**Gyancity Journal of Electronics and Computer Science,**
**Vol.8, No.1, pp. 1-18, March 2023**
**ISSN: 2446-2918 DOI: 10.21058/gjecs.2023.81005**


# THE DESTABILIZING EFFECTS OF CRYPTOCURRENCY CYBERCRIMINAL

Jackie Chong Cheong Sin
*International Institute of Applied Science of Swiss School of Management, Switzerland*
*jackie@unies.my*

***Abstract***

*This paper investigates the financial market effects of recent cybercriminal in cryptocurrency markets. Hacking events are found to increase both the price volatility of the targeted cryptocurrency and broad cross-cryptocurrency correlations. Further, cybercrime events significantly reduce price discovery sourced within the hacked currency relative to other cryptocurrencies. Finally, abnormal returns in the hours prior to the cybercrime event, revert to zero when news is publicly announced.*

***Keywords:*** *Cryptocurrency, Cybercriminal, Returns of Cryptocurrency, Bitcoin, Cryptocurrency Risk, Price volatility, Cryptojacking*

.

## 1. Introduction

Cryptocurrencies have become popular because they enable efficient payment systems through a decentralised distributed ledger, which does not depend on a political process or governmental regulatory system. Our research attempts to develop our understanding of the widespread illicit behaviour that has been witnessed in cryptocurrency markets. With access to the public's credentials, hackers can steal electronic identities and move funds from legitimate accounts [1]. Hackers may engage in phishing attacks in which the hacker steals credentials by faking the appearance of trustworthy sources. Hackers may further steal information through direct security breaches.

The continued evolution of cryptocurrencies and the underlying exchanges on which they trade has generated tremendous urgency to develop our understanding of a product that has been identified as a potential enhancement of and replacement for traditional cash as we know it. The market efficiency of Bitcoin and found through a battery of tests that Bitcoin was inefficient, although it was becoming less inefficient over time [2]. Much research continues to identify this asset class to contain exceptionally high

levels of volatility when compared to more established counterparts. However, cryptocurrencies as a new asset class are not without its substantial issues, particularly that of the provision of a platform for criminality and, indeed, major cybercriminal events. While much debate surrounds the process in which this product can be regulated, there exists a wide variety of channels in which criminality can develop and thrive. Regulatory bodies and policy-makers alike have observed the growth of cryptocurrencies with a certain amount of scepticism, based on this growing potential for illegality and malpractice [3]. Around $76 billion of illegal activity per year involve Bitcoin (46% of Bitcoin transactions). This is estimated to be in the same region of the U.S. and European markets for illegal drugs, and is identified as 'black e-commerce'. While the volatility of cryptocurrency price returns has been studied, the potential for market manipulation appears to have been broadly identified in cryptocurrency cross-correlations and market interdependencies. Such researches have fine-tuned the focus of regulators, policy-makers and academics alike, broad trust in both cryptocurrencies and the exchanges on which they trade cannot be sustained with such significant questions of abnormality remaining unanswered [4]. Developing understanding of these new products and how to mitigate cybercriminal and their illicit use is an exceptionally important task in order to validate their further use and development.

Crypto currency is a collection of technologies based on Satoshi Nakamoto's 2009 invention, Bitcoin, which is counterfeit-proof and decentralized. Several cryptographic technologies (hash sums, asymmetric keys, and proof-of-work) are combined to make this possible via a global, peer-to-peer network. The currency is in use today: It can be traded for other currency, or used to buy goods and services. Bitcoin is an electronic currency designed to use public protocol that implements it in a totally decentralized manner, so as not to need the control of any central issuing organization that manages it [5]. Though still in development, it has been proven to be a modern payment system referred to have been used in some procedures commonly associated to money laundering or trafficking of illegal substances of various kinds. Thus, in this article, we analyse those features which transform such a crypto currency in a useful tool to perform any kind of transactions far from the control of any kind of regulatory agency, as well as we pinpoint some of the fields in which their usage can derive in new illicit behaviours.

## 2. The risks in cryptocurrency environment

It is considered that you have agreed to all risks at account creation time [6], [7].

- **Scam Checks**

Unfortunately, there are many scams within crypto and these scams are becoming increasingly more sophisticated, such as malicious contracts and rug pulls which are very difficult to detect for the average investor [8].

To help protect against these potential scams as well as provide additional (technical) analysis of the project, there are many free online tools that can help. Some of the tools I use include [9], [10], [11]:

- **Scamsniper**

Provides token information, honeypot check, liquidity check and audit information. Also uses data collected from BSCheck.eu, TokenSniffer.com & StaySafu.org → Scamsniper.net

- **BSCheck**

Provides overall risk assessment, dev wallet information, token owner and top holder information.

- **RugDoc**

Offers overall assessment of smart contracts and identifies potential rugs. Works for BSC, FTM and POLY contracts.

- **Token Sniffer**

Offers overall assessment of smart contracts for ETH contracts.

- **StaySafu**

Offers overall assessment of smart contracts.

- **Price Change Risk**

The price of cryptocurrency fluctuates constantly. Your cryptocurrency trade or balance could surge or drop suddenly. Please note that there is a possibility that the price of cryptocurrency could drop to zero.

- **Business Hours Risk**

The price of cryptocurrency could fluctuate, sometimes heavily, after bitFlyer market hours. bitFlyer does not take any responsibility for not being able to buy and sell cryptocurrencies after bitFlyer market hours.

- **Liquidity Risk**

There is a possibility that trades cannot be settled, may be difficult to settle, or can be traded only at significantly adverse prices depending on the market situation and/or market volume.

- **Cryptocurrency Network Risk**

Cryptocurrency transactions (transaction authentication on the Blockchain) will be held for a certain period of time until an adequate amount of trade confirmations have been received. Transaction results will not be reflected to your bitFlyer account balance until

an adequate number of confirmations have been received and confirmed by bitFlyer. There is a possibility that your transaction may be cancelled on the Blockchain. Risk of Losing the Private Key or Password of the External Wallet Services.

In the case you use an external wallet, you may not be able to access your cryptocurrency if you lose your private key or password. bitFlyer does not take any responsibility in this case.

- **System Risk**

There is a risk that your transactions may be affected due to system failures resulting from events such as changes in the external environment.

A system failure is considered to have occurred when our company determines that a clear failure has occurred in our system, and the customer is either unable to place orders on the internet or is delayed in doing so, or otherwise not able.

With regards to opportunity loss (e.g., a customer's order could not be received and the customer lost the opportunity to place the order, resulting in loss of profits which could have been obtained) due to things such as emergency maintenance or system failure of our company's system, we shall not take corrective actions on such error because we are not able to determine the details of the original order which was attempted to be placed. There may be a possibility that our system calculates an abnormal cryptocurrency buy or sell price. Please note that we reserve the right to cancel transactions which have been completed with an abnormally valued price.

- **Bankruptcy Risk**

There is a risk that we cannot continue our business due to events such as changes in the external environment. In the case that we cannot continue our business, all processes including the treatment of customers' assets shall be done according to insolvency law, corporation law, corporate rehabilitation law, civil rehabilitation law and other related laws.

- **Visiting a project's official website is a must!**

There is no excuse for a poorly developed website. Today it is very easy and relatively inexpensive to develop a clean and functional website. The project website should be well put together, functional and openly share details about the project, the people behind it, the roadmap and the investors (if applicable).

If the website is of poor quality, has spelling mistakes, is reluctant to disclose to the team members or even worse is a copy-and-paste of a prior fork, then these are all cause for concern and should be avoided.

- **The Team (developers, executives, partners, advisors)**

For most projects, especially newer projects it is the team and developers involved in the project who are the most valuable assets. It's the credibility and experience of the team behind the project which will have a direct result in the success or failure of the project. It's for this reason, I personally am reluctant to move forward on projects whose team is not openly disclosed.

When assessing the team, determine the prior experience in the market and prior projects. Is this their first project or do they have a solid history developing successful projects in this market?

Unfortunately, many smaller projects have been known to fake their team (using AI-generated photos), so it isn't enough to take at 'face' value what the website says. If LinkedIn of other social profiles of the team is provided, it's always prudent to follow up and verify their authenticity [12].

When assessing the team, it's also important to take into account the leadership (executives). Projects with partnerships with well-known firms are also a good sign, but as with most information on the website, verify where possible.

- **The Road Map & Vision**

As an investor, you are looking into the future potential for the project and the road map and vision are also critical components to the assessment.

A solid project will have a strong and well-defined vision with a roadmap and dates attached providing details for the development at each stage. It goes without saying, without a clear vision and roadmap, the future success of the project is in doubt.

- **Investors**

Does the project already have investors and if so, who are they? Projects which have already been invested in by well-known investment firms are an excellent sign. These firms often specialize in specific niche markets and if they have already invested, chances are they have also done their due diligence and believe in the project.

If everything looks good at this point, the next step is to check the social media profiles. This step will take a bit more time to assess.

- **Twitter**

The first social media site to visit is the project's Twitter account. Twitter is a quick method to determine how socially active the project is and the most recent tweets. It's also good to note the interaction within the tweets. The number of Twitter followers is another important metric to be aware of.

- **Telegram / Discord**

Telegram and Discord are chat groups that can offer even greater insight into the project, the team and their community. The follower count is a good indicator to look

for. Within chat groups, take some time to read through the posts and get a feel for the type of people interested and involved. Are their questions being answered? Groups that overly engage in psychological tactics such as inducing FOMO should be considered red flags.

- **Reddit**

One of my favorite sites is Reddit. Oftentimes Reddit will have non-project sponsored groups and or discussion subreddits about the project which are not under the direct control of the project. With the upvoting system employed by Reddit, it is a great source for 'street knowledge' which may not be otherwise publically available.

Things to look for on Reddit include, how active is the community? How many followers are on the sub-Reddit? Does the team offer AMAs (ask me anything)? Is the team helpful in sharing information about the project? [13], [14].

If the coin has potential, there is almost always a Reddit discussion about it. If Reddit isn't yet talking about it, you are either really early to the party or it's yet another potential red flag.

## 3. Cryptojacking - cybercriminals can unknowingly use your computer to generate cryptocurrency

Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.

This usually occurs when the victim unwittingly installs a programme with malicious scripts which allow the cybercriminal to access their computer or other Internet-connected device, for example by clicking on an unknown link in an e-mail or visiting an infected website [15]. Programmes called 'coin miners' are then used by the criminal to create, or 'mine', cryptocurrencies.

As they are digital currencies, only computer programmes and computing power are needed to create cryptocurrencies. The type of cryptocurrency we see primarily mined on personal computers is called Monero [16].

Cryptojacking might seem like a harmless crime, since the only thing 'stolen' is the power of the victim's computer. But the use of computing power for this criminal purpose is done without the knowledge or consent of the victim, for the benefit of the criminal who is illicitly creating currency [17]. As a large number of infected devices generates a huge amount of cryptocurrency, cybercriminal see this as a lucrative crime.

The primary impact of cryptojacking is performance-related, though it can also increase costs for the individuals and businesses affected because coin mining uses high levels of electricity and computing power [18]. [19].

**Signs you could be a victim of cryptojacking**

- A noticeable slowdown in device performance
- Overheating of batteries on devices
- Devices shutting down due to lack of available processing power
- Reduction in productivity of your device or router
- Unexpected increases in electricity costs

**Prevention tips**

- Continuously monitor resources on your computer (processing speed, power usage)
- Use browser extensions that are designed to block coin mining
- Use more privacy-focused ad blockers
- Install the latest software updates and patches for your operating system and all applications especially those concerning web browsers

Block pages that are known to deliver cryptojacking scripts.

## 4. Recognizing the bitcoin scams

It's easy to look at these individual cases and marvel at how foolish the victims seem to be. Why was Mike listening to a woman he'd never actually met and agreeing to invest hundreds of thousands of dollars? How could anyone give away $500,000 worth of Bitcoin to a business partner without at least picking up the phone to discuss the deal? How could someone believe that they could get a guaranteed 50% return? [20].

The problem is that it's easy to lose your sceptical faculties when you feel like you've met your future spouse, you're chatting with who you think is a close partner or you believe you've found a sure thing. It's easy to lose sight of red flags when these confounding factors cloud your judgment.

That's why it's important to keep a few rules of thumb in mind whenever someone you've never actually met comes to you with a chance to make money in Bitcoin [21], [22].

• Don't believe the hype. Any claim of a guaranteed return, especially a very sizable guaranteed return, should always be treated as a scam. There are practically no legitimate investments that can double your money in a week or a month, or even a year, as Bernie Madoff's victims can attest. Likewise, ignore any claim that your Bitcoin investment can be "multiplied."

• Bitcoin for Bitcoin's sake. The reason why Bitcoin has risen so dramatically in value recently is because genuine investors believe they can sell it to someone else for a higher price at a future date. That's what makes crypto a highly speculative

investment. Always ignore "investment opportunities" that claim to be helping you get in on special or rare deals that involve Bitcoin.

• Obsessed with Bitcoin. Let's say you meet someone online, and they really want you to invest in Bitcoin. They're almost certainly lying to you. Meanwhile, the government–especially the Social Security Administration–doesn't track you down and demand instant crypto payments. If you're dealing with someone who is demanding that you adopt Bitcoin in some fashion, disengage and call the cops.

If you suspect that you've been the target of a crypto scam, file a report with the FTC. When you share information about Bitcoin scams, it can help the FTC investigate fraud methods and keep Americans aware of new scams.

## 5. The 4 bitcoin scams and how to overcome

Bitcoin scams are like a box of chocolates. You never know what kind you're going to get. While the brashest crypto scams end up in the headlines, like the case of a Las Vegas poker player who pilfered $500,000 from another card shark, most shakedowns are more prosaic. Think of schemes that use threatening phone calls, a desperate plea for money or a demand to transfer sums of cash or else [23].

Whatever form it takes, there's no denying that cryptocurrency fraud is on the rise. The Federal Trade Commission (FTC) received 7,000 reports of crypto theft, with a combined value of more than $80 million, between October 2020 and March 2021. That's a 12-fold increase in cases and a 1,000% jump in cash amount compared to the same period a year prior.

When it comes to Bitcoin fraud, the strengths of cryptocurrency are turned against the victims. "Bitcoin-related scams track with other criminal exploits online until you try to recover your assets," said cybersecurity expert Adam Levin. "Cryptocurrency is designed to be hard to track and even more difficult to recapture. Once transferred, it's gone, with a few very high-level exceptions."

While the number of Bitcoin transactions has remained static in recent years, the value of cryptocurrency has surged. One Bitcoin was worth $9,000 in April 2020 compared to roughly $43,000 now [24]. Here are the Bitcoin scams that you should be on the lookout to avoid.

### 5.1 Bitcoin Fraud and Imposters

In the poker scam mentioned above, the perp allegedly posed as the victim's business partner on the encrypted text app, Telegram. The faux partner wanted to exchange $500,000 worth of Bitcoin, plus a $50,000 fee, for cash. The victim sent the Bitcoin, but never got the cash. When he reached out to his real associate by other means, the associate had no clue what was going on [25].

The numbers involved in Bitcoin imposter schemes aren't always this large. For instance, one scammer who posed as a Coinbase reporter contacted public relations companies offering positive coverage for clients in exchange for a measly sum of $600.

And then there are twists on old-fashioned Social Security scams. For instance, a Naples, Fla. resident was told by a perp that her Social Security number had been stolen and was being used to open fraudulent bank accounts. She was instructed to download an app, then transfer all of her money from her bank account into Bitcoin. Thankfully, a fraud alert popped up on her phone before the deed was done.

"Always take a moment before clicking on links sent via email or SMS, and don't install apps on your mobile device unless you're 100% certain they are legit by checking the reviews on the platform where you found them," said Levin [26].

The FTC warns of another Social Security scam where folks are told to deposit cash in Bitcoin ATM machines to pay scammers who are claiming to be from the Social Security Administration.

## 5.2 Fake Bitcoin Investing Scams

Bitcoin is an abstraction of an abstraction. It's a store of value that not only doesn't take any physical form, but also lacks any backing by the full faith and credit of a sovereign government.

Enthusiasts find these aspects of cryptocurrency deeply appealing [27]. Many Bitcoin investors believe the less government involvement in money, the better. Others prefer to engage in financial transactions that are hard to trace by the authorities.

Unfortunately, these are also big advantages for scammers who set up fake websites purporting to offer new investors the chance to make a quick buck. This is what happened to one victim of a 2017 scheme from Australia.

The man, whom ABC Everyday identified as Jonathan, saw an Instagram post that advertised the chance to make a 50% return mining for Bitcoin. He initially sent the site $50, and soon thereafter got $30 back in profit.

Moreover, the Instagram account was full of testimonial videos and other folks endorsing the service, and had thousands of followers. It looked legitimate.

He then prostelyzed his newfound opportunity to friends and family. All in all, Jonathan, his family and friends chipped in about $20,000. Then the account disappeared, and the thief with it. Not only did he lose his money, but some of his friends no longer speak to him. The entire cost of these types of Ponzi-style Bitcoin scams can be enormous [28].

"Many people have reported being lured to websites that look like opportunities for investing in or mining cryptocurrencies, but are bogus," per the FTC. "Sites use fake testimonials and cryptocurrency jargon to appear credible, but promises of enormous, guaranteed returns are simply lies.".

## 5.3 Bitcoin Giveaway Fraud

In July 2020, something truly remarkable happened. Celebrities and famous figures around the world all went to their Twitter accounts simultaneously to promote the same Bitcoin giveaway offer. Shockingly, it seemed too good to be true.

"I am giving back to my community due to Covid-19!" wrote former President Barack Obama on his Twitter account. "All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!" [29].

The accounts for Joe Biden, rapper Kanye West and former New York City mayor Mike Bloomberg, among others, published the same message.

As you probably guessed, the giveaway offers were all part of an unprecedented Twitter hack. Jack Dorsey, the former chief executive officer of Twitter, called it "a tough day" for the social media company.

These types of scams, though, are nothing new. The FTC estimates that over a six-month period in late 2020 and early 2021, people reportedly sent more than $2 million in cryptocurrency to investment frauds pretending to be fronted by Tesla Inc. founder and crypto enthusiast Elon Musk [30].

## 5.4 Crypto Romance Scams

Bitcoin's meteoric rise has dovetailed with the mass adoption of dating apps that make it really easy to find new romantic partners. While that may be a boon for people who are looking for love, it's also a goldmine for scammers.

In fact, cryptocurrency was the top payment choice for romance scams reported to the FTC in 2021 ($139 million), followed by bank transfers ($121 million), wire transfers ($93 million) and gift cards ($36 million) [31].

While romance scams are nothing new, cryptocurrency adds a new twist: Unsuspecting paramours believe they're getting in on a crypto investing opportunity.

Take Mike (not his real name), who was recently profiled by NBC News. Mike met a woman named Jenny on Tinder. They struck up a relationship, texting on Tinder and WhatsApp.

After about a month, Jenny told Mike that she had a good tip. She claimed that her uncle worked at JPMorgan Chase, and "…was the world expert in Bitcoin options."

Mike was in the market for love, not Bitcoin, but he soon grew interested and invested $3,000 on Crypto.com, a legitimate cryptocurrency exchange.

Eventually the con grew deeper. Jenny persuaded him to move his money to a different exchange and to keep investing. His portfolio soon hit $1 million in value.

Mike grew suspicious when Jenny told him to send his tax payments to the Department of Homeland Security instead of the Internal Revenue Service (IRS). Then he found he couldn't withdraw his money from the new crypto exchange account, at which point he realized it was all a long con. Mike ultimately lost nearly $280,000 [32].

## 6. Cryptocurrency being used in cybercrime

It has been a little over a decade since we have heard the term cryptocurrency for the first time. But even in this short span, it has been attacked by criminals an infinite number of times. The history of the crypto market is itself proof of this statement. What makes cryptocurrencies so vulnerable to cyberattacks? And how do these cybercrimes take place? In this blog we will study how cryptocurrencies are affected by cybercrime.

- **Glossary**

Before relating the two important terms together i.e., cryptocurrency and cybercrime. Let us first consider these terms separately. Here is the list of important terms that we are going to repeat again and again in the blog [33].

- **Cryptocurrency:** Cryptocurrency is often referred to as the virtual currency or the digital currency. Secured by cryptography, cryptocurrency is the decentralized network that works on blockchain technology.
- **Bitcoin**: One of the most leading cryptocurrencies. Bitcoin has high interchange and exchange value as compared to other altcoins.
- **Bitcoin address:** Bitcoin addresses are 26-to-34-character long strings. It directly connects the user to a bitcoin payment window.
- **Cybercrime**: Cybercrime is a criminal activity related to the virtual world. It is not meant as some physical criminal activity of the world such as kidnapping, murder, etc.

But it is the criminal activity that happens by the medium of digital devices such as computers and the internet. It is the most prevalent criminal record in the modern world. The Information Technology Act provides necessary information related to it.

- **Cybersecurity**: Cybersecurity is the steps and guidelines taken to prevent activities related to cybercrime. Cybersecurity, sometimes referred to as IT security, is the practice of protecting critical systems and digital attacks.

- **Cryptocurrency and Cybercrime**

Day by day, the frequencies of cyberattacks are increasing. The ransom payments made to the hackers are also exceeding the count every day. One of the basic characteristics of cryptocurrency is that it can be traded anonymously. Thus, it emerges as the most potential platform for the cyber extortionists.

So just like any cybercrime, it starts with a ransomware attack on a company or organization. Later, the executive realizes that his business site is down and broken [34]. Once the administrator overrides don't work on sites, a random mail will arrive via Gmail or other email.

That mail might contain a Bitcoin address where the payments are required to be made, if the company wants to make their site operational again along with the deadline. This is how cryptocurrency plays its role in enhancing the cyber risks and cybercrimes.

Cryptocurrencies are not regularly governed by the government; this makes them more vulnerable to cybercrime around the globe. Also, cryptocurrencies carry millions of dollars across borders without detection, thus, criminals find it the most suitable slot to attack. Here are some top reasons that make cryptocurrencies vulnerable to cybercrimes.

- **Pseudonymous**

This is the major reason that makes the cryptocurrency so sensitive. The transactions and accounts in cryptography are not connected to the real-world identities [35]. Most of the time it works on digital strings. So, it becomes quite easier for the criminals to hide their identity while using crypto.

- **Easier access**

When payments are made from Bitcoin addresses the hackers or criminals can easily create new addresses. Unlike the real world, creating a new identity in a crypto network is not a big deal and doesn't require much validation and documentation [36].

These addresses help to analyze the transaction flow, but still doesn't allow them to connect with the real-world identity of the users.

- **Fastest network**

Physical and traditional transactions take time, this helps the users to increase more security to their money. But digital transactions and crypto transactions are done nearly in fractions of seconds [37]. Thus, there is very little or no time to ensure the intermediate security and safety from the cyber-attacks.

- **Global network**

Unlike physical money, which is validated to a particular region or nation, cryptocurrency is a global standard. It is accepted anywhere and everywhere. A man from Russia can easily manage digital trade with a person from America, see Figure 1 [38]. This easy access to several locations increases the vulnerability of cryptocurrency.

**Figure 1**
*Attack Types Via Cryptocurrency*


There are different types of cyberattacks where criminals are easing the process by the means of cryptocurrency. Here are the few examples:

- **Ransomware**

Ransomware is the most advanced trend in history. It is designed to extort money by encrypting user data. As explained above, ransomware flashes a message or mail with a link inside. This message is a threat asking the user to deposit the money if he wants to regain his access or control [39]. The criminal can't be traced or connected to real-world data and asks a heavy amount by the means of bitcoin or any other altcoin. In 2017, two ransomware WannaCry and NotPetya had brought down the market and ruined many companies and organizations. Well, reason can also contribute to the steep rise in bitcoin prices the same year.

- **DDoS Extortion**

DDoS extortion also known as RDoS which is expanded as ransom-driven DDoS. It is the oldest and easiest way to earn profits. These kinds of malware are very capable of using cryptocurrency payments. And are very difficult for the investigators to track the flow of money. And thus, money is easily swept from victims to criminals. The criminals hijack the operational site by a DDoS attack, and then ask the organizations to pay them a heft bitcoin amount if they want to regain the control of their site [40]. In 2014, an extortion technique DD4BC emerged that attacked several sites. Later in 2016, the group was arrested by Europol. Even after that, attackers did several minor DDoS attacks to let the public feel the fear of their powers and capabilities.

- **Cryptojacking**

Crypto Jacking is the type of attack in which hackers use computer power of a compromised device to generate cryptocurrency. This is done without letting the owner be aware of it. Cryptojacking can affect digital devices such as smartphones, servers, computers or IoT devices. The result of Cryptojacking is device slowdown, increased energy consumption, overheating batteries, reduction in productivity and device failure.

In 2017 and 2018, Cryptojacking shot the crypto market. The reason behind it is increase in crypto prices and general revival of the crypto market [41].

- **Cryptomining**

Cryptomining is also responsible for illegal mining of cryptocurrencies. There are two types of Crypto Mining, active Crypto Mining and passive Crypto Mining. Both techniques are used to exploit a victim's processing power without authorization from the owners. Earlier, Bitcoin was the target of criminals, but later their focus shifted to Monero in 2019 [42].

- **Cryptocurrency Hacks**

Cryptocurrencies itself have been hacked by criminals so many times in history. It has always been an appealing target to the hackers. Hackers attack on crypto assets, crypto exchanges and other platforms. In 2018, many cryptocurrencies were hacked, and more than 1-billion-dollar cryptocurrencies were stolen from exchanges and platforms [43].

**How to protect Cryptocurrencies from Cybercrime?**

There are steps that can be taken to protect cryptocurrencies from cybercrime and related criminal activities [44].

1) Don't open suspicious email attachments or unknown links.
2) Make regular offline backups and install software updates from time to time.
3) Don't install free apps from unofficial sources.
4) Use strong passwords for computers, mobile and IoT devices.
5) Use highly approved antivirus software.
6) Check when the computer or device lags or stops working.
7) Consider a DDoS protection solution to protect the major and minor attacks

Cryptocurrency is still in its neonatal stage. Roughly the count of its existence is less than a decade. But still, it is prone to different risks. Even the history itself is proof of how many times cryptocurrencies have been attacked by hackers. Therefore, protection and security should be increased to protect this field.

## 7. Conclusion

This research provides a number of novel findings related to our selected cryptocurrency markets. Primarily, there are significant differences identified in the volatility responses of cryptocurrencies to attacks on exchanges and ICO-fraud, both of which can be heavily dependent on perceptions of stability and financial safety. In a DCC-GARCH analysis, we observe that there are lower volatility estimates identified for smaller capitalisation cryptocurrencies when compared to the cross-correlations between their larger counterparts. We identify the largest sustained increase in cross-cryptocurrency correlations between the 6th of December 2017 and the 13th of January 2018, incorporating a number of significant hacks in our sample. Peak cross-

correlations occur on the 18th of December 2017, indicative of a substantial loss of confidence in the cryptocurrency market during this time due to sustained internationally relayed coverage of multiple significant cybercrime events.

The second distinct phase of elevated cross-correlations occurs during the period between the 4th of March 2018 and the 9th of April 2018 which represent the theft of approximately $300 million during the multi-level-marketing scheme created by GainBitcoin and the ICO scam inspired by Ifan and Pincoin that resulted in the loss of $650 million. Two distinct novel results are presented:

1) we find evidence of broad comovement in cryptocurrency markets during periods of extreme stress and severe reputational damage; and

2) these same relationships change substantially in the period after cryptocurrency cybercriminal, indicating that not only is the price volatility of these financial products directly influenced, but also the manner in which the information shares, information leadership share and the component share of the price discovery is processed.

## References

Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

"Blockchain". Investopedia. Archived from the original on 23 March 2016. Retrieved 19 March 2016. Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system.

Iansiti, Marco; Lakhani, Karim R. (January 2017). "The Truth About Blockchain". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.

Raval, Siraj (2016). Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc. pp. 1–2. ISBN 978-1-4919-2452-5.

Park, Sehyun; Im, Seongwon; Seol, Youhwan; Paek, Jeongyeup (2019). "Nodes in the Bitcoin Network: Comparative Measurement Study and Survey". IEEE Access. 7: 57009–57022. doi:10.1109/ACCESS.2019.2914098. S2CID 155106629.

Hern, Alex (17 January 2018). "Bitcoin's energy usage is huge – we can't afford to ignore it". The Guardian. Archived from the original on 23 January 2018. Retrieved 23 January 2018.

Baraniuk, Chris (3 July 2019). "Bitcoin's global energy use 'equals Switzerland'". BBC News. Retrieved 2 February 2020.

"Blind Signatures for Untraceable Payments" (PDF). Archived from the original (PDF) on 18 December 2014. Retrieved 26 October 2014.

"Untraceable Electronic Cash" (PDF). Archived (PDF) from the original on 3 September 2011. Retrieved 10 October 2012.

Pitta, Julie. "Requiem for a Bright Idea". Forbes. Archived from the original on 30 August 2017. Retrieved 11 January 2018.

"How To Make A Mint: The Cryptography of Anonymous Electronic Cash". groups.csail.mit.edu. Archived from the original on 26 October 2017. Retrieved 11 January 2018.

Law, Laurie; Sabett, Susan; Solinas, Jerry (11 January 1997). "How to Make a Mint: The Cryptography of Anonymous Electronic Cash". American University Law Review. 46 (4). Archived from the original on 12 January 2018. Retrieved 11 January 2018.

"Bitcoin: The Cryptoanarchists' Answer to Cash". IEEE Spectrum. Around the same time, Nick Szabo, a computer scientist who now blogs about law and the history of money, was one of the first to imagine a new digital currency from the ground up. Although many consider his scheme, which he calls "bit gold", to be a precursor to Bitcoin

Jerry Brito and Andrea Castillo (2013). "Bitcoin: A Primer for Policymakers" (PDF). Mercatus Center. George Mason University. Archived (PDF) from the original on 21 September 2013. Retrieved 22 October 2013.

Bitcoin developer chats about regulation, open source, and the elusive Satoshi Nakamoto Archived 3 October 2014 at the Wayback Machine, PCWorld, 26 May 2013

Wary of Bitcoin? A guide to some other cryptocurrencies Archived 16 January 2014 at the Wayback Machine, ars technica, 26 May 2013

"UK launches initiative to explore potential of virtual currencies". The UK News. Archived from the original on 10 November 2014. Retrieved 8 August 2014.

"UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence" (PDF). HM Treasury. Retrieved 1 October 2021.

"China declares all crypto-currency transactions illegal". BBC News. 24 September 2021. Retrieved 24 September 2021.

Lansky, Jan (January 2018). "Possible State Approaches to Cryptocurrencies". Journal of Systems Integration. 9/1: 19–31. doi:10.20470/jsi.v9i1.335. Archived from the original on 12 February 2018. Retrieved 11 February 2018.

"The Dictionary Just Got a Whole Lot Bigger". Merriam-Webster. March 2018. Archived from the original on 5 March 2018. Retrieved 5 March 2018.

Yang, Stephanie (31 January 2018). "Want to Keep Up With Bitcoin Enthusiasts? Learn the Lingo". The Wall Street Journal. Retrieved 25 October 2020.

Browne, Ryan (5 December 2017). "Bitcoin is not a bubble but other cryptocurrencies are 'cannibalizing themselves,' fintech exec says". CNBC. Retrieved 25 October 2020.

Kharif, Olga (15 January 2018). "These Digital Coins Soar (or Fall) With Bitcoin". Bloomberg. Retrieved 25 October 2020.

Hajric, Vildana (21 October 2020). "Bitcoin Surges to Highest Since July 2019 After PayPal Embrace". Bloomberg Law. Retrieved 25 October 2020.

"Forget Bitcoin: Inside the insane world of altcoin cryptocurrency trading". CNET. Retrieved 22 November 2021.

Vigna, Paul (19 December 2017). "Which Digital Currency Will Be the Next Bitcoin?". The Wall Street Journal. Retrieved 25 October 2020.

Steadman, Ian (11 May 2013). "Wary of Bitcoin? A guide to some other cryptocurrencies". Ars Technica. Retrieved 19 January 2014.

Popper, Nathaniel (1 October 2017). "Understanding Ethereum, Bitcoin's Virtual Cousin (Published 2017)". The New York Times.

"Ethereum Upgrade Adds to Crypto Mania Sparked by Bitcoin's Surge". Bloomberg.com. 25 November 2020.

Popper, Nathaniel (27 March 2016). "Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's". The New York Times. Retrieved.

Y. A. Baker El-Ebiary et al., "Blockchain as a decentralized communication tool for sustainable development," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 127-133, doi: 10.1109/ICSCEE50312.2021.9497910.

Y. A. Baker El-Ebiary et al., "Track Home Maintenance Business Centers with GPS Technology in the IR 4.0 Era," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 134-138, doi: 10.1109/ICSCEE50312.2021.9498070.

S. I. Ahmad Saany et al., "Exploitation of a Technique in Arranging an Islamic Funeral," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 1-8, doi: 10.1109/ICSCEE50312.2021.9498224.

J. A. Jusoh et al., "Track Student Attendance at a Time of the COVID-19 Pandemic Using Location-Finding Technology," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 147-152, doi: 10.1109/ICSCEE50312.2021.9498043.

Y. A. Baker El-Ebiary et al., "E-Government and E-Commerce Issues in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 153-158, doi: 10.1109/ICSCEE50312.2021.9498092.

Y. A. B. El-Ebiary et al., "Determinants of Customer Purchase Intention Using Zalora Mobile Commerce Application," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 159-163, doi: 10.1109/ICSCEE50312.2021.9497995.

S. Bamansoor et al., "Efficient Online Shopping Platforms in Southeast Asia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 164-168, doi: 10.1109/ICSCEE50312.2021.9497901.

S. Bamansoor et al., "Evaluation of Chinese Electronic Enterprise from Business and Customers Perspectives," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 169-174, doi: 10.1109/ICSCEE50312.2021.9498093.

A. Altrad et al., "Amazon in Business to Customers and Overcoming Obstacles," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 175-179, doi: 10.1109/ICSCEE50312.2021.9498129.

Y. A. Baker El-Ebiary et al., "Mobile Commerce and its Apps - Opportunities and Threats in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 180-185, doi: 10.1109/ICSCEE50312.2021.9498228.

M. B. Mohamad et al., "Enterprise Problems and Proposed Solutions Using the Concept of E-Commerce," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 186-192, doi: 10.1109/ICSCEE50312.2021.9498197.

P. R. Pathmanathan et al., "The Benefit and Impact of E-Commerce in Tourism Enterprises," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 193-198, doi: 10.1109/ICSCEE50312.2021.9497947.

K. Aseh et al., "The Future of E-Commerce in the Publishing Industry," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 199-205, doi: 10.1109/ICSCEE50312.2021.9498175.