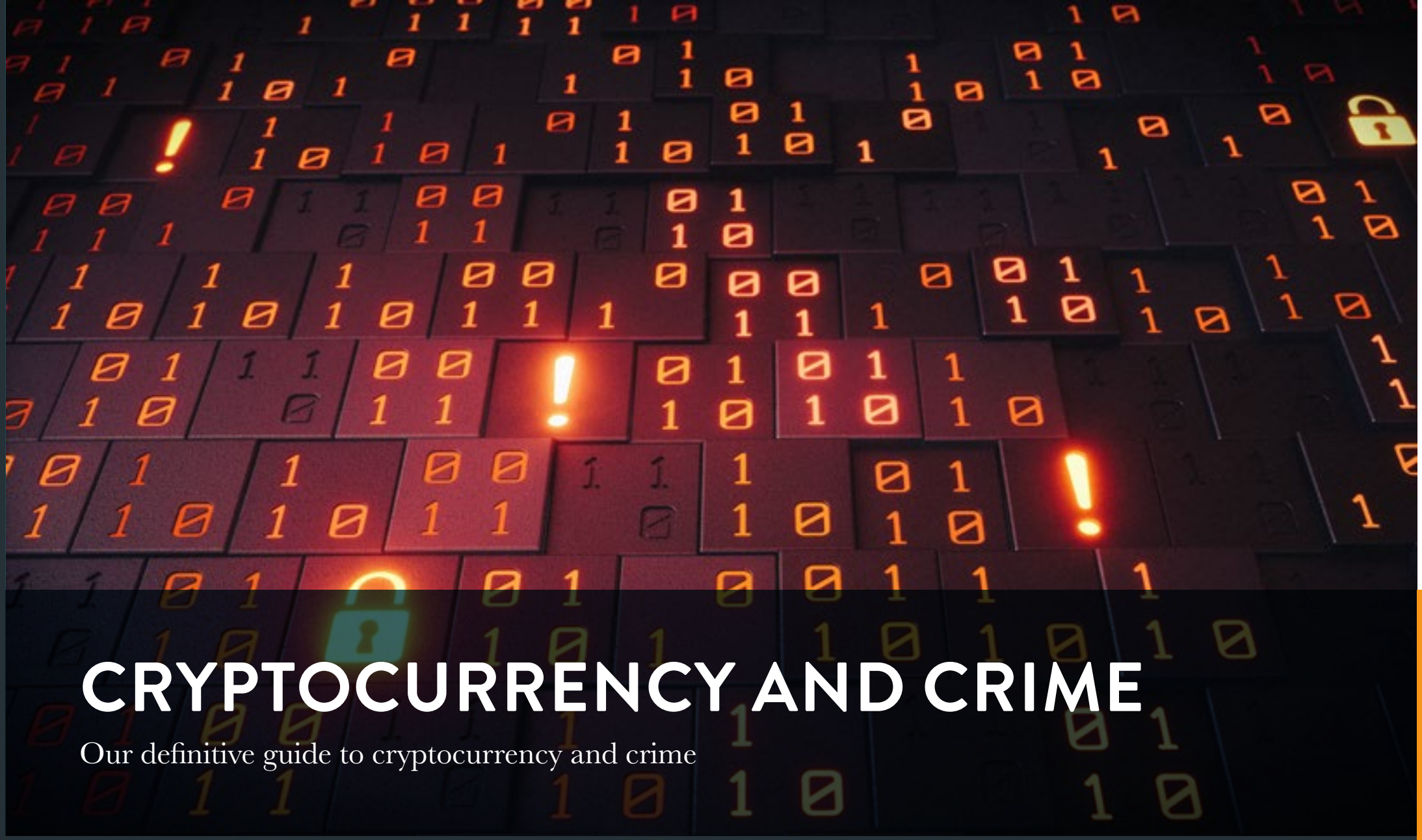


CRYPTOCURRENCY AND CRIME

Our definitive guide to cryptocurrency and crime

COIN RIVET

Independent British blockchain and crypto news

CONTENTS

HOW TWO INDUSTRIES CAN GO HAND-IN-HAND

It's not secret that criminals and terrorists use and exploit cryptocurrency. In this guide, we look at all types of criminality from small email scams right through to real-life kidnappings, all in the name of crypto.

There are some outstanding projects in the cryptocurrency space. There are also decent intentions and genuine actors who believe in an alternative financial system and the separation of money and state. However, just like all walks of life, there are also plenty of criminals laced throughout this nascent industry.

Cryptocurrency crime is rife and sometimes it feels as if the two industries go hand in hand. Why is that?

$1.7bn of cryptocurrency stolen in 2018

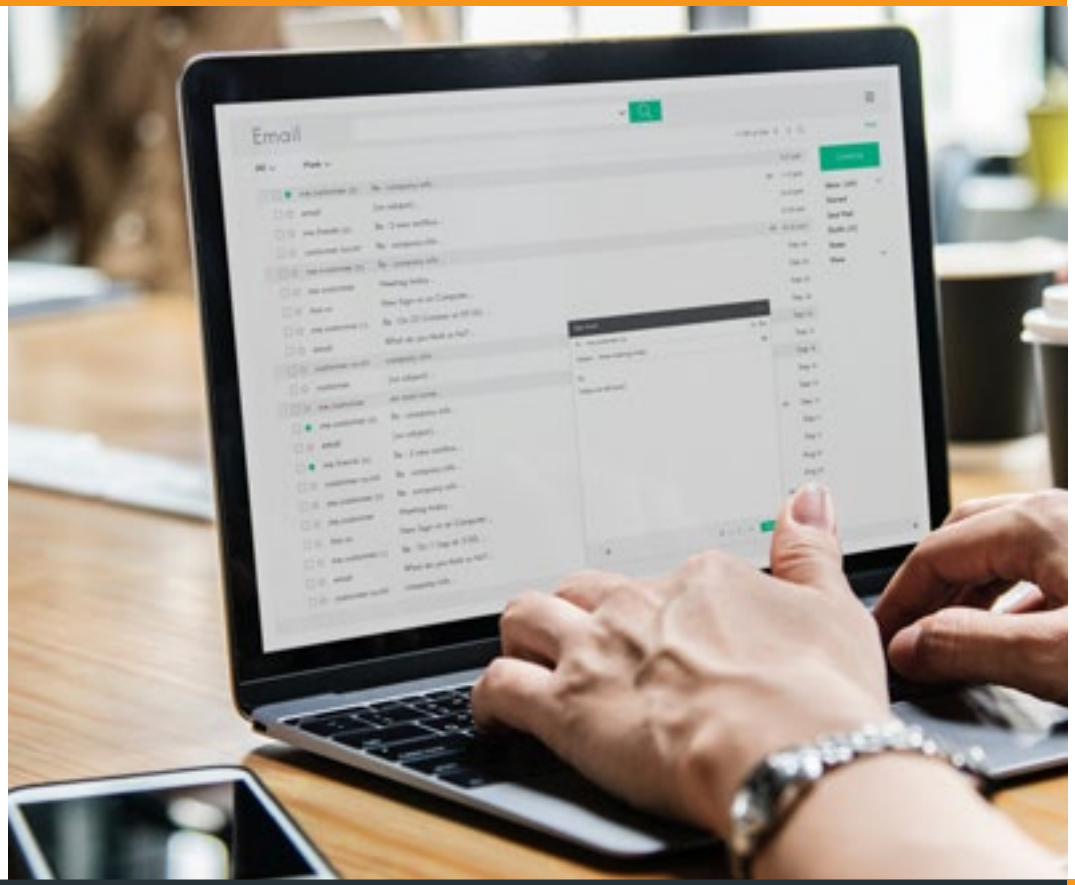
When trying to defend cryptocurrency and its groundbreaking technology, cold hard statistics don't help. A total of $1.7bn of cryptocurrencies was stolen throughout 2018, with some $950 million coming from exchanges.

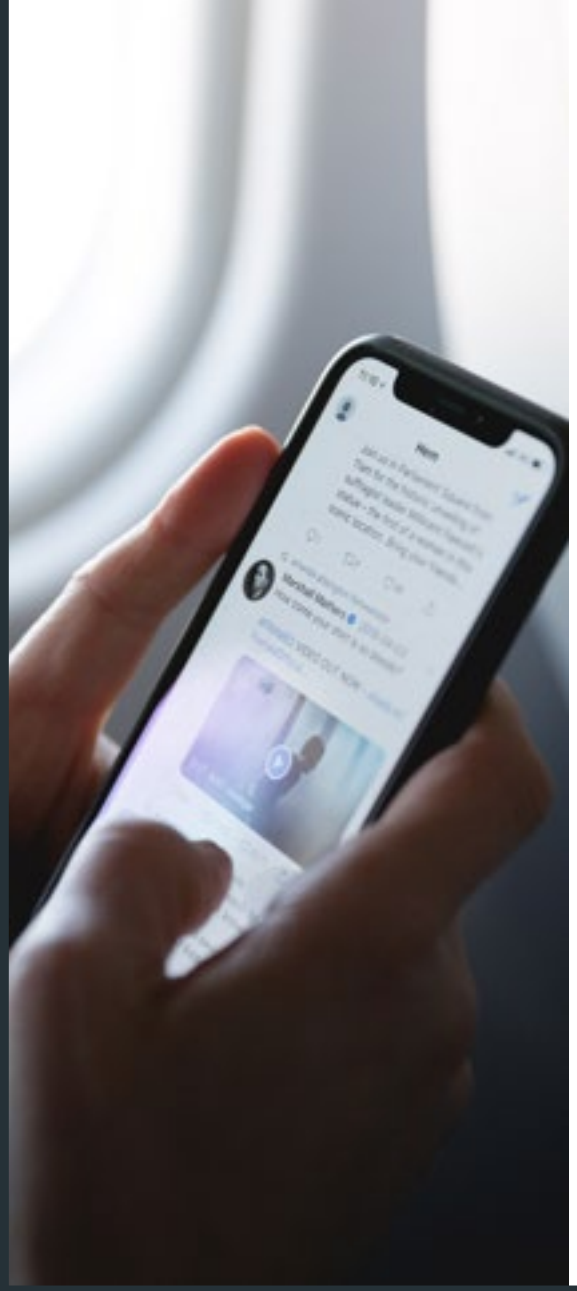
The proliferation of cryptocurrency crime in the form of hacks, **ICO exit scams**, and Ponzi schemes is impossible to deny.

A further report from CipherTrace found that as much as 60% of all attacks were orchestrated by **just two professional groups**, whom they name as Alpha and Beta. That means that organised criminals seized over $1 billion worth of cryptocurrency!

While the intentions of the Beta group seem to be for personal gain, Alpha's are more disturbing. Whether for laundering money, facilitating crime, or even shutting down a network, crime and crypto prove to make good bedfellows.

Beyond the massive hacks that steal the headlines, CipherTrace identified 10 major new trends in criminal activity in the space right now. These include crypto dusting (spamming wallets with small amounts of tainted cryptos) and **cryptojacking**.





While some of the top 10 threats are more pressing, CEO of CipherTrace Dave Jevans told Coin Rivet that cryptojacking is:

> "No different from viruses and malware infecting computers. It will not shut down a company, it will not steal $500mn from an exchange. It makes small amounts of money from unused computing power on people's computers and browsers."

And it's not always so small, when you consider the case of Shominru Mining Botnet. This mega-malware managed to infect over half a million devices and mine a whopping $3.5mn of Monero.

Cryptocurrency crime is often exacerbated as perpetrators of ransomware prefer payment in cryptocurrencies like Bitcoin as they are harder to trace than credit card payments.

Bitcoin's shady past is hard to shake off

Bitcoin's intentions as a peer-to-peer exchange of value with no interference from centralised institutions got off to a genuine start. However, when it became the preferred method of payment for the dark web's **Silk Road**, cryptocurrency crime kicked off in earnest.

Bitcoin became synonymous with criminal activity, being used to pay for weapons and drugs as well as financing terrorists. This went a long way toward making cryptocurrency and Bitcoin, in particular, a threat in the public's mind. On top of ransomware payments demanded in Bitcoin, it became well-known as a currency for facilitating nefarious deeds.

Federal agencies shut the Silk Road down in 2011, but Bitcoin's reputation was stained forever.

No one needs anonymity like a criminal

Cryptocurrency and crime go hand in hand thanks to its anonymous nature. After all, no one needs anonymity like a drug baron or child trafficker. If you're buying illegal goods, evading taxes, or laundering money, cryptos have so far been a pretty good bet.

Many people have also used cryptocurrency as a way of sending money outside of their country. And with unlimited amounts on unregulated exchanges, unlike banks, the sender doesn't have to justify the source of the funds. Lack of regulation in the space further highlights cryptocurrency crime in the news.

However, as the new **AML/CFT regulations** arrive in 2019, criminals will find it much harder to cover their tracks.

Steeper AML/CFT regulations will mean that the 38 member countries, including the US, EU, and G20, must subject cryptocurrency exchanges and custodial services to KYC in their jurisdictions.

This will mean that criminals will have to resort to more creative ways of laundering the money they steal.

Cryptocurrency crime – The association lives on

One can argue that cryptocurrency crime receives an unfair amount of attention when you consider the history of traditional banks and money laundering. It's actually much easier to launder money with cash without leaving a trail than through cryptocurrency and the inevitable digital footprint you leave behind.

As regulation begins to follow a clearer path and weed out shady ICOs and money launderers, perhaps moving forward, cryptocurrency and crime can finally part ways.

CRYPTOWARNINGS AND REGULATION

Cryptocurrency is still a largely unregulated industry which makes it an easy target for criminals. On the whole, there's a lack of consensus across the globe when it comes to legislation.

Where there are loose guidelines in place, these aren't consistent from country to country. We take a look at the current state of play for cryptocurrency regulation across the globe, starting from the east.

China: Supporting blockchain with financial stability

Blockchain and cryptocurrency regulation is arguably one of the most controversial topics in China – an economic powerhouse that appears fraught with confusion on how to handle this high-growth technology. The government is predicated on maintaining control over business and operations, which is a bit contrary to the basis of blockchain being decentralised.

Mainland China dominated the industry as "an eye-popping 95% of all BTC trading took place in the country". That changed in 2017 when the government cracked down on ICOs and domestic crypto exchanges.

However, all hope is not lost since the country seems to be supportive of blockchain. China was described by President Xi Jinping as being part of a wave of technological revolution that also includes AI, quantum computing, the Internet of Things and mobile communication.

They are exploring ways to regulate the industry and it's partly the job of the community to educate government officials on its massive potential as China is undeniably becoming a "hotbed for innovation".

The Cyberspace Administration of China (CAC) released a draft of a policy that would require users of any blockchain service to register with their real names and national ID numbers. While many believe this might be a setback for the industry, it very well could be a positive move forward to achieving security with greater transparency. It comes as no surprise that the government is steadfast on financial stability and it will do everything in its power to ensure its citizens are protected.

On the flipside, Hong Kong's Securities and Futures Commission (SFC) believes that an outright exchange ban is not the solution. The SFC and BitMEX, a Hong Kong-based exchange will collaborate to put together clearer regulation that "is comparable to that of a licensed trading venue".

Japan: Differentiating between virtual currencies

Meanwhile, Japan has already put Fund Settlement Law and the amended Payment Services Act in place. According to **Bitcoin.com**, the former defines "virtual currencies," which include cryptocurrencies, as a means of payment and exempts them from consumption tax. The latter requires cryptocurrency exchange operators to register with the Financial Services Agency (FSA).

To that end, they have begun evaluating different types of coins that have emerged in the industry like stable coins. In their view, "stablecoins pegged by legal currencies do not fall into the category of 'virtual currencies' based on the Payment Services Act." However, it remains to be seen how they will approach other types of stablecoins like algo-backed, crypto-backed, or collateral-backed stablecoins.

South Korea: General, yet inviting

South Korea, a booming crypto space, takes a more "black and white" approach as they believe that cryptocurrency funds don't meet the requirements of the country's Capital Markets Act. It encourages investors to consult with the relevant authorities before investing.

UK: Steady as she goes with formalising regulation

Probably the most divided of all regions is Europe as there seems to a variety of different viewpoints from each country. In the UK, the FCA is considering a ban on the sale of crypto-based derivatives due to its risky nature.

The government Taskforce's newly-published report proposed "a three-fold framework for cryptoassets, depending on whether they are used as a means of exchange, for investment, or to support capital raising and the development of decentralised networks through ICOs". This is a promising step forward for the UK which has previously taken a more casual approach to regulation.

Malta: Formalised regulation is on the horizon

Malta seems to be the most innovative and action-oriented of the European nations. It participates in ongoing discussion at UN forums on the institutionalisation of blockchain on a global scale. Malta has passed two bills:

1. **The Virtual Financial Assets Act (VFA):** This addresses the procedures and requirements that ICOs will have to follow. An important feature of this law is that companies launching ICOs will have to disclose their financial history.
2. **The Innovative Technology Arrangement and Services Act (ITAS):** This provides the legislative foundation for the regulation of the cryptocurrency and blockchain industry.

US: Carefully evaluating valuation and liquidity

This brings us to the US. Since the enactment of the Howey Test, there hasn't been any additional conclusive regulation from the SEC or the CFTC. However, the authorities are not sitting around idle. The SEC recently launched a FinHub, which will serve as a resource for public engagement on the SEC's FinTech-related issues and initiatives.

The hot ticket item that everyone is waiting on is when there will be approval for a crypto ETF, like the VanEck SolidX Bitcoin ETF which is still pending. Kara Stein, SEC Commissioner, spoke on a recently released letter to staff indicating some of the critical issues they will be looking at which include valuation, liquidity and custody.

While there is some movement on approvals on a regional level in the US, there are still open-ended concerns that government authorities are still grappling with as it relates to the acceptance of digital currencies.

According to the Financial Stability Board (FSB), which makes recommendations about the global financial system, some concerns include "low liquidity" and the "use of leverage" in crypto trading.

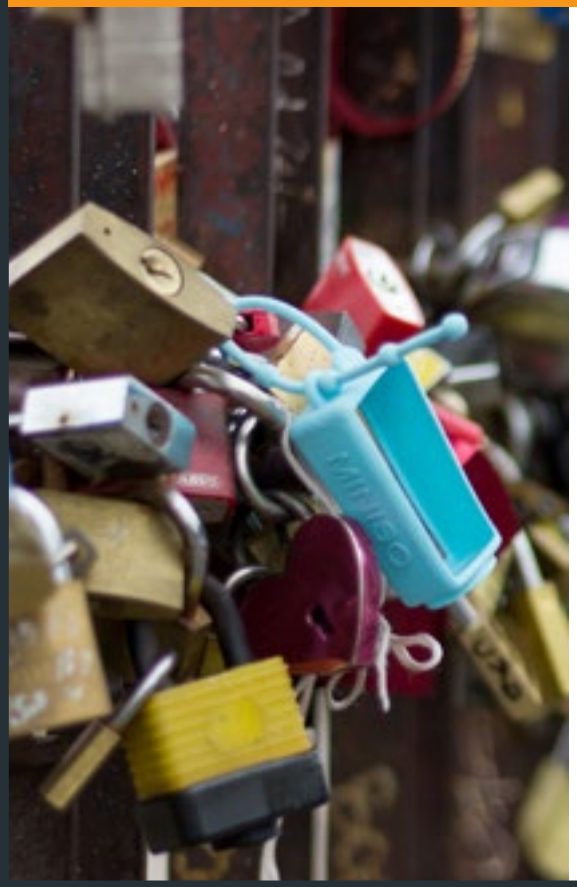
Based on panel discussions around the conference circuit, the SEC is planning on implementing a streamlined one-page document that should clarify these issues by the end of the year.

Regulators need to keep pace

In short, blockchain is going to revolutionise our lives whether we like it or not. The genie can't be put back in the bottle, but it can be tamed, and harnessed to reach its full potential. While there are still many issues to resolve, the industry will only continue to gain momentum and regulators need to keep pace.

CYBERCRIME, KIDNAPPINGS, AND THEFT

There are a wide variety of wallets available on the market, with each coin typically offering its own wallet. For serious traders who dabble in more than one currency, though, there are multi-currency cryptocurrency wallets available.



In fact, you don't have to look too far to see the dark side of these virtual coins. Below, we provide a quick wrap-up of some the biggest stories in cryptocurrency.

Cryptojacking rose by 44% in 2018

Cybercrime is nothing new. It's been prominent in the form of ransomware for years. Typically, ransomware infects devices and prevents access to other devices or files. In most cases, they require the user to pay a ransom to solve the issue. Now, cryptojacking is beginning to take its place as the vogue cybercrime.

The number of users who reported they **had encountered cryptojackers rose by almost 44.5%**. The exact figures are 1,899,236 in 2016-17 rising to 2,735,611 in 2017-18.

The report from Kaspersky Labs outlines how "mining is a discreet and modest way to make money by exploiting users," before continuing on to state, "although there are groups of people who hoodwink unwitting users into installing mining software on their computers, or who exploit software vulnerabilities to do so, mining is legal. It simply results in the threat actors receiving cryptocurrency, while their victims' computer systems experience a dramatic shutdown".

Kidnappers demand €9 million cryptocurrency ransom

In one instance of criminal activity, cybercriminals demanded a €9 million cryptocurrency ransom for a missing 68-year-old woman in Norway.

Anne-Elisabeth Falkevik Hagen, who is married to one of Norway's richest men, had been missing for 10 weeks before the news broke. In addition to investigations by local police, Interpol and Europol also looked into the case, although they had received "no signs of life" from Hagen since her disappearance in October.

Norwegian police believe that the 68-year-old was taken from her home in Sloraveien, with forensics teams analysing traces of the kidnappers in the bathroom of Hagen's detached house.

Aside from the ransom, a written message was found in the house stating that if the police were to be notified, the woman would be killed.

The ransom **demanded €9 million payable in privacy coin Monero**, which would account for 1% of the coin's total market cap. Monero is a favourite among cyber-criminals due to its anonymity.

$2.5 million is stolen from crypto exchanges every day

Blockchain security expert Hartej Sawhney has claimed that, on average, around $2.5 million worth of cryptocurrency is stolen from crypto exchanges every day, with most hacks being unreported to the public.

Mr Sawhney is a co-founder of **hosho.io**, a global leader in blockchain security. His company provides security services for clients including smart contract auditing and penetration testing for a range of cryptocurrency protocols.

Low-hanging fruit

He said: "Hackers have low-hanging fruit to penetrate exchanges." Examples may include forms of smart contract hacking and order book manipulation to offset bets at competing liquidity providers.

He went on to claim that exchanges need to learn how to properly hold private keys as this is still a major security barrier. This applies to both hot and cold wallet solutions that may provide a wider net for targets.

> "Exchanges need to learn to value security, but they are not getting regular penetration testing from cybersecurity companies."

A love for dogs

Mr Sawhney described an example of a recent hack, stating:

> "An employee of a Bitcoin exchange was a competitive dog walker. The hacker monitored the social feeds of this employee and gained access to realise that fact. They made a fake website and application for this employee to apply to compete in a local dog walking competition. The victim then opened up the wrong email, opened up the wrong PDF, and ended up applying to a fake dog walking competition, and the hacker gained access to her keystrokes."

The hackers then gained access to her usernames and passwords for the crypto exchange, and the exchange lost millions of dollars within 48 hours.

He concluded the interview by discussing the relative scarcity of "full-stack developers who know solidity and have a QA mindset" who qualify to work and certify in this field.

If you can strike the correct business model as a custodial exchange in this space, then you will certainly see the benefits of this type of security auditing. Due diligence is clearly required in the management of private key solutions, but the question still lingers – who is going to audit your own code?

HOW TO SPOT A SCAM

So with all the vulnerabilities surrounding cryptocurrency, how can you possibly stay safe? Well, it's important to know how to spot a cryptocurrency scam and ICO scam.

While we've discussed more elaborate schemes, the good old fashioned phishing email is still a popular choice for many of today's cryptocurrency criminals.

Below, we take a look at how to spot a Bitcoin scam, but this could be equally relevant for whatever coin you're using.

Internet scams are very common, and they are becoming more difficult to spot every day. Here are some Bitcoin blackmail email scam red flags to look out for to ensure you don't end up having to pay a Bitcoin ransom.

(Note: If a legitimate hacker has gained access to sensitive information and is threatening to release it unless you pay a fee, you should always call the police.)

How do these scams arise?

Hackers may be able to obtain old passwords of yours and use them to try and scare you. They can do this by infiltrating a site you used a long time ago that had weak security. If you haven't used that password in a long time, you might be safe. If it is still your password, then you need to act fast. Hackers can also steal passwords if you've visited a site that had a lot of malicious malware on it. Malware can infect your computer, and this provides a window for a hacker or scammer to target you.

If you are being presented with an old password that is no longer in use, it is likely a scam. This is because if they had actually hacked you and wanted to put pressure on you, they would have chosen to reveal a newer password. If they do present you with your current password, this is where issues might arise and you should change your passwords immediately.

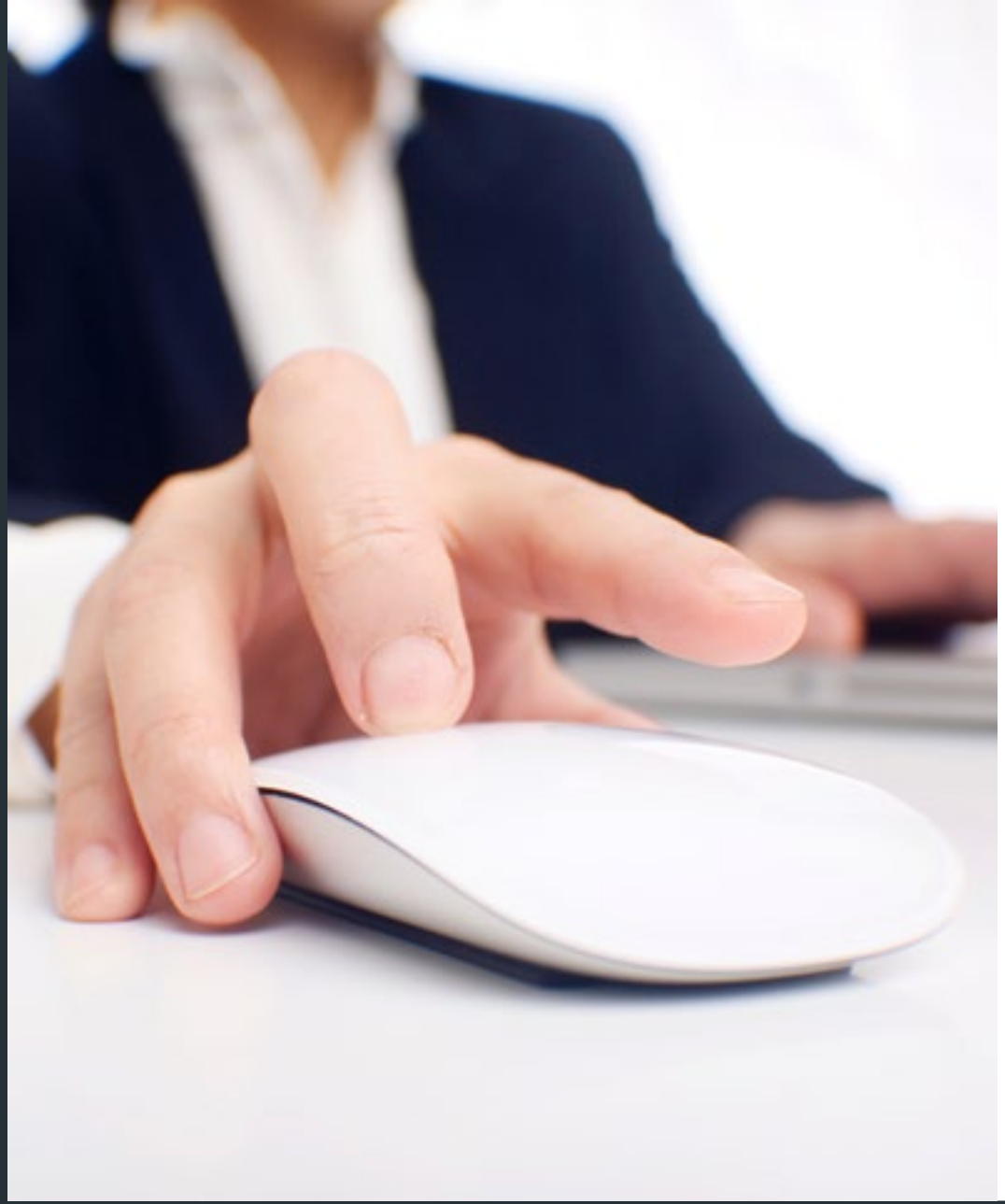
The most important thing to note with these scams is whether or not they have included other personal information. If it is only an old password, it tends to imply the scammer does not have anything else on you. If they do reference anything else about your personal life that can be leveraged against you, call the police.

Example

One example of an email scam may read something like this:

> We have recorded you watching pornography sites behind your wife's back. If you do not want these videos released, then you must pay us $1,000 in Bitcoin.

It is targeted at a male and the scam is suggesting that the male has been watching pornography behind his wife's back. This is common in Bitcoin blackmail email scams, since the most targeted gender is males (although many women have also been subject



to similar scams). The threat may be completely fabricated and the hackers may be playing the odds in the hope that eventually a victim falls for their trap.

Another example may read:

"You recently logged into PayPal with the password 123456 and we've seen how much money you have. If you do not pay us $`1000 in Bitcoin, we will hack your PayPal."

This type of email can be more daunting simply because it has identified an old password. If the password is no longer used, then this can be seen as a scam that likely has no basis in reality, but if it is a current password, you should call the police.

Remember
Remember never to click on any links in suspicious emails, and always check the sender address to make sure any emails you receive that claim to be from reputable sources are legitimate.

It is also worth noting that a lot of these email scams do not originate from hackers, but people merely pretending to be one. Someone may have purchased old passwords from a hacker and is simply sending emails out to a number of people in the hope they find a victim. Furthermore, the level of spelling and punctuation is typically quite bad in these scams. A serious blackmailer would put significantly more effort into extorting you.

Make sure you protect all of your personal details, since scams that leverage old passwords against you are incredibly common. If other personal information is leveraged against you, and you cannot be sure it is not a scam, contact the police or other authorities.

HOW TO KEEP YOUR CRYPTOCURRENCY SAFE

It won't be possible to completely prevent criminality in cryptocurrency. While it remains a largely unregulated industry, pretty much anything goes.

What's important for you to know is that you are responsible for your own safety, and the safety of your funds, when interacting in the crypto community. That's why we're going to equip with you some the skills you need to make transactions safely online – or even if you just want to hold your funds.

Understand the differences between hot and cold wallets

To trade cryptocurrencies of any kind, you will need to invest in a wallet. **Different types of wallets offer varying features**, options, and – most crucially – different levels of security for your cryptocurrency. Hot wallets are connected to the internet and bring with them the risks of online criminality. Cold wallets aren't connected to the internet and so keep funds protected from hackers.

Two-factor authentication

Two-factor authentication, commonly abbreviated to '2FA,' is a must when it comes to protecting your cryptocurrency wallet. Most, if not all, the top exchanges utilise 2FA. This practice requires users to enter two layers of identification to access their accounts. This gives users extra assurances about the level of security available, while deterring cybercriminals from malicious activity. In instances where a hacker obtains your password, they would still need a second method of identification to access the account. This second method involves a human element that hackers aren't able to replicate.

Strong passwords

Despite **91% of people knowing that using the same password for multiple accounts is risky**, 59% still do it. Using a weak password or one that is used for another login can leave your wallet exposed to vulnerabilities. Intelligent hacking tools often have dictionaries embedded into them to search through possible password combinations. To strengthen your password you can use an original combination of numbers, letters, and special characters.

Don't share your password with anyone and if you need to write it down, don't lose it. Forgetting or losing your password can often prevent you from accessing your cryptocurrency. Above all else, don't share or lose your private key, otherwise you will lose access to your funds.

Explore different types of wallets

Online wallets and mobile wallets are inherently vulnerable to criminality in the cyber space. Luckily, these aren't the only wallets available to cryptocurrency users. To improve overall cryptocurrency security, you could consider using hardware wallets.

Hardware wallets can be more secure as they give you direct, offline access to your coins, they're protected by a private key, and they eliminate the risks of being hacked.

Two-factor authentication and strong passwords should still be used to enhance the security of your hardware wallet. This protects you in instances of wallet loss. If you misplace the physical wallet, you still have access to the currency address which allows you to programme a new hardware wallet. Access to your coins doesn't need to be lost.

Paper wallets are also an option for users who want to minimise their online footprint. Keep your addresses and keys written down on paper and keep them in different locations. Using a paper wallet eliminates the need for any third party sites or applications, arguably providing you with the upmost security. However, lose any part of your keys or addresses and you'll also lose access to your cryptocurrency.

Avoid carrying large amounts of crypto in a mobile wallet

Mobile wallets and exchanges make trading on the go quick and easy, making them increasingly attractive to crypto users.

Keeping a small amount of funds in your mobile wallet is a great idea for making instant purchases, however the simplicity of these wallets is often their downfall. Generally, you just need to download an application and go through a minor registration process but this simplicity also attracts hackers and other malicious attacks. With this in mind, it's not advisable or secure to carry large amounts of cryptocurrency in your mobile wallet. Your funds could be easily compromised. If you're a serious investor or trader then consider hardware wallets.

Only allow authorised devices to access your wallet

Strengthen your security by only allowing logins from authorised devices. Any suspicious activity from unauthorised devices will result in the user being frozen out of your accounts. Some users even go so far as to use a dedicated device to access their funds. This ensures that no malware has been picked up from general web browsing and gives the user extra reassurances that the account hasn't been compromised.

CONCLUSION

Whether you're investing, holding, or even brand new to the industry, we always recommend that you thoroughly research your options.

Keep on top of the **latest news to hear about new scams**, crimes, and regulation changes. As cryptocurrencies, from Bitcoin right through to altcoins, continue to evolve, so could the types of attacks on the industry. Always stay aware and be prepared.

At Coin Rivet, we deliver the latest insights and guidance on how you can stay safe in the cryptocurrency community.

Bringing you news, analysis, opinion and insight from the fast-moving blockchain world. Our team of journalists and contributors cover the likes of cryptocurrencies, wallets, exchanges and ICOs across a wide range of sectors including retail, fintech, banking and gaming. We go beyond the press releases and marketing hype to tackle all the industry topics that matter.

Featured in

FOX NEWS EXPRESS COINGEEK

coinrivet.com