HISAR SCHOOL
JUNIOR MODEL UNITED NATIONS 2025

Protecting Democracy in an Age of Severe Political Polarization and Extremism by promoting constructive discourse

Legal Committee (GA6)

Creating international legal frameworks striving to prevent the usage of cryptocurrencies for cyber crime

ADRIAN NABATOV

RESEARCH REPORT

Forum: Legal Committee (GA6)

Issue: Creating international legal frameworks striving to prevent the usage of cryptocurrencies for cyber crime

Student Officer: Adrian Nabatov - President Chair

Introduction

Cryptocurrencies are a relatively new invention, the first example being Bitcoin, launched in 2009 by the mysterious Satoshi Nakamoto. Despite the growing popularity of cryptocurrencies, their extreme fluctuations (changes) in value and their independence from governments have prevented them from being adopted as mainstream currency - with the notable exception of El Salvador, which declared Bitcoin as legal tender in 2021. In theory, the blockchain mechanism, which relies on the computational power of all users of the cryptocurrency to ensure security and verification, is extremely safe and should lead to a stable currency. However, in practice, several factors such as anonymity, untraceability and ease-of-use have made cryptocurrency viable for use by criminals.

Definition of Key Terms

Cryptocurrency: A digital currency that does not rely on any central authority, such as a bank or a government, to keep track of it.

Fiat currency: A currency issued by a government that is not backed by a commodity (precious metal, etc.) At present, most government currencies are fiat currencies, and this report uses “fiat currency” to refer to “conventional” currencies issued by governments.

Blockchain: The mechanism by which the safety and verification of transactions involving cryptocurrency is ensured, relying on independent users performing computational work.

Meme coin: A cryptocurrency which grows in value extremely fast as the result of online trends, or “memes”, with little to no real economic reason.

Cryptocurrency exchange: A platform (website, service, application, etc.) that allows users to buy and sell cryptocurrency.

Insider trading: A financial crime in which someone with insider knowledge (knowledge unavailable to the public) about a project or business will invest money into it, profiting from their ability to know the future value.

Money laundering: The act of converting assets with a criminal origin into assets which appear to have a legitimate origin, so that the criminal origin of those assets cannot be tracked.

Misappropriation: The illicit use of an organization’s funds for personal purposes.

Dark web: Parts of the World Wide Web that can only be accessed through specific software, such as The Onion Router(TOR). Dark web websites are not always illegal, criminal or nefarious, but the added privacy and security of the dark web causes many criminals to prefer it.

Ponzi scheme: A fraudulent scheme which pretends to offer investment opportunities, but in reality takes money from the next "investors" it finds and gives it to the previous "investors", falsely claiming that the money comes from legitimate investment.

Legal tender: A currency officially recognized by a government.

General Overview

Cryptocurrency's relation to crimes can be broken up into two issues: **fraud involving cryptocurrency investment schemes** and **the use of cryptocurrency in criminal financial transactions**.

Fraud involving cryptocurrency investment schemes is an issue not directly caused by how cryptocurrency operates, but rather by its popularity and the trend-based nature of the growth of certain cryptocurrencies. One of the main legal uses of cryptocurrency is for investment - making a profit by buying a coin at a low price and selling it when it increases in value. The cryptocurrency investment market, being relatively new and featuring many inexperienced investors, is populated with fraudulent schemes designed to steal money from investors.

The fact that the value of many new cryptocurrencies is driven by online trends and hype causes many inexperienced people to invest in them, creating a phenomenon known as "meme coins". While this in itself is not criminal, meme coins are sometimes created with the intent to immediately sell the creators' share and keep the money, stop transactions and keep the money, or as a disguise for a Ponzi scheme. These are known as "rug pull" schemes, and are a crime which falls under financial fraud, as they are a form of insider trading and/or false advertisement. Examples of rug pulls include the 2014 Ponzi scheme OneCoin, the 2021 rug pull "Squid Coin" (unrelated to the TV series Squid Game, though it was falsely promoted as being related), and most recently the 2024 rug pull "HAWK Coin".

Occasionally, cryptocurrency exchanges commit fraud by lying about internal accounting to investors. A prominent example of this is the case of Futures Exchange (FTX). FTX, founded by Samuel Bankman-Fried in 2019, was an exchange which reportedly allowed customers to buy cryptocurrencies and withdraw them freely. However, in reality, most of the customers' money was "held" in FTT tokens, a token made by FTX itself, while the actual money was misappropriated by Bankman-Fried for personal use and political donations. According to the US Department of Justice, FTX robbed its customers of over $8 billion dollars. In 2022, the Federal Bureau of Investigation (FBI) launched an investigation into FTX as a result of an article published by CoinDesk exposing its fraud. After a trial, US courts found Bankman-Fried guilty on seven counts of fraud and conspiracy, sentenced him to 25 years in prison, and FTX filed for bankruptcy.

The use of cryptocurrency in criminal financial transactions is the use of cryptocurrency as a means of payment for illegal goods and services, as well as a means of money laundering. Criminals prefer cryptocurrency due to the anonymity it inherently offers, as cryptocurrency is not tied to any bank account or government identification. As such, cryptocurrency is a fast, anonymous and secure way to send money in a way that is difficult to trace.

One prominent use of cryptocurrency by criminals is money laundering. This is most often done through dedicated money laundering services, which are employed by various criminal organizations to hide their earnings. For example, between 2022 and 2024, the services Blender.io and Sinbad.io were found by the US Office of Foreign Assets Control (OFAC) to have laundered money stolen by DPRK-based hacking groups and sanctioned as a result. These companies are "mixers", meaning they mix illegal and legal cryptocurrency transactions by creating fake transactions to hide the source of illegal transactions. If money laundering through cryptocurrency is to be stopped, a way needs to be found to address the illegal activities of such companies.

Another use of cryptocurrencies is as an anonymous payment method for the purchase of illegal goods and services online. According to the UNODC, it is estimated that over 10 billion USD in cryptocurrency was used as payment for criminal activity in 2020 alone. Cryptocurrency is widely used by illegal online marketplaces on the dark web, such as Abacus Market, BriansClub and the now-defunct Silk Road, to sell drugs, stolen identities/accounts, credit card information and firearms.

Finally, cryptocurrency is often used by fraudsters and scammers as a "payment" method because payments are usually non-reversible. Scammers, who rely on making their victims send money before they realize that they have been defrauded, opt for cryptocurrency because it lacks many of the protections of conventional bank transfers and money transfer services. A victim who has sent a cryptocurrency payment to a scammer cannot freeze the payment or get a refund. Thus, although the decentralized nature of cryptocurrencies offers more flexibility and privacy, it also reduces security in some regards.

Major Parties Involved and Their Views

United Nations Office on Drugs and Crime (UNODC)

The UNODC is dedicated to fighting cyber crime and the drug trade worldwide, and as such considers cryptocurrency a critical matter to investigate. For example, in September 2024, the UNODC hosted the 8th Global Conference on Criminal Finances and Cryptocurrencies organized by Europol and the Basel Institute on Governance. The UNODC remains one of the most impactful forces when it comes to fighting cyber crime, especially in relation to the online sale of drugs.

European Union Agency for Law Enforcement Cooperation (Europol)

Europol, an agency that aids in joint investigation of crimes in Europe and beyond, takes the issue of cryptocurrency seriously and has engaged in a multitude of operations to curb the use of cryptocurrency in crime. For example, on the 15th of March, 2023, Europol took down the crypto money laundering

company ChipMixer, which had laundered assets worth 2.73 billion Euros through Bitcoin transactions. Europol is responsible for a lot of the research and data available on the use of cryptocurrency by criminals.

Timeline of Events

October 31, 2008	*The paper "Bitcoin: A Peer-to-Peer Electronic Cash System" is released by Satoshi Nakamoto, outlining the mechanisms behind Bitcoin and other cryptocurrencies.*
January 3, 2009	*Bitcoin, the first cryptocurrency and largest so far, is launched.*
February 2011	*The illegal dark web marketplace Silk Road is launched, the first example of a large-scale marketplace with accepted cryptocurrency payments for illegal goods.*
October 2013	*Silk Road is shut down by the FBI.*
2014	*Bolivia becomes the first country to ban the use of cryptocurrency, banning any form of currency "not regulated by a country or economic zone".*
May 2019	*FTX is founded by Samuel Bankman-Fried and Zixiao Wang.*
2021	*The People's Republic of China bans cryptocurrency, forbidding its use in any way that replaces fiat money.*
June 2021	*El Salvador becomes the first, and so far only, country to accept Bitcoin as legal tender.*
November 2, 2022	*An article is published by CoinDesk revealing the multi-billion dollar fraudulent activities of FTX, leading to its bankruptcy and the arrest of Samuel Bankman-Fried.*

Evaluation of Previous Attempts to Resolve the Issue

Complete bans on cryptocurrency

Countries such as Bolivia, China, Egypt, Nepal and more have banned cryptocurrency in an attempt to mitigate the risk of anonymous payments. However, there are significant concerns about government overreach in such actions, as this limits the freedom of innocent citizens. Many financial websites such as Forbes have raised concerns about the effectiveness of banning cryptocurrency, as there is no proof that such policies have resulted in a reduction in cybercrime. On the other hand, these countries believe that

making it harder for criminals to process transactions untraceably will allow law enforcement to target their operations.

Interpol Investigations into Cybercrime

Interpol has conducted many investigations into cybercrime, exposing large-scale schemes and helping prevent criminal activity across borders. Since cybercrime easily spreads across borders, international organizations such as Interpol are crucial in preventing it. Through operations such as Operation Night Fury and Operation Goldfish Alpha, Interpol is able to target and eliminate hackers who steal money from legitimate websites and criminals who run illegitimate websites. These investigations prove to be highly effective as they happen with international cooperation. However, new criminal organizations and types of criminal activity are constantly evolving, and as such it is difficult for Interpol to find a permanent solution to the issue.

Possible Solutions

When discussing possible ways to stop the use of cryptocurrency in cybercrime, it must first be decided if the country is willing to ban cryptocurrency outright, depending on its stances on government oversight. Some governments might be willing to make the use of cryptocurrency illegal, restricting its innocent uses but helping prevent its use for criminal activities, while others might decide that it is not a worthwhile tradeoff.

All other solutions must either raise awareness about cryptocurrency or target the crime itself, as regulating cryptocurrency partially is near-impossible. Raising awareness might help prevent fraud where cryptocurrency is used as payment as well as fraudulent cryptocurrency investment schemes by educating potential victims. Targeting cybercrime itself should be done with international cooperation, in a way that allows countries to share intelligence and allow international forces to conduct operations on their soil - however some countries might raise concerns about how this violates their national sovereignty (addressing those concerns should require more attention than writing “without violating national sovereignty” in the clause).

Additional Resources

https://www.youtube.com/watch?v=bBC-nXj3Ng4 - A detailed explanation of how cryptocurrency and the blockchain works by YouTube channel 3blue1brown.

https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work - A page that outlines the UK National Crime Agency’s approach to dealing with various cybercrimes. Use this to get an idea of realistic solutions to specific crimes.

https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122 - An overview of some countries’ stances on cryptocurrency. Delegates might find this beneficial in getting an idea of which viewpoints their country might support.

Bibliography

Works Cited

CPS. “Money Laundering Offences | the Crown Prosecution Service.” *Www.cps.gov.uk*, 11 June 2021, www.cps.gov.uk/legal-guidance/money-laundering-offences .

EUROPOL. *Cryptocurrencies: Tracing the Evolution of Criminal Finances*. 2021, www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf .

Europol. “One of the Darkweb’s Largest Cryptocurrency Laundromats Washed Out.” *Europol*, www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out .

Office of Public Affairs. “Office of Public Affairs | Samuel Bankman-Fried Sentenced to 25 Years for His Orchestration of Multiple Fraudulent Schemes | United States Department of Justice.” *Www.justice.gov*, 28 Mar. 2024, www.justice.gov/opa/pr/samuel-bankman-fried-sentenced-25-years-his-orchestration-multiple-fraudulent-schemes .

---. “Operators of Cryptocurrency Mixers Charged with Money Laundering.” *US Department of Justice Office of Public Affairs*, US Department of Justice, 10 Jan. 2025, www.justice.gov/opa/pr/operators-cryptocurrency-mixers-charged-money-laundering#:~:text=Both%20Blender.io%20and%20Sinbad,to%20launder%20stolen%20virtual%20currency . Accessed 13 Jan. 2025.

U.S. Department of the Treasury. “U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats.” *U.S. Department of the Treasury*, 6 May 2022, home.treasury.gov/news/press-releases/jy0768 .

United Nations Office on Drugs and Crime. “8th Cryptocurrency Conference Vienna.” *United Nations : Office on Drugs and Crime*, 2024, www.unodc.org/unodc/money-laundering/global-programme-against-money-laundering/8th-cryptocurrency-conference-vienna.html .

---. “Payment through Cryptocurrencies.” *United Nations : UN Toolkit on Synthetic Drugs*, syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/onlinetrafficking/payment/index.html .