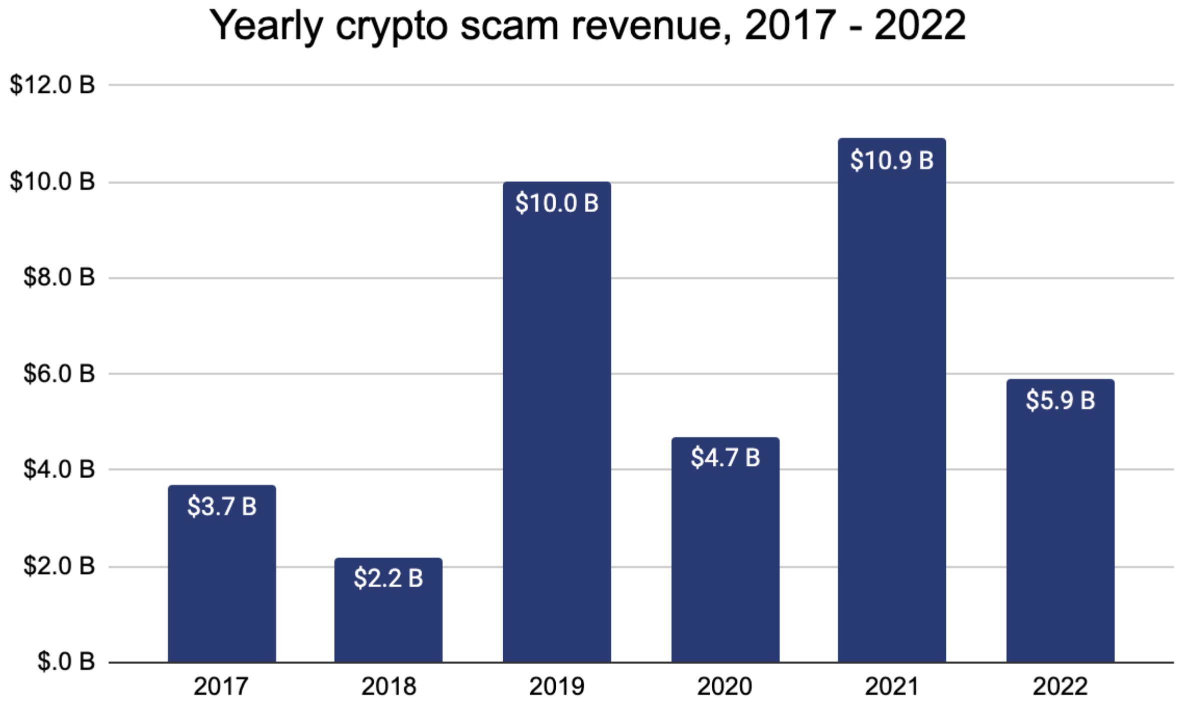
Crypto Scam Revenue Dropped 46% in 2022, While Blockchain Analysis Finds Links Between What Appear to be Distinct Scams

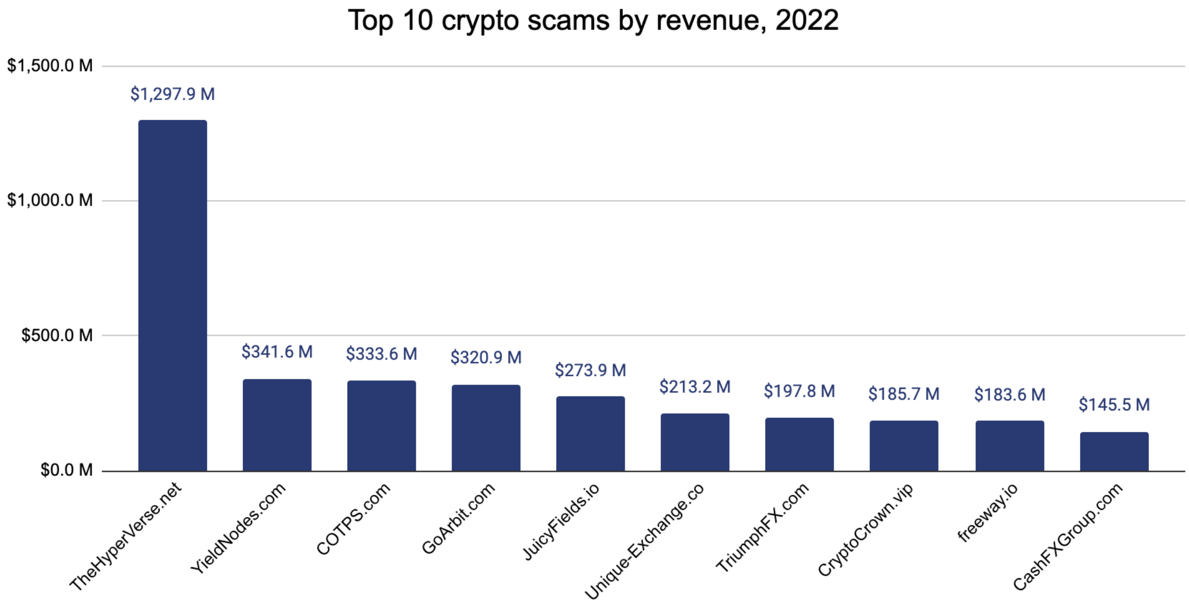
While scams remain the largest form of cryptocurrency-based crime (that is, if we ignore transactions associated with OFAC-sanctioned entities, which can be criminal or not depending on jurisdiction), crypto scam revenue fell significantly in 2022, from $10.9 billion the year prior to just $5.9 billion.



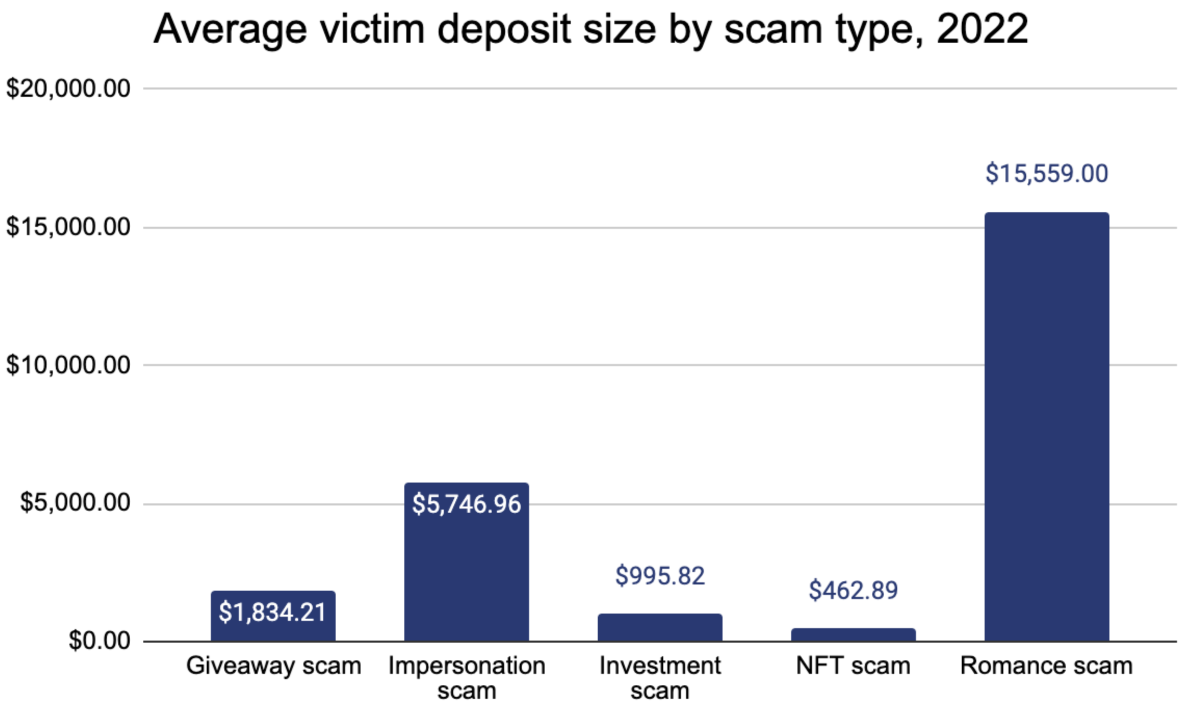
As we'll explore below, we attribute most of this decline to market conditions, as scam performance tends to worsen when cryptocurrency prices are in decline. However, some crypto scam types are growing despite the ongoing bear market. We must also add that our numbers are a lower-bound estimate, and that as with all forms of crypto crime, our estimates of the true amount lost to fraudsters will grow as we identify more addresses associated with scams. Underreporting exacerbates this problem, particularly in the case of so-called "pig butchering" scams, which we know to be a growing problem. In addition to scamming trends, we'll look at how some investigators on the cutting edge are using blockchain analysis to combat pig butchering scams, and also share data that points to the interconnected nature of the crypto scam ecosystem.

2022 crypto scam activity summarized

While scam revenue dropped overall, we still saw a number of highly successful scams, the top being Hyperverse, which pulled in nearly $1.3 billion in revenue.



All ten of 2022's top scams were investment scams, which as a category dominated overall revenue last year. However, that doesn't mean we can ignore other types of scams. Despite having lower overall revenue as a category, romance scams appear to have been the most destructive on a revenue-per-victim basis.



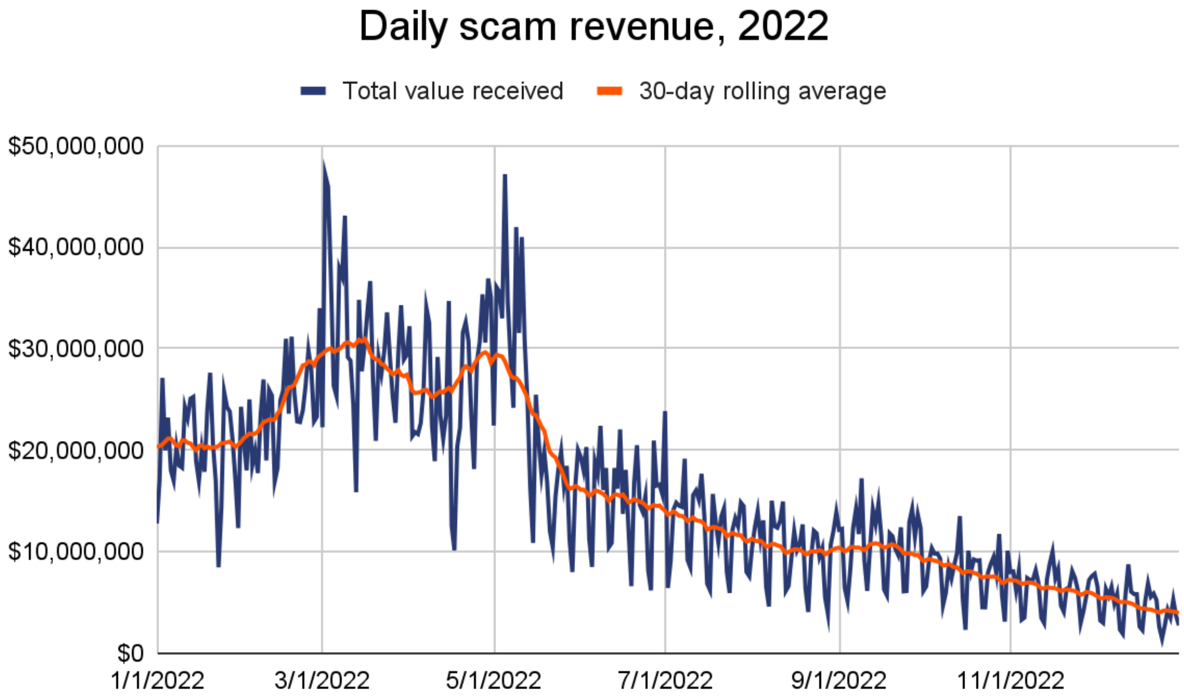
A guide to the scam categories we track:

- ***Giveaway scams*** *are scams in which fraudsters solicit victims to send them cryptocurrency, promising to send them more in return. Giveaway scammers often impersonate celebrities to lend credence to the promise.*
- ***Impersonation scams*** *are scams in which fraudsters pretend to be someone in a position of authority or expertise — for instance, an IRS or Social Security representative — and tell victims they must send in cryptocurrency to correct some kind of problem or avoid getting in trouble.*
- ***Investment scams*** *are scams in which fraudsters promote a fake investment company promising outsized returns.*
- ***NFT scams*** *are scams in which fraudsters trick victims into buying fake NFTs designed to resemble more notable collections.*
- ***Romance scams*** *are scams in which the fraudster pretends to build a romantic relationship with the victim in order to convince or guilt them into sending them money. Romance scams can also include "pig butchering scams," which blend elements of romance scams and investment scams.*

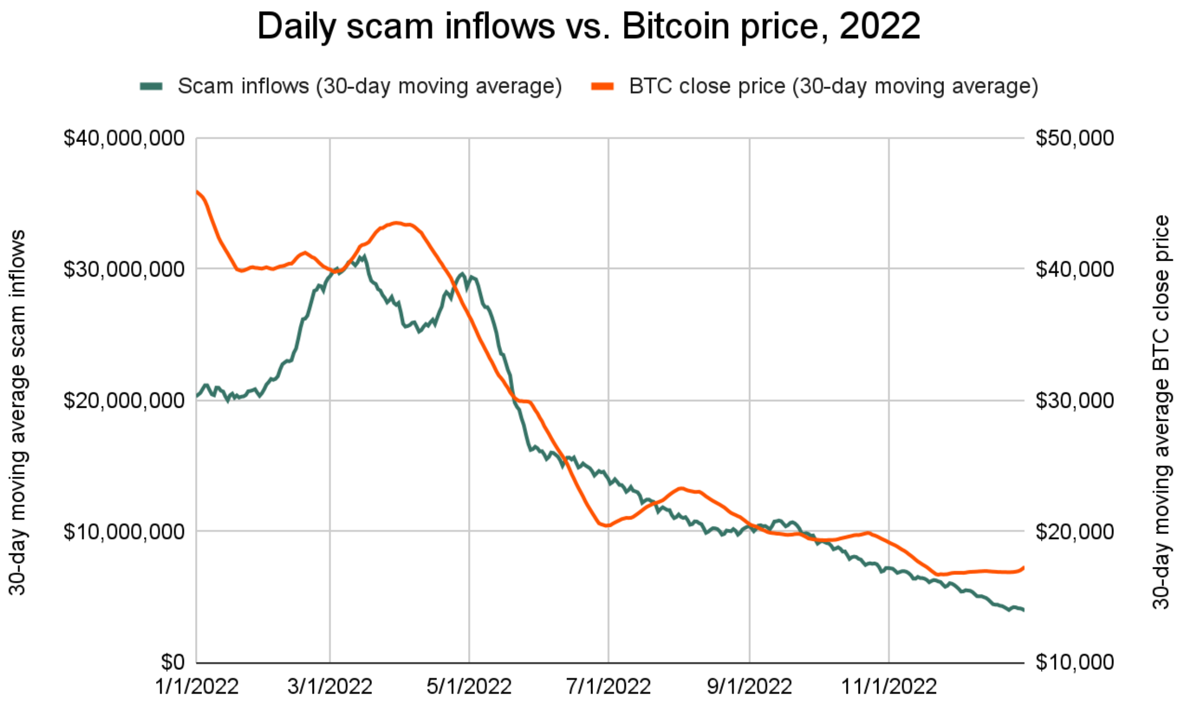
Romance scams took an average victim deposit of nearly $16,000, nearly triple the next-closest category. It's also important to remember that underreporting by victims is likely more prevalent in romance scams due to their uniquely personal nature, so their total revenue and overall reach is probably higher than one would think based strictly on on-chain data.

Crypto scams and market dynamics

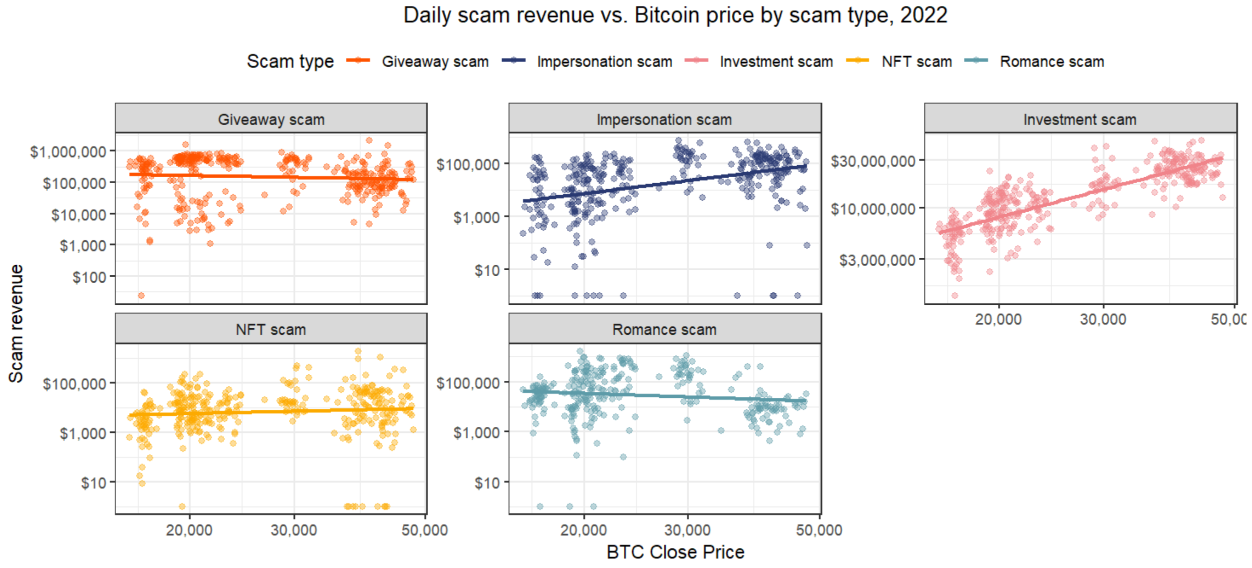
Cryptocurrency scam revenue began the year trending upwards, but plummeted in early May — the same time the bear market set in following the collapse of TerraLuna — and then declined steadily throughout the rest of the year.



This fits with trends we've previously observed on how wider trends in crypto markets affect scamming. Generally speaking, scams take in less revenue from victims at times when crypto asset prices are declining. We can see this clearly on the graph below, which tracks scam revenue against the price of Bitcoin throughout 2022.

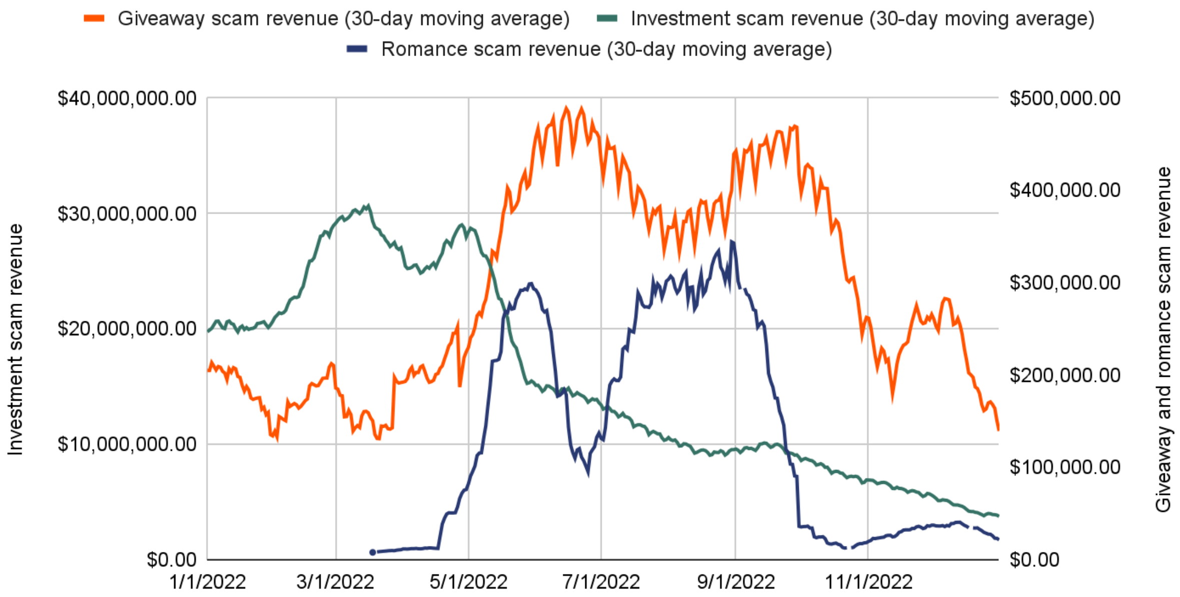

Daily scam inflows vs. Bitcoin price, 2022

Scam revenue throughout the year tracks almost perfectly with Bitcoin's price, consistently maintaining a three-week lag between price moves and changes in revenue. However, not every distinct type of scam follows this pattern — some types of scams see revenue changes increase as crypto asset prices decrease.

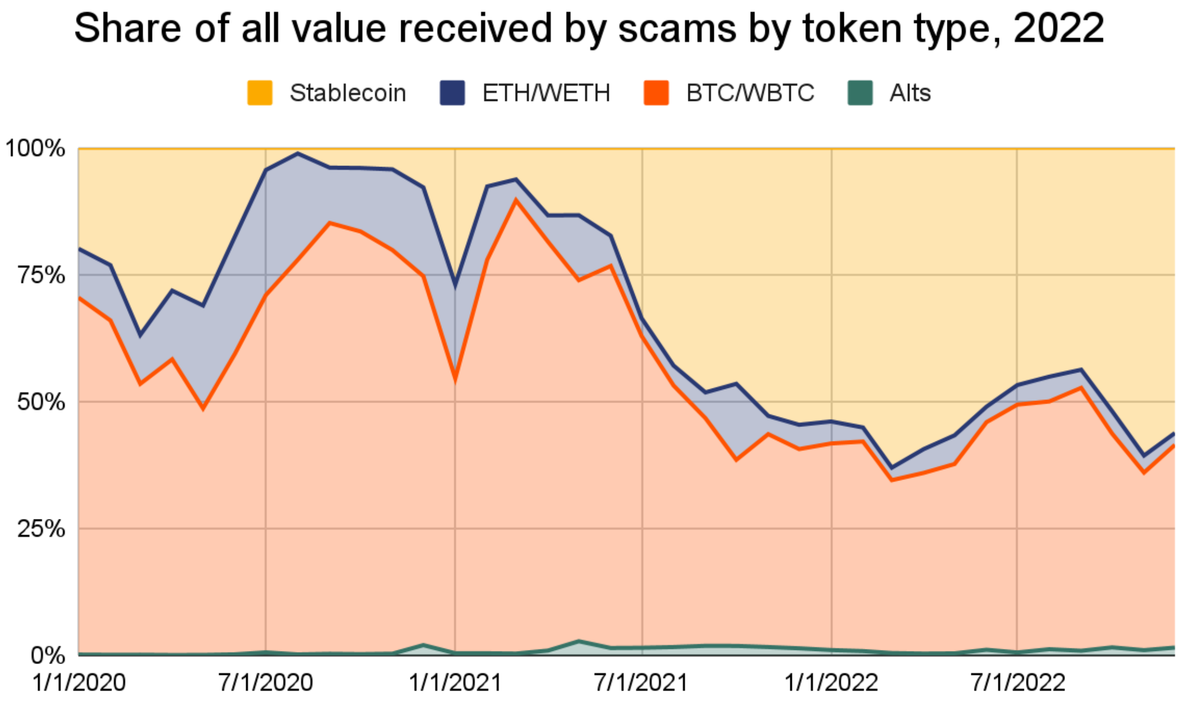

Daily scam revenue vs. Bitcoin price by scam type, 2022

For instance, unlike other kinds of scams, romance and giveaway scams don’t show a positive correlation with Bitcoin’s price (we use Bitcoin here because it’s the biggest cryptocurrency by market cap and its price movements are generally correlated with those of other crypto assets). Investment scams, which also happen to get by far the most revenue of any other scam type, are one of the most correlated with Bitcoin’s price. The reason for the difference likely lies in how the scams are pitched to victims. Investment scams typically promise users outsized investment returns, often based on an algorithmic, “can’t lose” trading strategy. That pitch is probably more likely to succeed when the asset prices are growing, and the news is filled with stories of crypto investors striking it rich. Romance scams, on the other hand, are more about building a personal relationship with the victim, and the scammer convincing them that they care about the victim and need their help. That kind of emotional pitch is probably equally effective regardless of trends in the wider market, because the victim’s primary goal isn’t to get rich quick, but rather to help someone they believe to be a potential romantic partner. In fact, scammers may even pivot to romance scams versus investment scams in times of declining asset prices for those very reasons, which would intensify this trend further. For those reasons, romance scams and other scam types whose performance doesn’t track with Bitcoin price followed different revenue patterns throughout the year compared to investment scams.

Daily scam revenue by scam type: Investment scams vs. Giveaway scams vs. Romance scams, 2022



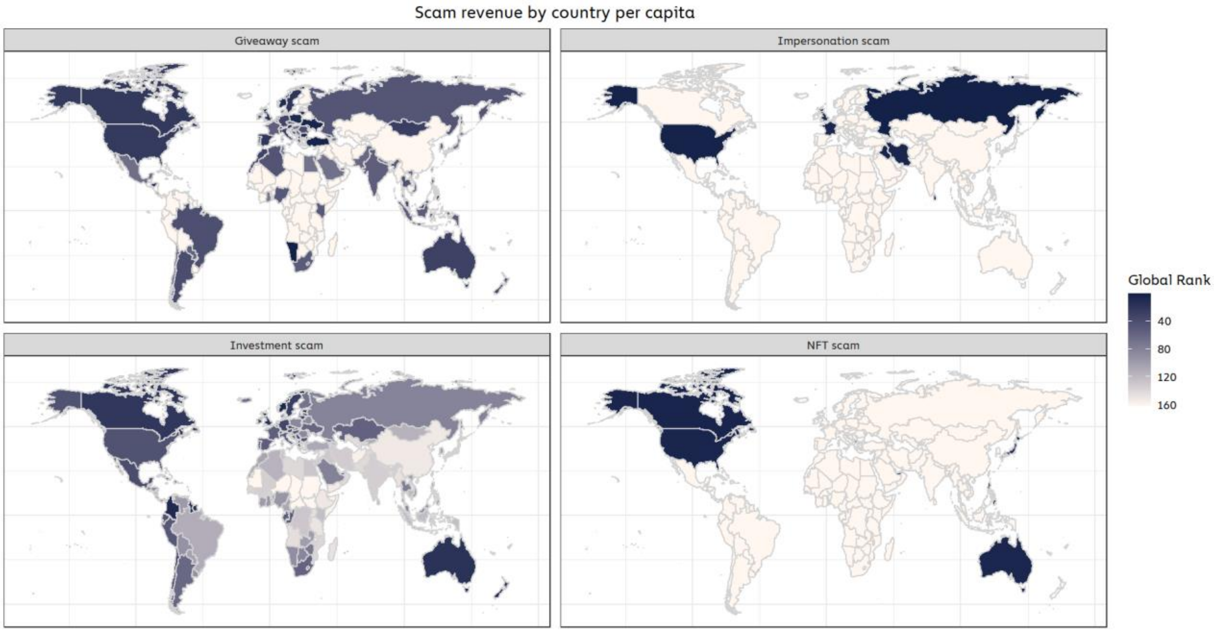
Market conditions may have also influenced another trend we’ve seen develop over the past two years: the rise in usage of stablecoins by scammers.



Prior to 2022, most scams took payments primarily in Bitcoin. But this started to change in 2021, with scammers taking more and more of their revenue from victims in stablecoins, during a period of time when the price of crypto assets like Bitcoin was trending upward. Similarly, we see a spike in scammers' use of Bitcoin in mid-2022, when asset prices were trending down. This seems counterintuitive — wouldn't scammers prefer to accept victim payments in Bitcoin when Bitcoin is trending up? Scammers' solicitation of stablecoins over Bitcoin during bull markets may represent a hedge against a possible market crash. Scammers may also have better luck soliciting stablecoins in a bull market given that they have no price upside, while potential victims may be more inclined to hold their Bitcoin in the expectation it will go up in value.

Who's falling victim to scams?

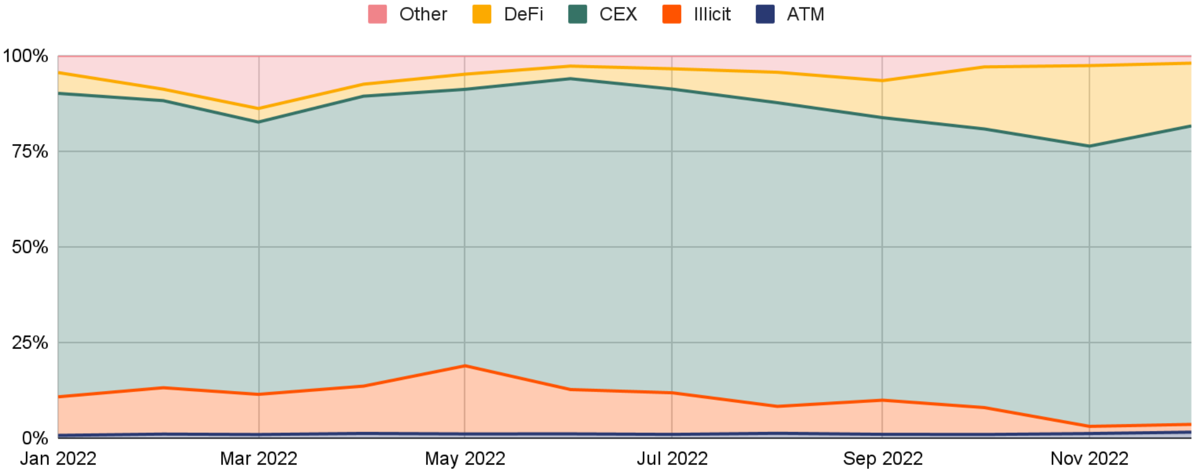
Different types of scams show different levels of effectiveness depending on the geographic area of the victim. Much of this is likely due to the location of the scammers themselves, as this will impact their ability to pitch victims based on their shared language and cultural context. But the geographic trends in scamming in many cases also match the geographic trends we've seen in the wider cryptocurrency ecosystem. We can see this on the chart below, which quantifies the amount different types of scams have taken from victims in different countries on a per capita basis.



Most scam types disproportionately receive revenue from the U.S., but this is especially true for NFT-related scams. We've written previously about the fact that NFTs are especially popular in North America, particularly when it comes to onboarding new cryptocurrency users — who are probably more likely to fall for scams given they're less experienced in the space — so this doesn't come as a huge surprise. Investment scams, which are the largest type of scam by revenue, draw on a wider array of countries, with Australia and parts of South America being the hardest hit.

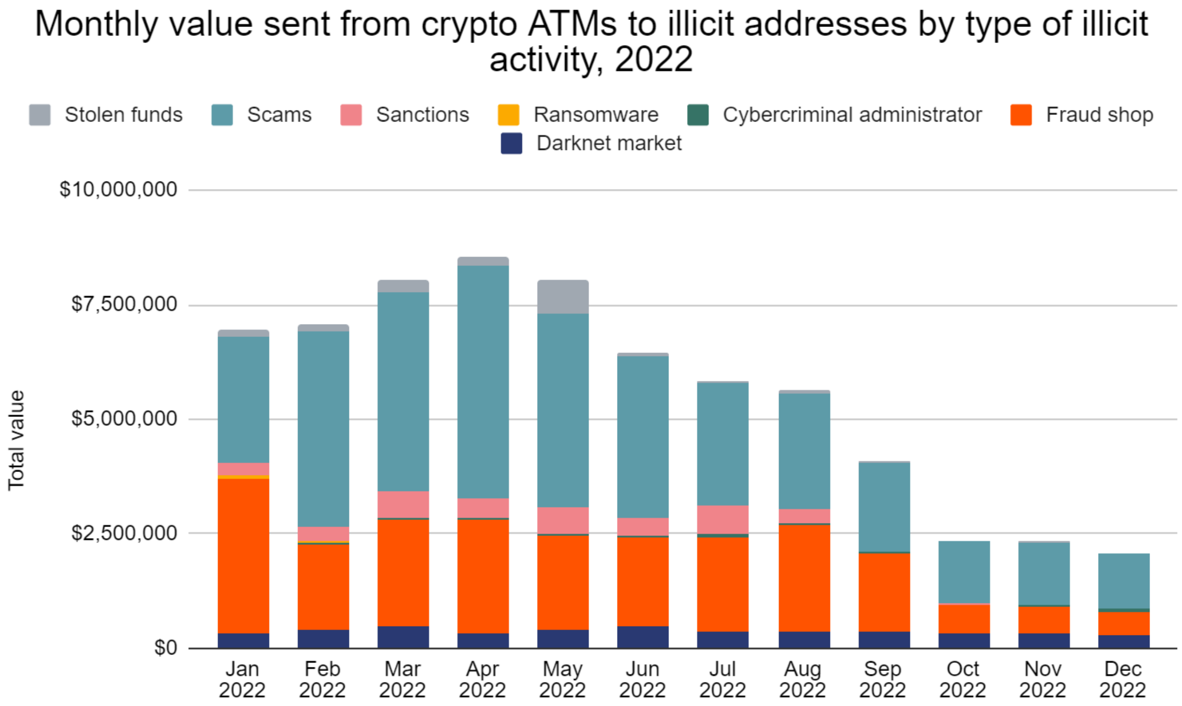
What services are these users relying on to send to scams?

Monthly share of value sent to scams by sending service type, 2022



The vast majority of victim payments to scams come from centralized exchanges. We also see scams receiving significant amounts from other illicit addresses, much of which are themselves other scams and could indicate that many distinct scams are actually controlled by the same individuals or groups, which is a topic we'll explore further below. DeFi protocols also send a significant amount to scams.

Our data also indicates that roughly 1.0% of victim payments to scams come from crypto ATMs. ATMs are an interesting category to dig into, as they aren't generally used to send funds to many other illicit address types — in fact, just 2.2% of funds sent from ATMs in 2022 went to illicit addresses, for a total of $67.5 million. However, a disproportionate share of that total goes to addresses associated with scams. Industry observers and law enforcement have noted this trend before, and blockchain analysis allows us to quantify it.



In 2022, crypto ATMs were used to send at least $35.3 million to scammers, which represents more than half of all funds sent to illicit addresses using ATMs. While the dollar figures represent lower-bound estimates, the disproportionate share of funds leaving ATMs for scam addresses may be a result of crypto scammers' targeting of those who are new to cryptocurrency and not technologically adept. For that audience, an ATM similar to the ones they use for fiat may offer what appears to be the easiest way to initiate a cryptocurrency transaction, as users can simply insert cash, type in a cryptocurrency address, and complete their transfer. The data indicates that crypto ATM businesses could better serve their customers and significantly reduce their exposure to illicit activity by educating customers on scams, or even taking steps to warn customers before they transfer funds to an address known to be associated with a scam.

Concentration in crypto scamming: Blockchain analysis indicates large scam networks may account for lots of fraudulent activity

We've often talked about how many forms of cryptocurrency-based crime appear to be driven primarily by small groups of prolific criminals despite what appear at first glance to be a large number of distinct on-chain entities participating in a given type of crime. For instance, in our ransomware section, we discuss how despite there being many ransomware strains active in any given year, a small group of ransomware affiliates are responsible for many of the attacks carried out by different strains, which we can see by analyzing those affiliates' wallets and observing that they receive cryptocurrency from many different strains.

Does the same thing hold true for crypto scams? We attempt to answer that question below by looking for evidence of on-chain interconnectedness between several different scam entities active in 2022. We'll also show how analysis of off-chain data — specifically, the copy on the public-facing websites associated with many crypto investment scams — can enable investigators to find more scams once they've identified one.

Our analysis starts with five crypto scams the CFTC identified and filed charges against in September 2022:

- Cryptostockoptionstrade Ltd
- Global Smart Option Broker Ltd
- Hypertradingoption Ltd
- Stockbrokertechniques Ltd.
- SprintTrade

The CFTC's press release doesn't explicitly state whether all five scams are believed to be controlled by the same individual or group, but it does note that they purport to be located at the same Los Angeles street address. That alone doesn't necessarily mean all of these scams are associated with the same individual or group — the idea of a scammer simply copying text from the website of another scam, such as the listed street address, doesn't seem to be out of the question. With that in mind, we decided to search the web for other websites of purported crypto investment companies whose websites contained identical copy to those of the scams in the CFTC press release — not just street addresses, but other pieces of web copy such as customer testimonials — and cross-reference them with our own data to see if textual analysis of scam websites could turn up other scams that may or may not be connected to the original five named by CFTC. Ultimately, we were able to find functioning websites and cryptocurrency addresses for three of the five scams named by CFTC, so those three were what we used as reference points to find more scams.

In total, this analysis uncovered another 200 confirmed scams whose websites contain pieces of copy identical to that of the three CFTC-identified scams for which we found active websites. In other words, website analysis led to a 66x increase in the number of scams uncovered. The grid below breaks down the newly identified scams by the specific website elements they had in common with the five scams in the CFTC press release.

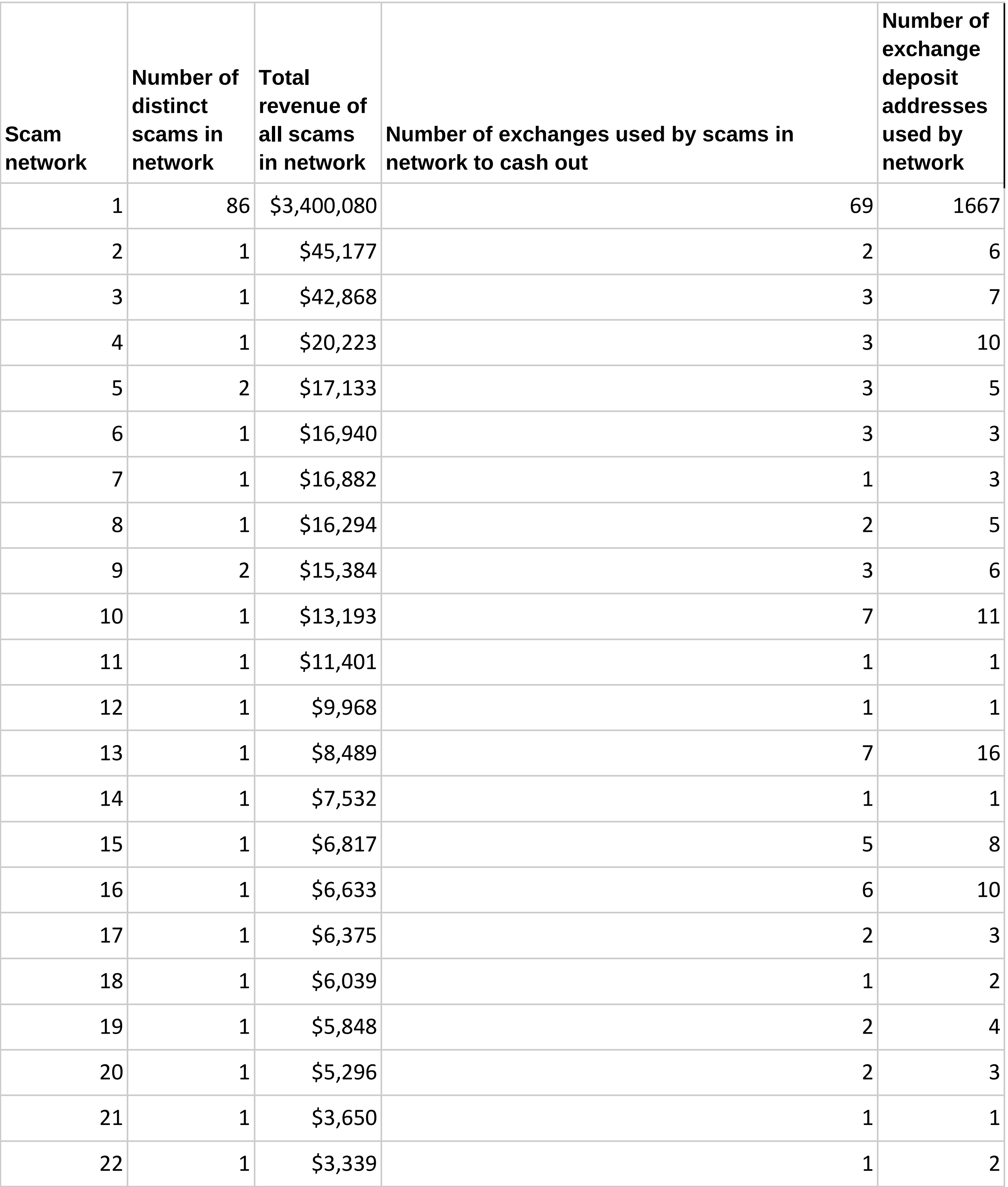
Number of new scams identified	How we found them
88	Same street address as CFTC-identified scam
102	Identical customer testimonial as CFTC-identified scam

Right off the bat, we can see how scanning for websites with copy identical to that of known scam websites can be valuable, as we quickly unearthed an additional 200 scams. But again, that on its own doesn't prove that all 200 are run by the same individual or group, as it's entirely possible scammers are just stealing web copy from each other due to laziness, or even in an effort to throw investigators off and give the impression that their scam is the work of someone else. However, we can use blockchain analysis to find another commonality between scams in this set of 200 that could be a stronger indicator of interconnectedness or common control: Deposit address overlap.

As we discuss in our money laundering analysis, criminals dealing in cryptocurrency generally want to move their ill-gotten funds to a fiat off-ramp service where the crypto can be converted into cash — usually, this means a centralized exchange. If we see two scams moving their cryptocurrency to the same deposit address at an exchange, it means one of two things: Either one scammer controls the deposit address, meaning they are behind both scams, or the deposit address belongs to a nested service that's being used to launder funds — in that case, a single scammer may still be behind both scams and simply prefers to funnel funds from both to the same nested service, but it could also mean that two separate scammers simply happen to use the same service. So, while deposit address overlap isn't proof positive that two scams are controlled by the same individual or group, it certainly adds to the likelihood that they are.

Given that, our next step was to analyze the exchange deposit addresses to which all 203 scams had ever sent funds, and sort the scams into distinct, mutually exclusive **scam networks** based on deposit address overlap. For the purposes of this analysis, we consider two scams to be part of the same network if they sent any amount of cryptocurrency to the same deposit address. Two scams can also be part of the same scam network without depositing to the same deposit address if they are both connected to a third scam via another deposit address. In other words, if Scam A sends funds to Deposit Address 1 and Deposit Address 2, Scam B sends funds to Deposit Address 2 and Deposit Address 3, and Scam C sends funds to Deposit Address 3 and Deposit Address 4, then we would consider all three scams to be part of the same scam network. Scams that never deposited anything to an exchange were excluded from the analysis.

After applying this methodology to the 203 scams in our dataset — the original three identified by CFTC plus the 200 additional scams with website commonalities — we found that 73 of them had never deposited to an exchange. The remaining 130 fit into 43 distinct scam networks based on deposit address overlap, but ultimately, one network stood out above the rest.



Scam network	**Number of distinct scams in network**	**Total revenue of all scams in network**	**Number of exchanges used by scams in network to cash out**	**Number of exchange deposit addresses used by network**
1	86	$3,400,080	69	1667
2	1	$45,177	2	6
3	1	$42,868	3	7
4	1	$20,223	3	10
5	2	$17,133	3	5
6	1	$16,940	3	3
7	1	$16,882	1	3
8	1	$16,294	2	5
9	2	$15,384	3	6
10	1	$13,193	7	11
11	1	$11,401	1	1
12	1	$9,968	1	1
13	1	$8,489	7	16
14	1	$7,532	1	1
15	1	$6,817	5	8
16	1	$6,633	6	10
17	1	$6,375	2	3
18	1	$6,039	1	2
19	1	$5,848	2	4
20	1	$5,296	2	3
21	1	$3,650	1	1
22	1	$3,339	1	2

23	1	$3,210	5	43
24	1	$2,876	9	66
25	1	$2,823	1	3
26	1	$2,417	2	6
27	1	$2,105	1	1
28	1	$2,061	2	2
29	1	$2,015	1	2
30	1	$1,885	1	4
31	1	$1,773	1	1
32	1	$1,387	1	3
33	1	$1,080	1	2
34	1	$971	4	11
35	1	$831	1	3
36	1	$755	1	1
37	1	$295	1	2
38	1	$170	1	1
39	1	$150	2	2
40	1	$137	1	1
41	1	$123	1	1
42	1	$117	1	1
43	1	$110	1	2

Network 1 contains 86 active scams that have made a combined $3.4 million from victims, and utilizes 1,667 total exchange deposit addresses. Interestingly, all of the scams identified in the CFTC press release that kicked off this analysis are part of Network 1 as well. Two of the remaining 42 networks are composed of two scams, while the rest only have one scam apiece. Overall, the 86 scams in Network 1 account for 91.6% of the total revenue of all 130 scams included.

We can’t know from on-chain data alone whether the 86 scams in that network are each run by the same individual or group. The only way to know for sure would be for law enforcement to carry out an investigation, which would likely include sending subpoenas to the exchanges to which the scammers are depositing funds to see whose user accounts they’re associated with. However, even if the scams in each network just coincidentally depend on the same nested services or money launderers to convert their crypto into cash, that would still be positive news for investigators, as it would mean that they could disrupt several scams at once by going after a small number of money laundering service providers.

Overall, our data suggests that the cryptocurrency scamming ecosystem is smaller than it appears at first glance. We look forward to applying our scam network methodology to a wider number of scams beyond the 203 included in this analysis, and will share insights from that expanded analysis where possible.

How investigators are fighting back against pig butchering scams

What are pig butchering scams?

One particularly sophisticated type of crypto scam, pig butchering, gained media attention in 2022. Analogized to fattening a pig before slaughter, pig butchering is a slow-burn scam focused on building trusting relationships. Most of these operations function in similar fashion. Scammers find targets with whom they develop relationships over time. They create fake social media accounts and dating site profiles showcasing lavish lifestyles and send random messages to connect with victims. Frequently used apps include WeChat, WhatsApp, and even LinkedIn.

While the scammers are relationship-building, they're also performing reconnaissance to see which victims have the most investment potential. Once targets are identified and trust is built, the scammer subtly mentions a crypto investment website with which they've had personal success.

Alastair McCready, Southeast Asia Editor at Vice World News says, “You're not getting an email saying ‘there's a million dollars that needs releasing in a bank account in Switzerland.’ This is just kind of subtle little messages, like on WhatsApp. And if you were the kind of person who was kind of looking for some sort of connection, you could see how you'd be easily lured in, sucked in by a seemingly innocuous conversation with a nice person.”

Over weeks or months, scammers coach victims on how to use these fake sites, convincing them to invest everything they possibly can. These platforms falsify returns and make it appear as though victims have access to the funds. Initially, they can make withdrawals. Once scammers believe they've exhausted their victims' potential, they try convincing them to take out loans. When victims become wary, the scammer restricts access to funds and attempts to extort them for even more money.

Sadly, those on the receiving end of pig butchering are not the only victims. Most of these crimes originate in Southeast Asia and require human trafficking to run. Around 2016, a large construction project began in Sihanoukville, a coastal town in Cambodia. Chinese investors built hundreds of casinos to attract tourists from mainland China, where gambling is illegal. In 2019, Cambodia banned online gambling and then COVID-19 hit, devastating Sihanoukville's tourist economy. Many businesses turned to criminal activity to generate revenue; some recruited workers for customer service jobs under false pretenses. On arrival, new employees were ushered into hotel casino complexes — now walled, guarded compounds — and weren't allowed to leave. Casino-based scam centers like these are also found in Laos and Myanmar.

As for pig butchering scam victim profiles, those run the gamut from elderly to millennial and across genders, too. Asian Americans are often targeted because it's easier for scammers to communicate with them using a common language. Pig butchering also preys on people's kindness and vulnerability; one woman was targeted after she responded to a Facebook ad about adopting a dog.

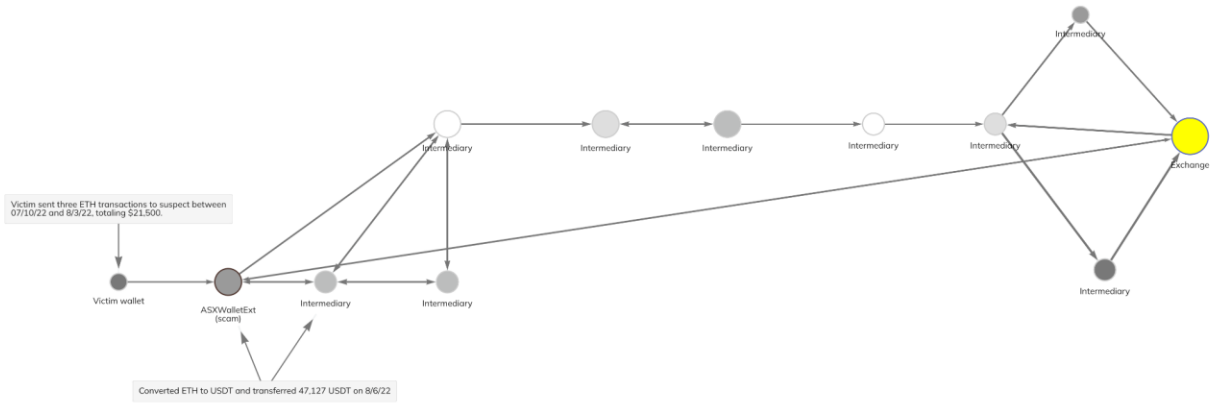
How the REACT Task Force and Santa Clara County are helping victims

Agents from California's Regional Enforcement Allied Computer Team (REACT) investigated several pig butchering scams last year; to date it has investigated over 50 cases. Comprised of local, state, and federal agencies covering five counties in the Bay Area, the REACT task force, including Santa Clara County's Deputy District Attorney, Erin West, is demonstrating how law enforcement can successfully conduct crypto crime investigations and recover funds for victims.

Rather than shutting down easily-replaceable websites or trying to arrest overseas scammers in problematic jurisdictions, REACT's main goals are to quickly assess stolen funds by tracing the victim's initial transfer out of an exchange or wallet to a suspect, and attempt to effect a seizure. When tracing funds during investigations, the agency doesn't dwell on pass-through wallets; it targets those containing funds that it can directly attribute to victims as California law states that law enforcement can only seize funds that meet that criteria.

Since many citizens and even law enforcement agencies believe that crypto transactions aren't traceable, these investigations are full of unique challenges. REACT detective Chris Vigil says that when crypto scams affecting private individuals occur, investigators don't typically get involved until weeks or months later — victims often don't realize they have any recourse or don't know where to go for help. Meanwhile, most local law enforcement doesn't have the resources to investigate these crimes. However, in cases where victims do reach out to more than one agency, deconflicting information poses a substantial challenge.

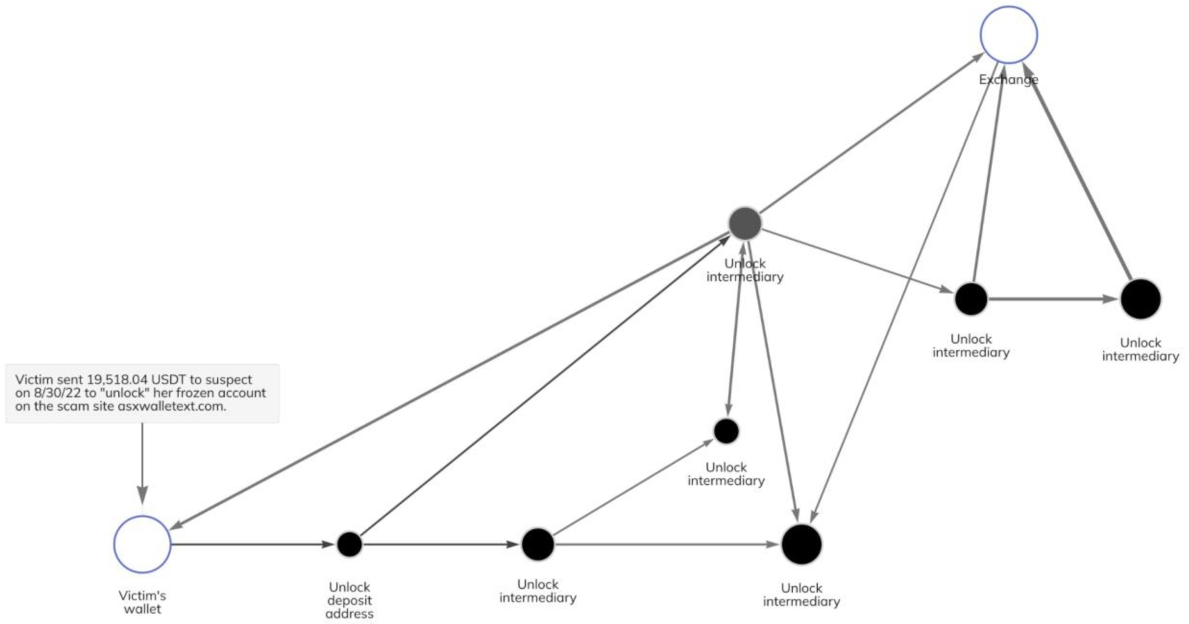
To successfully investigate crypto scams requires tools that help law enforcement trace funds in order to effect seizure. The graph below illustrates how REACT tracks cryptocurrency transactions for a typical pig butchering scam, and demonstrates how bad actors transfer funds through intermediary wallets in order to move them to an exchange. In this case, the victim transferred cryptocurrency to wallets associated with four different versions of the same scam over a period of months. By following transfers across intermediary wallets, the investigation tied different pig butchering sites together, too.



Victim sent three ETH transactions to suspect between 07/10/22 and 8/3/22, totaling $21,500.

Converted ETH to USDT and transferred 47,127 USDT on 8/6/22

Between July 10 and August 3, 2022, the victim sent three ETH transactions to the fraudulent investment site ASXWalletExt.com, totaling almost $21,500. From there, the suspect converted the ETH to USDT and transferred funds to various intermediary wallets with exposure to three other investment scam sites. They later cashed out funds at an exchange. Next, the scammer extorted the victim further, saying they would “unlock” her frozen account on ASXWalletExt.com, compelling her to send roughly $19,500 USDT from her exchange account, as we see on the second graph below. By tracing subsequent transactions across intermediate addresses, REACT observed the suspect cashing out at a large exchange.



Victim sent 19,518.04 USDT to suspect on 8/30/22 to "unlock" her frozen account on the scam site asxwalletext.com.

Once REACT agents are able to obtain judicial authorization for a seizure, the cryptocurrency is then transferred to a government-controlled account. When the funds are secured, the case is referred to West who works with the courts to release the funds to the rightful owner. To date, REACT and Santa Clara County have recovered funds in 15 of the pig butchering cases they have investigated. While the organization can only work cases with a victim or suspect in its jurisdiction, it often advises adjacent agencies and others across the country, too. REACT sees education and resources as the biggest roadblocks for law enforcement in investigating crypto crimes, but believes there are ways for more agencies to get involved. Having the statutory authority to effect seizures and obtaining buy-in from leadership — along with backing from prosecutors — are key to getting started. Then having the right policies in place to conduct investigations and using robust blockchain analysis tools to trace funds are essential for success.

###