Crime Prevention and Criminal Justice

Implementing Measures to Prevent Cryptocurrency Fraud

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Michel Gerges

Forum	Commission on Crime Prevention and Criminal Justice
Issue:	Implementing Measures to Prevent Cryptocurrency Fraud
Student Officer:	Michael Gerges
Position:	Deputy President

Introduction

Crypto-currencies are a relatively new technology in the finance industry. They have seen massive public interest and investment, which has been motivated by large scale advertising across mega-events such as the Super bowl and the 2022 World Cup, as well as celebrity endorsements.

Cryptocurrencies have had one of the most volatile valuation records in history. In November 2021, the net market capitalization of all cryptocurrencies combined reached an all-time peak market capitalization of $2 trillion. However, just three months later, this valuation halved. This unprecedented volatility has been caused, in large part, by the spread of cryptocurrency fraud and theft, which have caused traders to lose faith and withdraw their investments in cryptocurrencies.

Cryptocurrency fraud also presents a challenge to legal authorities. They are difficult to trace by law enforcement to any one individual buyer or seller and are used to facilitate illegal activities worth over $20 billion as of 2022. This number continues to rise as cryptocurrencies become more popular. Hence, it is imperative that nations negotiate regulations around cryptocurrency use and coordinate initiatives to enforce such regulations on the required international level of this decentralized threat to finance.

Definition of Key Terms

Cryptocurrency

A digital trading token, often given a name, which can be bought and sold to other online clients on a digital cryptocurrency exchange.

Dark-web

An anonymous, specially-accessed web separate from the world wide web. This part of the internet is most commonly used by criminal organizations for requesting and selling illicit goods and services.

Cryptocurrency Exchange

An online platform where cryptocurrencies held by users online can be exchanged for real currencies or other cryptocurrencies.

Ransomware

Software that, when installed on an electronic device, locks data on the electronic device and allows it to be copied or deleted from the device to the owner of the ransomware. This software can then be leveraged on the user of the data by threatening to delete or copy the data unless a payment would be made to the ransomware owner to remove the ransomware.

General Overview

The Rapid Growth of Cryptocurrency Fraud

Cryptocurrencies began as a niche product for risk-forward investors. The first prototype of a cryptocurrency trading system was invented in 1983 by David Chaum, dubbed e-cash. However, the company ultimately failed in the late 1990's because the internet was still in the early stage of its development. This concept was expanded upon in 2009 with the invention of bitcoin and blockchain technology, improving privacy of transactions (which could be done internationally more easily than regular bank wire transfers, as well as cheaper due to the lack of an intermediary entity). Bitcoin is the flagship cryptocurrency in the industry, and is the most valuable and bought, with an impressive upwards trend in value since its inception.

Soon after bitcoin was created criminal organizations became interested in the concept and began using cryptocurrency for trade of illegal goods. In the American state of Texas, in 2011, Ross Ulbricht, with a small group of supporting staff, decided to take advantage of bitcoin privacy to launch the Silk Road, a dark-web trading market. In the United States, the Federal Bureau of Investigations (FBI) were able to shut Ulbricht's website down and arrest Ulbricht and his team in 2013. The Silk Road managed to trade $200 million in illicit goods such as weapons, drugs and forged legal documents to over 100,000 buyers in its two-year lifespan, and was the first case of cryptocurrencies being used for criminal commerce.

In 2014, hacker groups were becoming capable of bypassing the security measures of cryptocurrencies in order to steal cryptocurrency from any digital wallet. Two Russian nationals were able to steal 647,000 bitcoins from the customers of the massive cryptocurrency exchange Mt. Gox, at a time when 1 bitcoin was worth $320, amounting to a heist worth roughly half a billion dollars. The severity of the theft caused Mt. Gox to file for bankruptcy which played a role in the stagnation of cryptocurrencies' values from 2014-2016.

During the Covid-19 pandemic of the years 2020-2021, cryptocurrency-based crime saw a massive increase. The value of cryptocurrencies received by suspicious users grew from $8.4 billion to $18.4 billion. This was because of the huge influx in the amount of people accessing the internet daily, inevitably increasing the exposure to dishonest cryptocurrency schemes.

Types of Fraud

Due to the deep involvement digital goods have in the operating of the world, malicious actors can use various methods to breach into the data, or steal the cryptocurrencies of any web users.

Ponzi Schemes

Ponzi Schemes occur when a company falsely reports its earnings to draw in investors whose funds then allow the company to maintain an honest image. This is done by using those same funds to pay those who withdraw their money from the business. This scheme causes an increase in cash flow into the business; allowing the scheme to continue to grow and succeed as long as the amount of cash entering the business is greater than the amount exiting. If the cash exiting the company becomes greater than the amount entering, a liquidity crisis occurs and the scheme collapses. While this scheme is ongoing, it is possible for the owner of the illicit business to use these funds for their own purposes.

In the cryptocurrency industry, this type of fraud has seen prolific success. One notable case was FTX (Futures Exchange), a company that operated from May 2019 up until November 2022, when it filed for bankruptcy due to the aforementioned liquidity crisis that occurs when Ponzi schemes fail. The company's CEO, Sam Bankman-Fried, was seen as a revolutionary in the cryptocurrency industry and was embraced by 40 investors who bought shares in the company. At its peak, the company was valued at $32 billion. When it collapsed, those invested in crypto worldwide began to lose faith in other companies in the

cryptocurrency industry. As a result, the industry fell below $1 trillion in valuation as a consequence of FTX's malpractice.

Ransomware

Ransomware attacks target servers and databases of critical infrastructures such as hospitals and schools and can cause the complete halt of procedures, often costing businesses more money than the requested ransom payment. For hospital patients, ransomware attacks could be life-threatening, as medical professionals are unable to treat their patients without access to their computers. Cryptocurrencies have been used in conjunction with ransomware to facilitate untraceable, irreversible payment of ransoms by malicious hacker groups. As an example, in January 2022, two major German oil companies were simultaneously attacked by ransomware, halting the operation of 233 gas stations across the country. Half a billion dollars were paid out to ransomware terrorists in 2022.

Social-media scams

Social media scams involve the advertising of a false cryptocurrency promotion through popular platforms like Twitter, Facebook or Instagram. In some cases, famous celebrities or philanthropists' accounts, such as Bill Gates, Elon Musk and Barack Obama, have been hacked to publish messages online promoting fraudulent cryptocurrency schemes. Additionally, private messaging groups on WhatsApp or Telegram can share messages promoting cryptocurrency scams, spreading quickly between large amounts of users. These types of fraud represent 25 percent of the $20 billion dollar estimate mentioned above and are the largest form of cryptocurrency fraud by volume.

Dark-web trade

The dark-web almost exclusively uses cryptocurrencies for trading between users. This type of crime has been the most persistent: whenever policing institutions are, after many months and occasionally years of effort, finally able to infiltrate and destroy dark-web trading platforms, smaller markets still available to users will capture the freed-up traffic.

Even after Hydra, the largest dark-web trading market in history, was shut down in April 2022 by collaborative efforts between American and German governments, criminals simply

migrated their business to other available dark-web markets and trade quickly returned to normal daily levels in the second half of 2022.

Major Parties Involved

INTERPOL (The International Criminal Police Organization)

Interpol work closely with governments to seek and destroy illicit cryptocurrency businesses and organisations. Independently, they have launched operations and established centres with the mission of reducing cryptocurrency-related crimes. Between June and November of 2022, Interpol launched a cryptocurrency fraud focused police operation dubbed HEACHI-III, which saw the seizure of $150 million in digital assets as well as the arrest of over 900 individuals responsible for various types of online investment and extortion scamming. The operation was run by the financial crime and anti-corruption centre (IFCACC) of Interpol. They also host the annual conference on criminal finances and cryptocurrencies, in turns with Europol and the Basel institute on governance, discussing and sharing experiences in the growing crime sector between the organizations.

Global Programme on Cybercrime

A programme established by the UNODC under resolutions 22/7 and22/8 in 2013, with the mission statement of assisting member states in policing digitally-based crimes. As of 2023, the program is funded entirely by Australia, Canada, the United Kingdom, Norway and the United States. The program aims to help developing nations improve their technical capacity to tackle cybercrime, including ‘online frauds and online money laundering’.

IMF (International Monetary Fund)

The IMF has worked to produce several guidelines and recommendations to nations in order to reduce the likelihood of cryptocurrency fraud. They published a nine-point plan detailing the most important aspects that cryptocurrency laws should enforce and track digital assets in banks. They have also made efforts to include anti-money laundering and counter-finance-terror assessments in their Financial Sector Assessment Program, considering cryptocurrency assets during the assessments.

UNODC (United Nations Office on Drugs and Crime)

The UNODC has worked closely with the CCPCJ in preparing the United Nations with the necessary technical capabilities to tackle cryptocurrency crime. They have shared information on organised crime activity as well as money laundering data to aid domestic policing forces in arresting criminal organizations promoting cryptocurrency fraud.

World Economic Forum (WEF)

In conjunction with the IMF and the World Bank, the WEF has held over 20 conferences in the past decade opening the discussion on the security of cryptocurrencies and their macro-economic effects to bankers worldwide. They have published numerous warning reports to nations on the dangers of unregulated cryptocurrency markets to banking systems and have urged. In addition to this, the World Economic Forum hosts the Digital Currency Governance Consortium, where public and private sector representatives from 33 countries come together in roundtables and workshops to 'address key questions and governance gaps in digital currency'.

Timeline of Key Events

This timeline shows some key events for the development of cryptocurrencies, major fraud attacks and the actions that were taken to prevent them by cryptocurrency institutions across the globe.

Date	Description of event
January 2009	Bitcoin- the world's first fully developed cryptocurrency- launches publicly by an anonymous entity.
October 2009	The first cryptocurrency exchange- New Liberty Standard - launches at a rate of 1 dollar to 1.3 million bitcoins.
February 2011	Silk Road launches: the first dark-web trading market that used cryptocurrency. At the same time, bitcoin reaches equivalency with the US dollar.
2012	The first ransomware to use cryptocurrency for payments launches, dubbed Reveton.

December 2013	People's Republic of China bans cryptocurrencies altogether, making a statement to the world on its lack of faith in the prospect.
2014-2015	Cryptocurrencies stagnate, prices remain consistent and there is little public interest in them.
January 2017	Bitcoin prices begin to skyrocket to over $1000 per bitcoin, attracting interest into the cryptocurrency market to the public.
October 2018	Malta becomes the first country to add cryptocurrency regulations to its laws.
March 2022	Interpol Launches the centre against financial crime and corruption, aiming to reduce cryptocurrency crime online.
June 2022	Markets In Crypto Act (MICA) agreed upon in EU, setting a comprehensive framework for cryptocurrency regulations.
2022	Cryptocurrency-related crimes at an all-time high, valued at $20.6 billion.

UN involvement, Relevant Resolutions, Treaties and Events

- Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime (CCPCJ/Res/22/8, from the 22nd session of the CCPCJ, 7 December 2012 to 26 April 2013)
- Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity December 2021 (A/RES/76/187)

- Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity 18 December 2019 (A/RES/74/177)
- Countering the use of information and communications technologies for criminal purposes, 17 December 2018 (A/RES/73/187)
- Countering the use of information and communications technologies for criminal purposes, 27 December 2019 (A/RES/74/247)

Previous Attempts to solve the Issue

The European Union has taken extensive measures in regulating cryptocurrencies as well as policing cases of fraud. The Markets in Crypto Act created a comprehensive set of guidelines around cryptocurrencies in 2022; economists are optimistic that this should stabilize the cryptocurrency market in Europe. However, it remains to be seen whether this act will have an effect on cryptocurrency crime in Europe as it has yet to be put into effect. They also successfully shut down Darkmarket, a dark-web trading platform that was the most successful before Hydramarket.

Between June and November of 2022, Interpol launched a cryptocurrency fraud focused police operation dubbed HEACHI-III, which saw the seizure of $150 million in digital assets as well as the arrest of over 900 individuals responsible for various types of online investment and extortion scamming. The operation was run by financial crime centre (IFCACC). They also host the annual conference on criminal finances and cryptocurrencies, in turns with Europol and the Basel institute on governance, discussing and sharing experiences in the growing crime sector between the organizations. Unfortunately, Interpol's successes are dwarfed by the massive scale of the cryptocurrency crime industry, with this seizure only accounting for about 1.3% of the scam sector of cryptocurrency fraud's revenue in 2022.

Many nations have taken the route of banning cryptocurrencies altogether. China has labelled cryptocurrencies as too dangerous to allow into their domestic economy and trade. Although this is an extreme solution, it should be noted that there has always been scepticism on the motivations behind the invention and use of cryptocurrency altogether, and some market analysts have argued that cryptocurrencies have done more harm than good to society. Nevertheless, the activity of cryptocurrency crime in China despite the ban has shown that an all-out ban does not guarantee that cryptocurrency crime will disappear in a state.

Possible Solutions

The first and most logical step that could be taken to reduce the impact of all cryptocurrency related crimes would be to increase the amount of funds, or allocate a larger proportion of the available UN funds going towards cybercrime-focused institutions, including the Global Program on Cybercrime. The improved financial support could then be spent on recruiting more cyber-security specialists and providing them with the necessary standard of technological hardware. It is also necessary to expand the enforcement of cryptocurrency regulations, perhaps by the establishment of a cryptocurrency division in the IFCACC branch of INTERPOL.

Another would be to modify the nature of cryptocurrencies to make them traceable by certain bodies of international government and making the previous version illegal entirely. This would make the process of policing cryptocurrencies easier for policing organizations, thus allowing them to be able to detect more cases of criminal behaviour on the cryptocurrency market. Although, it could be argued that this would defeat the purpose of cryptocurrencies entirely, and nullify its value to those living in countries with oppressive governments, who use cryptocurrency for privacy purposes. Additionally, this could cause governments to lose their power over private cryptocurrencies as regulations would not be able to be imposed on an illegal commodity.

Lastly, it may be possible for nations to, with extensive cooperative measures, create a new, cryptocurrency-focused regulating and policing body, as a new UN Branch. This would serve the benefit of having one singular authority on all cryptocurrencies worldwide, which is significant as the decentralization of cryptocurrencies makes independent domestic regulations have a mitigated effect on cryptocurrency crime. Additionally, this would reduce communications delay as it would remove the need to communicate across several organizations, as well as between state governments, as all information would be going through or to this new organization (this would also reduce the cybersecurity risk as there would be less possible nodules of cyberattack). This new organization would require new facilities and computer resources, however, and this would cost a fair sum to member states. This option also runs the risk of creating an oversaturated cryptocurrency enforcement space if the older organizations did not shut down their cryptocurrency crime related activities.

Bibliography

Stephen Graves. *Deep Dives*. 27 December 2022. https://decrypt.co/115567/crypto-ads-made-waves-2022. Accessed 26 June 2023.

Browne, Ryan . "EU Lawmakers Approve World's First Comprehensive Framework for Crypto Regulation." *CNBC*, CNBC, 20 Apr. 2023, www.cnbc.com/2023/04/20/eu-lawmakers-approve-worlds-first-comprehensive-crypto-regulation.html. Accessed 26 June 2023.

"China Arrests over 1,100 Suspects in Crackdown on Crypto-Related Money Laundering." *CNBC*, 10 June 2021, www.cnbc.com/2021/06/10/china-arrests-over-1100-suspects-for-crypto-related-money-laundering.html.

Cohen, Luc, and Luc Cohen. "No Way to Police All Cryptocurrency Fraud, CFTC Commissioner Says." *Reuters*, 24 May 2023, www.reuters.com/technology/no-way-police-all-cryptocurrency-fraud-cftc-commissioner-says-2023-05-23/. Accessed 28 June 2023.

"Cyber-Enabled Financial Crime: USD 130 Million Intercepted in Global INTERPOL Police Operation." *Www.interpol.int*, 24 Nov. 2022, www.interpol.int/en/News-and-Events/News/2022/Cyber-enabled-financial-crime-USD-130-million-intercepted-in-global-INTERPOL-police-operation#:~:text=you%20searching%20for%20%3F-. Accessed 28 June 2023.

"DarkMarket: World's Largest Illegal Dark Web Marketplace Taken Down." *Europol*, www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down. Accessed 28 June 2023.

"Digital Currency Governance Consortium." *World Economic Forum*, www.weforum.org/communities/digital-currency-governance-consortium. Accessed 26 June 2023.

ELLIOT, LARRY. "IMF Warns of Global Risks from Unregulated Cryptocurrency Boom." *The Guardian*, 1 Oct. 2021, www.theguardian.com/business/2021/oct/01/imf-warns-of-global-risks-from-unregulated-cryptocurrency-boom. Accessed 28 June 2023.

Lagarde, Christine. "Addressing the Dark Side of the Crypto World." *IMF*, 13 Mar. 2018, www.imf.org/en/Blogs/Articles/2018/03/13/addressing-the-dark-side-of-the-crypto-world. Accessed 28 June 2023.

Mangan, Dan. "World's Biggest Darknet Marketplace, Russia-Linked Hydra Market, Seized and Shut Down, DOJ Says." *CNBC*, 5 Apr. 2022, www.cnbc.com/2022/04/05/darknet-hydra-market-site-seized-and-shut-down-doj-says.html. Accessed 28 June 2023.

Murphy, Danny. "What Is BlackCat Ransomware?" *Lepide Blog: A Guide to IT Security, Compliance and IT Operations*, 28 June 2022, www.lepide.com/blog/what-is-blackcat-ransomware/#:~:text=Examples%20of%20BlackCat%20Ransomware%20attacks. Accessed 28 June 2023.

"Ransomware 2021: Critical Mid-Year Update [REPORT PREVIEW] – Chainalysis." *Blog.chainalysis.com*, 14 May 2021, www.blog.chainalysis.com/reports/ransomware-update-may-2021/.

Reiff, Nathan. "The Collapse of FTX: What Went Wrong with the Crypto Exchange?" *Investopedia*, 27 Feb. 2023, www.investopedia.com/what-went-wrong-with-ftx-6828447#:~:text=FTX. Accessed 26 June 2023.

"The Fight against Money Laundering and Terrorism Financing." *IMF*, www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism-financing. Accessed 28 June 2023.

UNODC. "Global Programme on Cybercrime." *Unodc.org*, 2017, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html. Accessed 26 June 2023.

Appendix or Appendices

I. World Crypto Crime Report 2023: (https://go.chainalysis.com/2023-crypto-crime-report.html)

II. Geography of Cryptocurrency Report 2022: (https://go.chainalysis.com/geography-of-crypto-2022-report.html)