Chainalysis

THE 2020 STATE OF CRYPTO CRIME

Everything you need to know about darknet markets, exchange hacks, money laundering and more

January 2020

Table of Contents

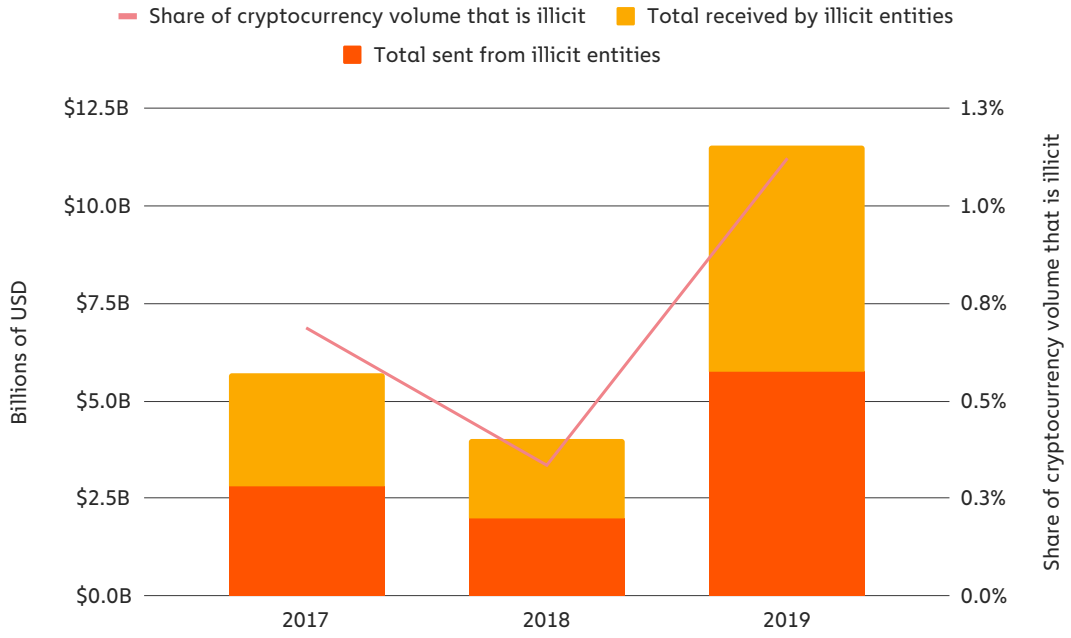
Introduction

2019 Crypto Crime Activity Summarized

If the last few years have proven anything, it's that cryptocurrency isn't just for criminals. Polling shows that adoption is increasing, as 18% of all Americans and 35% of American millennials have purchased cryptocurrency in the last year. Mainstream financial institutions like JP Morgan Chase are getting involved. Popular retailers like Amazon and Starbucks now allow customers to pay in Bitcoin.

Nonetheless, cryptocurrency's decentralized, semi-anonymous nature makes it a uniquely appealing option for criminals, and their embrace of the technology has helped shape its overall reputation. But the upside is that unlike cash and other traditional forms of value transfer, cryptocurrency is inherently transparent. Every transaction is recorded in a publicly visible ledger. With the right tools, we can see how much of all cryptocurrency activity is associated with crime, hone in on the types of crime that dominate the ecosystem, and share insights with law enforcement and the industry to curb its impact and stop bad actors from abusing the system and, in many cases, taking advantage of vulnerable people.

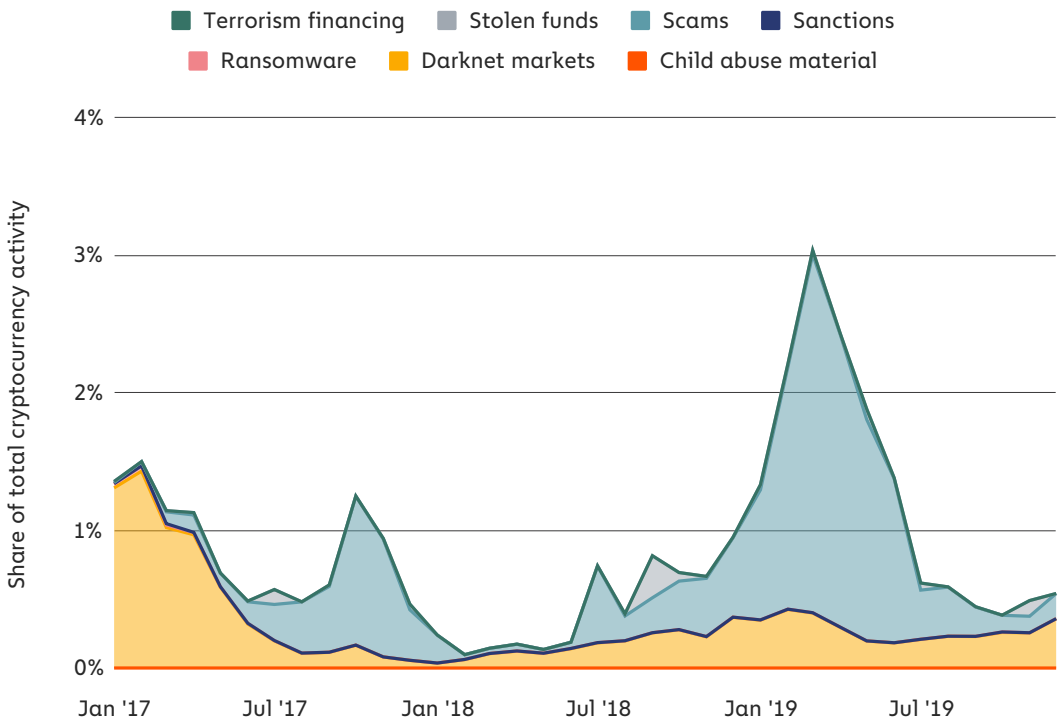
Total cryptocurrency sent and received by illicit entities vs. Illicit share of all cryptocurrency transaction volume, 2017-2019



Currencies included: BAT, BCH, BNB, BTC, CRO, CRPT, DAI, ETH, GNO, GUSD, HT, LEO, LINK, LTC, MCO, MKR, MLN, OMG, PAX, TUSD, USDC, USDT, WETH, ZIL, ZRZ

From the above, we see that illicit cryptocurrency transactions have risen, both in total value and as a share of all cryptocurrency activity. However, illicit transactions still make up a small share of all cryptocurrency activity at just 1.1%. What kinds of crimes are driving these numbers?

Share of total cryptocurrency transaction volume by illicit subcategory



Currencies included: BTC, ETH, LTC, BCH, USDT, PAX, ZRX, BNB, OMG, USDC, TUSD, DAI, WETH, HT, GNO, ZIL

The graph above shows which crimes take up the biggest share of overall cryptocurrency activity over time since 2017. We see that in 2019, scams made up the overwhelming majority of cryptocurrency-related crime, accounting for a whopping $8.6 billion in transactions. In fact, were it not for just three separate large-scale Ponzi schemes, the crime would account for just 0.46% of all cryptocurrency activity.

Of course, it's not just about the data when it comes to crypto crime. It's about the story behind the numbers. As the world's leading blockchain analysis firm, we're in a unique position to contextualize crypto crime data with real, in-the-trenches experience. In this report, we're going to share our expertise and tell you everything you need to know about what happened in crypto crime in 2019 across six key categories, including actionable takeaways for law enforcement, regulators, financial institutions, and cryptocurrency businesses.

In analyzing these six categories, we've identified three common threads that bind all of them together:

1. **Crypto crime is starting to look more like white collar crime.**
   When you think of white collar crime, you probably think of a small cadre of executives abusing the powers of their position or acting on privileged information to enrich themselves. Believe it or not, crypto crime functions in much the same way. Whether it's tight-knit criminal groups defrauding millions in brazen Ponzi schemes or elite hackers breaking into exchanges, we find that the majority of cryptocurrency gained through criminal activity goes to a small but powerful segment of criminals.

2. **Money laundering is the key to crypto crime.**
   Money laundering is the common denominator between all forms of crypto crime, because every criminal earning cryptocurrency illegally eventually needs to obscure the origins of their holdings in order to convert them to cash. So, it shouldn't come as a surprise that there are sophisticated services and networks designed to do just that. In this report, we show you what those money laundering providers look like and how they interact with different types of criminals.

3. **Scams are the biggest threat in crypto crime.**
   As we mentioned above, scams were by far the highest-earning category of crypto crime in 2019. Scammers take advantage of the unique position cryptocurrency currently occupies in the public eye: Most people have heard of it, and many believe it has "get rich quick" potential. But many of those people also don't know the industry well enough to spot a scam when they see one, making them ripe targets. Cryptocurrency-based scams tend to target vulnerable populations such as the elderly, and hurt the reputation of the industry as a whole. We believe the consumer protection implications make cryptocurrency scams an issue regulators must address and law enforcement must have the resources to investigate. Exchanges are also in a unique position to help, both in terms of protecting users from being scammed and preventing successful scammers from depositing funds or cashing out.

Be on the lookout for those themes as you read through the data and case studies presented in this report. The first topic we'll look at: Money laundering.

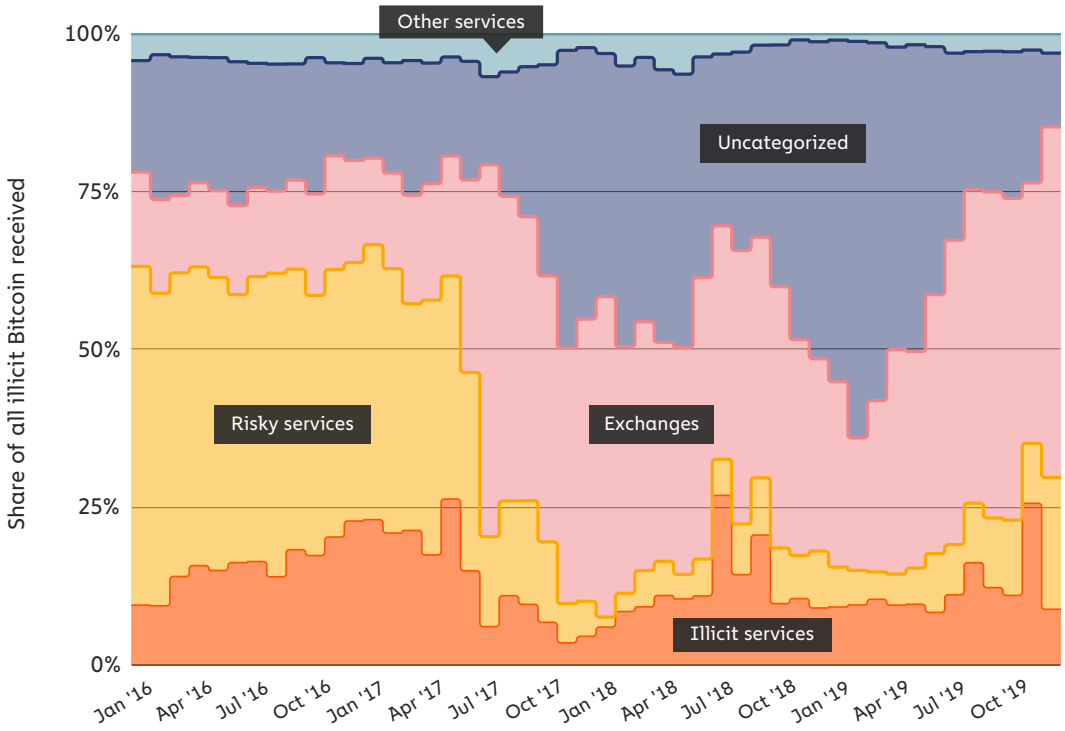
Money Laundering

Billions Laundered:
The White Collar Side of Crypto Crime

Once a criminal has a pile of illicitly-gained cryptocurrency sitting in a wallet, the next question they have to answer is, "How am I going to turn this into cash without getting arrested?" The need to launder funds is the common thread among all the forms of crypto crime we study in this report.

So, how do criminals do it? Thanks to the inherent transparency of blockchains, we can look at cryptocurrency's money laundering ecosystem from a high level, and draw insights that aren't possible when studying money laundering in the traditional fiat currency world. Let's start by examining the most common destinations to which criminals have sent Bitcoin over time. * **

Types of services receiving illicit Bitcoin, 2016-2019



Currencies included: BTC

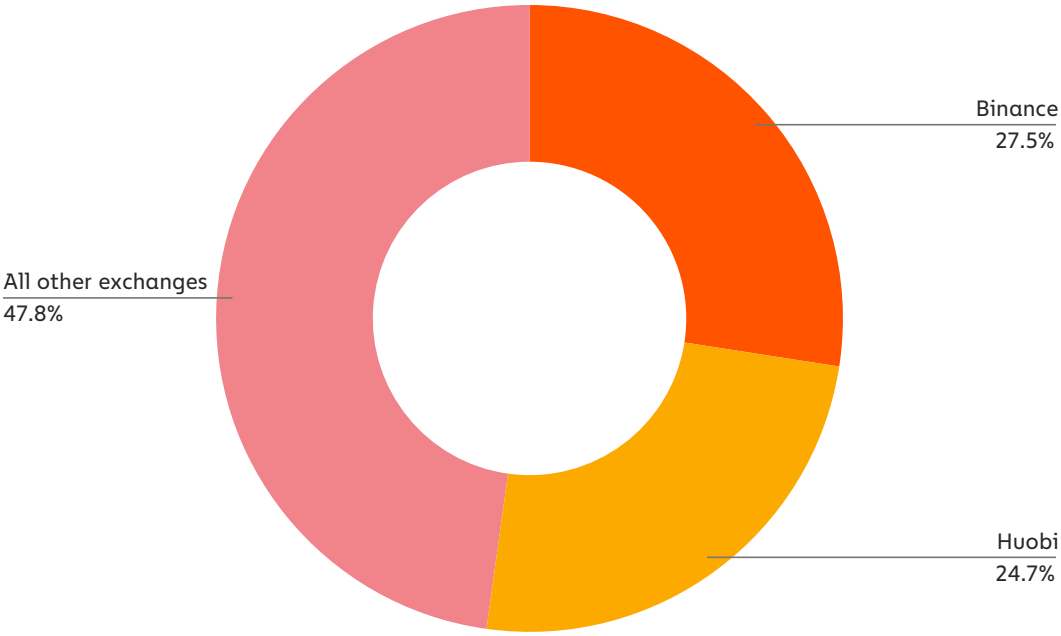
While exchanges have always been a popular off-ramp for illicit cryptocurrency, they've taken in a steadily growing share since the beginning of 2019. Over the course of the entire year, we traced $2.8 billion in Bitcoin from criminal entities to exchanges. Just over 50% went to the top two: Binance and Huobi.

---

* Please note that we only analyze Bitcoin transactions in this section for simplicity. As the most popular cryptocurrency, Bitcoin continues to represent the vast majority of funds used in criminal activity, so we think it's an adequate representation for examining money laundering in cryptocurrency as a whole.

** Please note that risky services include P2P exchanges, mixing services, high risk exchanges, and gambling sites. Illicit services include ransomware addresses, sanctioned entities, darknet markets, and addresses associated with scams and stolen funds.

Exchanges receiving illicit Bitcoin, 2019



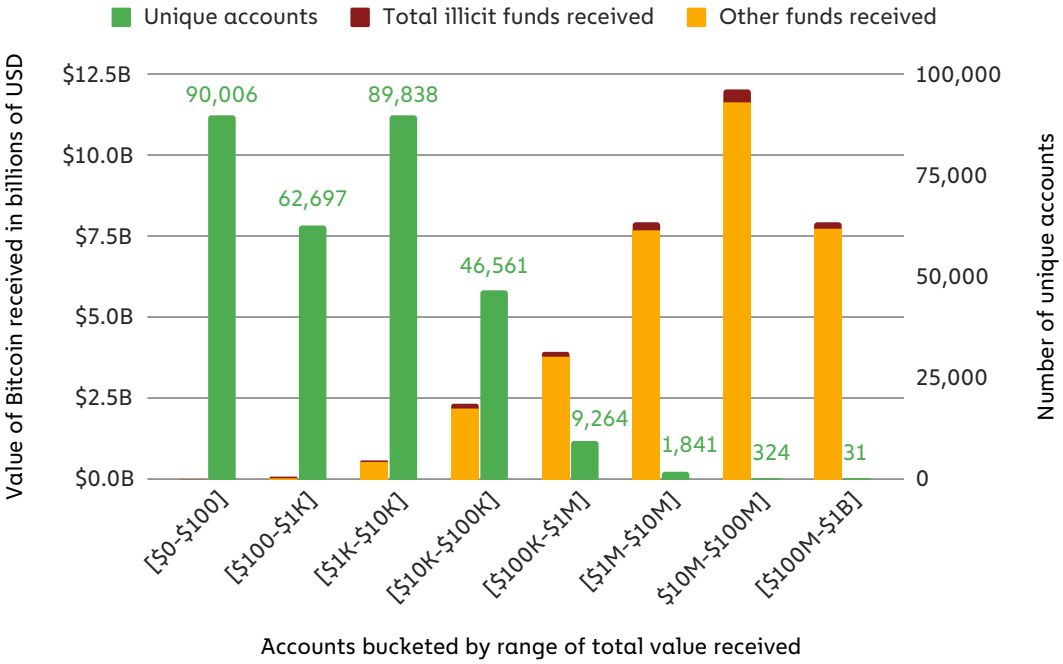
Currencies included: BTC

Binance and Huobi lead all exchanges in illicit Bitcoin received by a significant margin. That may come as a surprise given that Binance and Huobi are two of the largest exchanges operating, and are subject to KYC regulations. How can they be receiving so much Bitcoin from criminal sources? Let's start by looking at the specific accounts receiving illicit funds at both Binance and Huobi.

Overall, just over 300,000 individual accounts at Binance and Huobi received Bitcoin from criminal sources in 2019. Who's behind those accounts? Are any of them significant traders? Below, we've broken those accounts down into buckets based on the total value of all Bitcoin they've received in 2019, with illicit Bitcoin called out. ***

*** Please note that due to the nature of how we connect illicit funds to specific addresses, this chart considers only $1.1 billion of the total $1.4 billion worth of illicit Bitcoin received by Binance and Huobi.

Total Bitcoin received by accounts on Huobi and Binance with illicit exposure, 2019



Currencies included: BTC

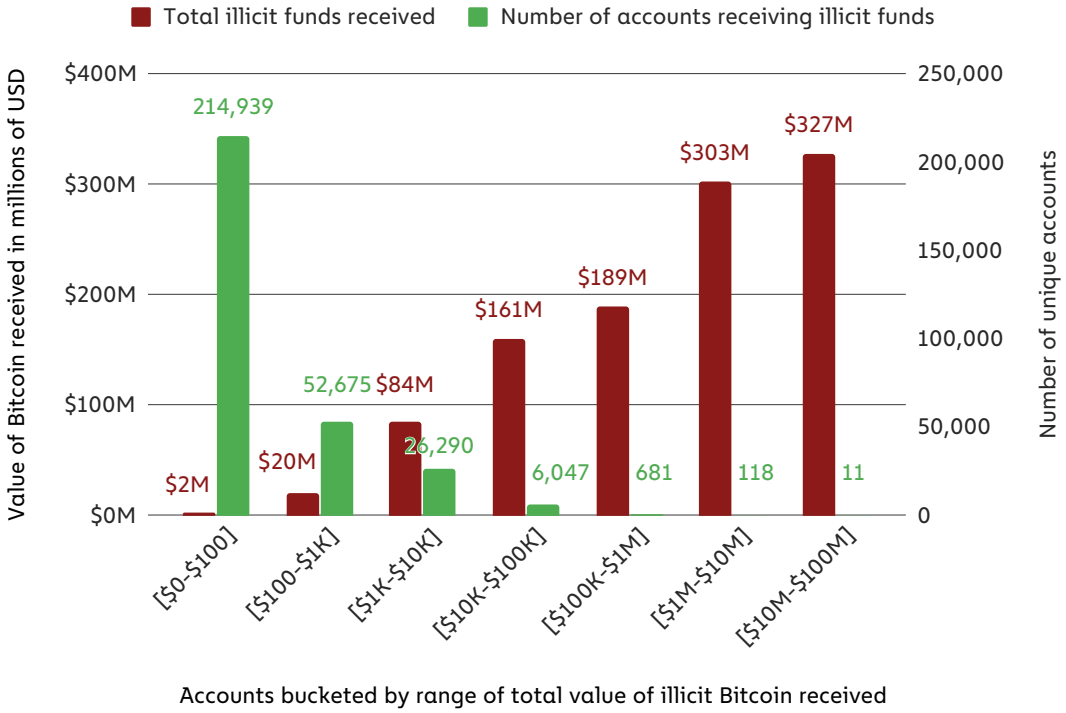
How to read this graph:

- The green bars represent the number of unique accounts in each bucket. Again, the buckets are based on the total amount of Bitcoin the accounts have received **individually**, from both criminal and non-criminal sources. All accounts shown have received at least some criminal funds.
- The yellow and red stacked bars show the total amount of cryptocurrency received **collectively** by all the accounts in each bucket. That means, for example, that the 31 accounts in the highest-earning bucket on the right-hand side have collectively received just over $8 billion worth of Bitcoin in 2019, and that each of those 31 accounts individually has received between $100 million and $1 billion.
- The red segment of the bars represents the amount of illicit Bitcoin received by all accounts in each bucket.
- The yellow segment represents the remaining non-criminal funds received by the accounts in each bucket.

We can see from this graph that a small segment of these accounts is extremely active. The 2,196 accounts in the three highest-receiving buckets received a total of nearly $27.8 billion worth of Bitcoin in 2019. The graph also makes it clear that Bitcoin from criminal sources represents just a small fraction of the total amount received by Binance and Huobi. Nonetheless, the illicit funds shown above comprise a high total value — the 31 accounts in the top-earning bucket alone received a total of over $163 million worth of Bitcoin from criminal sources in 2019.

Let's look at another version of this chart where we only include funds that have come from accounts we know are connected to illicit activity (i.e. those represented in red above).

Illicit Bitcoin received by Binance and Huobi accounts, 2019



Currencies included: BTC

A small segment of accounts is taking in most of the illicit Bitcoin being sent to Binance and Huobi. The 810 accounts in the three highest-receiving buckets have taken in a total of over $819 million in Bitcoin from criminal sources, representing 75% of the total. Who are the whales driving this activity?

Our analysis suggests that many are OTC brokers.

OTC (Over The Counter) brokers facilitate trades between individual buyers and sellers who can't or don't want to transact on an open exchange. OTC brokers are typically associated with an exchange but operate independently. Traders often use OTC brokers if they want to liquidate a large amount of cryptocurrency for a set, negotiated price. OTC brokers are a crucial source of liquidity in the cryptocurrency market. While it's impossible to know the exact size of the OTC market, we know that it's huge. Cryptocurrency data provider Kaiko even estimates that OTCs could facilitate the majority of all cryptocurrency trade volume.

The problem, however, is that while most OTC brokers run a legitimate business, some of them specialize in providing money laundering services to criminals. OTC brokers often have much lower KYC requirements than the exchanges they operate on. Many of them take advantage of this laxity and help criminals launder and cash out funds, usually first by exchanging Bitcoin and other cryptocurrencies into Tether as a stable intermediary currency before they presumably cash out into fiat.

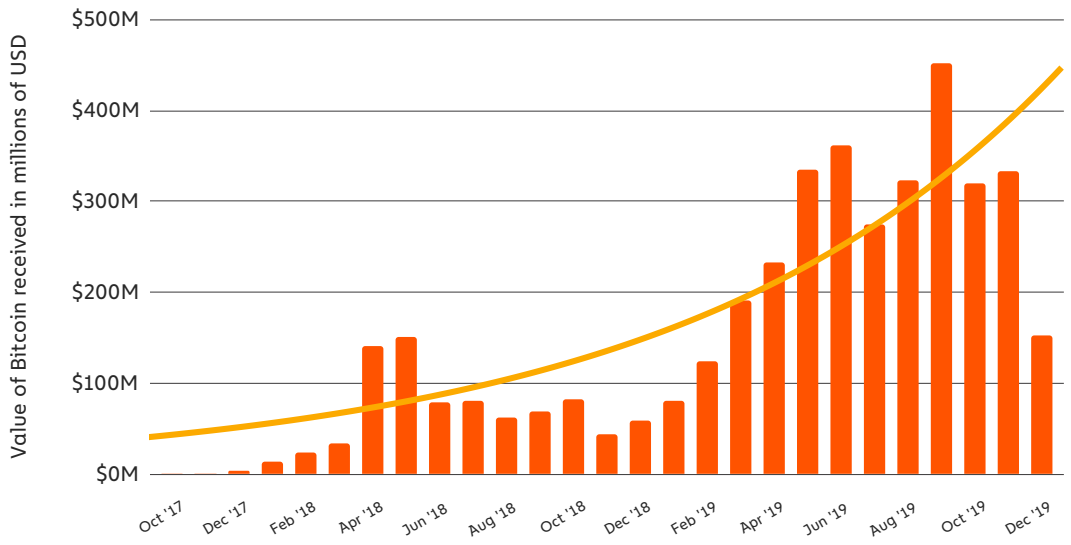
From our analysis of transactions by various criminal groups, we put together a list of 100 major OTC brokers we believe provide money laundering services, based on the fact

that they've received large amounts of cryptocurrency from illicit sources. This is not an exhaustive list of corrupt OTC brokers; rather it is a sample we assembled based on our experience investigating money laundering over time. We'll call them the "Rogue 100."

70 of the OTC brokers in the Rogue 100 are in the group of Huobi accounts receiving Bitcoin from illicit sources. 32 of them are in the group of 810 accounts receiving the most illicit Bitcoin, and 20 of them received $1 million or more worth of illicit Bitcoin in 2019. In total, these 70 OTC brokers received $194 million in Bitcoin from criminal entities over the course of 2019. Interestingly, all 70 operate on Huobi, though it's possible they also have accounts on Binance or other exchanges as well.

Keep in mind, the Rogue 100 only represents OTC brokers we've manually identified as money launderers over the course of our investigations on behalf of Chainalysis clients. We think it's extremely likely that some percentage of the other highly-active Binance and Huobi accounts taking in illicit funds also belong to corrupt OTC brokers we've yet to identify.

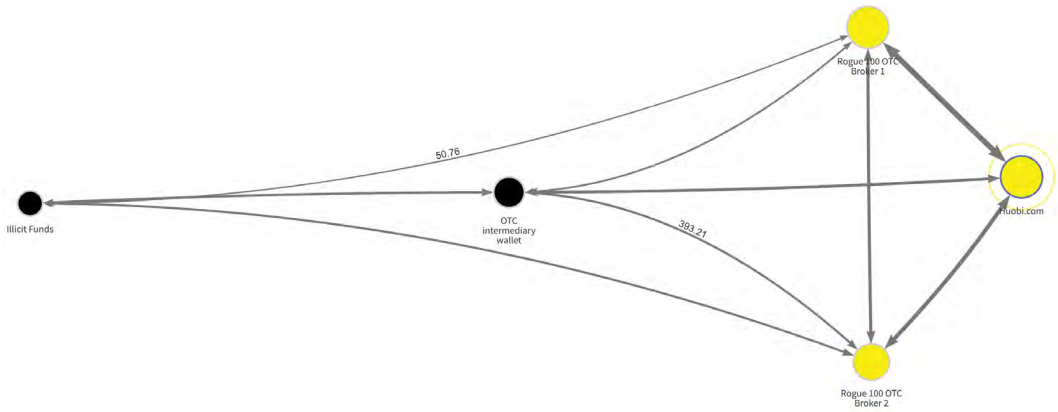
Total value of Bitcoin received by Rogue 100 OTC brokers by month, Oct '17 - Dec '19



Currencies included: BTC

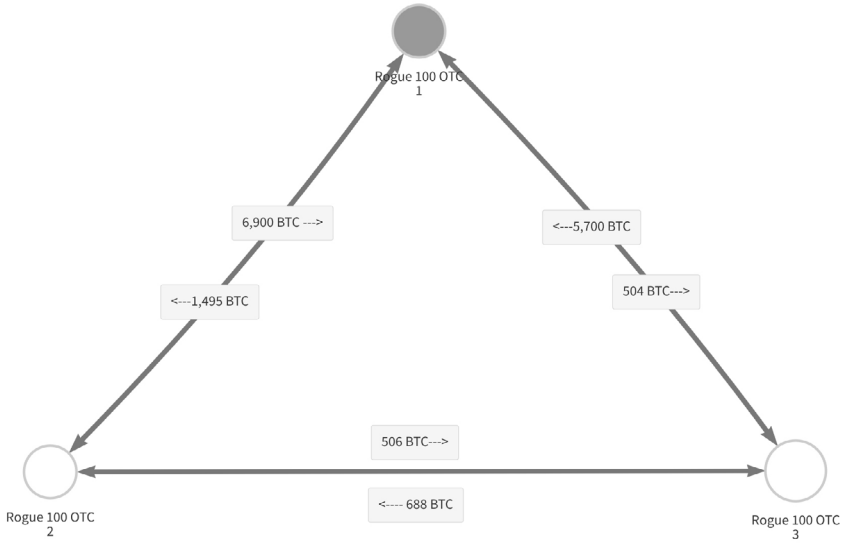
The Rogue 100 are extremely active traders and have a huge impact on the cryptocurrency ecosystem. They've received steadily increasing amounts of cryptocurrency each month since late 2017, but their activity skyrocketed this year. They received more than $3 billion worth of Bitcoin over the course of 2019, and many of them played a substantial role in the PlusToken scam we discuss later in this report. **Overall, the funds the Rogue 100 receive can account for as much as 1% of all Bitcoin activity in a given month.**

By analyzing their transactions in **Chainalysis Reactor**, we can see how two corrupt OTC brokers take in funds from criminal sources.



On the far left, we see funds start at a criminal entity, move through an intermediary wallet, and then move to two OTC brokers, both of whom are on our Rogue 100 list. The OTC brokers then move the funds to Huobi, most likely to be converted to cash.

We can also see in Reactor that corrupt OTC brokers frequently transact with one another. Below is an example looking at three OTC brokers from the Rogue 100.



These may simply be transactions being executed on behalf of legitimate OTC clients. However, we know from our on-the-ground intelligence that money launderers and other criminals often execute large transactions with one another in attempts to "fool" blockchain analysis software like Chainalysis by artificially lowering their exposure to criminal wallets — this could be an example of that.

While it's difficult to estimate what percentage of all cryptocurrency is sent from criminal wallets to OTC brokers, our analysis shows that OTC brokers who carry out a significant percentage of all Bitcoin transactions are receiving illicit funds, and behaving in ways that suggest a desire to hide the nature of their transactions.

What can the cryptocurrency industry do about OTC brokers and money laundering?

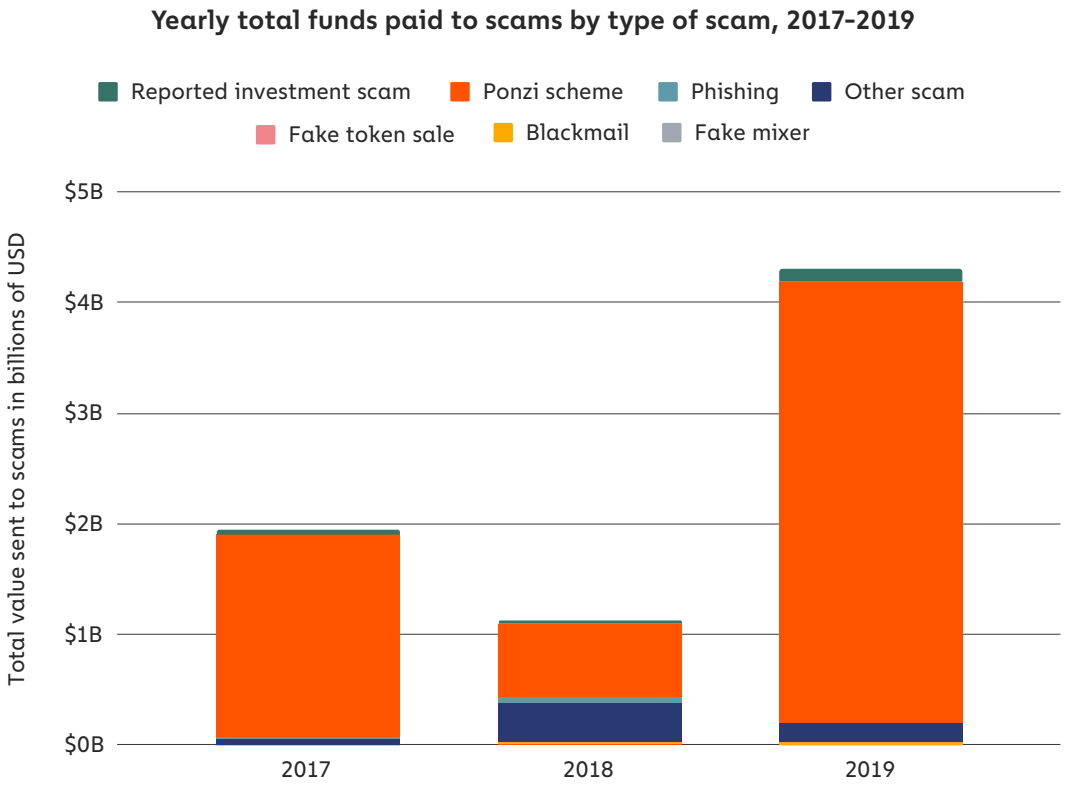
The money laundering infrastructure driven by OTC brokers enables nearly every other type of crime we cover in this report. After all, if there were no way for bad actors to cash out cryptocurrency they've received through illegal means, there'd be far less incentive for them to commit crimes in the first place. That would mean not only fewer victims affected by crimes, but would also help improve cryptocurrency's reputation as the industry seeks to work with regulators and traditional financial institutions and drive increased adoption.

Luckily, there are steps that law enforcement agencies, regulators, and cryptocurrency businesses can take to start stamping out money laundering. It all starts with transparency. Money laundering, especially in the fiat world, is typically thought of as a black box one can only open and begin to understand by getting a search warrant and poring over a suspect's bank records. But with blockchain analysis tools like Chainalysis, we can analyze transactions recorded on the blockchain and get insight into how criminals are laundering funds much faster, as we show above. Law enforcement agents and regulators need to become experts in this technology in order to start fighting money laundering in cryptocurrency.

We also call on exchanges to carry out more extensive due diligence on OTC brokers and other nested services operating on their platform. Most large exchanges, including Huobi and Binance, are already collecting KYC information on customers, as they're required to do by law in most jurisdictions. Our analysis shows that they need to extend that scrutiny to OTC desks consistently over time and ensure the OTC desks have effective KYC processes on their customers in order to do their part in the fight against money laundering.

Scams

2019: The Year of the Ponzi Scheme



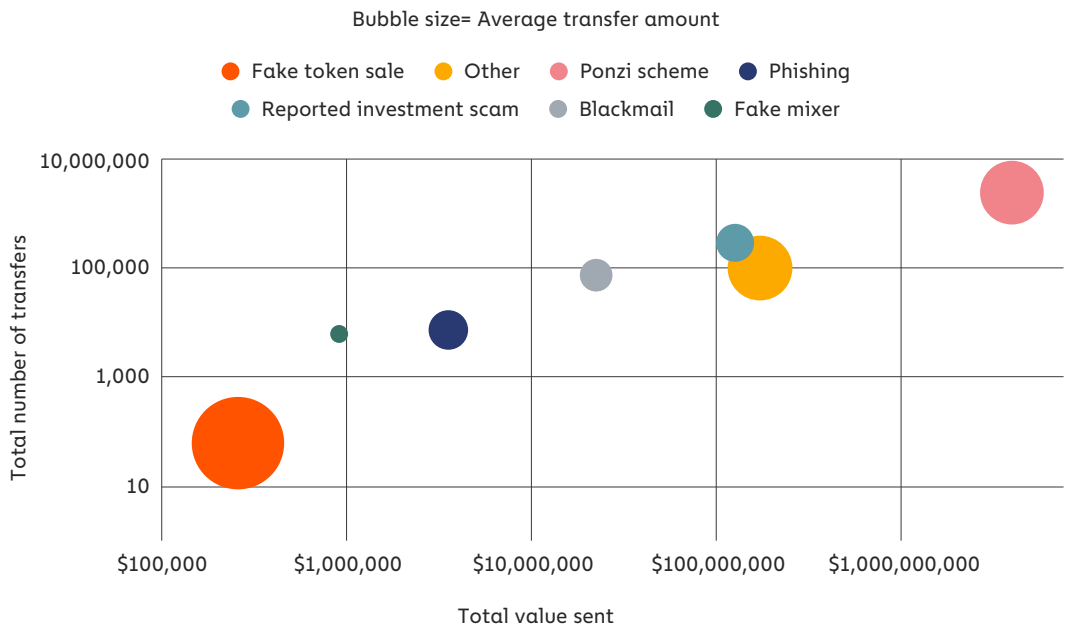
Currencies included: BTC, ETH, USDT, BCH, LTC, OMG, PAX, ETC

2019 was the biggest year for cryptocurrency scams yet. After drop in scam revenue in 2018, scammers more than tripled their revenue in 2019, bringing in $4.30 billion worth of cryptocurrency from millions of victims.

The vast majority of this came from Ponzi schemes, which accounted for 92% of the bottomline total. Blackmail scams also grew significantly for the second straight year, nearly quadrupling their total 2018 revenue to $22.5 million. This may be an underestimate however, and while blackmail scams represent a small portion of the total, they're a growing, scary threat that affects people outside the cryptocurrency ecosystem.

The total funds figure doesn't tell the whole story though. We can learn more about the strategy behind each scam category by analyzing how many victims they targeted, which we approximate by the number of individual transfers to scam-affiliated addresses and the average amount taken from each victim.

Types of scams by total funds received, number of transfers, and average transfer size, 2019



Currencies included: BTC, ETH, USDT, BCH, LTC, OMG, PAX, ETC

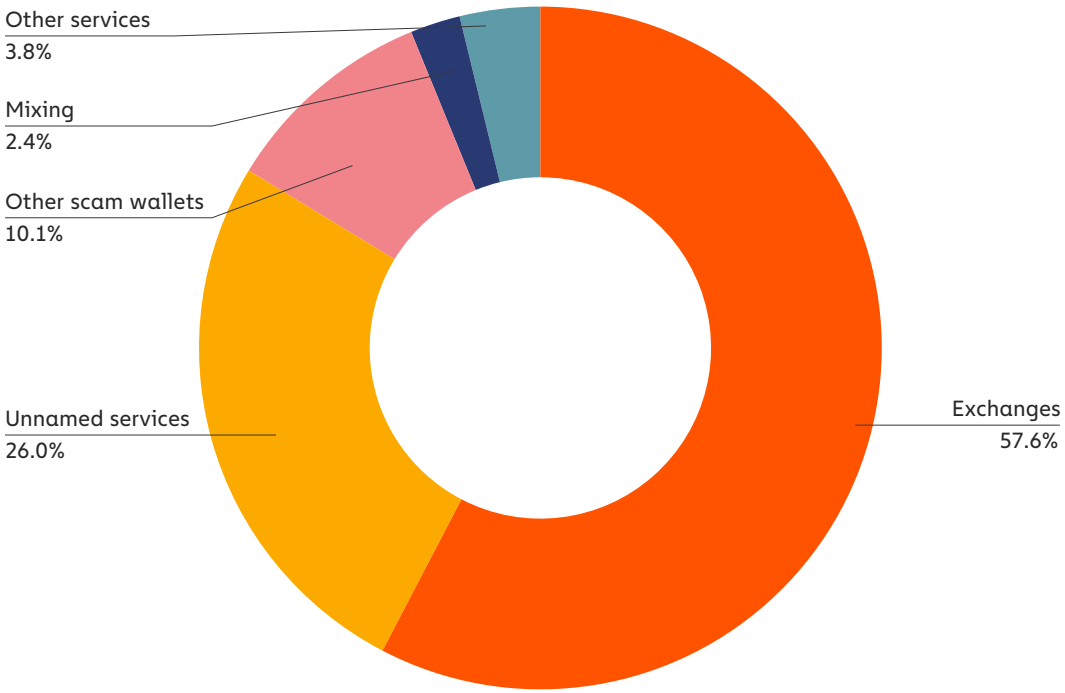
From this data, we see that Ponzi schemes are driven by collecting relatively large payouts from a high number of users. Over 2.4 million individual transfers were made to Ponzi schemes, a number that becomes even more incredible when you realize that the data above reflects just **six individual Ponzi schemes** in 2019. It's also worth noting that the 2.4 million figure is based on an ongoing investigation into 2019's most prominent scams — some media reports indicate that the PlusToken scam alone, which makes up the majority of Ponzi scheme revenue on this graph, reached 3 million victims on its own. While we can't confirm that number today, we'll explore PlusToken in-depth later in this section, including the scam's promotional strategies, laundering mechanisms, and potential impact on the Bitcoin market at large.

The average transfer to Ponzi schemes was $1,676 worth of cryptocurrency, second only to the $4,188 taken in the average transfer to fake token sales. These numbers make sense based on what we know about Ponzi schemes. Scammers promise massive, outsized returns for those who invest in their fake companies, convincing victims to invest substantial sums in the hopes of a big payout. Scammers typically promote themselves aggressively on social media and elsewhere, going so far as to build sophisticated websites and run aggressive marketing campaigns to attract investors.

Blackmail scams on the other hand are a bit different. For context, in the blackmail scams we're discussing here, scammers typically email victims claiming to have hacked their computer and stolen sensitive information on them, which they threaten to send to the victim's family and friends unless they pay a ransom in cryptocurrency. In nearly all of these cases, the scammers are bluffing and have no actual blackmail material. But they also typically ask for small enough amounts of money that some victims are willing to pay to assuage their fears.

The average payment amount for blackmail scams is just $306 per transaction, much lower than the average for Ponzi schemes. And while these scams as a whole affected a similar number of victims to Ponzi schemes, it's crucial to note that our blackmail data represents hundreds of individual scam campaigns. We'll explore the economic strategy, tactics, and questions around the perpetrators of blackmail scams in greater detail later in this section.

Destination of funds sent from scam wallets, 2019



Currencies included: BTC, ETH, USDT, BCH, LTC, OMG, PAX, ETC

Like most crypto criminals, scammers favor exchanges to cash out their funds. 57.6% of funds taken in from scams were cashed out through exchanges we've rated as having a standard risk level, meaning they comply with financial regulations and collect KYC (Know Your Customer) info on users. That suggests there may be an opportunity for investigators to trace these funds to specific addresses at those exchanges using blockchain analysis and subpoena them to investigate scammers and potentially recover funds for victims. It's also worth noting that most of the addresses comprising the "Unnamed Service" portion of the chart are likely high-risk exchanges that don't follow KYC processes. We base this guess on the fact that the transaction activity of these addresses mirrors that of other exchanges and have high exposure to illicit entities.

The anatomy of a $2+ billion Ponzi scheme: Inside PlusToken

Based in China, PlusToken presented itself as a cryptocurrency wallet that would reward users with high rates of return if they purchased the wallet's associated PLUS cryptocurrency tokens with Bitcoin or Ethereum. The scammers claimed those returns would be generated by "exchange profit, mining income, and referral benefits." PlusToken would go on to be listed on several Chinese exchanges and hit a peak price of $350 USD, raking in "investments" from millions.

Chinese media reports that the scam attracted over **$3 billion worth of cryptocurrency**. We tracked a total of 180,000 BTC, 6,400,000 ETH, 111,000 USDT, and 53 OMG (omisego) that went from scam victims to PlusToken wallets, equating to roughly $2 billion. Either figure would make PlusToken one of the largest Ponzi schemes ever.

While six individuals connected to PlusToken were **arrested in June**, the stolen funds have continued to move through wallets and be cashed out through independent OTC brokers operating mostly on the Huobi platform, showing that one or more of the scammers are still at large.

Relentless self-promotion: How PlusToken reached 3+ million victims

One of the most remarkable things about PlusToken was its aggressive marketing strategy. The PlusToken scammers convinced millions of people to invest — mostly in China, Korea, and Japan — but even some as far away as Germany and Canada.

Dovey Wan, a noted expert in the Chinese cryptocurrency industry, provided a great deal of insight into PlusToken's promotional strategies in an **interview with Bitcoin Magazine** earlier this year. She emphasizes that most of the investors were ordinary people without much background in cryptocurrency. PlusToken reached these people primarily through WeChat, China's most popular messaging app, where they heavily promoted promises of 10-30% returns in public groups. Crucially, PlusToken spent lots of energy promoting not just its product, but also beginner-level materials teaching users how to purchase their first Bitcoin. That strategy speaks to the low levels of cryptocurrency sophistication amongst victims that the scammers were able to exploit.

But that wasn't all. PlusToken supplemented its WeChat promotion with sophisticated campaigns designed to both reach more users and lend legitimacy to the company. PlusToken hosted several in-person meet-ups educating attendees on the company and on cryptocurrency as a whole. It also took out ads in supermarkets and other physical spaces. The PlusToken app itself was another marketing channel. In addition to a slick interface that let users easily convert Chinese yen into Bitcoin, Ethereum, and PLUS, it also featured a gamified referral program in which users were rewarded for convincing others to sign up. One of PlusToken's founders even **attended a charity event** with Prince Charles of England, taking pictures with him that later spread and further bolstered PlusToken's image.

Overall, PlusToken drew victims in with a marketing strategy resembling that of sophisticated, legitimate tech companies, enabling them to accomplish three things:

- Present cryptocurrency novices with an almost too good to be true high-yield investment opportunity in the space.
- Spread the message far and wide through several online marketing channels, including customer referrals.
- Project the image of a legitimate, promising cryptocurrency startup by allowing users to see the "employees" behind the company — this tactic appears to have been particularly effective at maintaining the company's air of legitimacy even as rumors of a scam surfaced prior to users being locked out of the PlusToken app.

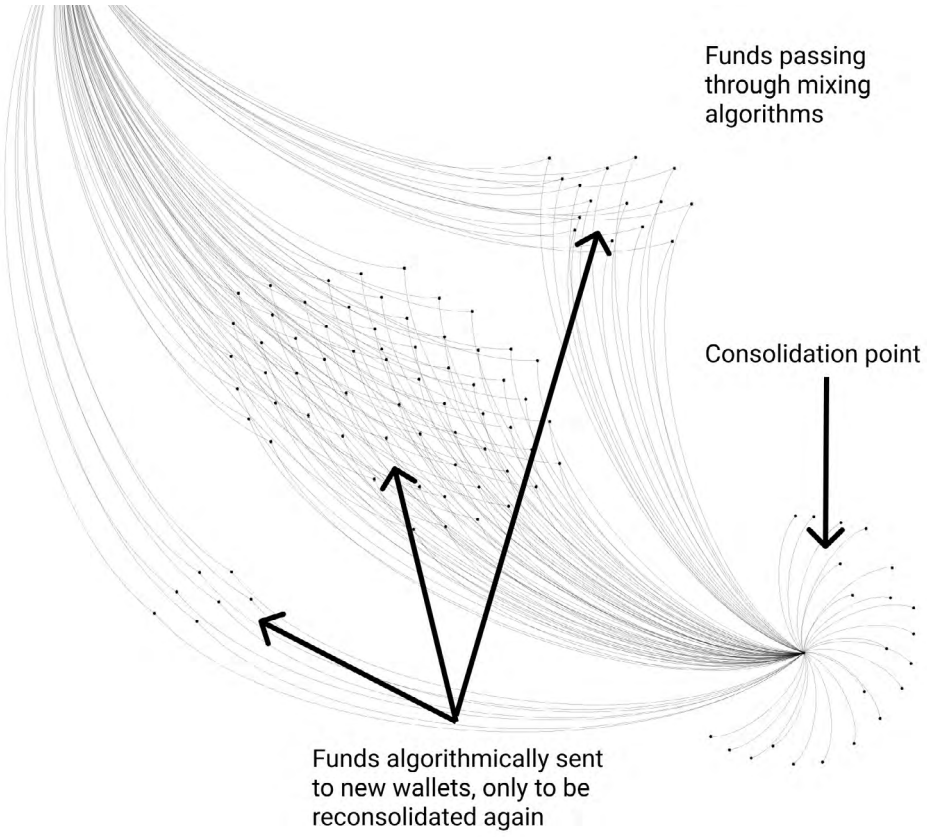
Law enforcement agencies and regulators should be on the lookout from now on, as other scammers may try to imitate PlusToken's brazen strategy.

How the PlusToken scammers utilize mixers, OTC brokers, and more to launder and cash out funds

While we tracked $2 billion worth of various cryptocurrencies that victims sent to the PlusToken scammers, some of that money was paid out to early investors, presumably to maintain the illusion of high returns while PlusToken presented itself as a legitimate company. In many cases, it's difficult to tell whether transfers made by the PlusToken scammers were going to those early investors or to addresses under their own control. Nonetheless, we've tracked roughly 800,000 ETH and 45,000 BTC we can definitively say the scammers transferred to their own addresses to launder. They've cashed out at least 10,000 of that initial 800,000 ETH, while the other 790,000 has been sitting untouched in a single Ethereum wallet for months.

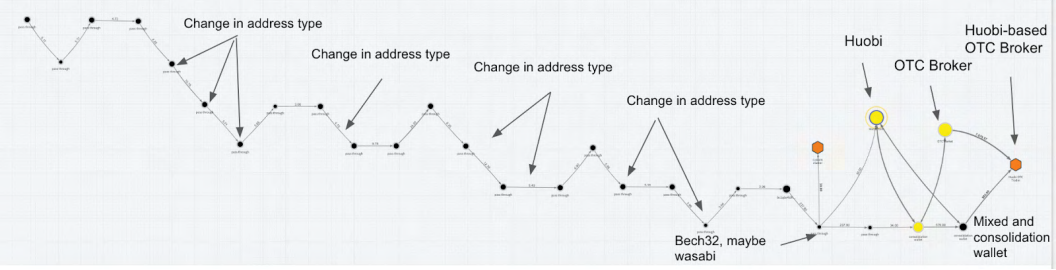
The flow of the 45,000 stolen Bitcoin is more complicated. So far, roughly 25,000 of it has been cashed out. The other 20,000 is currently spread out across more than 8,700 cryptocurrency addresses, which speaks to the high level of effort the scammers put into obfuscating the movement of funds. The scammers have transferred the Bitcoin more than 24,000 times, using more than 71,000 different addresses — and that's not even counting cash outs or transfers to off-ramps such as exchanges.

Many of those transactions were conducted through mixers like Wasabi Wallet, which utilizes the CoinJoin protocol to make it more difficult to trace the path of funds. You can see an example in the Chainalysis Reactor graph below.



Here, we see that the funds are split off into large groups of new unique addresses, and re-consolidated later, which is activity typical of a mixer.

At other points, the scammers utilized peel chains and other complex movements to obfuscate the path of funds. Peel chains are strings of transactions commonly used for money laundering, in which entities send funds through several wallets in quick succession, usually breaking off small amounts to cash out at each step and sending the majority on to the next wallet.



The graph above is a great example of the PlusToken scammers' obfuscation attempts. The funds start in the wallet in the upper left hand corner, and move to the right. Diagonal movements represent a change in the type of service used, while vertical movements represent the use of a mixer.

In the end, the funds moved to the address of an OTC broker operating on Huobi to be liquidated — that's how nearly all of the funds so far have been cashed out. For reference, OTC (Over The Counter) brokers facilitate trades between individual buyers and sellers who can't or don't want to transact on an open exchange. OTC brokers are typically associated with an exchange but operate independently. Traders often use OTC brokers if they want to liquidate a large amount of cryptocurrency for a set, negotiated price.

Some OTC brokers have significantly lower KYC requirements than most exchanges, which can make them attractive for criminals like the PlusToken scammers. Compliant exchanges monitor transactions and keep customer information on file so that they can report suspicious activity and comply with subpoenas from law enforcement. But OTC brokers play by different rules. While many are legitimate, others take advantage of lower KYC requirements to offer service to users with illicit funds. Some even specialize in the movement and laundering of criminal money.

And in this case, as we'll examine below, these cashouts via OTC brokers may be driving down the market price of Bitcoin.

Are PlusToken scam liquidations driving down the price of Bitcoin?

So far, the PlusToken scammers have cashed out at least $185 million worth of stolen Bitcoin via OTC brokers. Those who analyze cryptocurrency markets know that large liquidations generally tend to depress the price of Bitcoin, and **others have asked** if PlusToken-related cashouts are dragging down Bitcoin's price. We decided to run our own study of Bitcoin's price in relation to PlusToken cashouts via Huobi OTC brokers to try and answer that question.

For this analysis, we started by plotting Bitcoin's price listing on Huobi against two measures of PlusToken's Bitcoin transfers:

1. **On-chain volume**
   On-chain volume is the amount of Bitcoin moving from wallets controlled by the PlusToken scammers to any of 26 prominent OTC brokers on Huobi that we've previously identified as dealing with illicit funds.

2. **Trade volume**
   Off-chain volume refers to the amount of Bitcoin for Tether traded on Huobi. We chose this metric because we know from our analysis that PlusToken scammers have consistently exchanged their stolen Bitcoin for Tether, possibly converting it to fiat currency later. However, because these transfers are recorded only in Huobi's order books rather than on the blockchain, we have no way of knowing which of them are coming from the sale of Bitcoin from the PlusToken scammers as opposed to other users of the exchange.

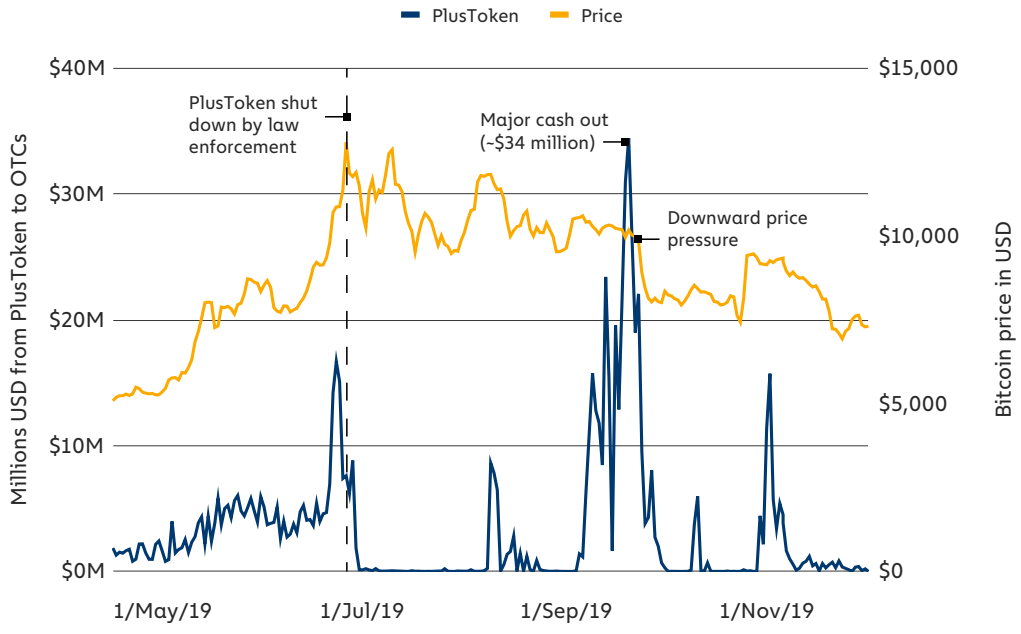
Our **hypothesis** consists of two parts:

- We expect that any uptick in on-chain volume would be followed by an uptick in trade volume, as OTC traders receive Bitcoin from PlusToken wallets and subsequently exchange it for Tether.
- We expect Bitcoin's price to fall soon after those upticks in on-chain and trade volume, as more Bitcoin is being unloaded onto the market.

Both parts of our hypothesis were proven true.

Our results

On-chain volume from PlusToken vs. Bitcoin price listed on Huobi, 16/Apr/19 - 2/Dec/19

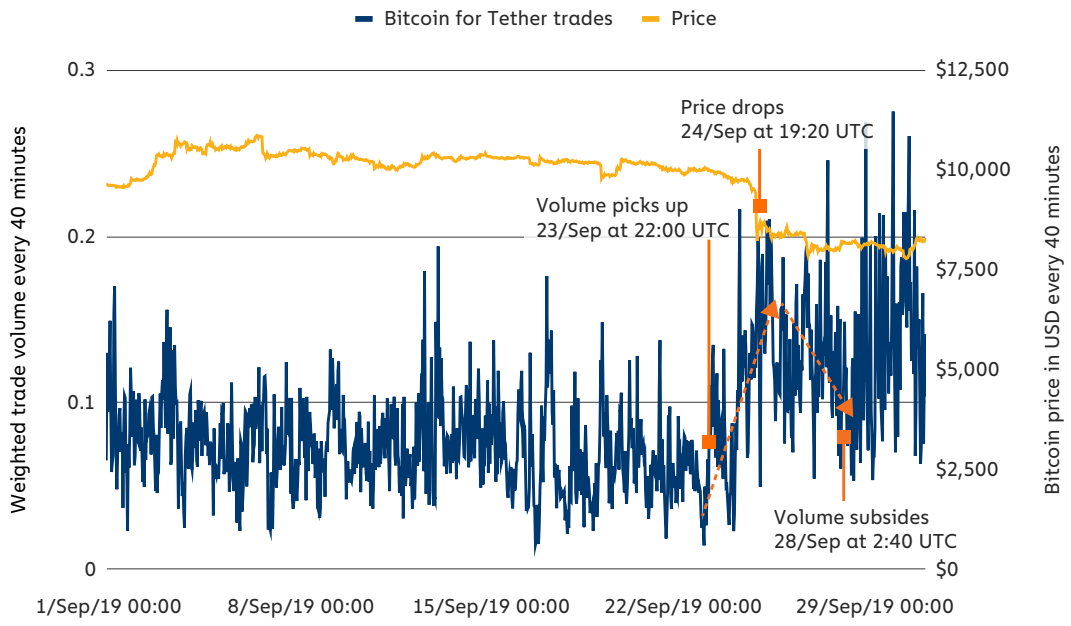


Currencies included: BTC

Above, we see that PlusToken wallets sent a steady flow of Bitcoin starting in mid-April and spiking just before the arrests in late June. After that, we see no movement until a few spikes in August, before transfers spike again and remain high throughout September. Then, we see a few more spikes in October. **As we hypothesized, spikes in on-chain flow to OTC brokers correlate with drops in Bitcoin's price.** There can be a lag, as Bitcoin that is moved on-chain to an exchange is not immediately traded. We see the best example on September 20th, when PlusToken scammers made a large cashout of roughly $34 million worth of Bitcoin. Following that transfer, Bitcoin's price drops steadily between September 24th and 26th, falling from just over $10,000 to about $8,000 and remaining there for roughly a month.

But what about trade volume? Check out the graph below.

Trade volume vs. Bitcoin price listed on Huobi, 1/Sep/19 - 30/Sep/19



Currencies included: BTC

Our hypothesis is proven correct here as well. As we expected, we see a rise in trades of Bitcoin for Tether starting on September 23rd, a few days after the PlusToken wallets sent a large volume of Bitcoin to Huobi OTC brokers. Shortly after on September 24th, the price of Bitcoin begins to drop.

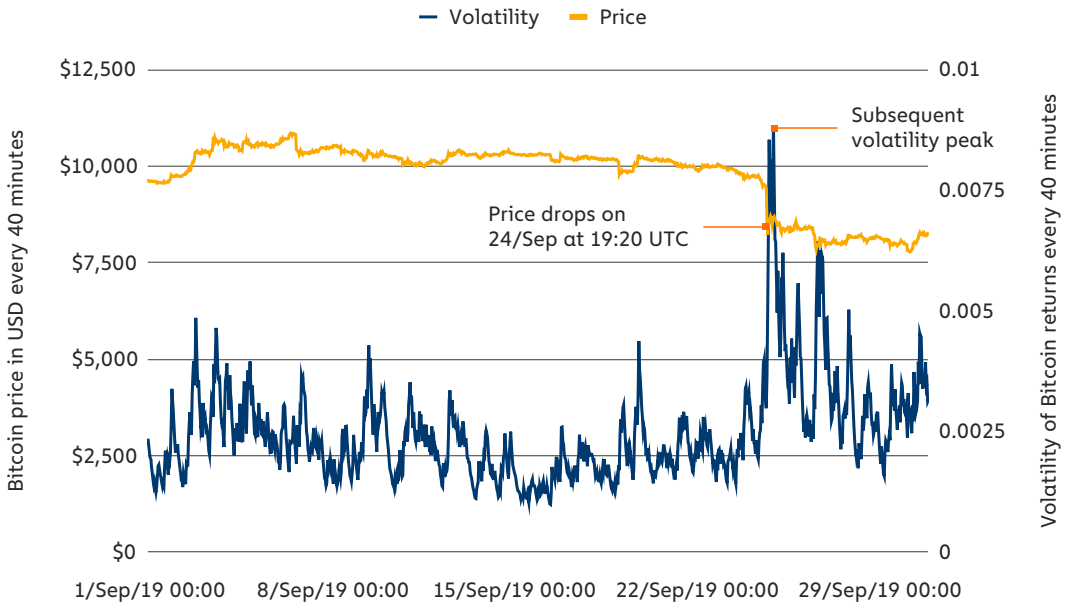
From this analysis, we can conclude that PlusToken cashouts correlate with drops in Bitcoin's price.

CAN WE PROVE CAUSATION?

We can't say for sure that Bitcoin price drops are caused by PlusToken cashouts. It's possible that price drops follow the cashouts by coincidence but are in fact caused by something else. In an attempt to settle the question of causation, we ran a regression analysis to test how the increase in trade volume between September 23rd and 28th impacted Bitcoin's price volatility. Ordinarily, we'd test how trade volume impacts the price itself, but there's only one large change in Bitcoin price for the time period we're measuring (on September 24th).

We need a measure with more variation to look for statistical causality and ensure results aren't driven by outliers. Volatility, which measures the deviation from the average Bitcoin price at a given time, has enough variation to do that, while also giving us a sense of how the PlusToken cashouts impact Bitcoin's price.

Bitcoin price listed on Huobi vs Bitcoin price volatility on Huobi
1/Sep/19 - 30/Sep/19



Currencies included: BTC

Our regression analysis shows a positive, albeit small, statistically significant relationship between PlusToken transfers to Huobi OTC brokers and Bitcoin price volatility for the period of time between September 23rd and 28th.

The cashouts likely caused increased volatility in one of two ways. They either cause it directly by increasing the supply of Bitcoin and changing market dynamics, or indirectly by affecting traders' perception of the market. Keep in mind that PlusToken cashouts are just one of many potential influences on Bitcoin's price. Media stories, concerted market manipulation efforts, algorithmic trading errors, or any number of other factors may have contributed to volatility as well. But none of those components on their own provides a compelling explanation for the large spike in volatility in the time period we studied absent the influence of PlusToken.

Unfortunately, because it's not possible to distinguish between trades made by OTC brokers in possession of PlusToken funds and all other trades made on Huobi, we can't say for sure that PlusToken cashouts caused Bitcoin's price to drop. **However, we can say that those cashouts cause increased volatility in Bitcoin's price, and that they correlate significantly with Bitcoin price drops.**

How do we prevent this moving forward?

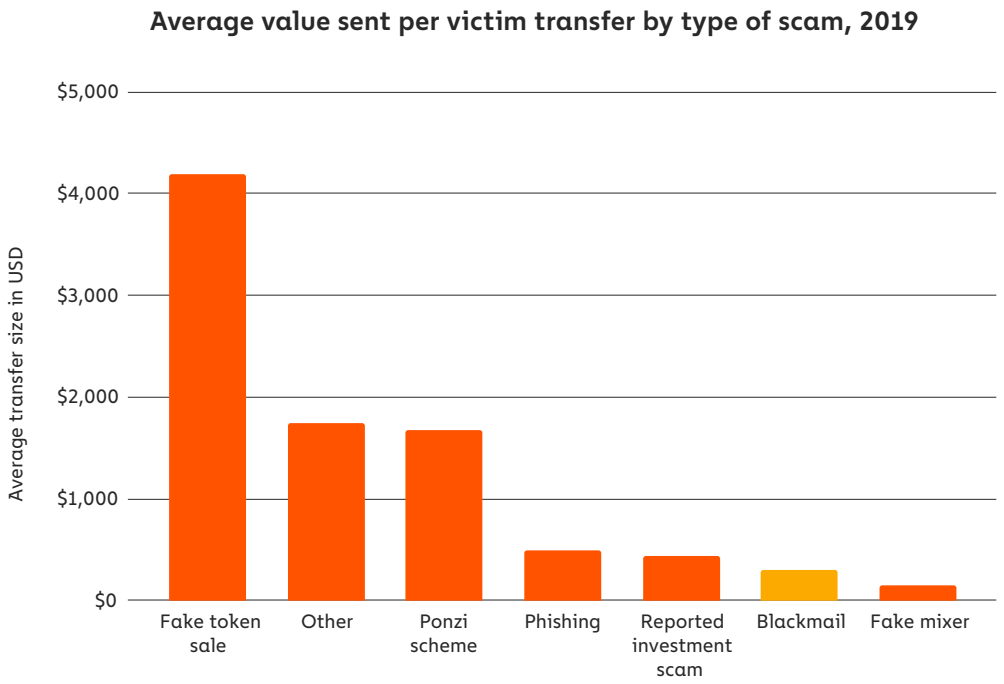
As of now, at least 20,000 Bitcoin — nearly $150 million worth — has yet to be cashed out. It'll be interesting to observe whether the relationship between those cashouts and Bitcoin's price continues. Given this analysis and the effects we've observed so far, liquidations of large amounts of illicitly obtained funds are likely to drive down the price of cryptocurrencies.

The PlusToken scam is a powerful example of how cryptocurrency scams harm the public and should alarm exchanges, law enforcement, and regulators alike. In this case, millions of fraud victims will most likely never recover the funds they were tricked into giving up. Allowing OTC brokers to operate without scrutiny gives criminals a simple, obvious way to launder their ill-gotten funds, and exchanges should conduct KYC and monitor activity. Regulators around the world should recognize this as a consumer protection issue and consider how they might apply anti-money laundering regulations to prevent scams like this from happening in the future.

The economic strategy and perpetrators behind blackmail scams

Blackmail scams, which generated the second-most revenue of any scam category, appear at first glance to operate much differently from Ponzi schemes. But as we'll explore here, they share a few key similarities.

Most blackmail scams fit the model known as "sextortion." In sextortion scams, the scammer sends the victim an email claiming to have hacked their computer and downloaded sexually compromising material, which they then threaten to send to the victim's friends and family. In reality, the hackers almost never have any blackmail material. Instead, hackers rely on fear, sometimes scaring the victim by including a password of theirs, usually obtained from a publically available data breach.



Currencies included: BTC, ETH, USDT, BCH, LTC, OMG, PAX, ETC

Blackmail scams function similarly to spam campaigns, in that the scammers blast their threatening emails out to as large an audience as possible and ask them to send a relatively small amount of money. Since the costs to run the scam are so minimal, they only need a small percentage of targets to pay up in order to turn a profit. The lack of expertise required to run a sextortion scam and huge number of victims targeted across multiple campaigns could lead one to believe that a fragmented group of low-level individual criminals are the ones behind these attacks. But research suggests this may not be the case.

Earlier this year, a team of cybersecurity researchers published a paper analyzing over 4.3 million sextortion emails sent over an 11-month period and payments sent to the Bitcoin addresses to which victims were instructed to send funds in those emails. Their work sheds light on the economics of sextortion campaigns, and also suggests that there may in fact be larger, centralized groups behind the most successful sextortion campaigns.

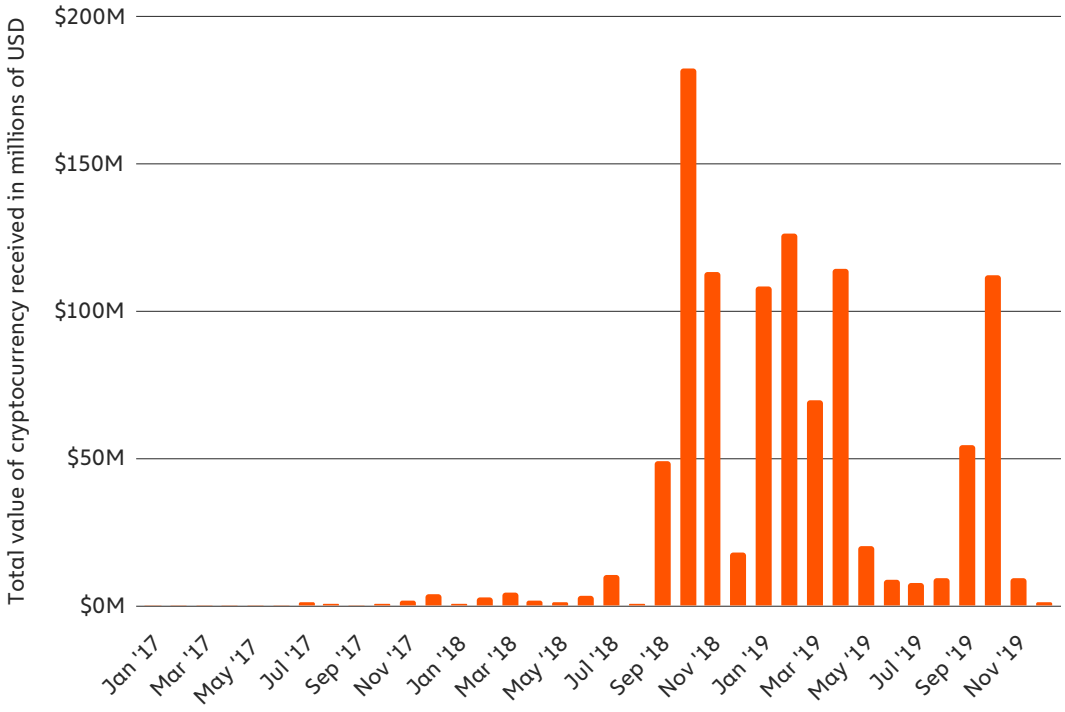
Using textual analysis, the team sorted all 4.3 million sextortion emails into 35 separate campaigns. Interestingly, they found that even within individual campaigns, scammers vary the amount of Bitcoin they ask for based on the victim's home country, approximated by the language in which the email was written.

The Bitcoin addresses analyzed received only 2,346 payments during the period studied. We should note that the 4.3 million emails analyzed were caught by spam filters and never reached the intended victim, meaning that these 2,346 payments came from victims outside of that set of emails. Nonetheless, the relatively low number of payments compared to the high number of emails we do know about suggest an extremely low success rate for sextorion scam emails. The low probability of payment illuminates the need for such high volumes of targets. Nonetheless, the researchers estimate that those payments added up to a total revenue of roughly $1.3 million, making sextortion one of the most profitable types of spam campaigns.

Perhaps most interestingly, the researchers found several instances of Bitcoin addresses being reused across the 35 campaigns they identified — enough overlap, in fact, to suggest that one entity was behind all of them. The researchers believe this could be a function of individual scammers renting botnets from the same provider in order to send the blackmail emails. For this to be true, it would mean that those botnets have been modified to generate Bitcoin addresses and possibly to perform Bitcoin transactions, but that's yet to be confirmed. If this were true, that botnet owner is likely receiving a cut of each payment made by victims.

Whether the overlap in addresses between sextortion campaigns is due to a common botnet provider or really is evidence that one entity is controlling all the campaigns, it suggests a degree of centralization similar to what we see in Ponzi schemes. In either scenario, one technologically sophisticated entity sits at the top of the sextortion food chain, taking in most of the money.

Total monthly funds received by blackmail wallets, Jan 2017-Dec 2019



Currencies included: BTC, ETH, USDT, BCH, LTC, OMG, PAX, ETC

We still need to do more research to understand the exact level and nature of centralization between sextortion scammers. But what's clear is that these scams are on the rise. Similar to Ponzi schemes, blackmail scams are an example of how bad actors can trick less sophisticated, vulnerable individuals into giving them money, with cryptocurrency being the transaction tool of choice. We believe the best way to fight blackmail scams is with education. Exchanges and other on-ramps for first-time cryptocurrency users need to warn their customers of the various scams they may encounter, including blackmail scams like sextortion, and help them understand what options they have besides paying and moving on. This would not only save individual victims money, but could also disincentivize sextortion scams altogether by helping a critical mass of potential victims understand that they don't need to pay.

We need to solve scams

Cryptocurrency scams represent a significant danger to consumer protection, and the growth of this activity in 2019 calls for increased action from regulators, law enforcement, and exchanges alike.

Indeed, Director Kenneth A. Blanco of the United States Financial Crimes Enforcement Network (FinCEN) recently **commented** that "convertible virtual currency kiosk operators also have increased their reporting on activity indicative of scam victims, particularly new customers with limited knowledge of CVC, including the elderly."

Luckily, there are actions for all parties to take. For instance, exchanges may want to consider preventing payment to known scam-affiliated addresses, or pushing warnings to users if they're going to send funds to an address owned by an entity that resembles a scam such as a Ponzi scheme — this could feasibly be implemented with a blockchain analysis tool like Chainalysis KYT.

On the government side, regulators need to be aware of how these scams function and how players like OTC brokers fit in so that they can craft more effective consumer protection laws. Law enforcement needs to be a part of that conversation as well, and should also encourage victims of these scams — especially the Ponzi schemes and sextortion scams that affect so many — to come forward with the Bitcoin addresses of those who have victimized them. Agents may be able to track down scammers who make transfers to compliant exchanges, and if victims come forward fast enough, they may even be able to recover funds.

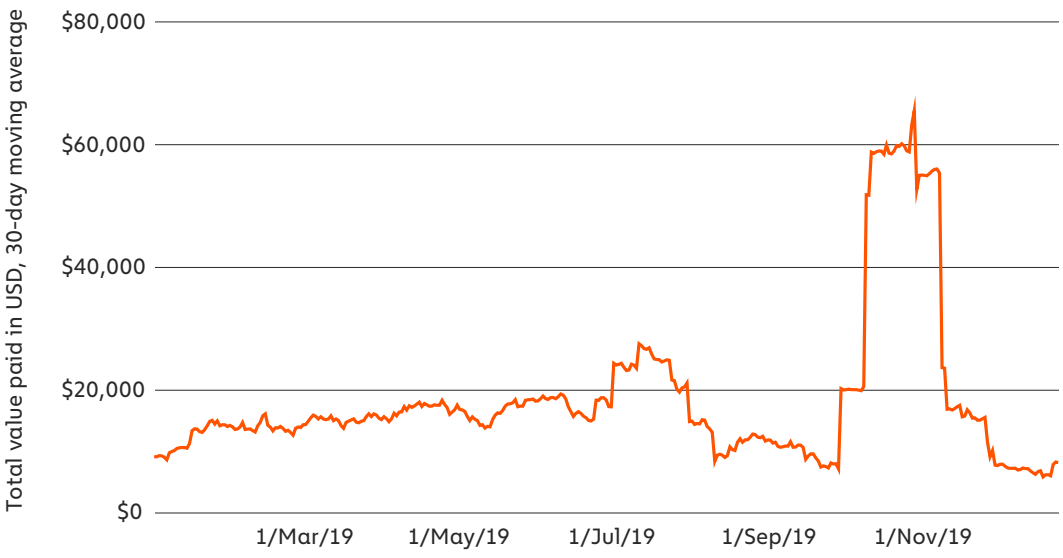
Ransomware

Ransomware Goes Mass Market

On December 13, 2019, the city of New Orleans was forced to declare a **state of emergency** after its computers were shut down in a ransomware attack. By December 19, the downtime caused by the attack had already cost the city **over $1 million**. Unfortunately, this story is all too familiar. Local governments around the world, from Baltimore to Johannesburg, have suffered extensive economic damage from ransomware attacks, not to mention hundreds of hospitals, schools, businesses, and **even the United States Military**.

Ransomware attacks are on the rise, but it's difficult to calculate their impact. According to statistics **posted** by the U.S. Department of Homeland Security, more than 4,000 ransomware attacks have taken place daily since 2016, a 300% increase over the approximately 1,000 attacks per day seen in 2015. **A report from McAfee Labs** in August stated that ransomware attacks more than doubled year over year. These figures likely underestimate the true scope of the problem, as many businesses simply opt to pay the ransom without reporting the attack. In fact, some companies worry that acknowledging a ransomware attack could **drive down their share price**. In addition to the direct costs of ransom payment estimated below, victimized businesses must also account for the indirect costs of downtime.

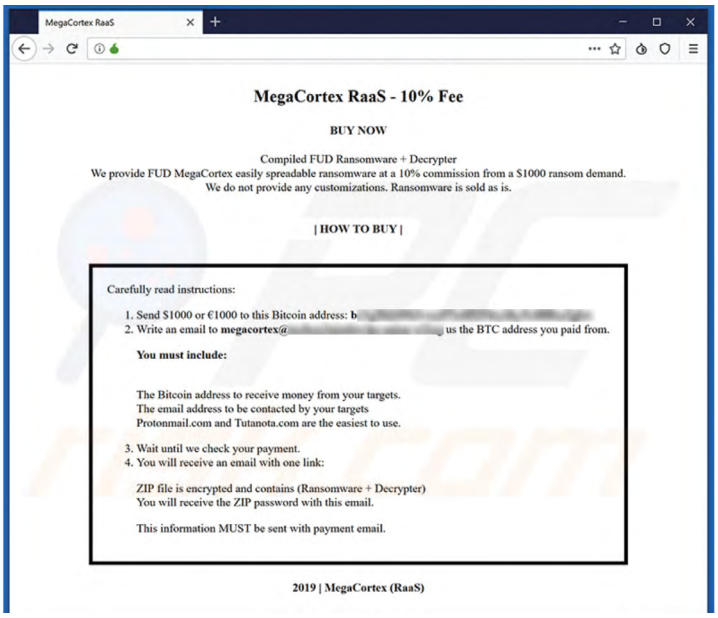
Total value paid to ransomware wallets, 30-day moving average, 2019



Currencies included: BTC

Our data shows a total of just over $6.6 million paid to ransomware-affiliated addresses in 2019, largely driven by an October surge in attacks carried out using the Bitpaymer, Ryuk, and Defray777 ransomware strains. However, this yearly total is almost certainly an underestimate. Even with blockchain analysis, it's difficult to quantify the number of ransoms paid if victims don't report attacks.

The problem is compounded by the prevalence of ransomware as a service (RaaS). Many hackers who develop ransomware technology now allow less sophisticated hackers to rent access to it, just as a business would pay a monthly fee for software like Google's G-Suite. The key difference is that the builders of the ransomware also get a cut of the money from any successful attack. Below is an example of an ad for a new RaaS strain called MegaCortex, explaining the cost structure and process for new buyers to get started.



MegaCortex RaaS - 10% Fee

BUY NOW

Compiled FUD Ransomware + Decrypter
We provide FUD MegaCortex easily spreadable ransomware at a 10% commission from a $1000 ransom demand.
We do not provide any customizations. Ransomware is sold as is.

| HOW TO BUY |

Carefully read instructions:

1. Send $1000 or €1000 to this Bitcoin address: b[redacted]
2. Write an email to **megacortex@**[redacted] us the BTC address you paid from.

You must include:

The Bitcoin address to receive money from your targets.
The email address to be contacted by your targets
Protonmail.com and Tutanota.com are the easiest to use.

3. Wait until we check your payment.
4. You will receive an email with one link:

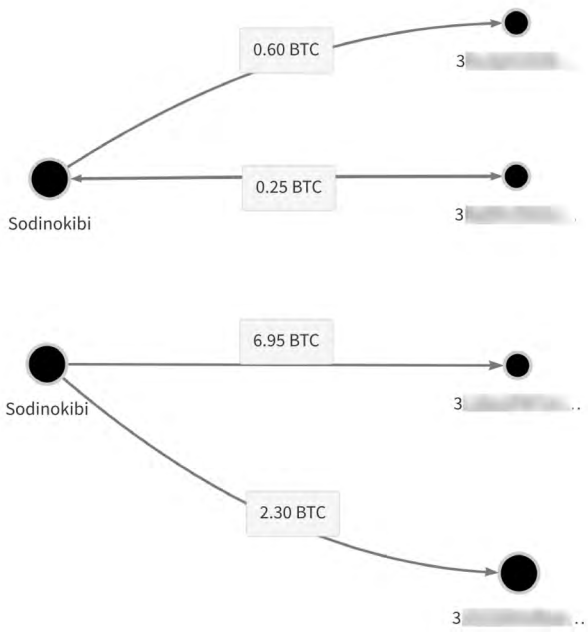
ZIP file is encrypted and contains (Ransomware + Decrypter)
You will receive the ZIP password with this email.

This information MUST be sent with payment email.

2019 | MegaCortex (RaaS)

Source: ***PCRisk.com***

The Chainalysis Reactor graph below shows two examples from one of 2019's most popular RaaS strains, Sodinokibi. In both cases, the Sodinokibi RaaS user on the left sends 70-75% of ransoms taken to one address, likely their own, and 20-25% to another address, likely controlled by the RaaS vendor.

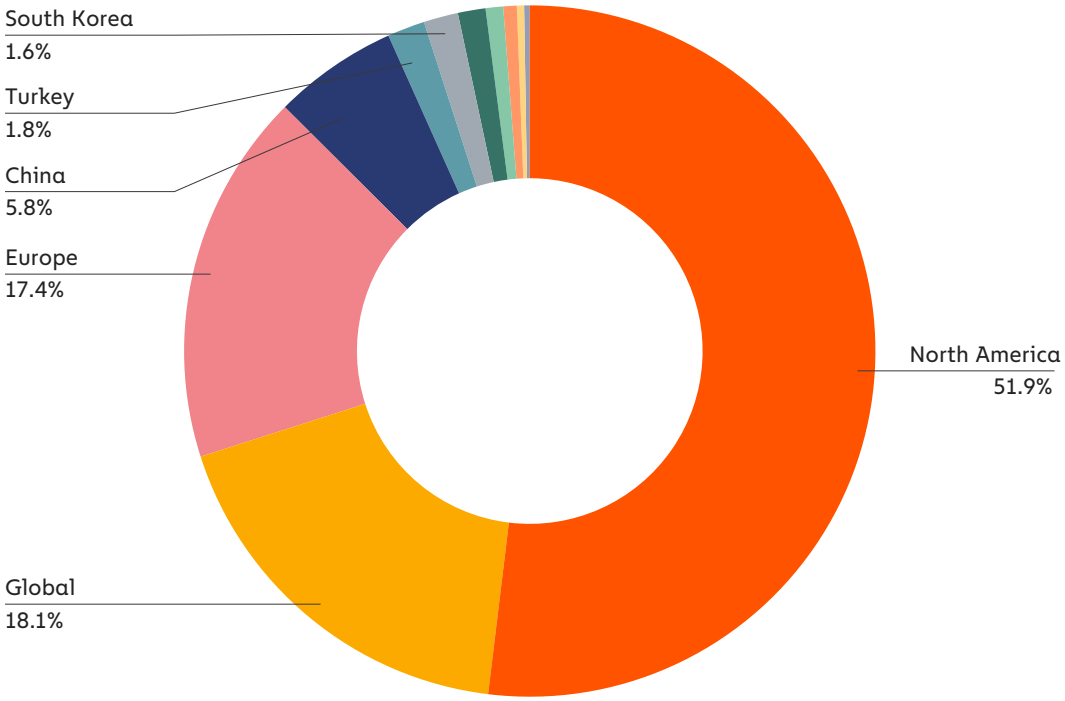


RaaS has led to more attacks, making it even harder to quantify the full financial impact. RaaS has also drastically changed the nature of ransomware attacks themselves, especially in terms of the size of ransoms requested and typical victim profile. We'll explore how RaaS attacks differ from traditional ransomware attacks in greater detail later.

Even though we can't measure the total impact and costs of ransomware, we can analyze the data we do have on a percentage basis to understand the trends that defined 2019 and could continue into 2020.

Let's start by looking at which regions are suffering the brunt of ransomware attacks. Below, we approximated victims' location based largely on the location of the exchanges they used to pay ransoms. *

Regions by share of all ransomware payments sent, 2019



Currencies included: BTC

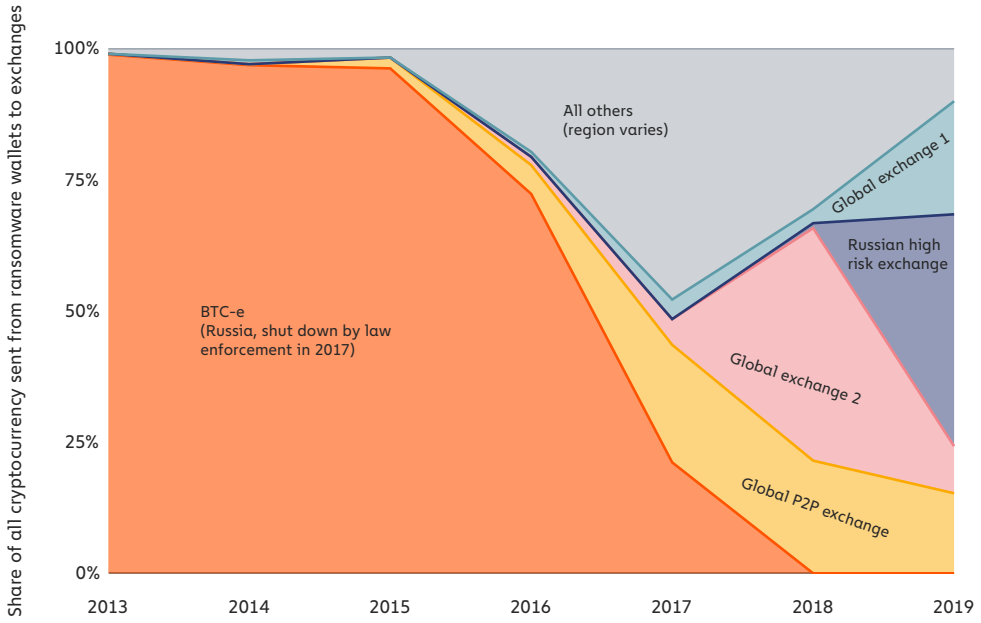
In 2019, 52% of ransomware payments we tracked came from North America, which is a large uptick from just 31% in 2018. **Outside reports** also support our finding that ransomware attacks increased in North America in 2019. The second-largest share of ransom payments came from users at global exchanges, followed by European exchanges.

* Assigning exchanges a location is a complex exercise in its own right. Since exchanges typically serve customers across borders, simply knowing where they're headquartered isn't enough to understand which market each primarily serves. There's no single indicator we use to determine an exchange's market categorization, but some of the factors we use include top fiat trading pairs, timezone analysis of transaction patterns, web traffic origin, company registration, public sourcing information, and direct conversations with the exchanges. Exchanges we place in the "global" category are those whose activity is dispersed across many regions. Likewise, exchanges under the "APAC" category serve all of the Asia-Pacific region, including China, while those under the "China" category serve only or mostly Chinese customers.

While it's tempting to do so, we decided not to try to approximate ransomware attackers' geographic locations based on the exchanges they used, as we did for victims. For one thing, attackers are likely attempting to obfuscate their activity and may be more likely to use services less tied to their own location, whereas victims are more likely to choose the exchange or service that's most convenient when paying ransoms.

As we dug into the data, we also found that ransomware attackers' cashing out activity is concentrated to just a few exchanges. Below, we'll look at the most popular exchanges for ransomware attackers over time.

Exchanges by share of all ransomware cashouts, 2013 - 2019



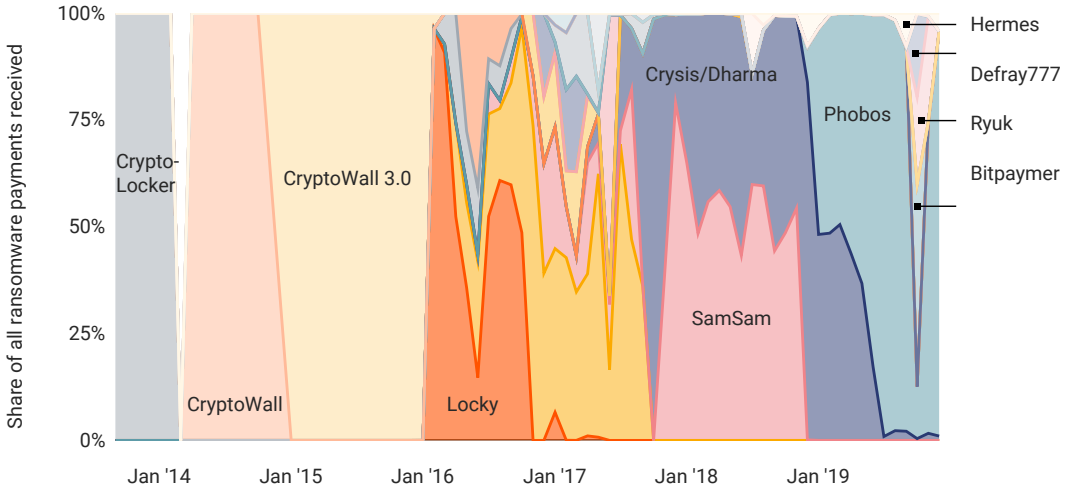
Currencies included: BCH, BTC

Digging in, we see that nearly all of the funds collected by the top ransomware strains from 2013 through 2016 were cashed out at one exchange: Russia-based BTC-e, which before its shutdown by law enforcement in 2017 was one of the most popular exchanges in the world. Given BTC-e's global reach, this data alone wouldn't be enough to conclude that most ransomware attackers in those years were based in Russia. However, we know from our on-the-ground intelligence that many of them were based in Russia, including the creators of popular ransomware strains such as CryptoLocker, Locky, and Cerber.

After BTC-e's shutdown in 2017, ransomware attackers shifted to cashing out at exchanges with large, international user bases, including one popular P2P exchange. This could be purely a function of the same attackers turning to other global exchanges after BTC-e's shutdown. However, the shift could also reflect the proliferation of RaaS, and how it enables a larger pool of lower-level cybercriminals to launch ransomware attacks. If there's a growing number of attackers around the world, it makes sense that we'd see a diversification in the number of exchanges attackers use to cash out. But we can't say for certain. It's also interesting to note that another Russia-based exchange began receiving substantial funds from ransomware addresses in 2018, soon after BTC-e's demise. Their share has continued to grow, as that exchange took in nearly 44% of all ransomware funds sent to exchanges in 2019.

Like the exchanges they use to cash out, we know that the ransomware strains favored by attackers also tend to be concentrated to just a few at any given time. You can see this on the chart below, which shows ransomware strains over time by the share of total ransomware payments they collected.

Ransomware strains by share of all ransomware payments sent, Sep'13 - Dec'19



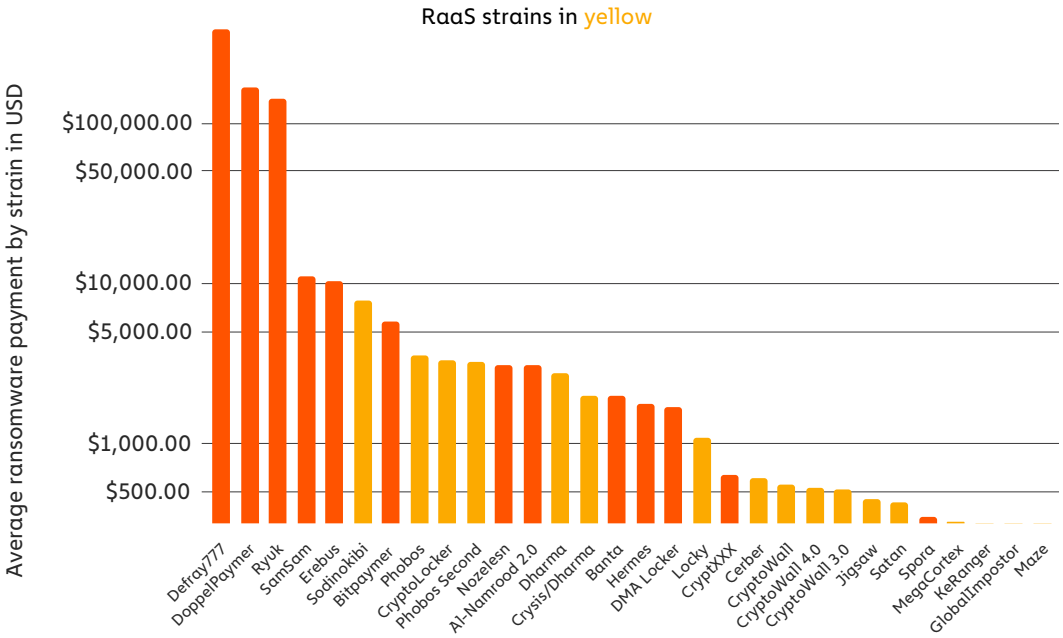
Currencies included: BCH BTC

Individual strains tend to dominate for five to seven months at a time, before dying out and being replaced by other strains. But not all strains behave the same way. In the next section, we'll explore the differences in attack patterns between the two major types of ransomware strains: traditional ransomware and RaaS.

How RaaS differs from ransomware

With RaaS on the rise, two distinct types of ransomware attacks emerge. On one end, we still see traditional, sophisticated ransomware campaigns targeted at large organizations or, in the case of nation-state aligned hackers, geopolitical targets. On the other end of the spectrum, we see RaaS attacks carried out on smaller organizations by less sophisticated hackers known as affiliates in the hacking world. "The victims definitely tend to be smaller in RaaS," says Bill Siegel, CEO of Coveware, a ransomware incident response provider. "The affiliates buying RaaS tend to be less sophisticated and have fewer resources, so they go after victims that are the lowest-hanging fruit."

Average ransomware payment by ransomware strain



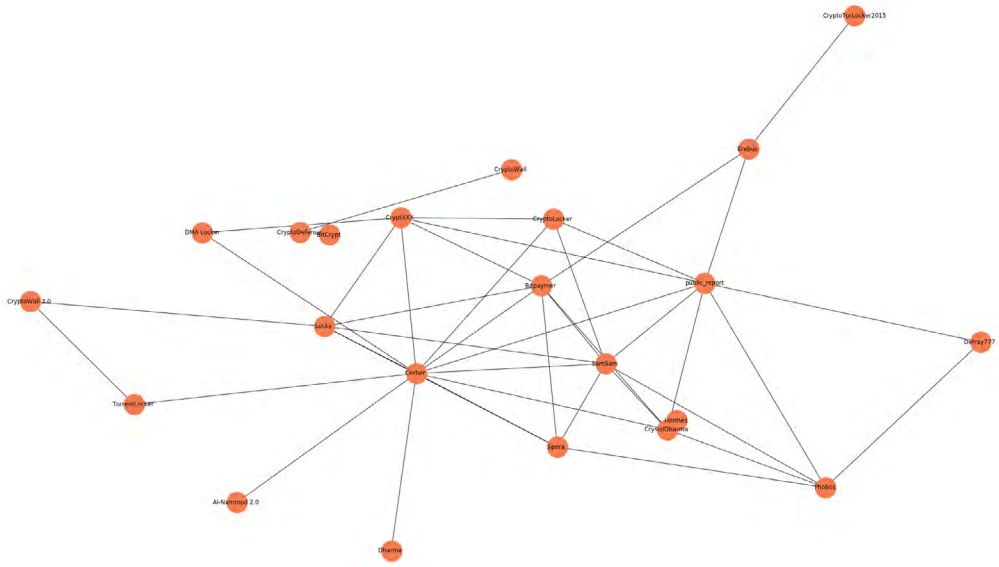
Currencies included: BCH, BTC

The data bears this out. Above, we see that the RaaS strains highlighted in yellow tend to receive lower average transfers from victims. Sodinokibi, which burst onto the scene in 2019, brings in larger transfers than any other RaaS strain, and is the only RaaS strain to cross the $5,000 average transfer barrier.

Bill and his team watched the growth and spread of Sodinokibi throughout the year first-hand, and their observations lend insight into how RaaS strains spread: "We saw the first Sodinokibi attacks in spring of 2019, which we believe were test runs for the developers and original affiliates. Soon after that, the developers were pitching Sodinokibi to select affiliates on popular hacking forums."

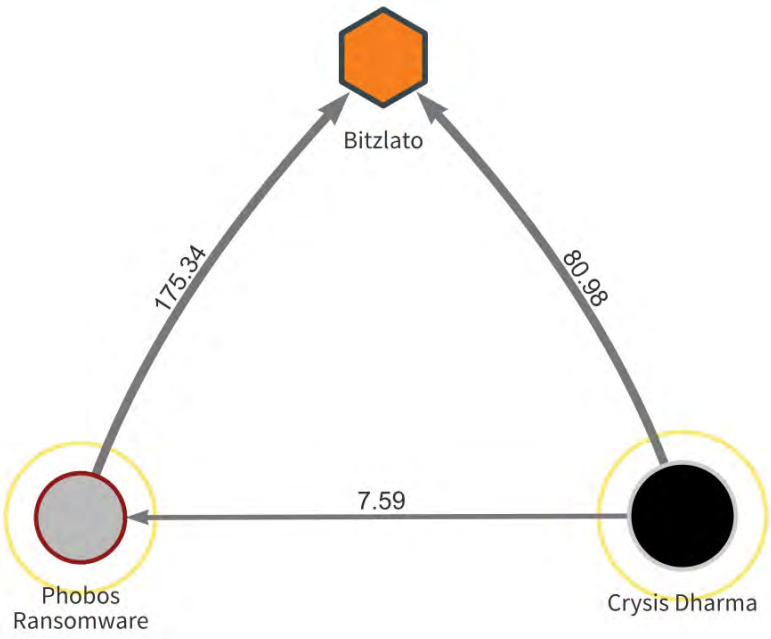
RaaS developers are able to shift careers from being on the "front lines" to running distribution and recruitment. It's the same industry, but a different role in the supply chain. Developers can make more money distributing and managing RaaS than they can pulling off attacks on their own.

The affiliates, for their part, seem perfectly willing to test the market and find strains that work for them. "Anecdotally, we definitely hear affiliates posting about their experience with different RaaS strains and looking for providers who give them a bigger cut," says Bill. We can see possible examples of this in the on-chain data.



The network graph above shows numerous transfers linking cryptocurrency addresses associated with different ransomware strains. It's possible that some of those connections are coincidental; for instance, some strains may be linked because attackers utilize the same mixing service. However, the sheer number of connections, combined with our anecdotal knowledge, suggest that some of these transactions are examples of RaaS users shopping around, or even RaaS vendors selling multiple strains. The latter could even suggest that a few large vendors are dominating the market, but we can't say for certain.

Let's take a closer look at the connections between two ransomware types – Phobos and Crysis Dharma – using Chainalysis Reactor.



Here, we see an address associated with Crysis Dharma sending funds to one associated with Phobos. Both send significant sums to the same wallet at Bitzlato, a Russian high risk exchange. While we can't say for certain, our best guess is that both addresses at the bottom are controlled by the same RaaS vendor who sells access to both Phobos and Crysis Dharma, and sends funds from both back to their account at Bitzlato.

The good news and bad news on ransomware

The bad news is that the spread of RaaS to the cybercriminal masses means firms of all shapes and sizes need to be on guard for attacks. There are now more attackers who don't need to go to the trouble of developing ransomware themselves, meaning it can be profitable for them to attack small organizations that more sophisticated hackers wouldn't bother to target. The RaaS problem could get worse as the "market" for these malicious viruses matures, with RaaS vendors seeking to differentiate themselves by releasing more and more dangerous strains.

But the good news is that any business can protect itself from ransomware attacks by diligently following a few simple steps. Bill Siegel **outlines some of these measures** on the Coveware blog. For one, businesses should save three copies of their most important documents: one to their local drive, one to a cloud backup system such as Dropbox, and one to an offline, physical storage unit such as a USB or external hard drive. That way, the files you need can survive in the event you are attacked. In order to prevent attacks from happening, Bill recommends businesses follow best practices such as updating their operating systems frequently to get new security patches, using strong antivirus software, and enabling security measures such as two-factor authentication and password managers.

In the event your business does fall victim to a ransomware attack, Bill outlines **a few steps** to take immediately. First, you should isolate any affected machines by disconnecting them from any networks they're connected to, such as wifi or bluetooth, and powering them down. Second, close all remote desktop protocol (RDP) ports, as they're a common vector for ransomware attacks. Finally, update all administrative and user credentials, so that hackers lose whatever access they have to your systems. From there, you should restore as much of your data as possible from backups. Bill, **along with the FBI**, recommends not paying ransoms to attackers unless there's no other way for your business to regain crucial data.

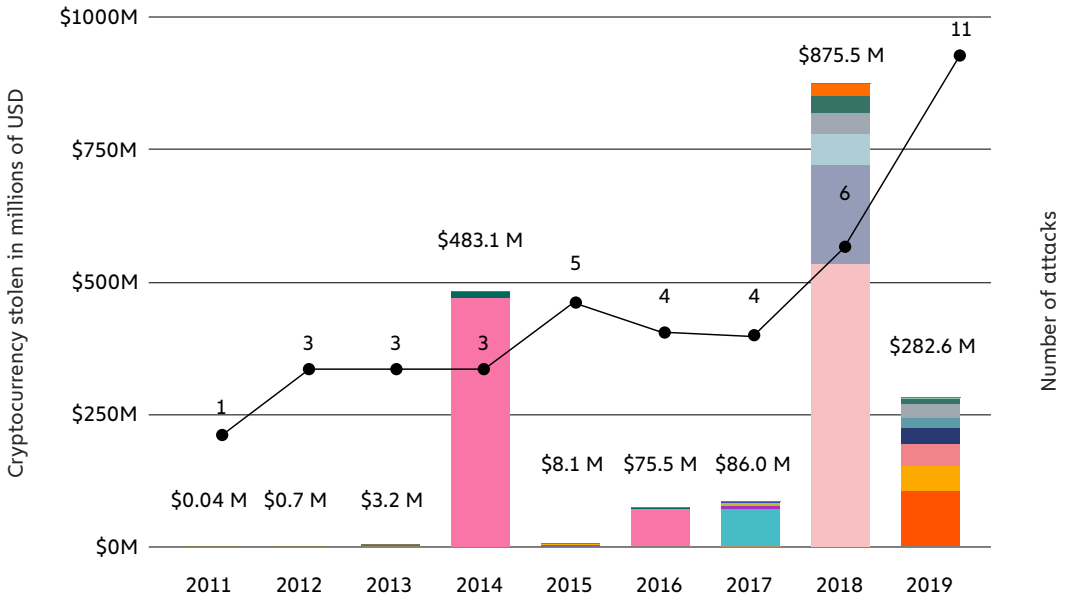
We also implore any company hit with ransomware to report the attack immediately. While it can feel scary to come forward and admit that your business has become a victim, it's difficult for law enforcement and the cybersecurity industry to understand the full scope of the problem and dedicate the appropriate resources to address it with so many businesses choosing not to report. That fear of scrutiny ultimately helps ransomware attackers stay under the radar and claim more victims. Given the number of prestigious organizations hit with ransomware, from FedEx to Britain's NHS to countless local governments, we think it's time to remove the stigma associated with these attacks — clearly, they can happen to any organization.

In the event you're attacked, you should collect as much evidence as possible, such as screenshots of ransom messages you receive, and send it to investigators so they can know what strain of ransomware you've been hit with and start formulating a response. You can also report attacks to Chainalysis directly using our brand new **ransomware reporting form**. The details you provide can help us collect more data on your attackers and work with law enforcement to stop them.

Hacks

As Exchanges Beef Up Security Measures, Hackers Get More Sophisticated

Number of exchange attacks vs. Total value stolen by year



Currencies included: ADA, BCH, BTC, ETH, EOS, LTC, NANO, NEM, USDT, XRP, and others (see "2019 Exchange Attacks Quantified"). The different colors on each bar show how much each individual hack contributed to the total stolen that year.

2019 saw more cryptocurrency hacks than any other year. But of the 11 attacks that occurred this year, none of them came close to matching the scale of major heists such as last year's $534 million Coincheck hack, or the $473 million Mt. Gox hack in 2014. Therefore, the total amount stolen from exchanges dropped sharply to $283 million worth of cryptocurrency despite the increased number of attacks.

Allow us to explain how we arrived at our final count of 2019 exchange attacks, given that other sources in the media and elsewhere may report different numbers:

- We counted both hacks involving exploitation of technical vulnerabilities and attacks conducted through social engineering or other forms of deception. *
- We only counted attacks that allowed bad actors to access funds belonging to exchanges, and not payment processors, wallet providers, investment platforms, or other types of services.

* A quick explanation on the attacks vs. hacks distinction: All hacks are attacks, but not all attacks are hacks. Hacks refer specifically to cases where a bad actor exploits a technical vulnerability in a piece of software, while attacks can include other, less technically sophisticated actions, such as phishing attacks that trick victims into downloading a malicious piece of software.

- We didn't count exchange exit scams or cases of users exploiting an exchange error, such as the pricing discrepancy that nearly allowed a Synthetix user to net over $1 billion in faulty trades.
- We only included attacks in which the amount stolen was measured and publicly confirmed by multiple sources. That means we didn't include incidents in which exchanges' user data was compromised, but no cryptocurrency was stolen. We also excluded hacks that have been privately reported to us, but are confident that including them wouldn't significantly skew the data we analyze here.

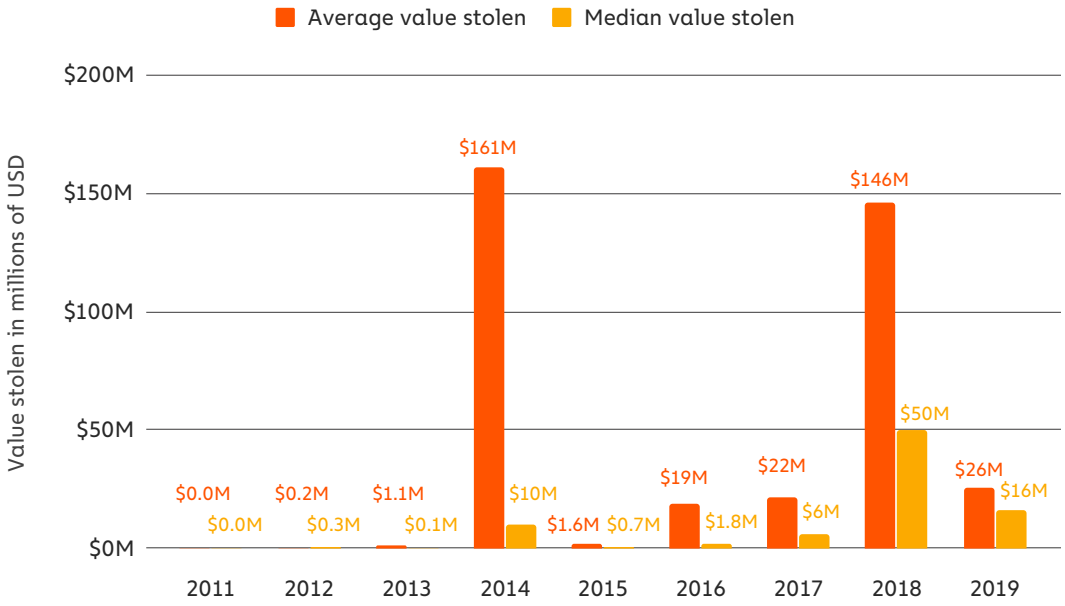
Under these constraints, nearly all of the hacks we didn't include were on smaller exchanges for relatively low amounts of cryptocurrency. Our estimates of the total amount stolen in exchange hacks are therefore likely a lower boundary, but one we believe isn't far off from the actual total.

2019 Exchange attacks quantified

Exchange attacked	Type(s) of cryptocurrency stolen	USD value reportedly stolen (rounded)	Details
CoinBene	109 different types of ERC-20 tokens	$105,000,000	Exchange denied a hack had taken place soon after the attack, but blockchain analysis shows hackers drained funds from CoinBene's hot wallet.
Upbit	ETH	$49,000,000	Hackers removed funds from the exchange hot wallet, though according to the exchange the funds did not belong to users.
Binance	BTC	$40,000,000	Hackers reportedly gained access to the hot wallet using a combination of phishing and viruses, and structured their withdrawal to pass Binance security checks.
BITPoint	BCH, BTC, ETH, LTC, and XRP	$32,000,000	Hackers gained access to the exchange hot wallet.

Exchange attacked	Type(s) of cryptocurrency stolen	USD value reportedly stolen (rounded)	Details
Bithumb	EOS and XRP	$19,000,000	Hackers withdrew funds from the exchange hot wallet. Bithumb suspects the hacker was an insider at the exchange.
Cryptopia	ETH and ERC-20 tokens	$16,000,000	Hackers reportedly gained access to tens of thousands of Cryptopia accounts. The exchange was forced to liquidate soon after the hack.
GateHub	XRP	$10,000,000	Hackers accessed nearly 100 XRP Ledger wallets.
DragonEx	BTC, EOS, ETH, LTC, USDT, XRP, and others	$7,090,000	Attackers associated with Lazarus Group gained access through sophisticated phishing attack.
Bitrue	ADA and XRP	$4,000,000	Hackers exploited vulnerability to Bitrue risk control review process to access 90 users' accounts, then used what they learned to access Bitrue's hot wallet.
VinDAX	23 cryptocurrencies	$500,000	An administrator confirmed the hack but declined to provide details.
LocalBitcoins	BTC	$27,000	In a phishing scheme, attackers placed a look-alike website on the official LocalBitcoins forum to capture login information of at least six users and stole their funds, as reported from the official LocalBitcoins Reddit account.

Average and median value stolen per exchange attack



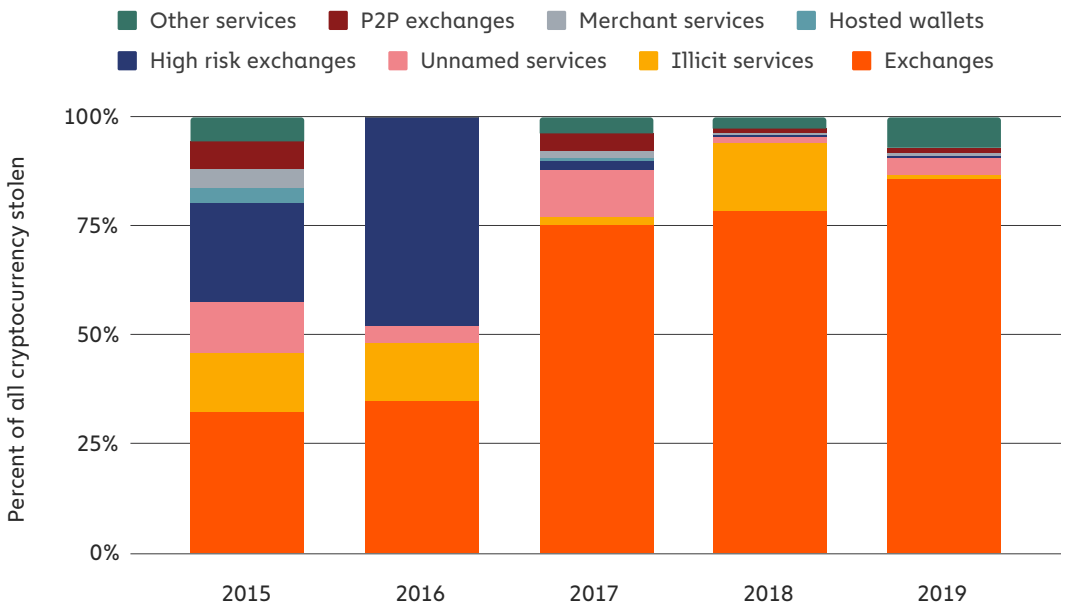
Currencies included: ADA, BCH, BTC, ETH, EOS, LTC, NANO, NEM, USDT, XRP, and others (see "2019 Exchange Attacks Quantified")

With no hacks taking in more than the $105 million stolen from Coinbene, both the average and median amount stolen per hack fell substantially in 2019, after having risen each of the three preceding years. Only 54% of the hacks we observed in 2019 took in more than $10 million, compared with all hacks in 2018. While the increase in the number of individual hacks should be concerning, the data indicates that exchanges have gotten better at limiting the damage any one hacker can do.

Where do funds go after the attacks?

Using blockchain analysis, we can analyze the movements of funds stolen in hacks to get a sense of how hackers liquidate funds. Below, we see the most common destinations for funds stolen in exchange attacks broken down by year.

Destination of stolen funds by year, 2015-2019



Currencies included: BCH, BTC, ETH, GNO, LTC, OMG, TUSD, USDT, ZIL, ZRX.
Please note that this graph doesn't include funds that sit unspent in the hackers' original wallet.

The majority of funds stolen in exchange attacks end up being sent to other exchanges, where they're likely converted into cash. However, a substantial portion of funds sit unspent, sometimes for years. In those cases, there may still be an opportunity for law enforcement to seize the stolen funds. And as we'll explore later, a small but significant — and, in 2019, increasing — portion of all funds stolen are passed through third-party mixers or CoinJoin wallets to obscure their illicit origins. Any mixed funds on the chart above, however, are categorized according to their final destination after mixing took place.

Hackers respond to exchanges' security measures

Exchanges have taken strides to better protect customers' funds from hacks and the sharp decreases in amount lost per hack indicate they've been successful. Many exchanges now keep a lower percentage of funds in less secure hot wallets, require more withdrawal authorizations, and monitor transactions more closely for suspicious activity so as to catch hacks earlier. We also know from the hacks we've helped investigate in 2019 that exchanges' increased willingness to come forward when attacked and share details with the rest of the cryptocurrency community have made it easier to track down stolen funds.

But at the same time, the most prolific hackers have also grown more sophisticated, both in how they carry out hacks and in how they launder their stolen funds afterwards. While this isn't a positive development, it suggests that the measures adopted by exchanges are effective enough to force hackers to adapt in the first place. And as we'll show you, there are concrete steps exchanges and law enforcement can take to counter hackers' new tactics.

Let's explore some of the new tactics exchange hackers have adopted by analyzing the activity of one high-profile cybercriminal organization.

How Lazarus Group became more advanced in 2019

Lazarus Group is an infamous cybercriminal syndicate linked to the North Korean government. Considered an advanced persistent threat by cybersecurity experts, Lazarus is widely believed to be behind the 2014 hack of Sony Pictures and 2017 WannaCry ransomware attacks, as well as a number of cryptocurrency exchange attacks. We can also reveal that Lazarus Group is the organization we dubbed "Beta Group" when we analyzed their exchange hacking activity in last year's Crypto Crime Report.

In 2019, Lazarus Group made three key changes to its hacking and money laundering strategies:

1. **More sophisticated phishing ploys.**
   Lazarus Group has historically relied on social engineering to attack exchanges, typically fooling employees into downloading malicious software that gives Lazarus access to users' funds. But in an exchange attack this past year, Lazarus took this strategy a step further and executed one of the most elaborate phishing schemes we've seen to gain access to users' funds.

2. **Increased use of mixers and CoinJoin wallets.**
   In 2019, hackers have more often sent funds stolen from exchanges through mixers or, to be more specific in the case of Lazarus Group, CoinJoin wallets. Mixers obfuscate the path of funds by pooling cryptocurrency from multiple users, and giving each one back an amount from the pool equal to what they initially put in, minus a 1-3% service fee. Everyone ends up with a "mix" of the funds everyone else put in, which makes it more difficult to connect the inputs to an output on the users' transactions. Many criminals use mixers to hide the source of illicit cryptocurrency before moving it to other services. CoinJoin wallets (named for the underlying CoinJoin protocol), such as Wasabi Wallet, accomplish the same thing by providing a wallet service that allows multiple users to trustlessly join their payments into a single transaction with multiple recipients.

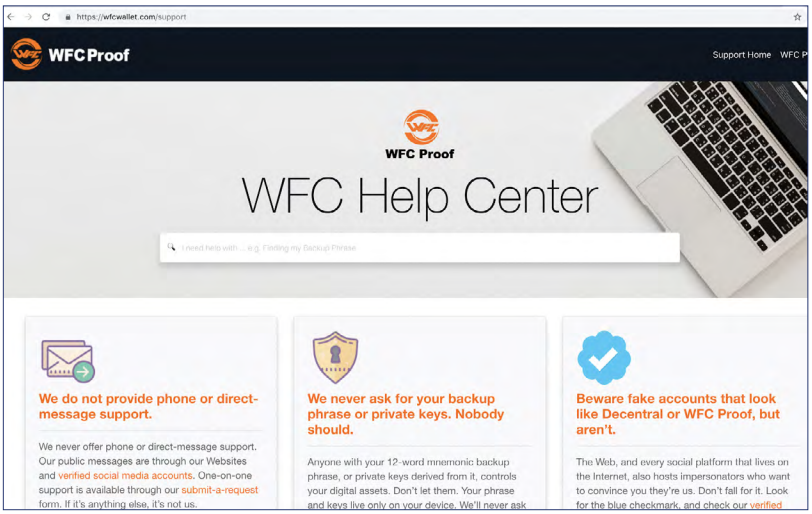
3. **Faster liquidations.**
   We've also seen hackers like Lazarus move their funds to exchanges and other services for liquidation in shorter amounts of time than in 2018. This trend could suggest that hackers in 2019 improved their money laundering capabilities, or that they're simply prioritizing faster access to stolen funds more so than in 2018.

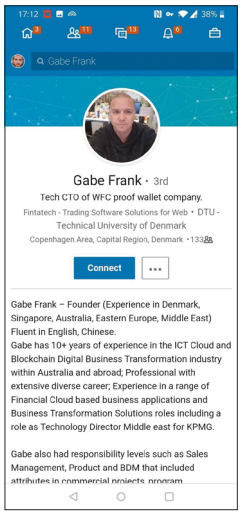
Let's look at examples of how Lazarus has employed these new tactics.

How Lazarus Group used a fake company as phishing bait

In March of 2019, hackers **breached** the Singapore-based DragonEx exchange, taking roughly $7 million worth of various cryptocurrencies, including Bitcoin, Ripple, and Litecoin. DragonEx **responded quickly**, announcing on various social media platforms that it had been hacked and releasing a list of 20 wallets to which its funds had been transferred. That allowed other exchanges to flag those wallets and freeze accounts associated with them, making it harder for the attackers to move the funds. DragonEx was also quick to contact Chainalysis and enlist our help alongside legal authorities.

While the DragonEx hack was relatively small, it was notable for the lengths Lazarus Group went in order to infiltrate the exchange's systems in a sophisticated phishing attack. Lazarus created a fake company claiming to offer an automated cryptocurrency trading bot called Worldbit-bot, complete with a slick website and social media presence for made up employees.





Lazarus even went so far as to build a software product resembling the trading bot they claimed to be selling. The key difference, of course, was that the program contained malware giving the hackers access to the computer of anyone who downloaded it. Lazarus Group hackers pitched a free trial of the software to DragonEx employees, eventually convincing someone to download it to a computer containing the private keys for the exchange's wallets. From there, the hackers were able to make off with millions.

Whereas most phishing attempts rely on little more than an email or small-scale website, Lazarus Group's fabricated Worldbit-bot company is on another level of sophistication. It reveals the time and resources Lazarus has at its disposal, as well as the deep knowledge of the cryptocurrency ecosystem necessary to successfully impersonate legitimate participants.

Increased mixer usage and faster cashouts highlight changes to Lazarus' money laundering strategy

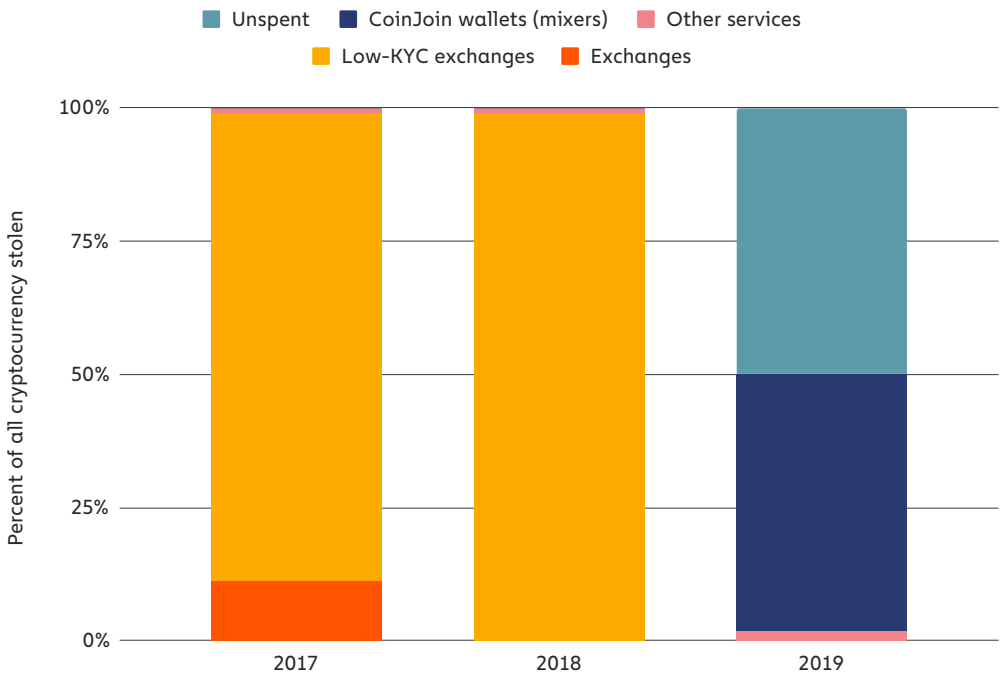
When we analyzed their 2018 post-hack money laundering transactions for last year's Crypto Crime Report, we found that Lazarus Group didn't use sophisticated money laundering techniques like mixers to "clean" and withdraw stolen cryptocurrency quickly like other prominent hacking groups.

Instead, they tended to park funds in a wallet, wait 12 to 18 months, and suddenly move all the funds to a low-KYC exchange when the coast seemed clear.

We concluded that this was due to Lazarus' motivations being primarily financial. Whereas other prominent hacking groups appear more interested in causing chaos for targets and avoiding detection, Lazarus' behavior indicated a singular focus on turning stolen cryptocurrency into cash, even if it meant waiting for long periods of time and moving them to an exchange in a way that's relatively easy to trace. The **U.S. government has reported** that North Korea uses funds from exchange hacks and other financial crimes to fund its weapons of mass destruction (WMD) and ballistic missile programs, supporting the theory that money is Lazarus' primary goal.

While we don't claim to know if Lazarus' motivations changed in 2019, we do know that their modus operandi for moving and cashing out funds stolen in exchange hacks did change. First, we see a much higher percentage of funds they steal moving to mixers.

Destination of exchange funds stolen by Lazarus Group, 2017-2019

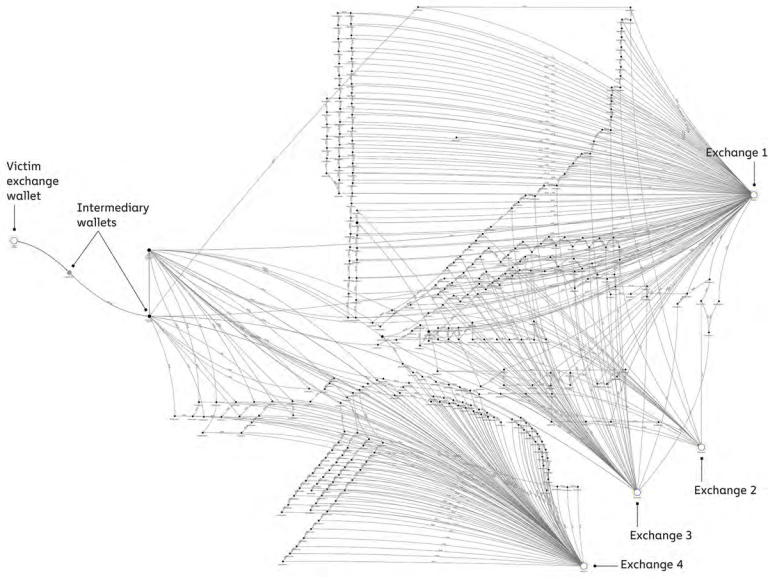


Currencies included: BTC

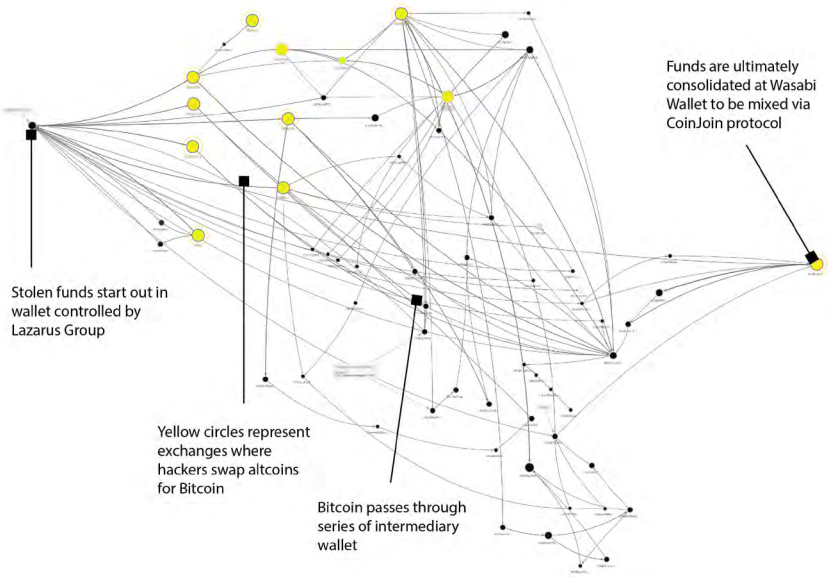
98% of all funds Lazarus stolen from exchanges in 2018 ended up being moved to exchanges, all of which have low KYC requirements, while none went to mixers or CoinJoin wallets. However, in 2019, 48% of funds stolen by Lazarus moved to CoinJoin wallets, while 50% sit unspent in the hackers' original wallet.

We can see this below using Chainalysis Reactor to compare transaction activity associated with a Lazarus hack from 2018 with one from 2019.

Chainalysis Reactor: 2018 Lazarus Group exchange hack

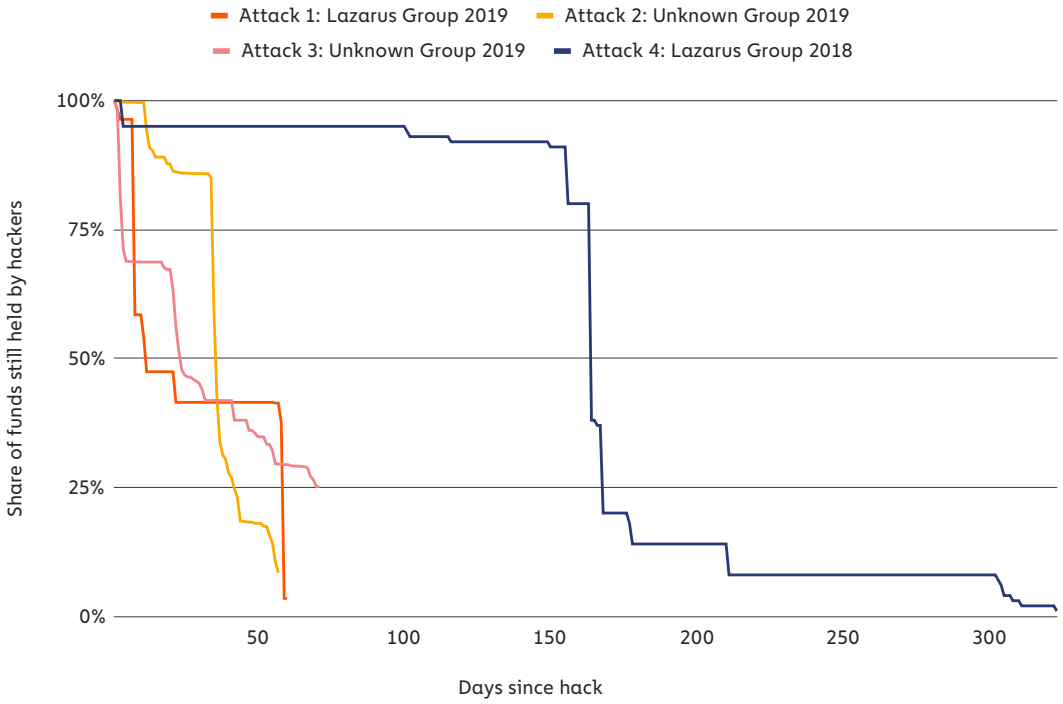


Above, we see how Lazarus moved stolen funds following one of its 2018 exchange hacks. While it may look complicated due to the large number of transactions, it's actually very simple. Funds leave the Victim Exchange wallet on the left, move through two intermediary wallets, and then are dispersed to four different exchanges on the right. The many hops in between represent unspent change moving from a wallet to an exchange. While the funds' path may be long, it's relatively easy to follow.



The Reactor graph showing how Lazarus moved funds following the 2019 DragonEx hack is much more complicated. In this case, stolen altcoins like Ethereum and Litecoin were moved to exchanges and swapped for Bitcoin. Next, they shuffle the Bitcoin withdrawn from exchanges between a variety of local wallets, before ultimately moving it to a Wasabi Wallet on the far right to mix the funds via the CoinJoin protocol.

4 Attacks compared: Time to liquidate stolen funds following exchange attack



Currencies included: BTC

Lazarus Group also moved stolen funds to services where they can be liquidated — mostly exchanges — much faster this year. In 2018, Lazarus took as long as 300 days to move funds from their initial private wallet to a liquidation service, and never did so in under 250 days. But that changed drastically in 2019. Nearly all of the funds stolen in both hacks attributed to Lazarus were moved to liquidation services in under 60 days, though some still remain unspent. Hacks attributed to other groups followed this trend as well.

Lazarus' growing sophistication and speed in laundering stolen cryptocurrency puts more pressure on intelligence agencies and exchanges alike to move quickly when cybercriminals attack exchanges.

Exchanges need to keep prioritizing security

Exchanges have raised the bar on anti-hacking security in the last few years, but the subsequent advancements of groups like Lazarus show that they can't afford to rest on their laurels. They need to remain vigilant and continue building on the improvements they've already made to stay one step ahead. We recommend exchanges continue putting guard rails in place to ensure suspicious transactions are flagged before completion and take steps to prevent employees from downloading malicious software that could compromise their network and give hackers access to the exchange's private keys. In the event exchanges are hacked, they need to report it to law enforcement immediately and provide key information such as addresses to which stolen funds have moved.

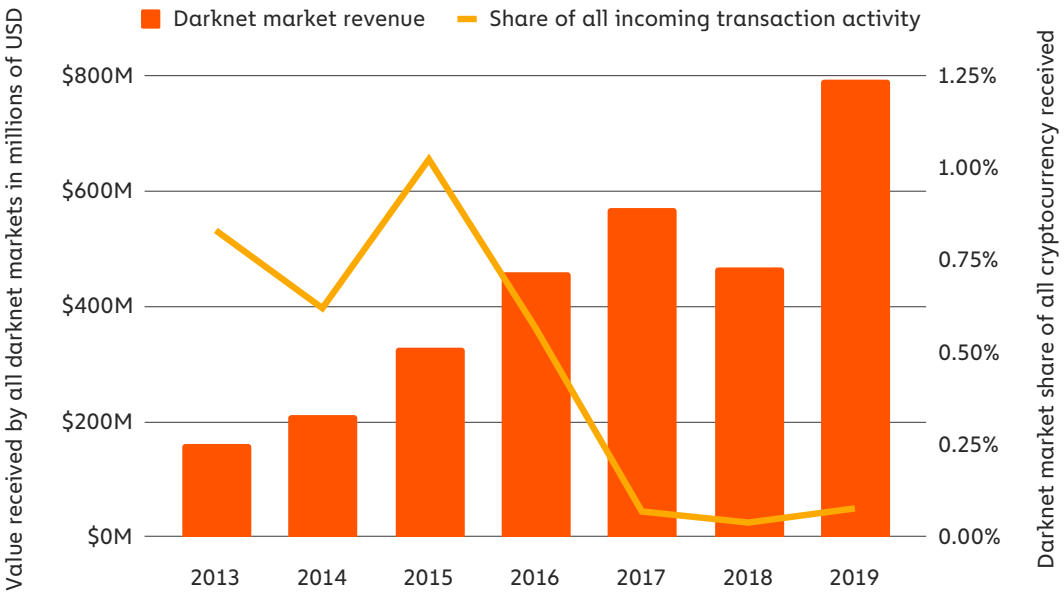
Aside from protecting themselves from being hacked, exchanges also have a responsibility to make sure criminals aren't using them to cash out funds from other exchanges that have been hacked. We suggest that exchanges treat large deposits — or high volumes of small deposits in a short amount of time — from mixers or CoinJoin wallets with increased suspicion. While there are legitimate uses for mixers, the data makes it clear that they're increasingly being utilized by hackers to obfuscate the path of stolen funds prior to cashing out. Exchanges can likely stop some of these cashouts and help law enforcement claw back stolen funds by halting suspicious transactions from mixers. **Binance** has already begun doing this, and we think their model could be a useful example for other exchanges to follow.

Finally, we believe that increased cross-border cooperation between law enforcement agencies can go a long way towards mitigating exchange hacks. If financial intelligence units (FIUs) around the world can swiftly share the information they get from exchanges upon being hacked, they may be able to freeze funds before hackers are able to move them to a mixer or low-KYC exchange.

Darknet Markets

Darknet market activity higher than ever in 2019 despite closures. How does law enforcement respond?

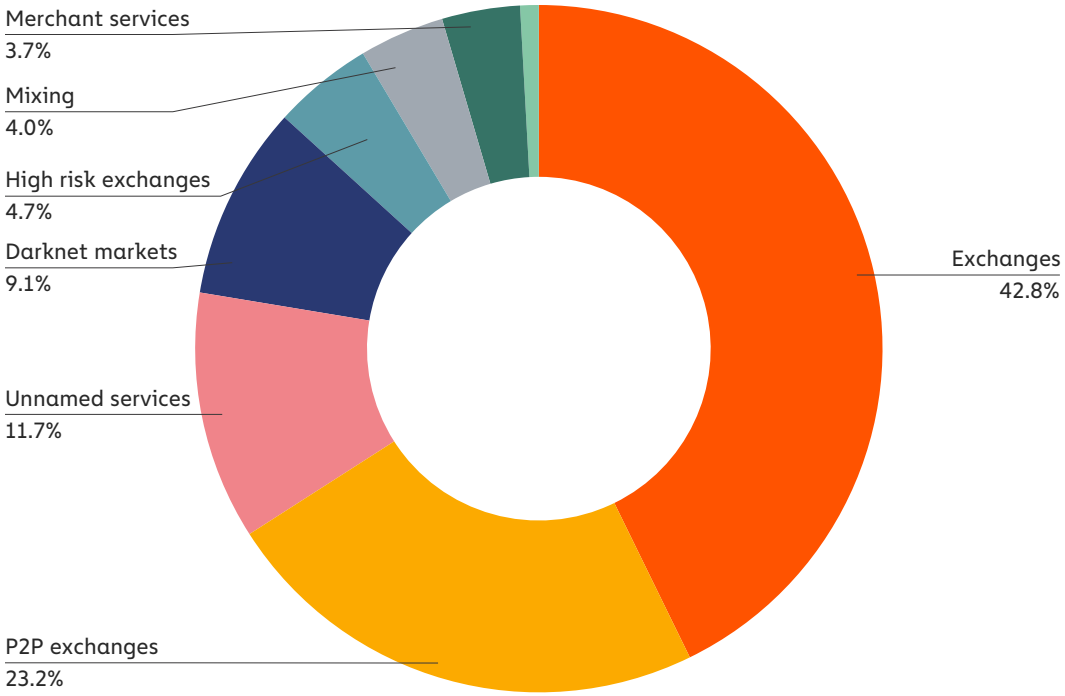
Darknet market revenue vs. Darknet market share of all cryptocurrency received by services, 2013-2019



Currencies included: BAT, BCH, BNB, BTC, CRO, CRPT, DAI, ETH, GNO, GUSD, HT, LEO, LINK, LTC, MCO, MKR, MLN, OMG, PAX, TUSD, USDC, USDT, WETH, ZIL, ZRZ

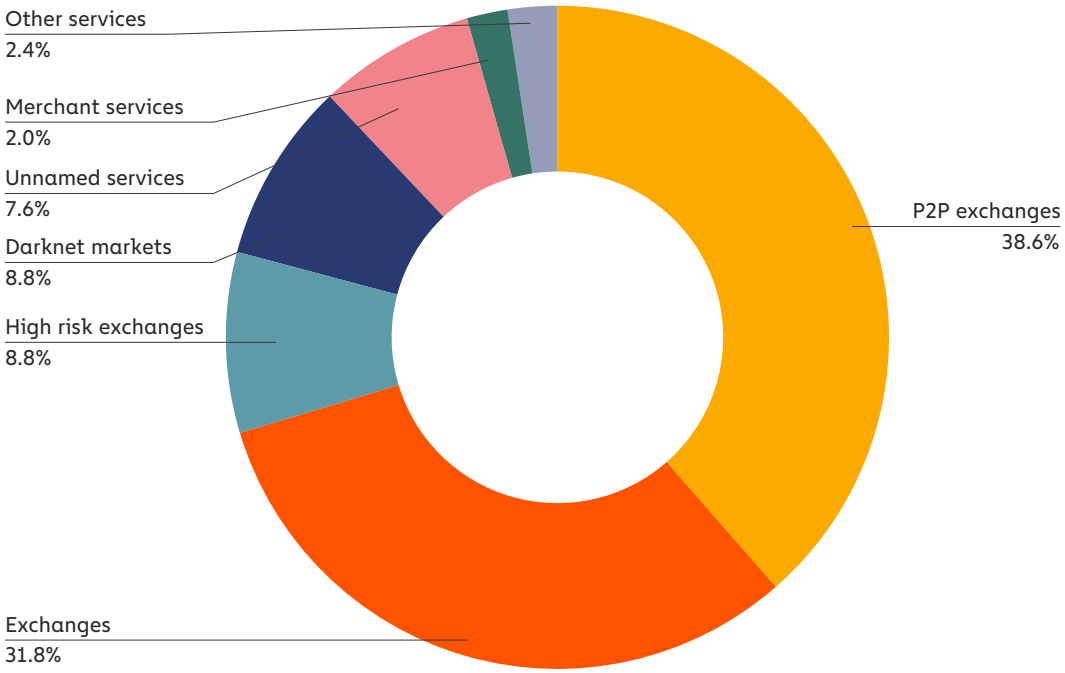
After a small decline in 2018, total darknet market sales grew 70% in 2019 to over $790 million worth of cryptocurrency, making it the first time sales have surpassed $600 million. Not only that, but for the first time since 2015, darknet markets increased their share of overall incoming cryptocurrency transactions, doubling from 0.04% in 2018 to 0.08% in 2019.

Destination of funds leaving darknet markets, 2019



Currencies included: BCH, BTC, LTC, USDT

Origin of funds sent to darknet markets, 2019

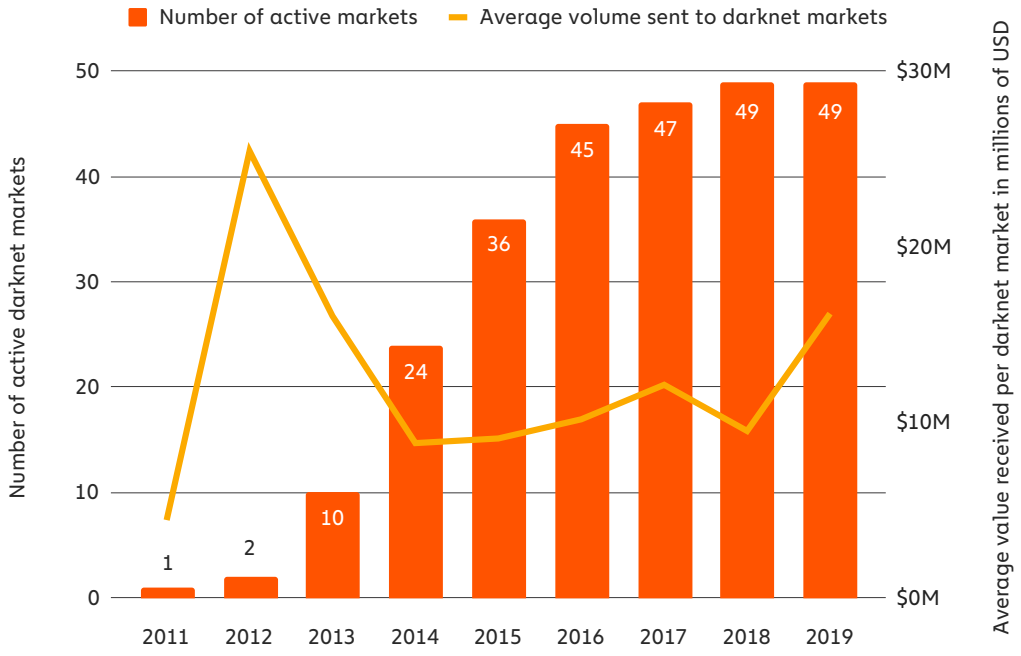


Currencies included: BCH, BTC, LTC
Please note that this chart doesn't include funds that sit unspent in the vendor's original wallet

Similar to previous years, the vast majority of darknet market transactions flow through exchanges. Exchanges are by far the most common service customers use to send cryptocurrency to vendors, and for vendors to send funds to cash out.

While darknet markets' total share of incoming cryptocurrency activity remains extremely low at 0.08%, recent increased volume speaks to the resilience of darknet markets in the face of heightened law enforcement scrutiny.

Number of active darknet markets vs. Average value received per darknet market, 2011-2019

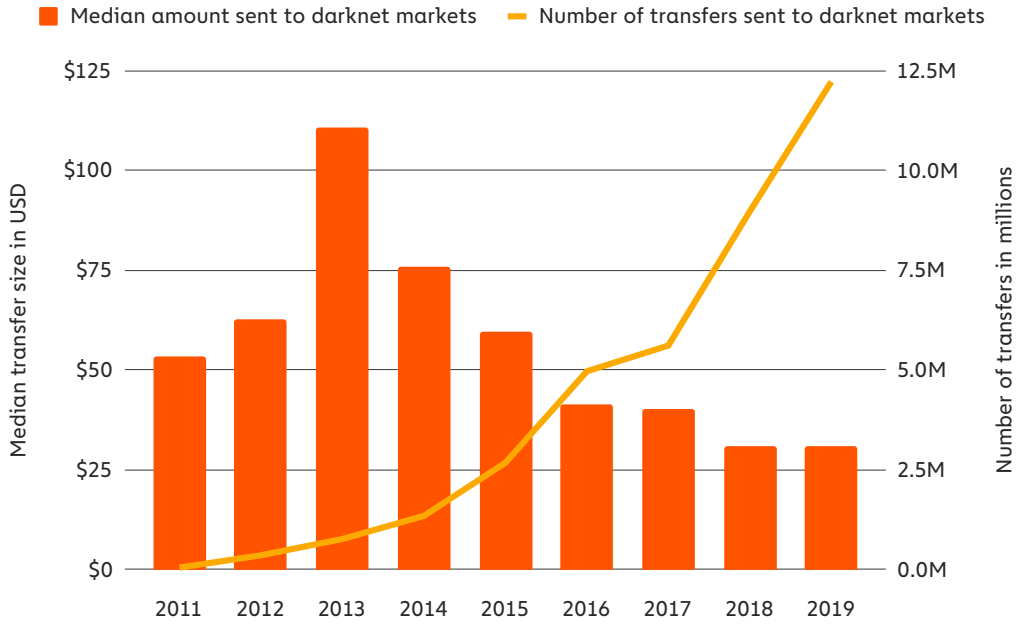


Currencies included: BCH, BTC, LTC, USDT

Although eight of the darknet markets active in 2018 closed in 2019, eight new ones opened, keeping the total number of active markets steady at 49. * On average, each active market in 2019 collected more revenue than those active in any other year, apart from during the height of Silk Road's heyday in 2012 and 2013. As we'll examine in more detail later, it appears that when some markets close, others are able to pick up the slack and satisfy customer demand.

* Note: For this analysis, we only count a darknet market as active if it receives more than $100 in revenue in a given year.

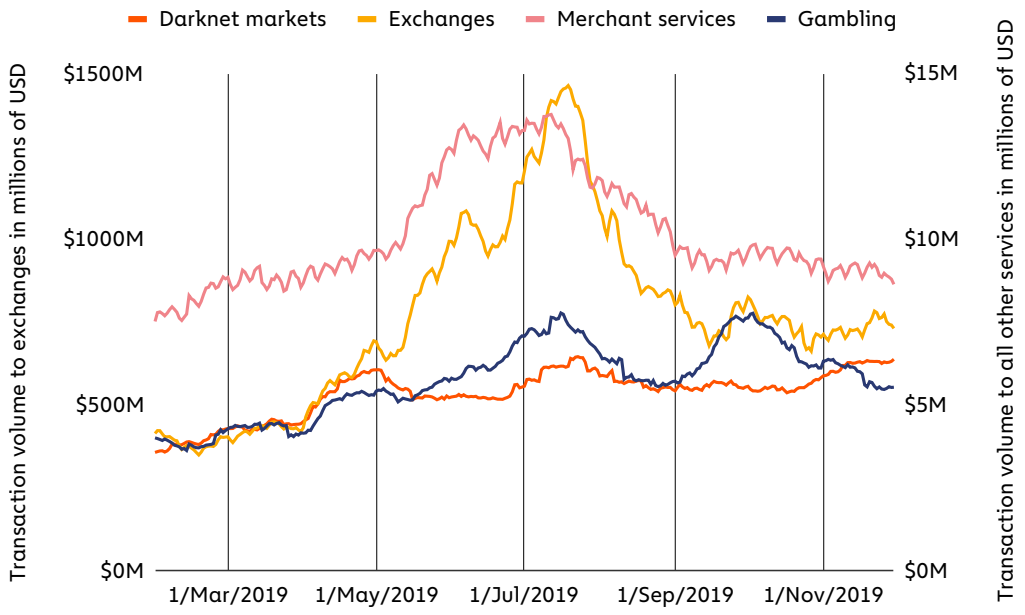
Median transfer size vs. Total transfers to darknet markets, 2013-2019



Currencies included: BCH, BTC, LTC, USDT

The data above also confirms that the increase in revenue is driven by more purchases rather than larger ones. The median purchase size has remained relatively constant in USD value, but we see that the number of transfers once again jumped significantly, from 9 million to 12 million. This suggests that either more customers bought from darknet markets in 2019, or that old customers are making more purchases.

Total Bitcoin transaction volume for darknet markets, exchanges, gambling sites, and merchant services, 30-day moving average

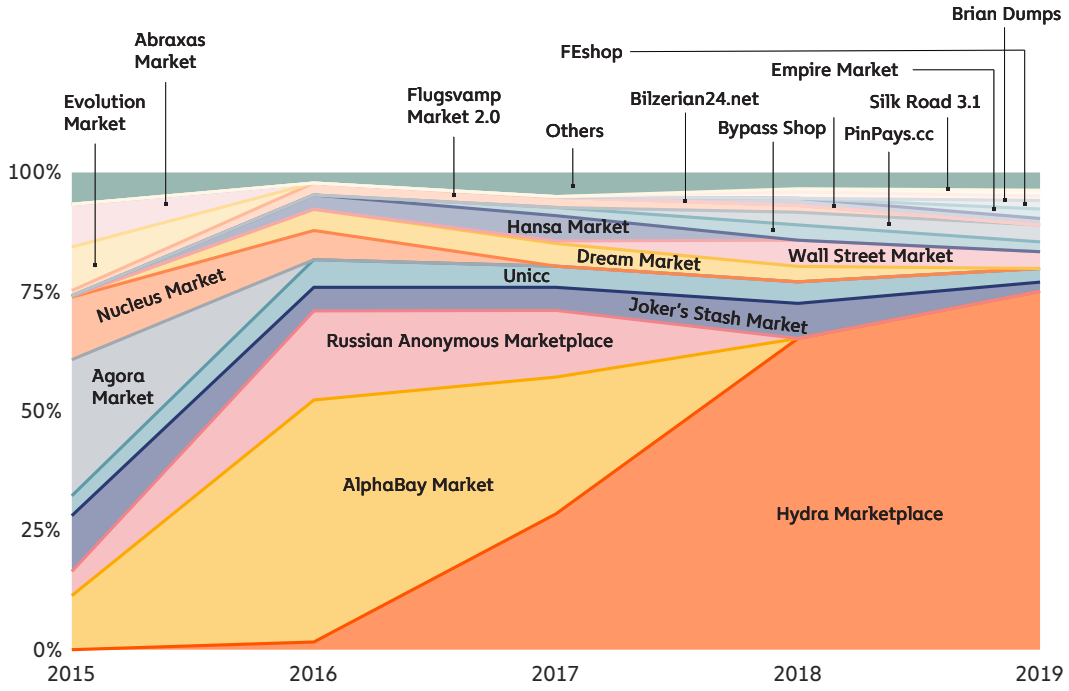


Currencies included: BTC. Please note that the transaction data for exchanges appears on its own axis on the left, because exchanges receive a much higher volume than the other services on this graph.

Perhaps our most interesting finding is that darknet markets' transaction activity appears to be less influenced by the ebbs and flows of the cryptocurrency markets and other forms of seasonality compared to other services. The graph above shows a comparison of total Bitcoin transaction volume between darknet markets and three other types of services over the course of 2019. While all categories see spikes in July around the same time as a Bitcoin price surge, darknet markets exhibit a much less dramatic spike than the others. Looking across the entire year, darknet markets' transaction activity remains within a much narrower volume range, suggesting that customer behavior is less influenced by changes to Bitcoin's price.

Drugs still rule the darknet, but aren't the only inventory on offer

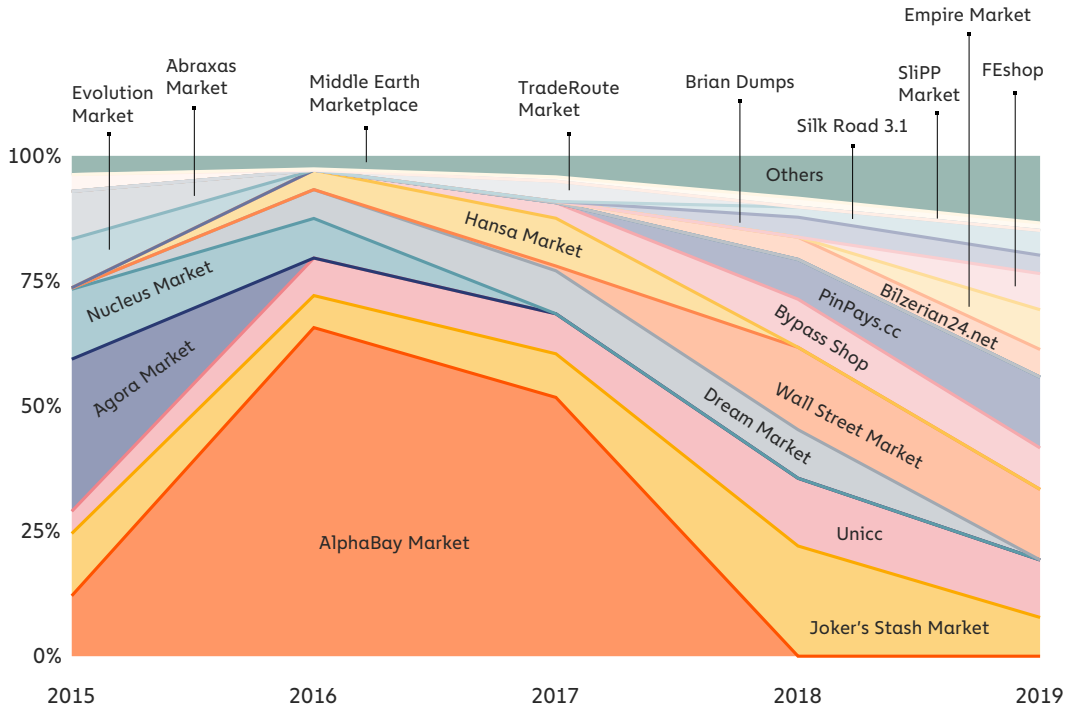
All darknet markets by share of total market size over time, 2015 - 2019



Currencies included: BCH, BTC, LTC, USDT

Above, we see how the top markets have shifted over time. Those focusing on drugs consistently remain the most popular. We should note though that some of the highest-earning markets shown above only serve specific countries or regions. For instance, Hydra Marketplace, by far the most popular market on the graph, caters only to customers in Russia. Below, we have another version of this chart showing only markets with a global customer base. Some of the markets shown in the second graph are more popular in some countries than others, but overall, the data shown below will be more relevant to investigators based in the U.S. and Western Europe.

Global darknet markets by share of total market size over time, 2015 - 2019



Currencies included: BCH, BTC, LTC, USDT

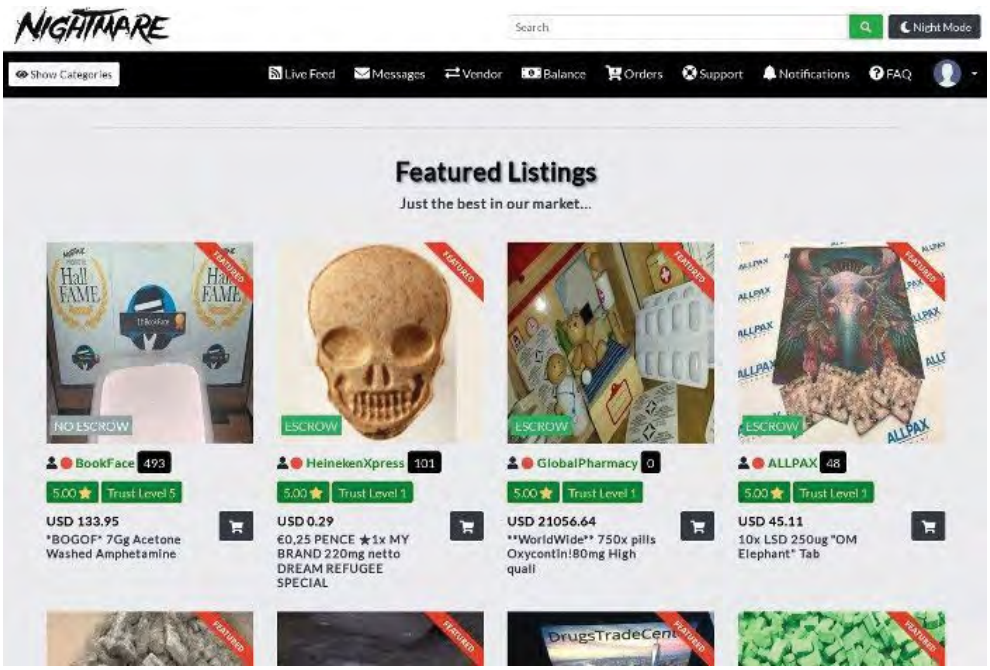
The dominance of drug-focused marketplaces holds here as well. However, it's worth noting that markets specializing in other illicit goods also bring in sizable funds. Joker's Stash Market and UNICC — two of the only markets to maintain steady popularity through the entire time period measured — are the best examples one popular market category known as card shops, which specialize in sales of stolen credit card information. We'll examine card shop activity in greater detail later in this section.

Combatting online drug sales: Should law enforcement chase vendors or shut down markets?

For a long time, the strategy for law enforcement has been to go after the darknet markets themselves. On its face, this appears to be the most logical course of action — why go after individual vendors if you can take them all down in one fell swoop? Law enforcement agencies have achieved big wins following this strategy, shutting down once-prominent markets like AlphaBay and Hansa.

But, the problem with shutting down markets is that other ones fill the void extremely quickly. As of the end of 2019, there are at least 49 active darknet markets, so both users and vendors are spoilt for choice when seeking a new one. Not only that, but it's easy for them to coordinate with one another to find new markets on forums such as Dread, a Reddit-like discussion site devoted to darknet markets.

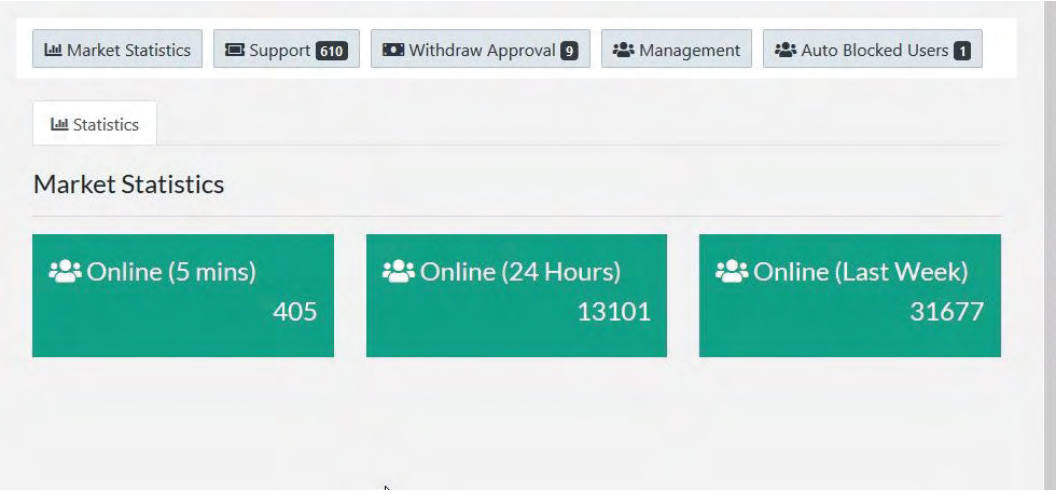
We see an example of this in the shutdown of Nightmare Market earlier this year.



Nightmare market was a short-lived, moderately popular market that closed down in July 2019. Unlike other examples we've cited previously, Nightmare wasn't shut down by law enforcement.

It's unclear exactly what happened, but the shutdown was set in motion on July 23, when someone appearing to be a disgruntled former employee posted on Dread claiming to have hacked the site.

The hacking claim may be true, as the alleged rogue employee posted vendors' mnemonic sequences — random series of words vendors could enter to recover their passwords — which several vendors then confirmed were correct. The hacker also posted screenshots of Nightmare's backend, such as its user analytics and financial data.



It appears likely that Nightmare's administrators decided to exit scam soon after the apparent hack. Users were soon posting on Dread about which forums to move to next.

1

[WARNING] BANDOBABY MIGRATED TO SAMSARA

by [redacted] • 50 minutes ago in [redacted]

0 comments

FUCK NIGHTMARE SAMPLES AVAILABLE ON SAMSARA/EMPIRE/CRYPTONIA

by [redacted] • 1 day ago in [redacted]

8 comments Save

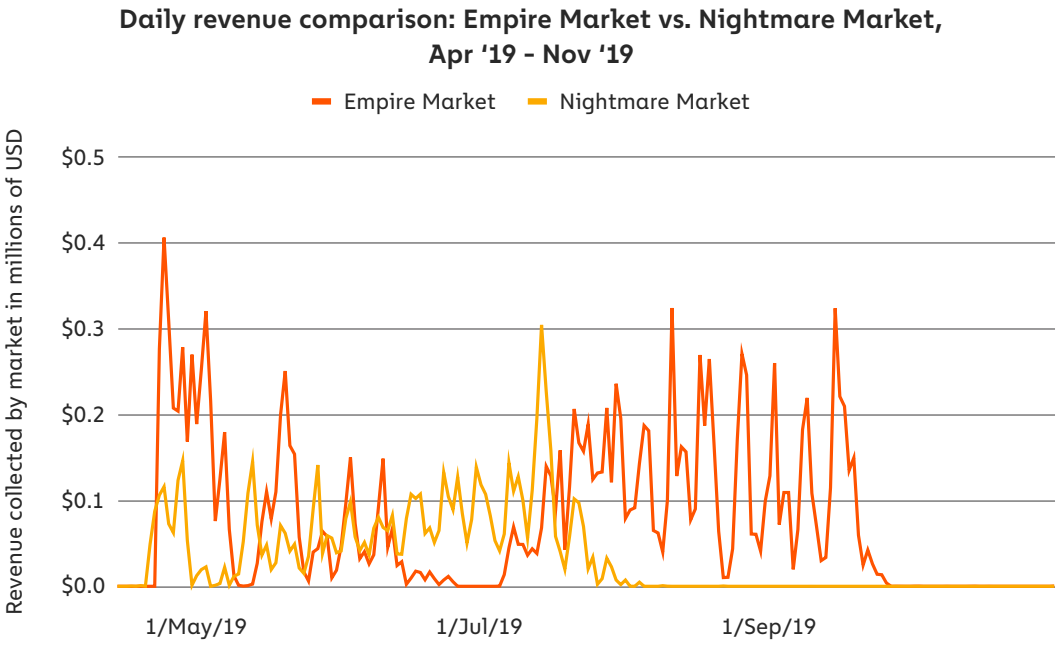
2

PLEASE STAY AWAY!! USE CRYPTONIA!!

by [redacted] • 17 hours ago* in [redacted]

5 comments

Sure enough, users fled in droves. By the end of July, transactions on Nightmare ceased almost entirely. As the data below shows, Empire was able to pick up much of Nightmare's former business, as its sales grew significantly just as Nightmare's fell.



Currencies included: BTC (Empire Market), BTC and USDT (Nightmare Market)

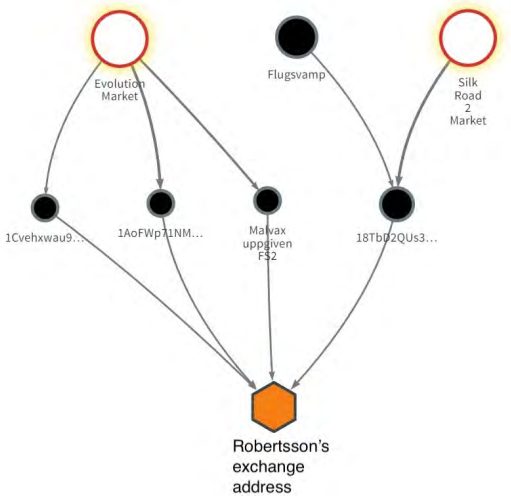
The Nightmare Market shutdown is a perfect microcosm of the issue with shutting down individual darknet markets. There are plenty of other markets out there, and it's extremely easy for vendors to tell their biggest customers which one they're moving to or are already active on.

That's why many law enforcement agencies have shifted their focus to arresting individual vendors. Below is a case study of how this can be done. We caught up with Stefan Kalman, a Chainalysis user and drug enforcement officer in the Swedish Police Authority focused on darknet markets, and he walked us through a recent case of his involving a prominent darknet dealer active across multiple marketplaces.

Case Study: How Swedish Police Chased "Malvax" Across Markets

In 2014, Stefan Kalman and his team at the Swedish Police Authority became aware of a darknet market vendor active on both Silk Road 2.0 and Evolution, going by the handle **Malvax**. By observing his activity on the Silk Road forums, they were able to learn that he was also active on two other darknet markets: Evolution and Flugsvamp, a darknet market exclusive to Sweden, where he went by the handle **Urbansgregor**. Malvax had over 280 products for sale, including the dangerous synthetic opiate fentanyl.

While police had managed to seize some of his shipments to customers that were flagged by PostNord, Denmark's main private mail carrier, they'd yet to uncover his real world identity. Malvax ran a sophisticated operation, relying on mixers and other obfuscation techniques to protect his identity. But police got a golden opportunity when they learned in mid-2015 that the FBI had seized the servers of Silk Road 2.0 after shutting it down the previous November. By reviewing the logs of those servers, they were able to get some of the Bitcoin addresses the dealer used under his Malvax alter ego, and used Chainalysis to trace some of them back to a regulated exchange headquartered in the UK.



Stefan and his team sent a subpoena to the exchange, which in turn provided them with enough information to figure out who Urbansgregor/Malvax really was: **Fredrik Robertsson**.

After conducting undercover purchases from Robertsson on Flugsvamp to confirm he was still selling drugs, Stefan and his team received warrants to tap Robertsson's phone, put a GPS tracker on his vehicle, and watch his house with cameras. By placing more test orders with him and observing his online and offline behavior, they were able to intercept more of his packages and build their case further.

Eventually, they got a search warrant for Robertsson's house, raided it, and found drugs. In addition, they found debit cards issued by a Hong Kong-based cryptocurrency exchange, which he could use to withdraw fiat currency from ATMs in Sweden. After cracking his encrypted email account, the agents found over 1900 invoices for drug orders, as well as messages confirming that Robertsson's brother, a Bitcoin and cybersecurity expert based in Asia, was also in on the scheme. Stefan and his team confirmed this finding by using to Chainalysis to trace some of the brother's Bitcoin withdrawals in Hong Kong and Thailand.

Thanks to the evidence Stefan and his team gathered on the Robertsson brothers, Swedish courts were able to convict them of selling drugs on the darknet.

Card Shop Deep Dive

As we mention above, while shops specializing in drugs are the most popular type of darknet market, they're not the only type of darknet market to achieve consistent sales. Below, we'll look at another popular type of market.

You've probably heard of big security breaches at companies like Capital One and Home Depot, in which tens of millions of customers' credit card information was compromised. Ever wonder where that stolen information ends up? There's a good chance it's available on card shops. Card shops are a category of darknet market where users can purchase stolen credit card information. We'll look at UNICC as an example.

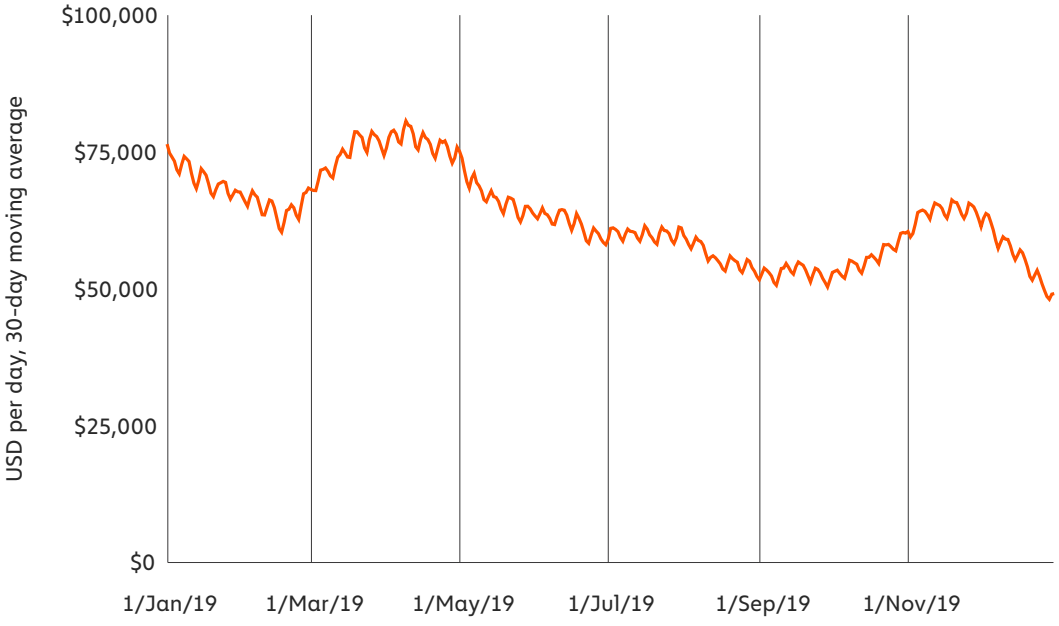
UNICC NEWS BUY ORDERS BILLING CHECKERS BINBASE SUPPORT BALANCE CART 0

RESET ADD TO CART SEARCH

Bin	Exp	First name	Last name	Address	City	State	Zip	Phone	Country	Fullz	Can I refund?	Price	Base Name
GOLD CREDIT	04/20					UT			USA	-	No	10.00$	NOV_#14_US_NO_REF
GOLD CREDIT	03/23					NJ			USA	-	No	10.00$	NOV_#14_US_NO_REF
PLATINUM CREDIT	04/23					TX			USA	-	No	10.00$	NOV_#14_US_NO_REF
PLATINUM CREDIT	04/24					NC			USA	-	No	10.00$	NOV_#14_US_NO_REF
PLATINUM CREDIT	06/24					TN			USA	-	No	10.00$	NOV_#14_US_NO_REF
PLATINUM CREDIT	07/24					NJ			USA	-	No	10.00$	NOV_#14_US_NO_REF
PLATINUM CREDIT	04/23					TN			USA	-	No	10.00$	NOV_#14_US_NO_REF

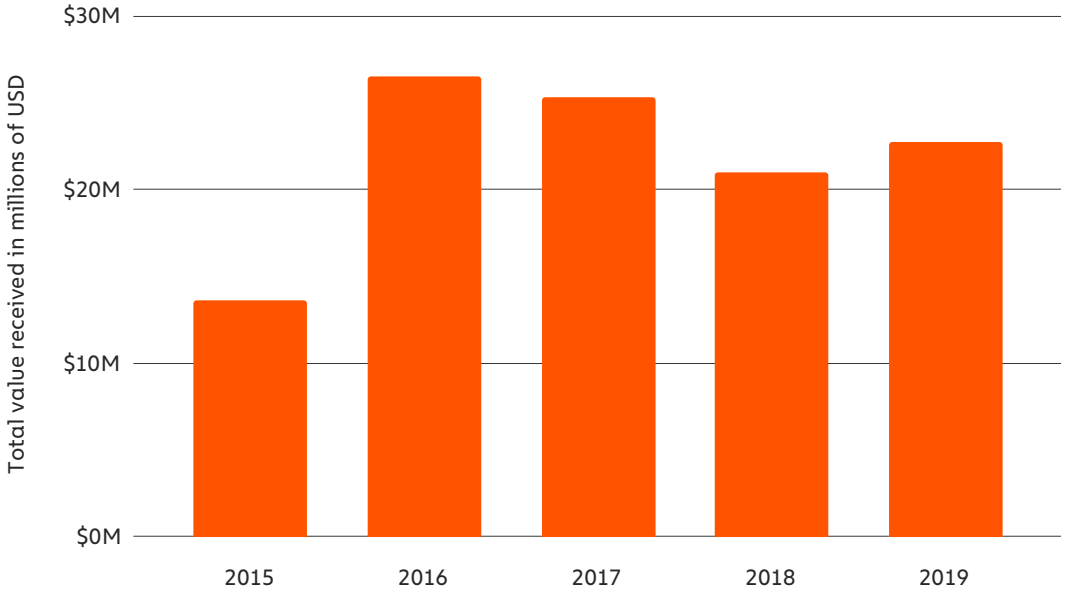
Above, we see some of UNICC credit card listings. Cards go for anywhere from $2 to $15, with the average sitting at about $10. The exact price depends on a few different factors. One is area of origin. U.S. and western Europe-based cards typically fetch a premium. Another influence on price is the amount of the cardholder's personally identifiable information (PII) that comes with the card, such as street address and phone number. Most reputable online stores ask for this information upon purchase, hence why having it drives up the card price.

Total funds sent to UNICC, 30-day moving average, 2019



Currencies included: BCH, BTC, USDT

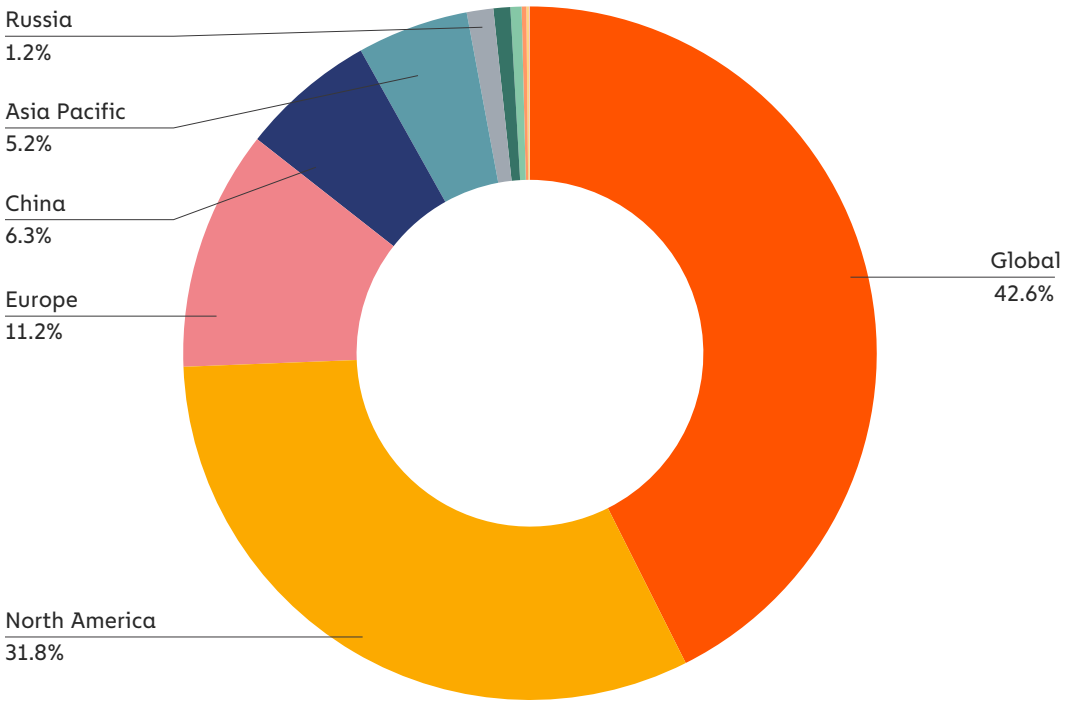
UNICC yearly revenue, 2015-2019



Currencies included: BCH, BTC, USDT

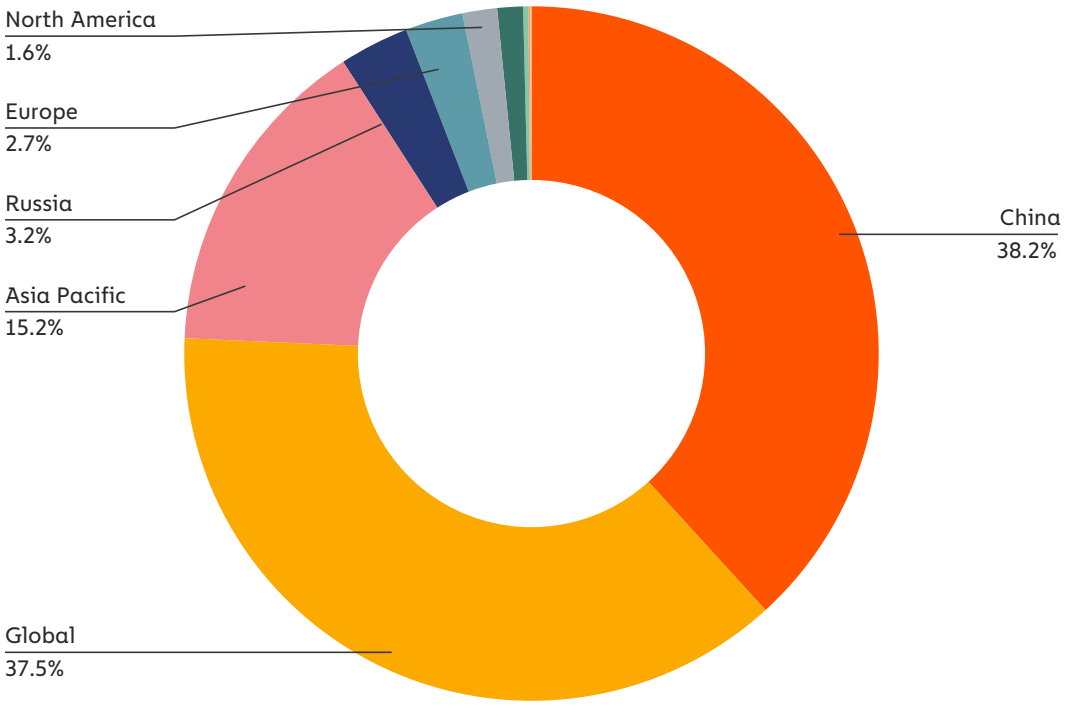
UNICC took in at least $22.7 million worth of cryptocurrency in 2019, making it the fourth most active market last year. Activity remained relatively steady over the course of the year, peaking in April. Based on that total sales figure and estimating an average cost of $10 per card, we estimate that UNICC sold card data belonging to nearly 3 million customers.

Regions by share of total funds sent to UNICC, 2019



Currencies included: BCH, BTC, USDT

Regions by share of total funds received from UNICC, 2019



Currencies included: BTC

Our regional data reveals that most people buying stolen credit card data on UNICC are from North America (after Global), while most of those selling it are from China. ** While it's difficult to say exactly why that is, it's possible that more criminals from China have the technological proficiency to steal credit card data.

Case study: Bringing down the world's largest child sexual abuse material darknet market

Most troubling of all is the existence of darknet markets that allow users to purchase child sexual abuse material (CSAM). While the proliferation of this material has become a **huge issue** on the clearnet in recent years, it's actually quite rare to find a large-scale, cryptocurrency-powered darknet market devoted to CSAM — in fact, nearly all darknet markets explicitly ban this material — but it isn't unheard of. This past year, Chainalysis worked with agents at Homeland Security Investigations (HSI) and IRS Criminal Investigation (IRS-CI) to bring down the biggest one discovered to date: a site known as Welcome to Video (WTV).

** Please note: Exchanges under the "APAC" category serve all of the Asia-Pacific region, including China, while those under the "China" category serve only or mostly Chinese customers.

How WTV worked

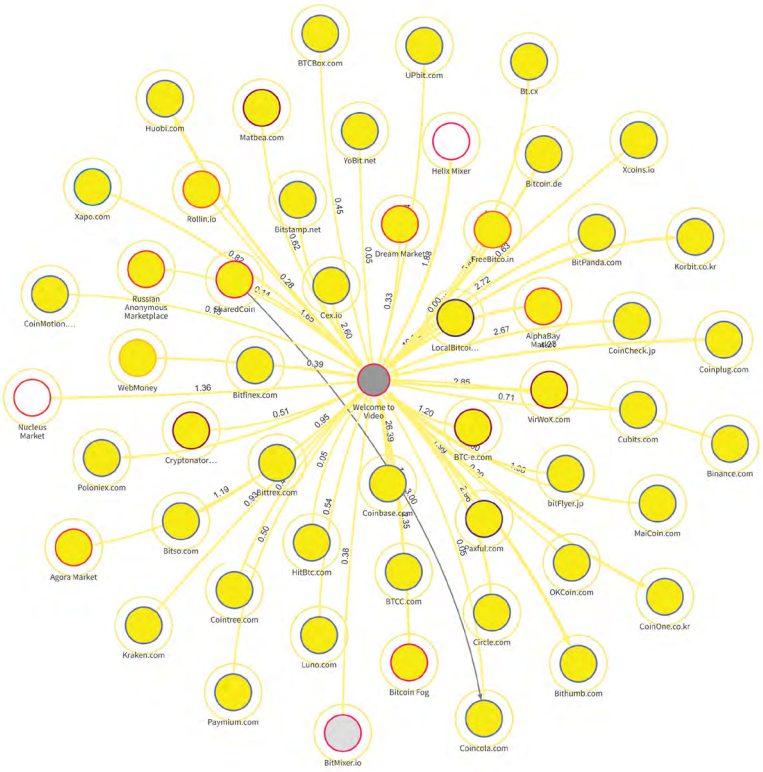
Welcome to Video (WTV) was a child pornography website that operated out of South Korea and allowed users to buy content with Bitcoin or to upload their own. Upon signing up for the site, users received a unique Bitcoin address where they could send funds to buy content to view.

When law enforcement shut down the site, they seized over 8 terabytes of child pornography, making it one of the largest siezures of its kind. WTV had 1.3 million Bitcoin addresses registered. Between 2015 and 2018, the site received nearly $353,000 worth of Bitcoin across thousands of individual transactions.

Taking down WTV

Cybercrime transcends national borders. Welcome to Video had a global customer and contributor base requiring cross-border collaboration among law enforcement agencies across the world. IRS-Criminal Investigations (IRS-CI), Homeland Security Investigations (HSI), and other agencies used Chainalysis software to analyze blockchain transactions and map out contributors and users of the site. This enabled them to disseminate the blockchain evidence to their partners in the United Kingdom, South Korea, Germany, Saudi Arabia, the United Arab Emirates, the Czech Republic, Canada, Ireland, Spain, Brazil and Australia, and ultimately make arrests.

With the site's listed Bitcoin address, IRS-CI and HSI used Chainalysis Reactor, our investigations product, to analyze transaction activity and build a graph showing the flow of funds in and out of the WTV address.



Here we see that WTV received funds from several different exchanges. This information allowed IRS-CI to contact exchanges for more information on the addresses sending money to WTV. Because exchanges typically perform Know Your Customer (KYC) processes, many were able to provide copies of identification, street addresses, and other relevant transactions associated with those accounts. While in many cases the information supplied by the exchanges was enough to identify WTV users, in other cases IRS-CI was able to combine the account information with open source intelligence and standard investigative techniques to identify users.

Chainalysis tools then augmented the work done by IRS-CI and Homeland Security Investigations (HSI) to break down regionally-specific information. This both helped law enforcement teams around the world make arrests related to WTV, and understand how blockchain evidence can be used to take down sites like WTV more generally.

By March 2018, agents arrested the WTV owner and shut down the site.

What comes next for darknet markets?

Some darknet markets have begun implementing user safety features that make it more difficult for them to be scammed by vendors or by the market itself. For instance, many have adopted multi-signature technology, meaning that both vendor and buyer have to confirm an order has been completed for funds to move. This way, buyers can approve their funds to move only when they've received their order. Another such feature is wallet-less escrow, also known as direct deposit. Wallet-less escrow makes it impossible for markets to exit scam users by removing the need for them to deposit funds to a wallet controlled by the market. Instead, they receive a new disposable wallet for every order they place, and the cryptocurrency they deposit goes straight to the vendor — the market itself never actually controls it. Cryptonia was an active market that incorporated both multi-signature transactions and wallet-less escrow, though it recently closed down voluntarily.

Some darknet markets are also adopting new infrastructures to avoid shutdowns by law enforcement. OpenBazaar, for instance, has a fully decentralized structure, similar to the blockchain itself or the Tor web browser, that would make it impossible to take down. Users simply download and run a program that allows them to connect directly, rather than through a website. Particl.io offers a similar marketplace with its own coin and wallet infrastructure. Neither of these markets have achieved widespread adoption yet. OpenBazaar, for instance, only has between 10 and 20 vendors with substantial traction, while the most popular markets have hundreds. Anecdotally, we believe the low adoption is because OpenBazaar and Particl.io are harder to use than standard darknet markets, but both would present new challenges to law enforcement if they gained popularity.

Finally, we may see more darknet markets accept, or perhaps even mandate the usage of privacy coins like Monero. Monero uses an obfuscated public ledger to make it more difficult to see the senders, receivers, or amounts of cryptocurrency exchanged on transactions. As of now, Empire appears to be the only major darknet market accepting Monero, but that could change in 2020.

Terrorism Financing

Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly

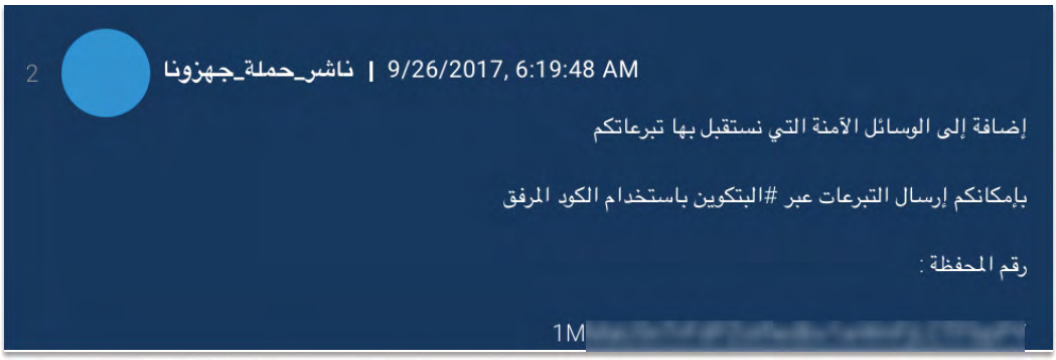
Cryptocurrency as a terrorism financing tool presents difficult issues for the intelligence community. Unlike social media profiles and bank accounts, agents oftentimes can't have a cryptocurrency address shut down due to the decentralized nature of blockchains. While knowledge sharing is crucial to take on such a dangerous threat, terrorism financing in cryptocurrency is also difficult to report on publicly, as most cases involve sensitive information or are classified for national security reasons.

But despite the difficulties in analyzing this subject, we can say from the investigations we've been involved with in 2019 that there's definite cause for concern. What's especially worrying are the advancements in technical sophistication that have enabled successful terrorism financing campaigns. Below, we'll compare case studies of two such campaigns — one that took place between 2016 and 2018, and one from 2019 — to illustrate these changes.

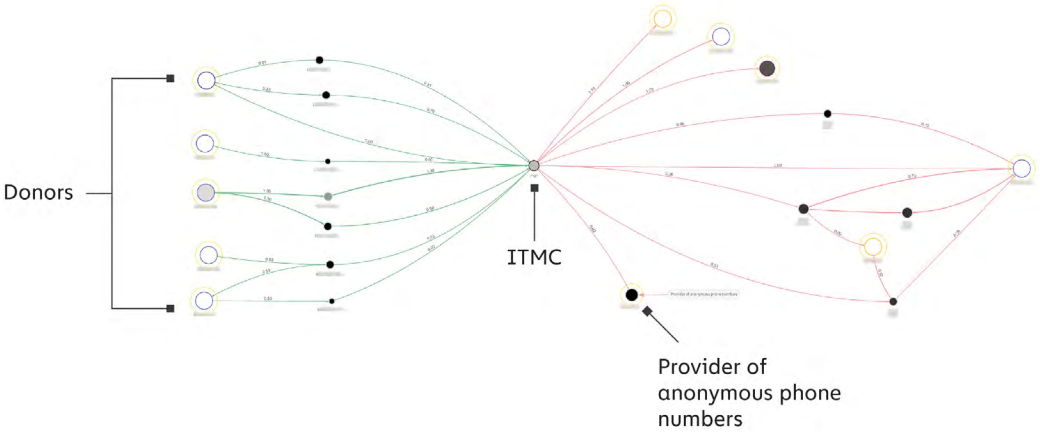
Looking back: Ibn Taymiyyah Media Center's 2016-2018 Cryptocurrency Fundraiser

Ibn Taymiyya Media Center (ITMC) is the media wing of Mujahideen Shura Council (MSC) in the Environs of Jerusalem, a jihadist group based in Gaza and designated as a Foreign Terrorist Organization by the U.S. State Department. In addition to producing propaganda supporting ISIS and other terrorist groups, it also publishes instructional material on how to make weapons and material advocating for terrorist attacks.

In 2016, ITMC became the first terrorist organization to launch a public crowdfunding donation campaign using cryptocurrency. ITMC named its campaign Jahezona ("Equip us" in Arabic) and explicitly told potential donors the funds they sent would be used to buy weapons. They also advertised the campaign as a way for Muslims around the world to join their cause, citing Koran verses to position donating to the fundraiser as a religious obligation.

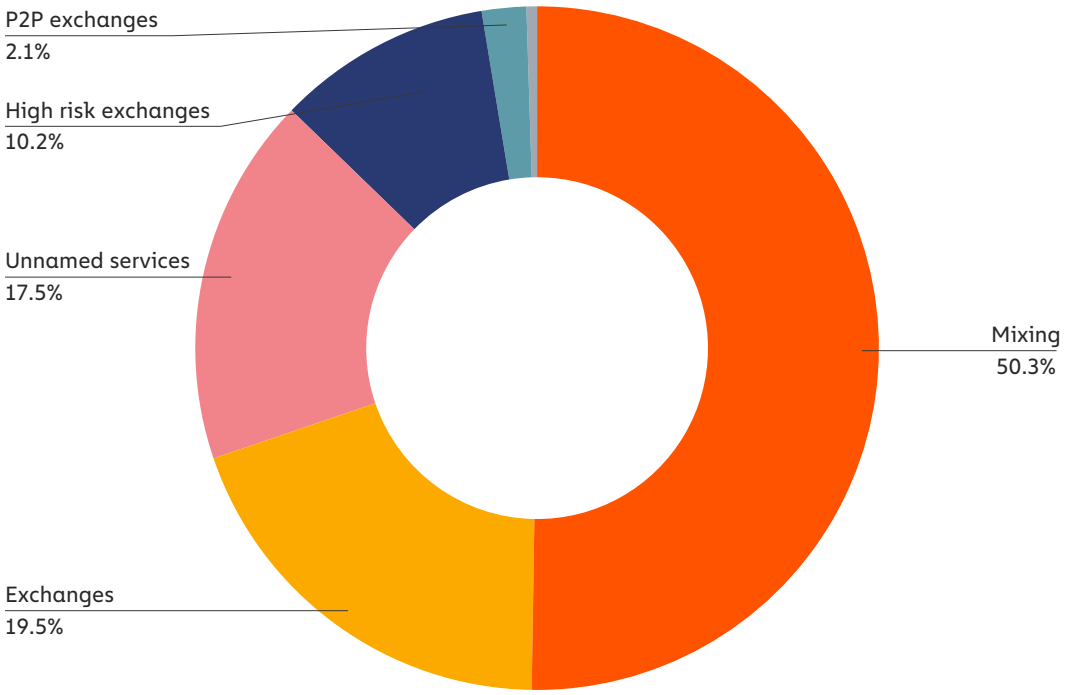


The Equip Us campaign ran from June of 2016 to June of 2018. ITMC promoted it on platforms like Twitter, YouTube, and Telegram, posting a Bitcoin address to which donors could send funds. While only a single Bitcoin address was disclosed as part of the campaign, we were able to discover an additional 27 addresses associated with the campaign using Chainalysis Reactor. This provides investigators with a more comprehensive picture of the transactions associated with the ITMC wallet.



On the left in the Reactor graph above, we see a sample of some of the donations, most of which came in from addresses at mixers, regulated exchanges, or P2P exchanges — in most cases, donations passed from those services to an intermediary private wallet before being donated. On the right, we see ITMC sending donations to various addresses, presumably to be converted into cash. Interestingly, we also see them sending funds to a wallet we know from Chainalysis' OSINT (Open Source Intelligence) is associated with a service that sells fake phone numbers in bulk. We know from previous investigations that many extremist groups purchase these phone numbers in order to create new social media accounts when old ones are banned — that may be what's happening here.

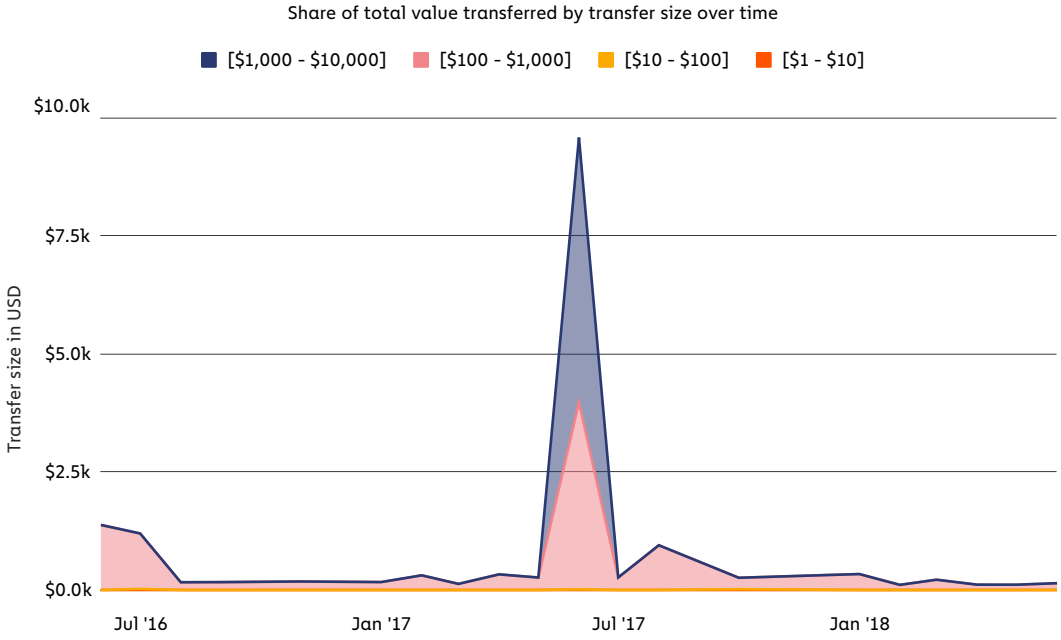
Services sending cryptocurrency to ITMC



Currencies included: BTC

Let's take a closer look at the donations themselves.

Donations to ITMC terrorism financing campaigns



Currencies included: BTC

Over the two years the fundraising campaign ran, ITMC received tens of thousands' worth of cryptocurrency across more than 50 individual donations, with a notable spike in June 2017. The median donation size was $164. The single largest donation was just under $2500, and just two other donations topped $1,000. 14% of donations were between $500 and $1,000, and nearly all of the remainder were between $100 and $500, with most of those falling between $100 and $250. We observed just four donations under $100 worth of cryptocurrency.

While that may not sound like much money over a two year period, it's important to recognize that terror attacks can be carried out cheaply with weapons made from relatively ubiquitous materials. And as we explore below in our case study of Al-Qassam Brigades' 2019 terrorism financing campaign, other groups have become much more sophisticated in the methods they use to solicit and accept cryptocurrency donations.

Tracking Cryptocurrency's Biggest Ever Terrorism Financing Campaign

In early 2019, the Izz ad-Din al-Qassam Brigades (AQB) — the military wing of Hamas and another designated terrorist organization — began soliciting donations in Bitcoin in one of the largest and most sophisticated cryptocurrency-based terrorism financing campaigns ever seen. AQB utilized multiple types of wallet infrastructures to receive donations before settling on a system that generated a new address for every donor to send funds to, the first verified example we've seen of such technology deployed by a terrorist organization. To date, the campaign has generated tens of thousands of dollars of Bitcoin for AQB.

Investigators and analysts are currently using Chainalysis to analyze these transactions, which could enable them to identify the origin of the donations and the destination of funds received by AQB during the campaign. This ultimately could help them identify the donors and financial facilitators at AQB who are running the campaign. While this investigation is ongoing, we can share some insight into this campaign based on Chainalysis data to show you how today's terrorists are utilizing cryptocurrency.

How AQB solicited cryptocurrency donations

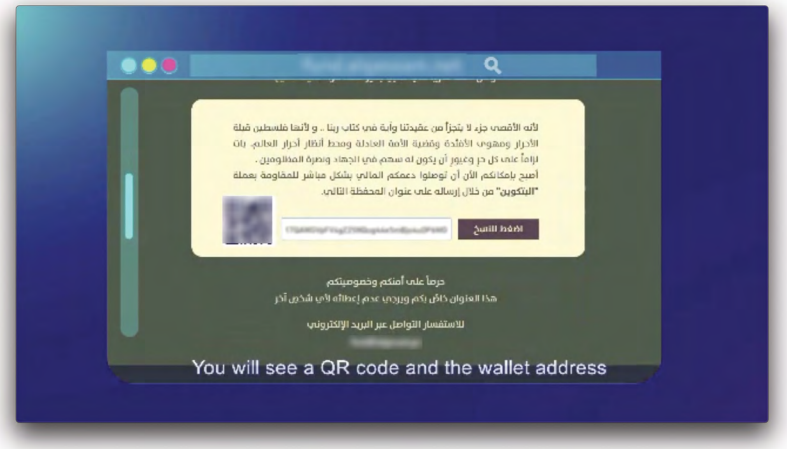
The easiest way to understand the evolution of AQB's 2019 campaign is to divide it into three sub-campaigns, based on the type of wallet the organization used to receive donations.

The first sub-campaign began in January of 2019, when the AQB website began displaying a message inviting users to "donate to the jihad" with a QR code underneath leading to a single Bitcoin address.

That Bitcoin address was associated with an account at a U.S.-based, regulated exchange. Law enforcement was quickly able to alert the exchange, have the account frozen, and investigate the individual who established it at the exchange, as well as transactions that contributed to that account.

The second sub-campaign began when AQB replaced the exchange address with a new one linked to a private, non-custodial wallet, citing the need for increased anonymity. Nonetheless, cryptocurrency analysts were still able to trace donations to and withdrawals from the address with the help of Chainalysis.

Soon after that, however, AQB launched the much more advanced **third sub-campaign**, with a Bitcoin wallet integrated into their website that generated a unique Bitcoin address for each donor to which they could send contributions. AQB also published a video on its website telling users exactly how to donate as anonymously as possible.



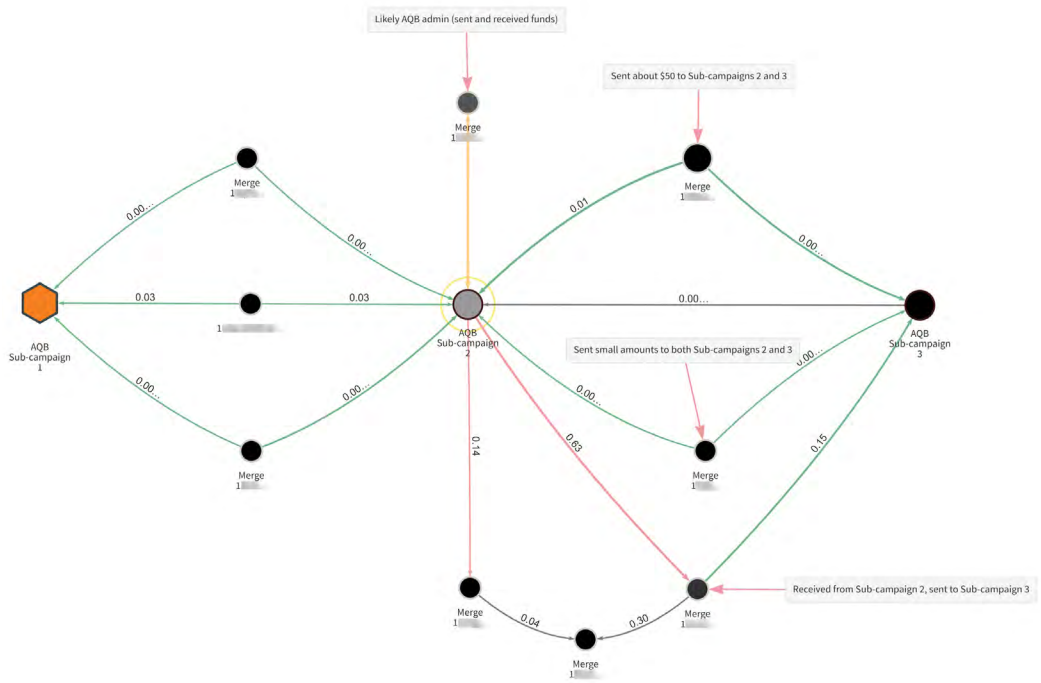
AQB's instructional video provided two methods for donors to send in Bitcoin. In the first method, donors were instructed to go to a **hawala**, a type of money service business that's popular in the Middle East. Donors could simply go to a hawala, hand over however much cash they wished to donate, and provide the donation address AQB gave them. From there, the hawala would send the equivalent amount of Bitcoin.

For the second method, donors were instructed on how to create their own private wallet from which they could send their donation — AQB's video even displays a list of recommended wallets and also exchanges where they can get Bitcoin.

AQB's instructions were quite thorough, even telling donors to use public wifi when creating their private wallet to avoid compromising their IP address. Overall, Sub-campaign 3 is the most advanced usage of cryptocurrency technology we've observed in a terrorism financing campaign.

Analyzing AQB's donations

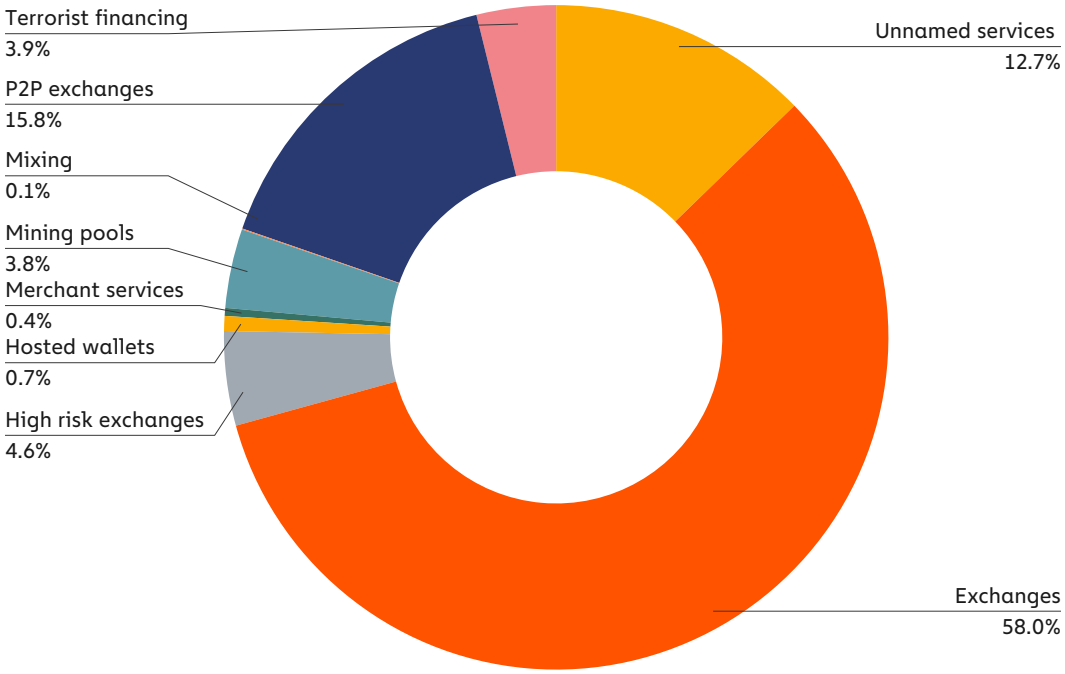
Sub-campaign	Bitcoin Payment Method	Amount raised (USD)
Sub-campaign 1	Bitcoin address at compliant, U.S.-based exchange	< $2,000
Sub-campaign 2	Bitcoin address with private, custodial wallet	< $5,000
Sub-campaign 3	Unique Bitcoin payment address generated for each donor	> $10,000



Looking at all three sub-campaigns in Chainalysis Reactor, we see that some donors contributed Bitcoin to multiple AQB campaigns. However, we'll focus most of our analysis on Sub-campaigns 2 and 3, as they attracted most of the donations and the latter of the two is still collecting funds.

The fact that the Al Qassam Brigades' website-based wallet generates a new unique address for each donor makes it more difficult to identify addresses associated with Sub-campaign 3 and track transactions in and out of those addresses. Under normal circumstances in a scenario like this, we would send a small amount of cryptocurrency to help us learn more about the address. But that option was off the table here, as it's illegal to transact with an address belonging to a designated terror organization. However, using court documents from associated cases and analysis of transactions from the first two sub-campaigns, we were able to discover addresses that received donations as part of the third sub-campaign. We then used Chainalysis Reactor to find many more addresses. As of December 27, 2020 we've identified over 100 addresses that received Bitcoin donations during Sub-campaign 3. Below is some of the data we've aggregated from analyzing donations to those addresses, as well as the address associated with Sub-campaign 2.

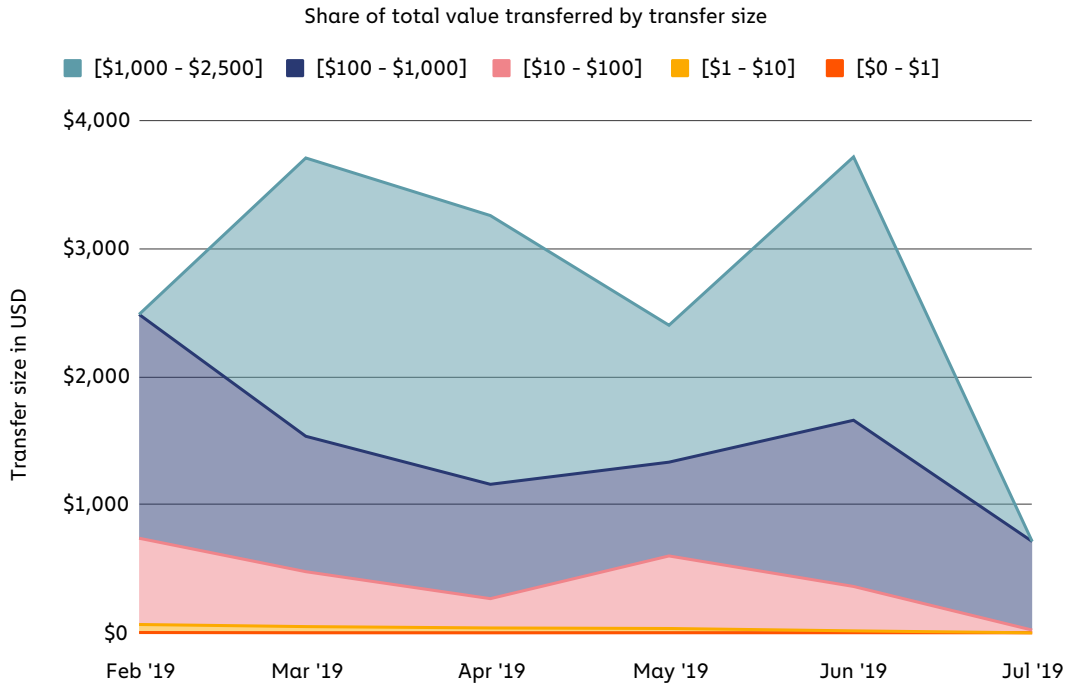
Origins of funds sent to AQB Sub-campaigns 2 and 3



Currencies included: BTC

Overall, the largest share of AQB's donations to Sub-campaigns 2 and 3 came from standard exchanges that collect KYC information from users. However, a substantial amount also came from high-risk exchanges, P2P exchanges, and other addresses associated with terror fundraising. Interestingly, AQB received no funds from mixers, which is where the bulk of ITMC's donations came from during its 2016 to 2018 campaign. One possible explanation is that ITMC's supporters are more knowledgeable of cryptocurrency and therefore know that a mixer can help obscure the path of their donations, but we have no way of verifying this. It's also possible that AQB's donors didn't use mixers because doing so wasn't included in the instructional video promoting the campaign, or because they thought the unique address generation component of Sub-campaign 3 ensured sufficient anonymity.

Donations to AQB Sub-campaigns 2 and 3



Currencies included: BTC

Across more than 100 donations, we found that the median amount sent was just $24, though the average was much higher due to a few large outliers. The highest amount sent in a single donation was $2154 — besides that, there were only two other donations above $1000. 13% of all donations were between $100 and $1000, 10% were between $50 and $100, and 75% were below $50.

While most donors gave relatively small amounts, there were still enough large donors for Sub-campaign 3 to bring in tens of thousands of dollars' worth of cryptocurrency for AQB. Given the success of AQB's donation campaign, we may see other terrorist organizations launch similar campaigns to this one in 2020 and beyond. We hope that by continuing to analyze these transactions, we can not only enable investigators to identify the donors and financial facilitators administering AQB's campaign, but also continue learning more about the changing tactics of terrorism financing in cryptocurrency.

What do these campaigns tell us about terrorism financing in 2020?

Comparing donations for ITMC and AQB terror campaigns

	ITMC "Equip Us" Campaign (2016-2018)	AQB Sub-campaigns 2 and 3 (2019)
Individual donations	50+	100+
25th percentile donation size	$114	$5
50th percentile donation size	$164	$24
75th percentile donation size	$337	$66
Largest donation	$2,495	$2,172
Total	$16,680	Tens of thousands (USD)

Across its three sub-campaigns, AQB raised roughly the same amount in cryptocurrency during its 2019 fundraising push as ITMC did during its campaign that ended the previous year. AQB also attracted more individual donors. This is more concerning when you consider the fact that AQB's campaign has been active for just nine months, compared to two years for ITMC. The comparison suggests that terrorist groups could be improving their ability to attract donors online.

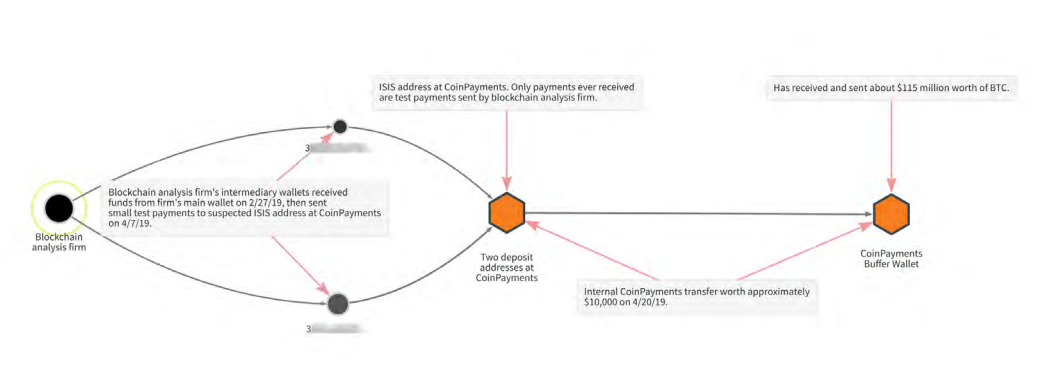
But what stands out most when comparing the two campaigns is how much more sophisticated AQB's address generation infrastructure is, as it presents a significant challenge to investigators tracing donations. It's possible that in 2020 and beyond, more terrorist organizations will embrace cryptocurrency as a fundraising tool and push for further advancements that allow them to take in more funds and enhance their privacy.

Terrorist groups have proven adept at leveraging emerging technologies to advance their agenda, with groups like ISIS' mastery of social media being a prime example. The last thing we want is for cryptocurrency to become another tool at their disposal. Law enforcement, intelligence agents, and the cryptocurrency community as a whole must remain vigilant to ensure this doesn't happen.

The importance of certainty when publicizing research on terrorism financing

As part of the cryptocurrency community, we also know how important it is to be responsible and judicious when releasing information on a subject as serious as terrorism financing. False reports can not only misinform analysis, but also damage the reputation of both individual cryptocurrency firms implicated and the industry as a whole.

We saw an unfortunate example of this earlier in 2019, when a blockchain intelligence firm reported that Bitcoin payments facilitated the Easter Sunday Sri Lanka bombings carried out by ISIS. **Media reports** amplified the firm's findings, which claimed that ISIS collected funds using CoinPayments, a cryptocurrency payment processor. The firm's conclusion was based on a movement of roughly $10,000 worth of cryptocurrency from one CoinPayments address controlled by ISIS to another shortly before the attacks. The firm also claimed that the balances in CoinPayments' wallets surged from $500,000 to $4.5 million just one day before the Easter attacks but dropped back to $500,000 right after the attacks took place. However, our analysis suggests those findings are likely incorrect.



Using the information provided in their report, we used Chainalysis Reactor to reconstruct the blockchain analysis firm's research which is illustrated in the above graph. In the middle of the graph, we see a wallet that the blockchain firm attributed to ISIS. On the left, we see the blockchain analysis firm make two very small transfers to that wallet — the only funds it has received to date — likely to learn more about its activity. On the right, we see the approximately $10,000 transfer the firm pointed to in its analysis. However, the second wallet is actually controlled by CoinPayments itself. The transaction worth approximately $10,000 was simply an internal transaction that is standard practice for a payment processor like CoinPayments. Likewise, the $4 million balance increase the firm points to directly before the attacks also occurred in that second, CoinPayments-controlled wallet. We can confirm from our coverage of millions of CoinPayments addresses that this was also an internal movement of funds from another CoinPayments wallet and has no coonnection to terrorism.

Conclusion

What comes next for crypto crime?

Crypto crime will likely continue to evolve in both scope and technological sophistication, just like cryptocurrency itself. As law enforcement, regulators, and cryptocurrency professionals improve their ability to prevent and respond to various forms of crypto crime, the criminals themselves will also grow more sophisticated — that's the one constant we've seen as blockchain investigators.

Here are some thoughts on for how crypto crime might evolve in the near term.

1. **More non-custodial mixers.**
   Following the closure of Bestmixer, we believe users — criminals and not — will search for alternatives to third party custodial mixers such as wallets that offer native mixing functionality similar to CoinJoin wallets like Wasabi. It's likely that more currencies besides Bitcoin will get analogs to CoinJoin, as we've seen with CoinShuffle for Bitcoin Cash and mixing via smart contracts for Ethereum.

2. **Chain hopping as another alternative to custodial mixing services.**
   In addition to native in-wallet mixing, we also think some criminals may begin to favor chain-hopping as an alternative to third-party mixing. Chain hopping is the process of swapping one type of cryptocurrency for another, often several times in quick succession, typically at low-KYC exchanges so as to further obfuscate the path of funds.

3. **Privacy coins.**
   As we mentioned in the darknet markets section, privacy coins like Monero are gaining popularity and could become the cryptocurrency of choice for more criminals in 2020. Privacy coins increase user anonymity by using an obfuscated public ledger rather than a fully public one like Bitcoin's. As more exchanges begin accepting privacy coins, they should also collaborate with regulators, law enforcement, and one another to establish frameworks for investigations of criminals who use privacy coins.

4. **More anonymous P2P exchange options.**
   We believe that non-custodial, decentralized exchanges like Bisq network will continue to gain popularity with criminals in 2020. Decentralized exchanges allow peer-to-peer transactions without the exchange acting as a mediating third-party. We may also see criminals using P2P exchanges benefit from upcoming **Bitcoin protocol changes** like Taproot and Schnorr Signatures, which make the complicated smart contract-based transactions carried out on P2P exchanges look identical to standard transactions on the blockchain.

All of these changes would give criminals more ways to hide their cryptocurrency activity and make transactions more difficult to track. Nonetheless, we feel confident that with collaboration between cryptocurrency businesses, law enforcement, regulators, and blockchain analysis companies like Chainalysis, we're more than capable of meeting the challenge. As the case studies presented in this report show, we've made huge strides in fostering collaboration between these stakeholders over the last couple of years already. Our goal for 2020 is to build on that momentum, continue to build trust in blockchains, and make cryptocurrency a safer industry for all participants.

Chainalysis

ABOUT CHAINALYSIS

Chainalysis is the blockchain analysis company providing data and analysis to government agencies, exchanges, and financial institutions across 40 countries. Our investigation and compliance tools, education, and support create transparency across blockchains so our customers can engage confidently with cryptocurrency. Backed by Accel, 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:

visit blog.chainalysis.com

Building trust in blockchains