as those of the North Korea-affiliated Lazarus Group utilize DeFi platforms for money laundering.
- A rash of darknet market closures as competition heats up in the space.

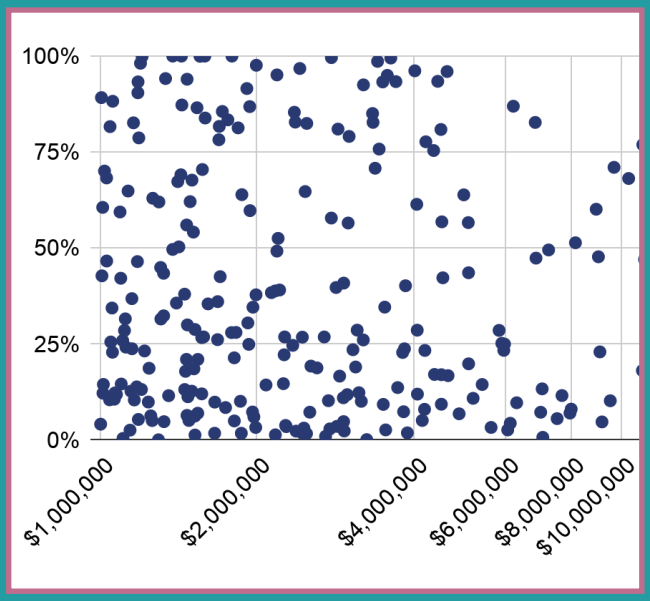
Money laundering: the key to crypto-crime

Cybercriminals can't simply send their ill-gotten cryptocurrency to an exchange and cash out as a normal user would.

Instead, they rely on a small group of service providers to liquidate their crypto assets. Some of these providers specialize in money laundering services while others are simply large cryptocurrency services and money services businesses (MSBs) with lax compliance programs. Investigators could significantly damage cybercriminals' ability to convert cryptocurrency into cash by going after these money laundering service providers, thereby reducing the incentives to use cryptocurrency in the first place.

Money laundering through cryptocurrency is concentrated, with over half (55%) of illicit funds being channelled to just 270 service deposit addresses. This being said, the ecosystem is modest and is driven by a small number of financial criminals.



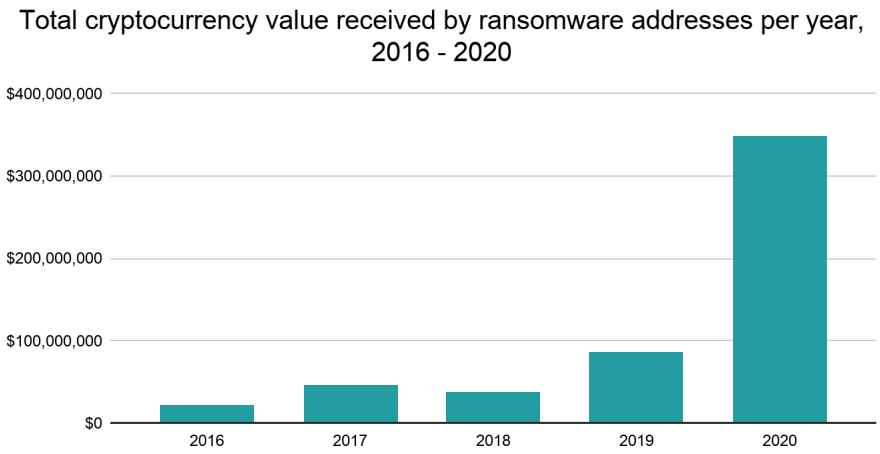


At deposit address level, activity becomes even more concentrated: in 2020, three quarters of cryptocurrency value sent from illicit addresses was received by just 1,867 deposit addresses. Of those addresses, just 270 received 55% of that value, equating to over $1.3 billion USD.

Many of those 270 deposit addresses also receive a high volume of funds from legitimate sources. In other words, the funds they take from illicit sources accounts for a small portion of the addresses' overall usage.

Most of the deposit addresses facilitating money laundering belong to nested services operating at large exchanges. By going after the worst of these nested services, law enforcement and cryptocurrency compliance teams can make it much harder to launder illicit cryptocurrency and strike a blow against cybercrime.

Ransomware



The past 18 months has seen ransomware value mushrooming, with victims' payments going up by 300% to almost $350 million from 2019's figure of under $100 million. No other category of crypto-crime had a higher growth rate.

Working from home has been an accelerator to this trend, with a number of new strains taking in large sums from victims, as well as pre-existing strains dramatically increasing their earnings.

Over $10 million was taken from victims by seven strains of ransomware, but once again, these totals are expected to be lower than the actual totals owing to the likelihood of underreporting.

2020's Top Ransomware Strains by Victim Payments

Strain	Victim payments received, 2020 (USD)
Ryuk	$95,993,674.13
Maze	$44,396,613.55
Doppelpaymer	$41,166,752.92
NetWalker	$30,017,195.26
Sodinokibi	$25,147,191.35
Conti	$20,985,731.09
Snatch	$11,450,845.63

analysts suggest the ransomware ecosystem is small. While the many active strains of ransomware have claimed huge amounts from their victims, it is believed that it's just a small group of cybercriminals behind the large part of scams.

Most ransomware attacks are carried out by independent affiliates that "rent" access to individual strains instead of building ransomware. Affiliates receive the majority of ill-gotten gains from successful attacks, but pay a cut to the strains' administrators.

Throughout 2020, we have seen several instances of this being executed. Again, the appearance is that the attacks are being orchestrated by separate criminal organizations, when in fact, a small group of criminals are the real perpetrators.

Similarly, the ransomware attackers are being assisted by the services of a small cell of money laundering services. Around 80% of all funds sent from ransomware addresses went to just 199 service deposit addresses.

The pattern repeats itself: ransomware is not a robust ecosystem of several competing organized entities, rather it is being driven by a much smaller group of individual cybercriminals.

Sanctions in ransomware

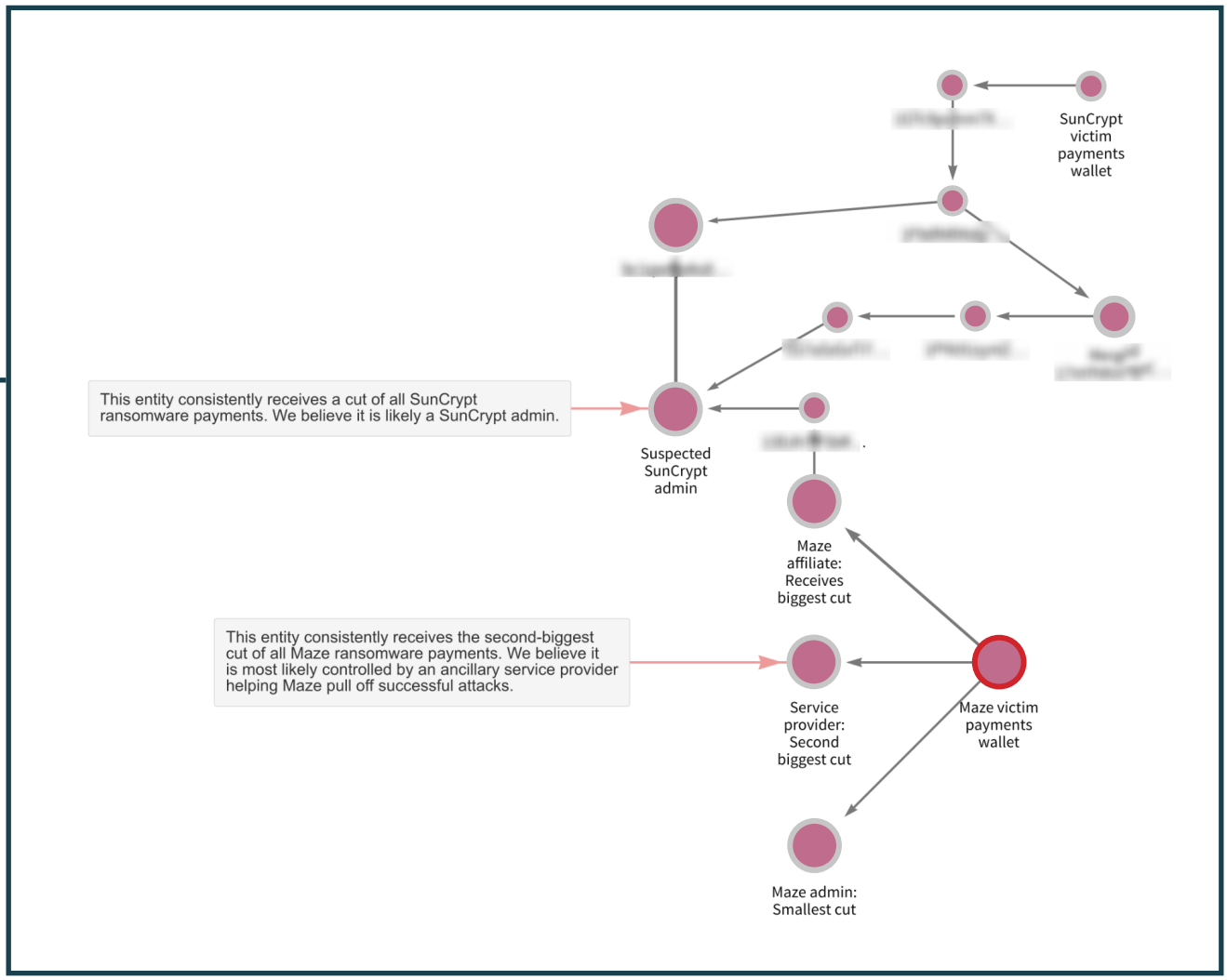
In October 2020, perhaps prompted by the massive uptick in ransomware attacks rocking both the public and private sector, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) released an advisory alert warning that making ransomware payments could be a sanctions violation for victims or companies that facilitate payments for victims.

The facilitation point is important, as there's a robust industry of consultants who help ransomware victims negotiate with and pay ransomware attackers.

The alert cited examples of ransomware creators and attackers who have been put on the OFAC sanctions list, such as the two Iranian nationals who laundered proceeds from the SamSam ransomware strain.

October's alert bolsters previous government guidance not to pay ransomware attackers, as this incentivizes future attacks.

However, this alert goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations.

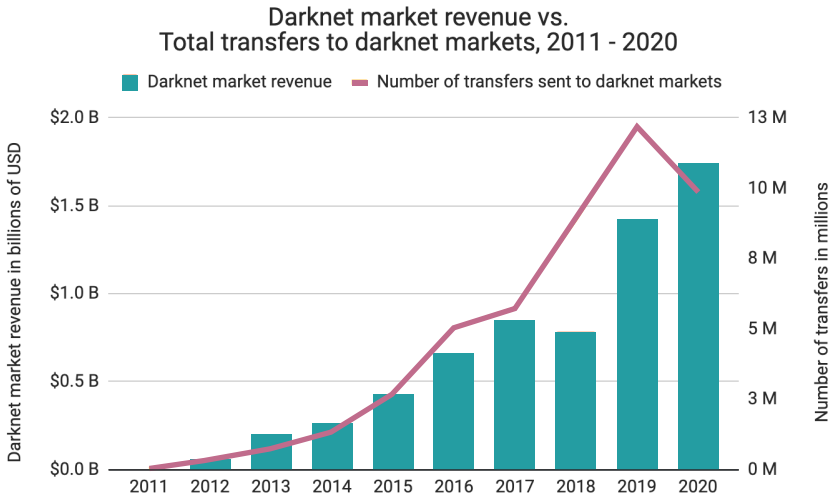


Darknet Markets

Darknet markets set a new revenue record in 2020, to bring in a total of $1.7 billion worth of cryptocurrency.

Interestingly, this record comes as individual purchases from darknet markets declined, falling from 12.2 million in 2019 to fewer than 10 million in 2020.

Looking more closely, we see that nearly all of the growth in darknet market activity 2020 can be attributed to one specific market: Hydra.



The challenge of Hydra

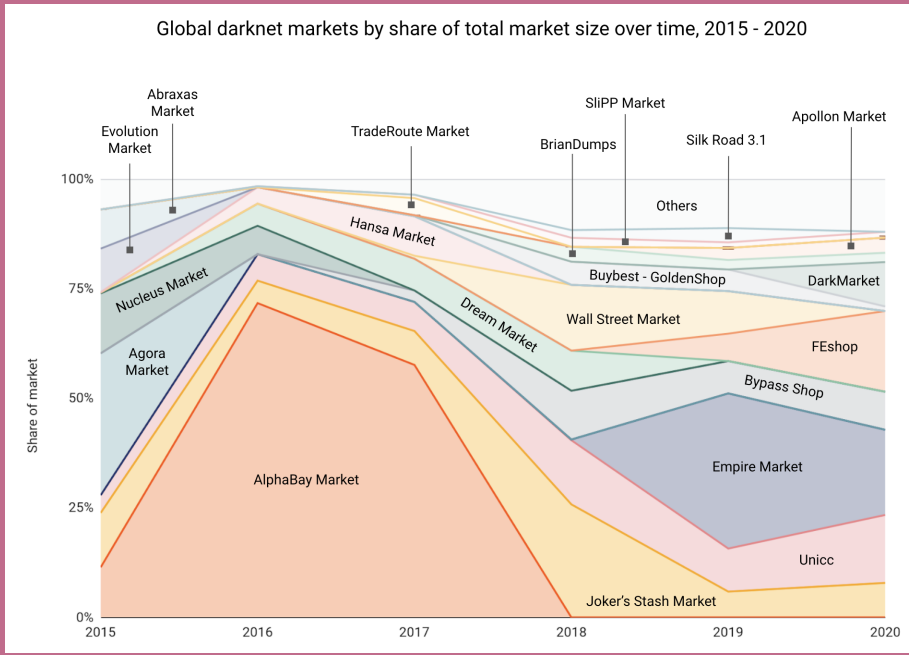
HYDRA

Hydra is unique in that it only serves Russian-speaking countries and is by far the largest darknet market in the world, accounting for over 75% of global darknet market in 2020. Without Hydra, darknet market revenue stayed roughly flat from 2019 to 2020.

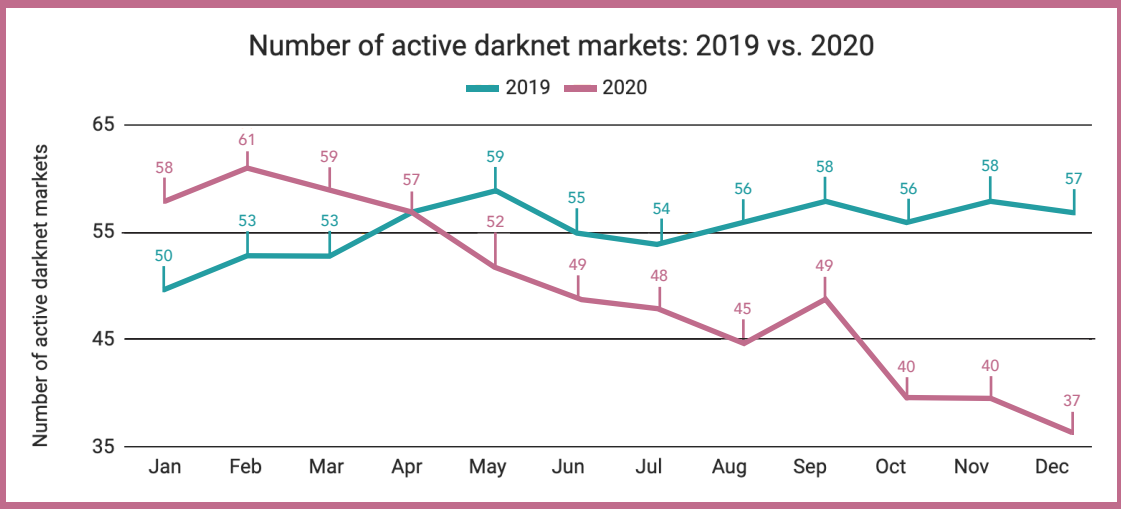
In December 2019, Hydra announced plans to raise $146 million in an ICO for a new global DNM service called Eternos. While it appears Covid put this plan on hold, the announcement suggests that Hydra plans to expand.

That could create a significant challenge for U.S. and European law enforcement, as Hydra has developed uniquely sophisticated operations, such as an Uber-like system for assigning drug deliveries to anonymous couriers who drop off their packages in out-of-the-way yet hidden public locations, commonly referred to as “drops,” which are then shared with the buyers.

The process avoids a physical exchange, and unlike with traditional darknet markets, vendors don’t need to risk using the postal system.



Active darknet market numbers fall



The course of 2020 also saw the number of active markets drop from 58 in January, to 37 in December.

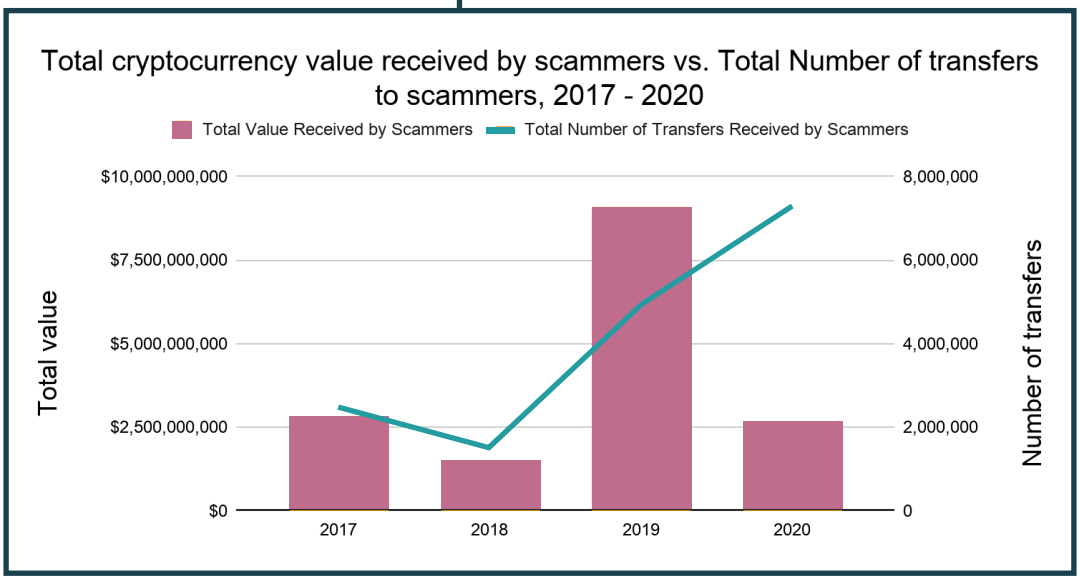
It is not clear that the Covid-19 pandemic is responsible for this trend, however. Criminology researchers Andréanne Bergeron, David Décary-Hétu, and Luca Giommoni recently published a study analyzing hundreds of darknet market drug sales made before and after Covid lockdowns began in Spring 2020.

While Covid caused shipping delays, the analysts did not conclude that those delays were the decisive factor in most market closures. Instead, they point to competitive forces in the darknet market landscape.

"It's becoming more challenging than ever to run a darknet market — you have to enable security and guard against DoS attacks, and then on top of that there's competition. All of these factors limit the availability of drugs," says Décary-Hétu.

"Excluding Hydra, if all darknet markets take in $250 million per year and administrators make 5% commission, that's $12.5 million total divided by all the markets, where a lot of employees have to be paid. It's simply not worth the risk of spending 100+ years in jail," Décary-Hétu adds.

Scams



While scams remain the highest-grossing form of cryptocurrency-based crime, total scam revenue fell drastically in 2020, from roughly $9 billion to just under $2.7 billion.

Interestingly though, the number of individual payments to scam addresses rose from just over 5 million to 7.3 million, suggesting that the number of individual scam victims rose by more than 48%.

Why did scam revenue decline even as the number of victims grew? There were no large-scale Ponzi schemes like those we saw in 2019.

Ponzi schemes

Ponzi schemes took in nearly $7 billion worth of cryptocurrency in 2019, which is more than double what all scam categories made in 2020. Even more shocking is the fact that just six individual Ponzi schemes accounted for that $7 billion.

Most notable of the six was the infamous PlusToken scam, a Ponzi scheme that reaped at least $3 billion worth of cryptocurrency from millions of victims, mostly in Asia. Since PlusToken coverage in the Chainalysis Crypto Crime Report 2021, Chinese authorities have arrested 109 individuals associated with the scam and prosecuted six of the most prominent.

Luckily, there's no evidence to suggest that Ponzi schemes comparable to PlusToken took place in 2020. This suggests that cryptocurrency users and the general public have grown more suspicious of such scams, or that potential Ponzi scheme operators have been scared off by the punishments doled out to the PlusToken operators.

Instead, nearly all scam revenue in 2020 went to smaller-scale investment scams. Investment scams have been a more consistent mainstay of cryptocurrency-based crime, as there are many more happening at any given time compared to Ponzi schemes.

Unlike Ponzi schemes, these more generic investment scams don't tend to pay out fake proceeds to early investors and take in less cryptocurrency from each individual victim.

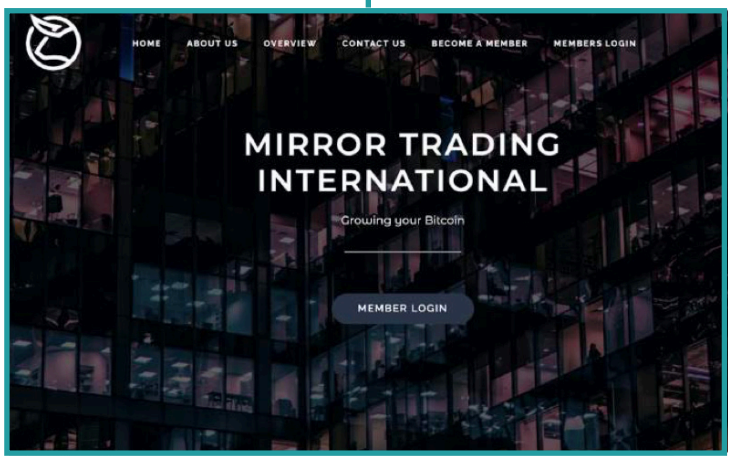
Mirror Trading International

Mirror Trading International was by far the biggest scam of 2020, taking in $589 million worth of cryptocurrency across more than 471,000 deposits, suggesting a number of victims in the hundreds of thousands.

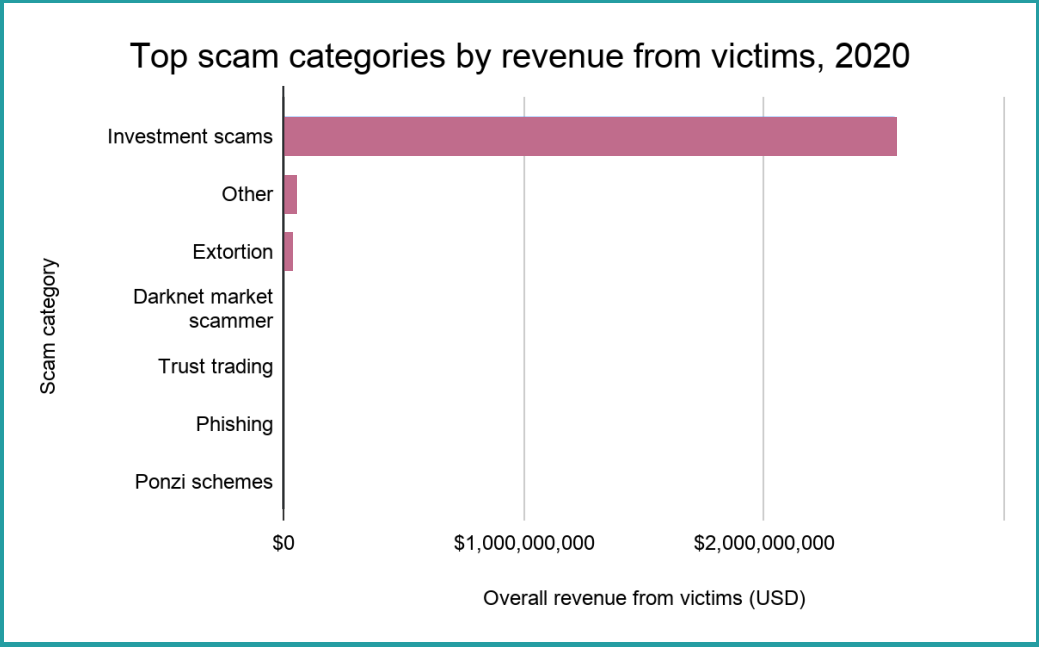
Mirror Trading International (MTI) primarily receives and sends funds from mainstream exchanges. Interestingly, the scam has also sent substantial funds to a popular gambling service, perhaps as part of a money laundering strategy.

As was the case in previous years, scammers moved cryptocurrency received from victims primarily to exchanges in order to convert it into cash.

However, there was also an increase in the share of scam proceeds sent to mixers and high-risk exchanges, meaning those with weak or non-existent compliance programs. This may be a sign that some scammers are becoming wary of compliant exchanges, which are more likely to flag illicit activity using a transaction monitoring solution and cooperate with law enforcement investigations.



Similarly, across the scamming world, we tend to see a disproportionate share of funds going into gambling in comparison to other forms of cryptocurrency-based crime.



MTI is based in South Africa, and claims to have offices in Stellenbosch and Johannesburg. Its web traffic falls in line with that, as more than half comes from South Africa.

The U.S., U.K., Canada, and Mexico also make up significant portions of MTI's web traffic. It is assumed, therefore, that most MTI victims hail from these countries in similar proportions as well.

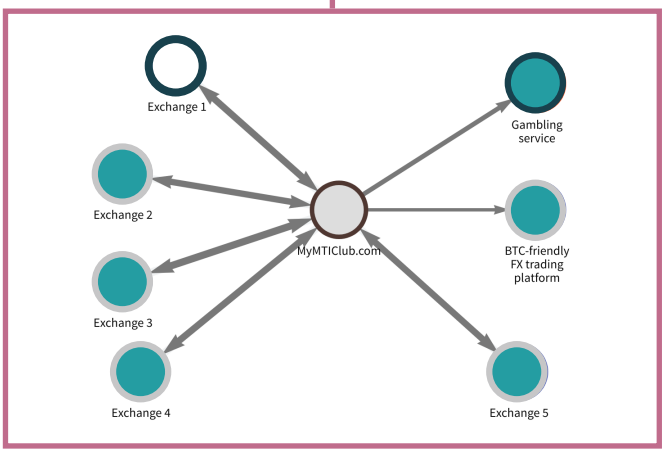
MTI presents itself as a passive income source. According to its website, users simply deposit a minimum of $100 worth of Bitcoin, and MTI promises to grow it using an AI-powered foreign exchange trading software.

The site indicates that customers can achieve consistent daily returns of 0.5%, which would translate to yearly gains of 500%. MTI has been actively receiving Bitcoin from "customers" since June 2018 and even has 150 employees listed on its LinkedIn company page.

Despite these airs of legitimacy, Google searches reveal that people have been rightly speculating that the company has been a scam for most of its existence. In August 2020, CoinDesk published an article encouraging all MTI users to withdraw their funds as soon as possible, citing the decision of Texas state regulators to formally label the company a scam, as well as a pending investigation by South Africa's Financial Services Conduct Authority (FSCA).

On December 18, 2020, the FSCA filed charges against MTI after its investigation found that the company falsified trade statements, didn't declare losses and committed other acts of fraud to deceive the market.

The investigation also found that MTI had over 16,000 Bitcoin of claimed customer investment funds unaccounted for. MTI claimed to have transferred those funds to a new FX trading platform after its old platform banned MTI due to its scamming reputation, but the new platform says these funds were never deposited.



Since those charges were filed, MTI customers have complained that they can no longer access or withdraw funds they've deposited to the platform, and MTI CEO Johan Steynberg has fled South Africa.

MTI Club has received $588 million worth of Bitcoin across more than 470,000 transactions, primarily from exchanges, but also from self-hosted wallets. MTI has also sent and received significant funds to and from a popular, Bitcoin-friendly FX trading platform.

Perhaps most interesting is MTI Club's apparent usage of a popular cryptocurrency gambling service as a money laundering and cash out mechanism. The platform is the biggest risky destination of MTI funds by volume, having received $39 million worth of cryptocurrency from the scam in 2020.

Cryptocurrency observer and venture capitalist Dovey Wan has remarked that this is becoming a common money laundering technique for many cybercriminals who use cryptocurrency, as gambling platforms can be used similarly to mixers to obscure the origins and flows of illicitly- obtained funds. Data suggests that this is especially true for scammers.

The danger of algorithmic trading platforms

Mirror Trading International is another example of why the industry must spread the word that algorithmic trading platforms promising unrealistically high returns are nearly always scams.

When cryptocurrency exchanges and other services learn of these scams and receive their crypto-currency addresses, they should discourage users from sending funds to those addresses or at least warn them that financial losses are highly likely.

In addition, exchanges, gambling platforms, and other services that these scams use to launder funds should consider blocking incoming transactions from businesses that relevant government bodies label as scams or potential scams, as removing the ability to convert funds to cash makes it more difficult for scams to operate.

The Ledger phishing scam: a wake-up call for exchanges

While phishing scams made up a very small share of overall scam revenue in 2020, one phishing scam in particular has received a great deal of attention due to its high visibility and the number of potential victims: The Ledger phishing scam.

Ledger is a popular provider of hardware cryptocurrency wallets – physical devices on which cryptocurrency can be stored, similar to a conventional cryptocurrency wallet. In July 2020, the company published a blog post revealing that many users' email addresses had been compromised in a data breach.

A few months later in October, Ledger customers reported receiving emails from closely spoofed versions of the Ledger website domain. The email claimed that Ledger's servers had been hacked with malware and that customers' funds were in danger of being stolen unless they clicked a link in the email to download the latest version of Ledger's software. Clicking the link leads users to a web page that mimics the Ledger website.

The email and website however, are part of a sophisticated phishing scam. Instead of a software update, Ledger users who click the download link on the fake web page actually download malware that drains their Ledger wallet.

Overall, CoinTelegraph reported that Ledger users lost 1.1 million XRP (roughly $645,000) within the first week of the phishing campaign. Also of note, is that since the leaked Ledger database was sold on the dark web, it's possible that more than one criminal group has launched phishing attacks against Ledger users.

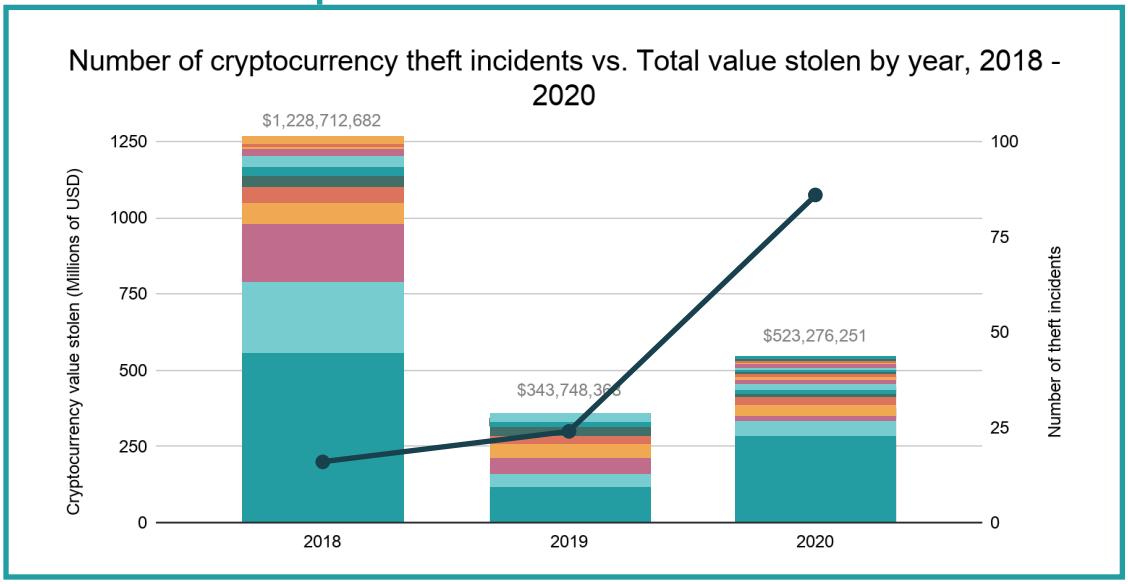
This possibility is backed up by the fact that since October 2020, Ledger users have received multiple waves of phishing messages, including some delivered by SMS and using different social engineering techniques.

Analysis of a selection of the suspected scammers' addresses reveals that their wallets have been active since 2018, suggesting that the cybercriminals may have been conducting phishing scams for at least two years preceding the publication of the Ledger scam in 2020.

In addition, it was found that assets stolen from Ledger customers span many cryptocurrencies, a large share of which have been moved to exchanges and other services. The stolen assets identified amount to upwards of €3 million.

The Ledger phishing scam shows how important it is for exchanges and other cryptocurrency services to educate customers on phishing techniques, especially if they know customers' emails or other personal information has been compromised, thereby making customers more vulnerable to phishing attacks.

Stolen Funds



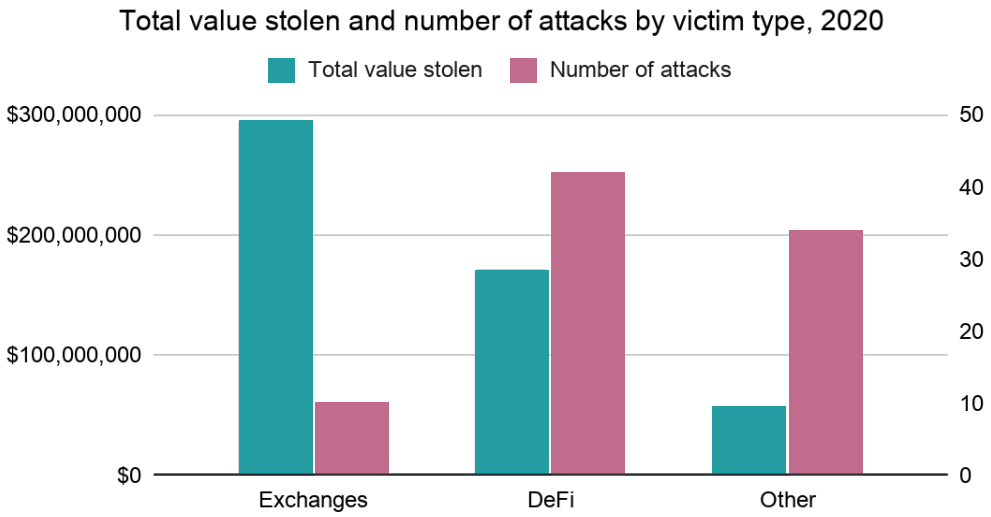
Out of all cryptocurrency stolen in 2020, around 33% was lost through decentralised financial (DeFi) platforms.

DeFi platforms are decentralized apps built on top of smart contract-enriched blockchain platforms — primarily the Ethereum network — that let users automatically execute specific financial transactions such as trades and loans when certain conditions are met.

While relatively high, the 33% figure accounted for just 6% of all cryptocurrency transaction volume through 2020.

Most of the funds stolen through DeFi platforms were lost via flash loan attacks – arrangements that allow users to borrow high volumes of cryptocurrency with no collateral, as long as the user pays back the loan within the same transaction. Flash loans are typically used to exploit arbitrage opportunities across different DeFi platforms.

Always ready to take advantage, bad actors manipulate this exchange by borrowing enough funds to artificially inflate asset process through complex, multi-layered transactions.



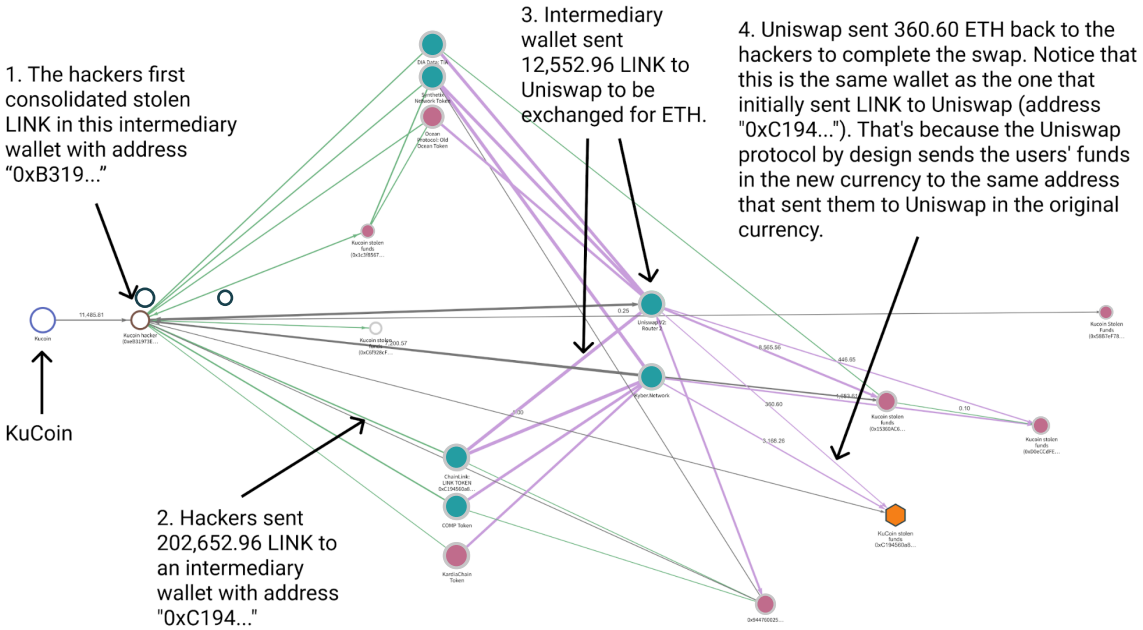
Lazarus Group strikes again for third-largest ever exchange

Lazarus Group is a notorious hacking syndicate closely linked with North Korea. It was active once more through 2020, stealing $275 million worth of cryptocurrency from Kucoin, a popular exchange.

While Kucoin chiefs say they were able to recover most of the funds, the event illustrates how important it is to fight rogue state actors and their ability to steal cryptocurrency.

Lazarus Group used DeFi platforms in their attempts to launder some of the funds stolen from Kucoin – a new strategy for Lazarus Group, which had previously moved stolen funds primarily to mixers and centralized exchanges.

Since 2017, Lazarus Group has stolen over $1 billion worth of cryptocurrency. US authorities have responded by filing indictments against several hackers and money launderers allegedly associated with the cybercrime syndicate.

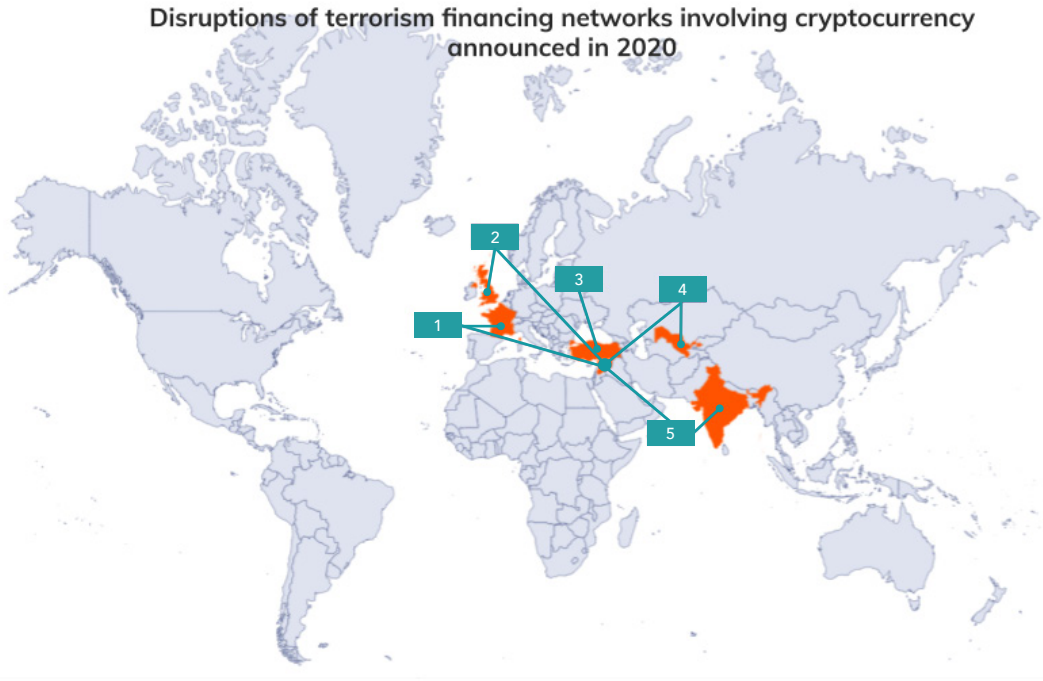


Terrorism and extremism financing

In 2020, government agencies around the world uncovered, investigated and prosecuted more terrorism financing schemes involving cryptocurrency than ever before.

Following an investigation into several different cryptocurrency donation campaigns, US government agencies recovered more than $1 million worth of Bitcoin from wallets controlled by terrorist groups and their financial facilitators.

Below, we summarize three cryptocurrency-based terrorism financing campaigns which law enforcement agencies investigated and prosecuted in 2020.



Case 1: al-Qaeda and ISIS

Country investigating: France | **Destination of funds: Syria** | **Date of activity: 2019 - 2020**

French authorities arrested 29 individuals in a cryptocurrency-based terrorism financing scheme. Dozens of people in France bought cryptocurrency coupons worth $11-$165. The coupons were credited to accounts opened abroad by jihadis who then converted them into cryptocurrency. Hundreds of thousands of euros are thought to have been supplied via the network, benefitting members of al-Qaeda still hiding out in northwest Syria, as well as jihadis of the Islamic State group.

Case 2: ISIS

Country investigating: UK | Destination of funds: Syria | Date of activity 2016 – 2020

Hisham Chaudary of Leicester, England is alleged to have gathered and transferred Bitcoin to jihadist groups, allowing captured ISIS militants to escape Kurd-controlled prison camps in northern Syria.

Case 3: The al-Qassam Brigades

Country investigating: US | Destination of funds: Multiple | Date of activity: 2019 – 2020

Starting in 2019, the al-Qassam Brigades posted calls on its social media pages for Bitcoin donations to fund terror campaigns, before moving solicitation to its official websites and incorporating more sophisticated cryptocurrency wallet infrastructure.

Conclusion

Cryptocurrency is an exciting industry because it's always evolving.

In 2020, we've seen DeFi take off, institutional dollars flow in thanks in part to tailor-made platforms like Coinbase Prime, and exchanges like Kraken become chartered banks following new regulatory guidance from the U.S. government.

Perhaps most exciting is that all of this happened in the face of a global pandemic — a true test of cryptocurrency's value as a safe haven asset — during which Bitcoin's price surged.

However, just as the cryptocurrency industry is always moving forward, so too are the bad actors who commit cryptocurrency-related crime. So, what trends do you need to prepare through the rest of 2021 and beyond?

The future of Cryptocurrency

DeFi will play a bigger role in crypto crime

As we alluded to above, DeFi has skyrocketed in popularity this year.

DeFi platforms never take possession of a user's funds, and instead simply route them between users' wallets based on the conditions outlined in the underlying smart contracts without human intervention. Many believe that means they aren't subject to the same regulations as typical cryptocurrency businesses that take custody of users' funds.

Furthermore, DeFi platforms can theoretically run without human intervention, so there's often no team or organization keeping records or intervening when something goes wrong.

The lack of intervention makes DeFi platforms appealing to users who value privacy, but potentially also to criminals looking to launder ill-gained funds. Therefore, it is expected that DeFi usage for money laundering will increase.

More decentralization in darknet markets

Darknet market decentralization is another trend that picked up in 2020, and which is expected to continue into 2021 and beyond.

More markets went out of business than ever in 2020, and not due to Covid. However, competition has intensified between darknet markets, with some initiating denial-of-service (DOS) attacks against rival markets, and several others exit scamming, which has significantly reduced buyer trust.

At the same time, law enforcement is shutting down more markets and putting administrators in jail, leaving market administrators — who despite all the risk they take on receive roughly 5% commissions on sales — less willing to continue their work.

But a new decentralized model embodied by platforms like Televend may solve many of these problems for darknet markets. Televend is a Telegram-based platform with over 150,000 users where darknet market vendors can sell drugs through automated chatbots, whose communications with buyers are highly encrypted.

Exchanges will treat other services with more scrutiny as risk-based compliance becomes the norm

Traditionally, too many exchanges have relied on other cryptocurrency services (including other exchanges) publicly stated KYC (know your customer) and AML (anti-money laundering) policies when assessing their riskiness.

If the policy checked out, many exchanges would treat the service as if it were safe. But that won't cut it anymore in an era when institutional dollars are flowing into cryptocurrency like never before.

Whether they're buying cryptocurrency of their own as an investment, offering custodial services, or accepting cryptocurrency businesses as banking clients, mainstream financial institutions are going to need to enforce compliance more stringently than cryptocurrency businesses themselves have.

That means they won't be taking compliance policies at face value. Instead, they'll insist on taking advantage of cryptocurrency's inherent transparency. In a monetary system where every transaction is recorded on a public, unchangeable ledger, why wouldn't a financial institution aggressively analye that information to ensure they're working with the safest possible businesses?

Exchanges and other cryptocurrency businesses who want to work with these financial institutions will need to follow suit and assess their own counterparties with equal rigor.

Increased compliance scrutiny by cryptocurrency exchanges will drive crypto-crime down, as more wrongdoers will be reported to the authorities and stopped sooner than they otherwise would have been. In the long run, these efforts by exchanges will also remove some of the incentive to use cryptocurrency in criminal activity, as it will become much harder for cybercriminals to convert cryptocurrency into cash if they can't use exchanges.

The crypto-crime outlook has never been better

Some of the upcoming advancements of cryptocurrency will make it more difficult for law enforcement and compliance professionals to detect and fight criminal activity.

However, we can be confident that both groups, along with the institutional investors, can come together to meet the challenge, and ultimately create a safer cryptocurrency ecosystem for all participants.

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 60 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.
For more information, visit www.chainalysis.com