Crypto Crimes – Comprehensive Overview

Author: James Page
Last Updated: December 2021

How have crypto crime rates changed over time?

As the popularity of trading in cryptocurrencies has increased worldwide, the level of crypto-related crime has also increased exponentially. Reports of crypto-related fraud and scams being run by criminals have been reported to authorities across the world, and as such, traders will have to be more aware of them.

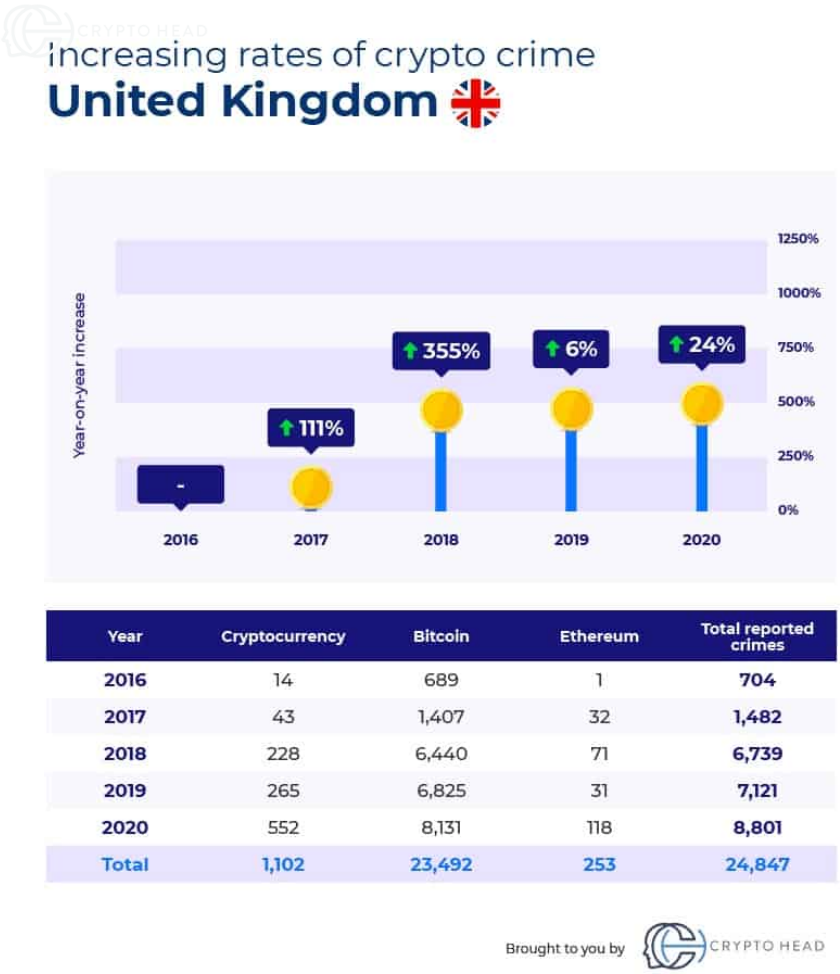
But what is the current state of crypto crimes, and how has it changed in the past five years in three of the world's more developed nations? By looking at crypto crime reports from the USA, UK, and Australia, we are able to analyse the rate and increase of crypto crime, while outlining how some of these scams operate, and how best to avoid them.

Increasing rates of crypto crime

Back in 2016, there were only 1,044 instances of crypto scams and fraud reported in the UK and USA (Australia does not have data this early) which is microscopic compared to the 159,413 instances in 2020. This massive growth has been seen in all three countries throughout the five year time period.

Of the three major popular cryptocurrencies, Bitcoin has the most crime-related reports, which is unsurprising as it is by far the world's most used cryptocurrency.

Crypto Crime in the United Kingdom

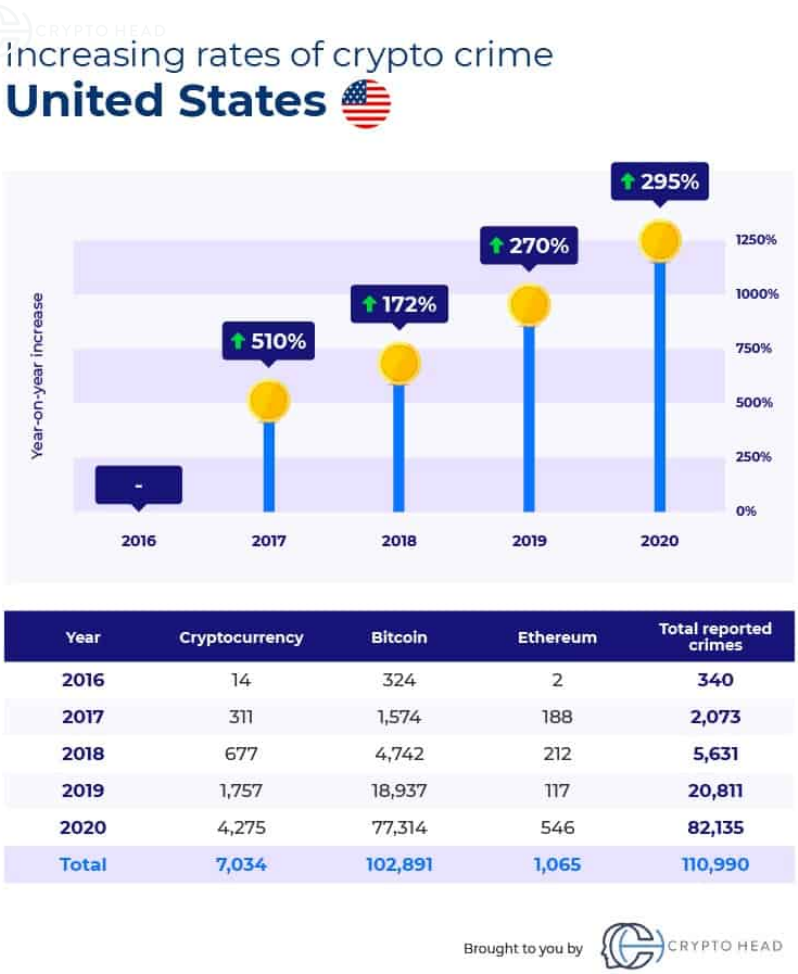


Year	Cryptocurrency	Bitcoin	Ethereum	Total reported crimes
2016	14	689	1	**704**
2017	43	1,407	32	**1,482**
2018	228	6,440	71	**6,739**
2019	265	6,825	31	**7,121**
2020	552	8,131	118	**8,801**
Total	**1,102**	**23,492**	**253**	**24,847**

Brought to you by CRYPTO HEAD

In the UK in 2020 there were 8,801 crypto crime reports to the UK action fraud team, and 8,131 of these were related to Bitcoin crimes. This was a 24% increase from 2019, where 7,121 reports were filed. Prior to this, crypto crime reports in the UK had been growing exponentially. Between 2017 and 2018 there was a 355% surge in crypto-related crime, as there were over 5,000 more reports in one year alone.

Crypto Crime in the United States



Year	Cryptocurrency	Bitcoin	Ethereum	Total reported crimes
2016	14	324	2	**340**
2017	311	1,574	188	**2,073**
2018	677	4,742	212	**5,631**
2019	1,757	18,937	117	**20,811**
2020	4,275	77,314	546	**82,135**
Total	**7,034**	**102,891**	**1,065**	**110,990**

In 2016 there were actually fewer reports of crypto crime in the USA than in the UK, but since then the issue has grown massively and the latest figures in 2020 show there were over 73,000 more crypto crime reports generated in the US than in the UK. Between 2016 and 2017 the number of reports rose by 510% to 2,073, and since then instances have increased by 312% on average each year. Just like with the UK, the majority of reports in the USA are related to the most popular cryptocurrency, Bitcoin.

Crypto Crime in Australia

The availability of Australian data is not quite as thorough as that of the UK or the USA, as records only start from 2018, at which point 5,011 crypto crimes were already being reported. The increase from when records began to the most recent data in 2020 show a total increase of 67% in reports. The 9,689 total searches in 2020 mean that there are slightly more crypto crime reports Down Under than in the UK, but still far less than in the USA.

Common crypto crimes

Crypto Scam Initial Coin Offering (ICO)

An ICO is when a cryptocurrency is offered to investors before it is launched in the market, but, when it's actually a scam, these ICOs could lose you all of your investment. Scammers will often lure people in with an ICO for a completely fabricated cryptocurrency, which will sometimes look very convincing with fake information taken from legitimate coin sites.

The main way to spot a scam ICO is by looking at the details – if it seems too good to be true then it probably is. By simply searching passages of the offering document on a search engine you can see if it has been lifted from another source.

The biggest ICO scams of all time

1. **Bitconnect – $2.6 billion stolen**

By far the biggest example of an ICO scam is that of Bitconnect, an open-source cryptocurrency that guaranteed investors 40% returns, but unfortunately turned out to be a Ponzi scheme that cost its investors an incredible $2.6 billion.

2. **Pincoin – $660 million stolen**

Another major scam that rocked investors was Pincoin, a Vietnamese cryptocurrency that raised about $660 million from 32,000 people. Rather than being paid back in cash, investors were rewarded with a new token called iFan, before the team behind Pincoin disappeared alongside all the invested money.

3. **ACChain – $60 million stolen**

ACChain was a highly promising ICO token created in Shenzhen, China, which managed to raise $60 million, but it quickly became clear that things weren't as they seemed when a picture of the ACChain headquarters leaked and turned out to be nothing more than an empty room. As you can imagine by that point, the company suddenly went very quiet, vanishing without a trace.

4. **Savedroid – $50 million thought to be stolen**

Savedroid is an interesting case, as at first glance it seemed like one of the most audacious ICO scams of all time, with founder Yassin Hankir posting an image of himself on a beach on social media with the caption "over and out", suggesting that he had fled with his investors' $50 million.

However, it appears that this was in fact a publicity stunt, but it still massively shook investor confidence and led to multiple lawsuits.

5. **PlexCoin – $15 million stolen**

The PlexCoin ICO scam was notable for the fact that it was shut down by the US Securities & Exchange Commission (SEC) and ordered to pay back much of the $15 million that it defrauded people of. The ICO initially promised people an incredible return of 1,354% which in hindsight probably should have seemed too good to be true.

Crypto Pump and Dump Schemes

A pump and dump scheme is a scam that has been around long before the cryptocurrency boom. It is where a small group of investors pump money into a low market capitalization. They then convince private investors to pump money in and create an artificial initial price jump. At this point, the initial investors sell their substantial shares in the company for a profit before the share price drops back down to its true value and leaves other investors out of profit.

In cryptocurrency pump and dump schemes, the same principle applies, apart from this time the investors artificially inflate the price of a low-value digital coin. To spot a pump and dump, often a coin will have risen a lot in value without any clear reason why. If it remains a mystery why the price is skyrocketing it is probably not a sound investment.

Crypto Theft

Cryptocurrency is not immune to old school theft, as although crypto wallets can be very protected, they are not completely secure.

Hackers can get into crypto wallets to directly steal your funds and they can also set up phony crypto exchanges where you put your money believing it is legitimate, only to find your coins have been stolen.

To avoid this, make sure you do not trade on new exchanges without verifying their legitimacy and security, and make sure you keep your cryptocurrency in an offline hardware wallet with a unique password that you change regularly. To help you in the search for a reliable crypto exchange we've created the following comparisons such as our list of the best crypto exchanges in Australia as well as this list of recommended Canadian exchanges and finally our top UK crypto exchange list.

The most common funnels of crypto scams

Imposter websites

With so many new people getting involved with the world of cryptocurrency, there are lots of websites that claim to be able to offer tips on where to invest your money. While some tips websites are genuine, others will be completely fake and look very authentic, often telling you to pay money into an account that promises great returns and instead stealing this investment. Check for the padlock sign in your browser to ensure that the site is secure and always be careful if you get redirected to another site when it comes to processing payment.

Social media bots

You may also run into social media accounts offering great crypto investing opportunities, but the likes of Twitter and Facebook are rife with fake accounts and bots. The bots will post links to fake news articles, often accompanied by a celebrity endorsement to appear more convincing, telling people how much money they have made and what a great money-making opportunity it is. These fake articles often link to websites that tell you to invest in an account that ultimately steals your money. Never part with cash via social media and always remain vigilant when browsing social platforms.

Email

Scam emails have been around since well before cryptocurrency took off and have become increasingly sophisticated over the years. Try to verify that an email address is actually affiliated to the company that you think it is before transferring any funds, and feel free to either reply to the email or reach out to someone else at the company to make sure that the email that you're dealing with is legitimate.

While the data shows that across the board cryptocurrency scams are on the rise, this shouldn't deter you from trading and investing. With sensible research, staying alert and using reliable platforms, scams and fraud are avoidable and if ever something appears too good to be true, check and check again.

Methodology

All crime statistics were sourced from Freedom of Information requests made to Action Fraud in the UK, Federal Trade Commission in the USA and the Australian Competition and Consumer Commission.

Note that these are only crimes which were reported to the above agencies and the actual numbers of offences could be higher, especially as such crimes are still relatively new and many are unaware of where to report them to.

Further information on scams was sourced from:
https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/

About The Author

James Page

James is the main editor. With a passion for finance and anything blockchain, cryptocurrency is right up his alley. He's responsible for most of the content on the site, trying his best to keep everything up to date and as informative as possible.

ABOUT CRYPTO HEAD

At Crypto Head we aim to give people the knowledge to get involved in the fastest moving industry on the planet.

The information on this website is for information purposes only. It is not intended as investment or financial advice and should not be relied on as such. Before making any financial commitment you should seek professional advice from a qualified investment or financial adviser.