Xangle

Crypto Investor Scam Report

Over $16 Billion Stolen From Investors Since 2012

Introduction

Cryptocurrencies are an exciting asset class. In just 12 years, the market has gone from $0 to over $900 billion as of today's writing. This growth has attracted investors of all sizes, from small retail investors to institutional investors with billions of dollars under management.

Unfortunately, it's also attracted hundreds — if not thousands — of bad actors who lie, steal, and cheat investors out of their capital. This is common when it comes to emerging technologies. Criminals use the hype and lack of regulatory infrastructure to take advantage of investors.

Despite the accelerated growth in the crypto assets market, scammers have plagued the market's reputation by luring investors with promises of quick and large returns, and then disappearing overnight with the invested capital. But how much harm have scammers brought to investors? How are authorities doing about prosecuting these scammers?

We wanted to answer these questions and more. In order to put some hard numbers to the size of this problem, we conducted research on crypto-related investment scams that took place from January 1, 2012 to December 31, 2020.

Our findings are based on media articles, press releases, legal filings, and court documents.

Key Findings

- **Over $16 billion lost**
  Investors have lost an estimated $16,546,541,956 since 2012.
- **136 scams**
  Investors lost that much from 132 different scams.
- **527 criminal charges**
  527 individuals have faced criminal charges for their roles in crypto-related scams.
- **160 years of combined sentence**
  The combined sentences for individuals involved in scams is over 160 years.
- **Members of 14 projects charged**
  14 crypto projects have seen their members charged and sentenced to date.
- **No charges on 24 projects**
  Of all reported scams, 24 projects or organizations have no known charges — civil or criminal.

Our Methodology

Because of the lack of standardization in the industry,
our research was conducted using the following guidelines:

- These findings include any organization that used cryptocurrency to defraud investors. This includes investment funds, ICOs, and trading schemes.
- The findings include only organizations or individuals who have received civil charges, criminal charges, or widespread allegations of fraud, such as the project's website or social media channels going dark after raising funds.
- It does not include projects that were hacked or breached.
- It does not include companies that were charged with running unregistered securities.
- It does not include those who were charged with crimes related to money laundering.
- The value of the investments were calculated in USD and are based on the amounts reported either by the media or through legal filings.
- Research was done in English so data could be missing for cases that were not covered by English speaking media.

All organizations and names listed are presumed innocent until found guilty by the courts.

Part 1

Over $16 billion lost

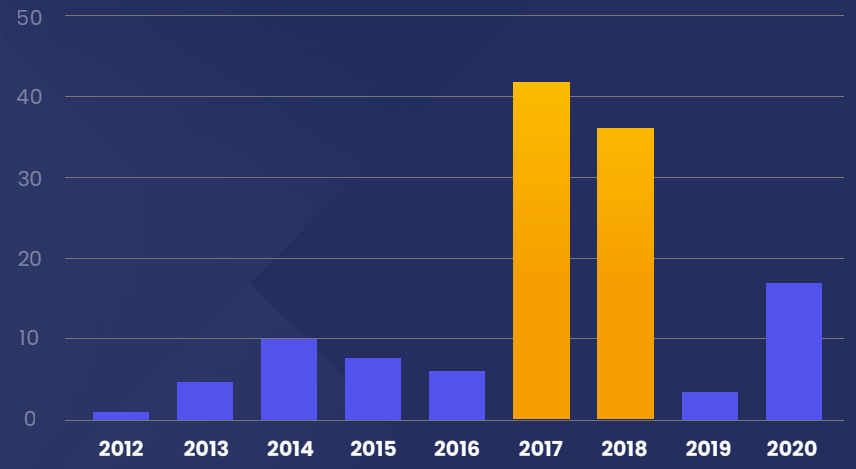
Based on our research, $16,149,661,014.00 has been stolen from investors since 2012 across 132 different scams.

The first big scam to rock the world of crypto was the Bitcoin Savings and Trust scam, which started in 2012 and eventually defrauded investors out of 146,000 bitcoin — roughly $97 million dollars at the time of the founder's initial charges by the SEC in 2013.

The founder, Trenton Shavers, was charged with one count of securities fraud and one count of wire fraud and faced up to 40 years in prison. He eventually pled guilty and received a sentence of 18 months in prison.

As the value of Bitcoin started to rise and other cryptocurrencies launched, scammers saw it as an opportunity to take advantage of enthusiastic investors who probably didn't know much about the space. There were 41 scams in 2017 — the biggest year for them to-date — followed by 39 in 2018. In the majority of cases, these scams took several years to uncover and see the founders charged, so it's worth noting that these numbers will likely increase dramatically in the years ahead.

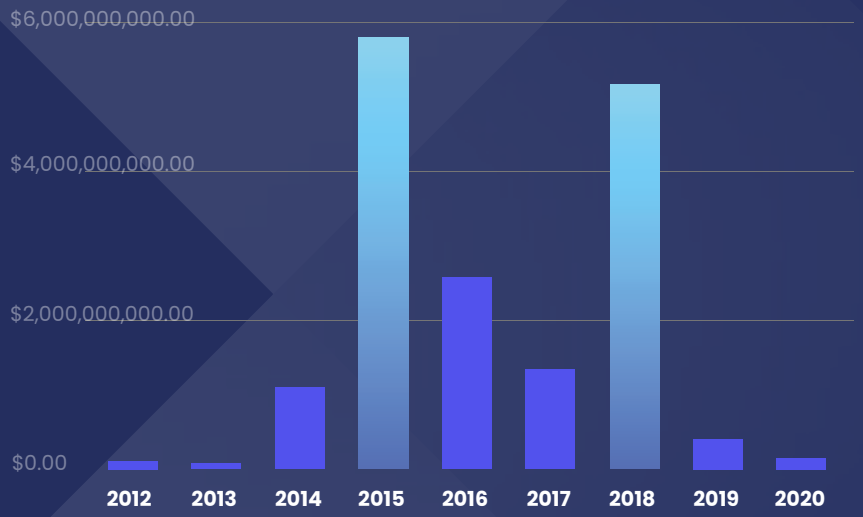
Crypto Investment Scam By Start Date



While 2017 saw the most scams launched, scams that started in 2018 led to the most investor losses. While these scams continued for years in most cases, the year listed represents the year that the scam was first launched.

Xangle

Crypto Investment Scams USD Total - Based on Start Date



In total, over $10 billion was stolen from five different mega scams. Arbistar 2.0, based out of Spain, was a Ponzi scheme, while all the others were pyramid schemes that leveraged their existing investor base to attract more investors into the scam.

Project	Type of scam	USD Value Stolen	Status
Arbistar 2.0	Ponzi	$1,000,000,000.00	Criminally charged
WoToken	Pyramid	$1,100,000,000.00	Criminally charged
PlusToken	Pyramid	$2,250,000,000.00	Criminally charged
BitConnect	Pyramid	$2,500,000,000.00	Criminally charged
OneCoin	Pyramid	$4,000,000,000.00	Criminally charged

Part 2

Criminal charges and arrests

Since 2012, 71 projects have suffered criminal charges, amounting to 527 individual arrests. OneCoin, which stole an estimated $4 billion USD from investors, had the highest number of arrests, with 140 individuals being arrested for their roles in the scheme .

Of these arrests, to date, only 14 projects have sent members to serve prison sentences for their crimes. The prison sentences total roughly 161 years.

Project	# of Members Sentenced to Date	Total Sentences	Country
CoinUp	5	41 years	South Korea
Plustoken	15	2-11 year sentences (individual sentences unknown)	China
WoToken	5	25 years	China
Argyle Coin	1	7 years	US
Blue Bit Banc (BBB)	1	7 years	US

Part 3

Uncharged Projects

Of the 132 identified scams, we've identified 324 that were widely reported to be scams yet could not find any reports regarding charges being filed or arrests being made.

While this could be due to the fact that they are currently under investigation, we wanted to reveal them here in order to raise awareness about the nefarious deeds taking place in the industry.

This report will be forwarded to the relevant authorities in each jurisdiction.

All organizations and names listed are presumed innocent until found guilty by the courts — our goal here is to simply ensure that this is on the radar of the appropriate authorities. If you feel there are any discrepancies here, please contact us.

Project	Believed Country of Origin	Amount Alleged to have been scammed
Emerald Mine	China	$2,500,000.00
Antimatter Kingdom	China	$35,000,000.00
Bitsane	Ireland	$570,000.00
Amplyfi.money	US	$866,000.00
BlockBroker	US	$3,000,000.00
CBDAO ($BREE)	Australia	$1,000,000.00
FairWin	China	$125,000,000.00
JoyToken	UK	$3,300,000.00
Miroskii	US	$833,000.00
Sharktron Defi	US	$10,000,000.00
Velox 10	Kenya	$2,500,000.00
Bitsonar	Ukraine	$2,700,000.00
Benebit	US	$10,000,000.00

Part 3

Uncharged Projects

Of the 132 identified scams, we've identified 324 that were widely reported to be scams yet could not find any reports regarding charges being filed or arrests being made.

While this could be due to the fact that they are currently under investigation, we wanted to reveal them here in order to raise awareness about the nefarious deeds taking place in the industry.

This report will be forwarded to the relevant authorities in each jurisdiction.

All organizations and names listed are presumed innocent until found guilty by the courts — our goal here is to simply ensure that this is on the radar of the appropriate authorities. If you feel there are any discrepancies here, please contact us.

Project	Believed Country of Origin	Amount Alleged to have been scammed
NVO	China	$8,000,000.00
CoinGather	China	$100,000.00
Compounder Finance	Ireland	$11,000,000.00
Yfdex	US	$20,000,000.00
BTC Global	US	$50,000,000.00
Ifan and Pincoin	Australia	$660,000,000.00
Optioment	China	$118,500,000.00
RepuX	UK	$4,700,000.00
Opair and Ebitz	US	$2,900.000,00
Confido	US	$375,000.00
Cryptokami	South Korea	$12,000,000.00

Conclusion

The findings of this study helped us quantify the crypto scam problem, assessing the harm that crypto scams have brought to investors and how effective authorities have been at prosecuting perpetrators thus far.

Adding to the hard numbers, here are our key takeaways:

- The longer bad actors are allowed to continue scamming investors, the longer it will take for the crypto asset class to institutionalize and mainstream adoption.
- Investigators should continue to keep track of this problem and monitor the evolution of these and later findings with the goal of cooperation between affected communities and authorities. Further research will also increase awareness of the methods scammers utilize to perpetrate their schemes so communities can protect themselves against them.
- We need to create, expand, and strengthen crypto regulatory frameworks worldwide to prevent scammers from taking advantage of loopholes with cryptocurrencies while being careful to not discourage the growth of the space.
- Education is key to help bring awareness to newcomers.

Our Methodology

Because of the lack of standardization in the industry,
our research was conducted using the following guidelines:

- These findings include any organization that used cryptocurrency to defraud investors. This includes investment funds, ICOs, and trading schemes.
- The findings include only organizations or individuals who have received civil charges, criminal charges, or widespread allegations of fraud, such as the project's website or social media channels going dark after raising funds.
- It does not include projects that were hacked or breached.
- It does not include companies that were charged with running unregistered securities.
- It does not include those who were charged with crimes related to money laundering.
- The value of the investments were calculated in USD and are based on the amounts reported either by the media or through legal filings.
- Research was done in English so data could be missing for cases that were not covered by English speaking media.

Know of Any Scam Projects?

This research will be updated every quarter. If you know of any scam projects that we should potentially include next quarter, please get in touch through our website.

Thank you.

Disclaimer: This report comes from Xangle, a leading crypto platform. Information on Xangle is sourced directly from the projects or through the Xangle Research team. While we have taken all reasonable care to ensure its reliability, we do not fully guarantee its accuracy or completeness.