

Cryptocurrency Use in the Online Sexual Exploitation of Children



Introduction

One of the most disturbing and heinous criminal acts that is rampant across the internet is the sexual exploitation of children via child sexual abuse material (CSAM) or child pornography, child sexual exploitation material (CSEM), the live streaming of child sexual abuse, and other forms of online child sexual exploitation.

Many of these activities involve a transfer of payment between criminals; new technology, such as cryptocurrency, is providing these individuals with the tools they need to continue

this activity while evading governments and law enforcement agencies and thus facilitating this abuse.

This article presents the intersection between cryptocurrencies and child exploitation and an understanding of the fundamental concepts and mechanisms of cryptocurrencies in order to address the opportunities and challenges they offer in the abuse and sexual exploitation of children across the globe.

The Rise of Cryptocurrency

Since the introduction of Bitcoin in 2009, cryptocurrency has taken the world by storm.

Unlike traditional financial systems and fiat currencies, which rely on intermediaries like banks and payment processors to validate and settle transactions, cryptocurrencies operate without a central authority.

Instead, cryptocurrencies are cleverly designed to function on an underlying technology called blockchain. Blockchain is a network of decentralized, distributed digital ledgers that record and validate transactions through a process called cryptography.

The key benefit of cryptocurrency is that the transactions occur on a transparent ledger and records cannot be changed or altered, making them less vulnerable to cyberattacks. This mechanism allows cryptocurrencies to serve as both a form of payment and a store of value. Today, the entire cryptocurrency ecosystem is valued at upward of \$1 trillion USD worldwide.¹

One main feature of cryptocurrency is its ability to provide pseudonymity. While transactions recorded on most blockchains are public and can be traced, the identities of the individuals involved are often obscured. Instead of being identified with physical information (social security numbers, government IDs, etc.) similar to traditional bank accounts or other payment methods, cryptocurrencies use cryptographic addresses providing autonomy and privacy to the user.

The pseudonymous nature of cryptocurrencies has had both positive and negative implications. On one hand, it offers individuals greater financial sovereignty and privacy, allowing them to transact globally without the need for traditional banking systems. This is especially helpful for people who live in regions where banking services are limited. On the other hand, the anonymity associated with cryptocurrencies has attracted illicit

activities, including money laundering, tax evasion, and the illicit trade of goods and services.

Criminal elements have taken advantage of the pseudonymity provided by cryptocurrencies to facilitate illegal transactions while attempting to evade law enforcement scrutiny.

To make matters worse, new cryptocurrencies have emerged over the years that further obscure the information that is visible to the public. Alternate cryptocurrencies, often referred to as altcoins (e.g., Anoncoin, Monero, and Darkcoin), boast complete anonymity, making it impossible to identify the user.

Replacing Traditional Payment Methods

To combat this problem, much of the global community has come together to prevent the purchase of CSAM through traditional payment methods (like credit cards and bank transfers).

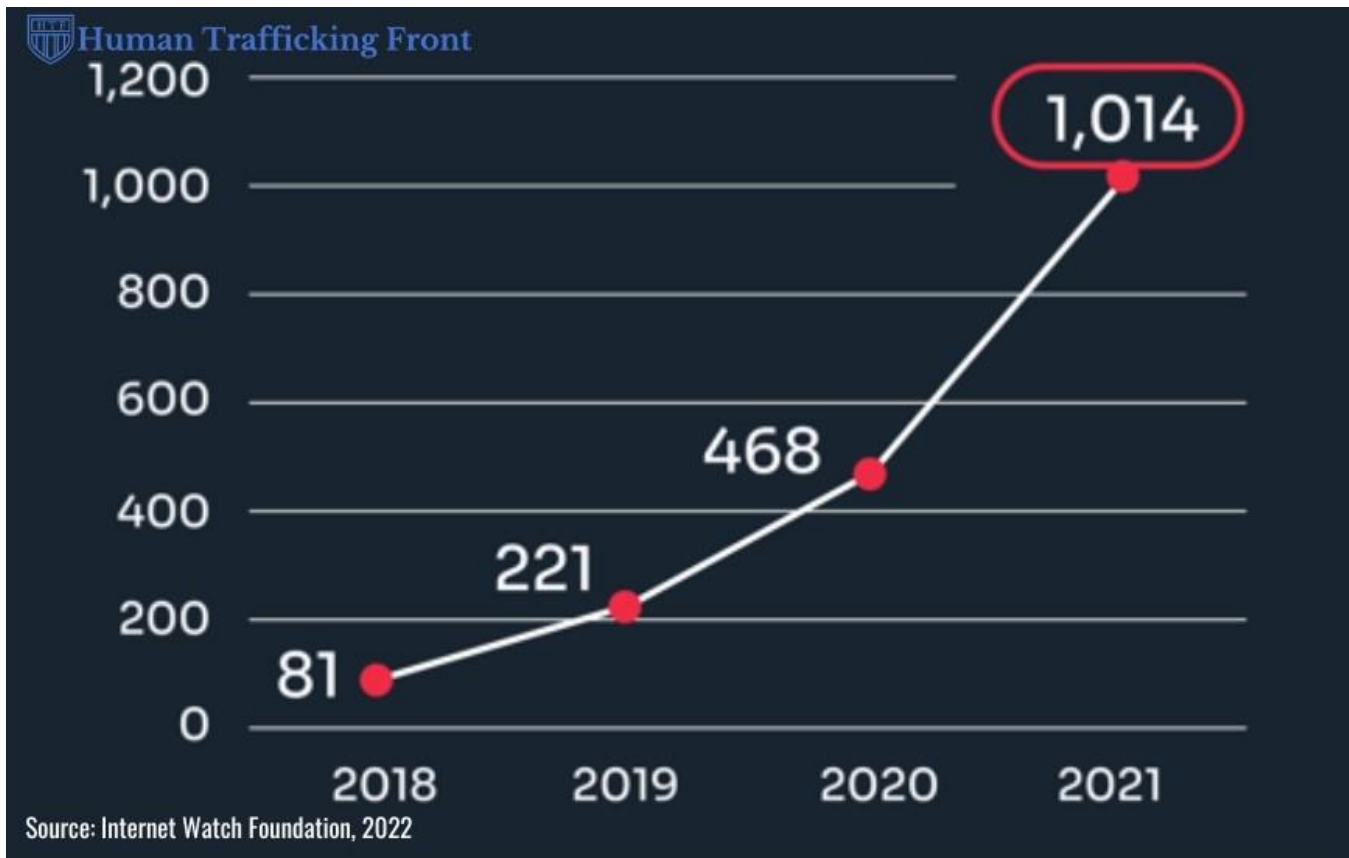
Most banks, credit card companies, electronic payment networks, and internet providers have aligned with the recommended guidelines of the US Financial Coalition Against Child Sexual Exploitation (US FCACSE) to help prevent payments being used for these purposes. The program, which began in the United States, is highly effective and has been expanded to Europe and the Asia Pacific region.

Due to these restrictions, sexual predators have been forced to adopt other methods of sending and receiving payments for trafficked children, encounters, and multimedia related to child sexual exploitation.

Today, these criminals find ways around the system by leveraging clever tactics such as prepaid credit cards, cryptocurrencies, and even new CSAM itself as payment.

Consequently, cryptocurrency has become one of the most popular and fastest-growing payment methods for accessing CSAM.

According to the Internet Watch Foundation, the number of dark websites that allow users to buy images and videos of sexually exploited or raped children with cryptocurrency has doubled every year since 2018.²

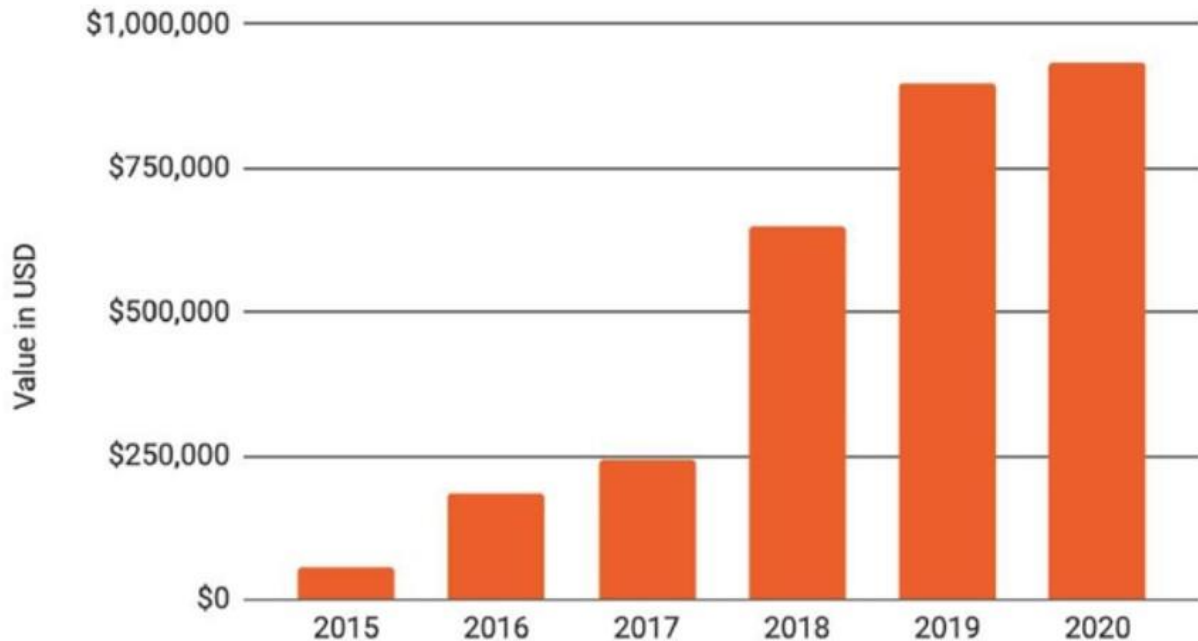


Cryptocurrency and Other Financial Transactions in Child Sexual Exploitation

Unfortunately, the global sexual exploitation of children is big business. The Federal Bureau of Investigation (FBI) estimates that the CSAM or child pornography trade alone is likely valued at over \$3 billion to \$20 billion annually.³

Offenders are selling and distributing CSAM involving the cruelest abuse against infants in exchange for cryptocurrency payments in the Dark Web.

It is estimated that the annual revenue of CSAM Dark Web sites has tripled in the last few years (between 2017 and 2020).⁴



Source: Chainalysis, The 2021 Crypto Crime Report

How Cryptocurrencies Enable Online Predators to Evade Law Enforcement

With cryptocurrency, it is extremely easy to process transactions but difficult to identify who the individual is and where the money went, thereby creating challenges for law enforcement.

The anonymous (pseudo) nature of cryptocurrency hides the identity of the predator making it practically impossible to figure out who these offenders are.

In the few cases where law enforcement is successful, it is usually through pure luck because the offenders made a simple mistake (such as accidentally sharing their location or other identifying information), rather than being tracked through the cryptocurrency transaction itself.

Other obstacles that cryptocurrency creates is that there is no centralized authority (such as a bank or government) that monitors the use and activity of its currency. Without this resource, it is nearly impossible to impose financial sanctions or seize assets of an

individual for the commission of the crime. This often leaves law enforcements' hands tied with fewer formal tactics to go after criminals.

Dark Web's markets allow CSAM to be hidden behind paywalls or cyberlockers, which require payment (often in cryptocurrency) to access, view, and download illicit content. These dark corners of the internet, while visited by many people, are less likely to be reported since criminals hide their illegal activities and identities well.

Finally, cryptocurrencies create obstacles for law enforcement in relation to money laundering services by helping criminals move illicit funds from illegal activities within and across borders and eventually withdraw them.

How Can This Problem Be Solved?

The biggest problem is that child sexual exploitation is not easily solved, especially when it comes to controlling decentralized payment methods like cryptocurrency.

Eliminating this form of crime and abuse will require a wide range of support from individuals to corporations to governments.

Individuals can support the efforts by using the tools available to report any potential or suspected online sexual exploitation. Without these reports, law enforcement and government agencies have little visibility.

Companies in the financial and technology sectors can expand cooperation with government agencies and the developers of cryptocurrencies to build safeguards to hinder sexual predators.

Governments across the globe can collaborate to create a unified effort against online child trafficking and exploitation to address legal fragmentation and enhance international coordination.

Recommended Measures that Governments Need to Implement

Governments can take specific and practical measures to deter, without stifling, the innovative nature of cryptocurrency itself. Some actions that governments can consider to combat the use of cryptocurrencies for online child sexual exploitation include:

- 1. Strengthening Legislation:** Governments can review and update existing laws to explicitly address the use of cryptocurrencies in online child exploitation. This may involve criminalizing the use of cryptocurrencies for such purposes, imposing strict penalties, and providing clear legal frameworks for investigations and prosecutions. The adaptation and implementation of regulations may include those intended to prevent money laundering in relation to these illegal activities. This may involve implementing stricter regulations for cryptocurrency exchanges and requiring transparent reporting of cryptocurrency transactions.
- 2. Improving International Cooperation and Alignment:** Online child exploitation is a global issue, and international cooperation and alignment is crucial to avoid the emergence of different standards across countries. Governments should strengthen collaboration with other countries to share information, intelligence, and best practices to combat the use of cryptocurrencies for child exploitation. International collaboration across government bodies, especially law enforcement, may involve establishing international task forces, participating in joint investigations, and sharing resources and expertise.
- 3. Collaboration with Cryptocurrency Exchanges:** Governments can work closely with cryptocurrency exchanges and financial institutions to enhance their understanding of the risks associated with cryptocurrencies and develop mechanisms to identify suspicious transactions related to child exploitation. Establishing reporting mechanisms and encouraging exchanges to implement robust Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures can help identify and report illicit activities.
- 4. Technology and Innovation:** Governments can invest in research and development of advanced technologies to combat the use of cryptocurrencies for child exploitation. This may involve developing blockchain analysis tools, artificial intelligence algorithms for content detection, and data analytics capabilities to identify patterns and trends in online child exploitation.
- 5. Coordination with Online Platforms:** Governments can collaborate with social media platforms, messaging services, and other online platforms to detect and report instances of child exploitation. Encouraging platforms to implement stricter policies, content moderation tools, and reporting mechanisms can help in the early identification and removal of illicit content.

It is important to note that combating online child exploitation involving cryptocurrencies is a complex and evolving challenge. Consequently, governments need to adapt and update their approaches regularly to keep pace with technological advancements and the changing tactics of criminals.

What is Human Trafficking Front Doing?

Human Trafficking Front provides a pathway to end the online commercial sexual exploitation of children. Our advocacy actions to prevent the use of cryptocurrencies for online child sexual exploitation, rescue children, and arrest offenders, include:

- 1. Training law enforcement agencies, the bank industry, and prosecutors** to understand the technical aspects of cryptocurrencies in connection with online child sexual exploitation. Our efforts enable them to effectively investigate cases involving cryptocurrencies and gather evidence for prosecutions.
- 2. Promoting responsible use of cryptocurrencies.** We encourage responsible use of cryptocurrencies by educating users and disseminating resources about potential risks associated with child exploitation.
- 3. Designing and implementing public awareness campaigns and education.** Our public awareness campaigns educate the general public about the risks associated with cryptocurrencies and online child exploitation. These campaigns aim at raising awareness about the signs of child exploitation, providing information on reporting mechanisms, and promoting responsible online behaviors.

Additional Details

This best-practices prevention guide and publication is part of the Human Trafficking Front's program: *Putting an End to the Online Sexual Exploitation of Children: Preventing Victimization and Strengthening Child Protection Systems*.*

Recommended Citation

Human Trafficking Front. (2023, June 25). *Cryptocurrency use in the online sexual exploitation of children*. <https://humantraffickingfront.org/cryptocurrency-use-in-the-online-sexual-exploitation-of-children/>

References

- ¹ CoinMarketCap. (2023, June 25). *Global cryptocurrency charts*. <https://coinmarketcap.com/charts/>.
- ² Internet Watch Foundation. (2022, November 1). *Websites offering cryptocurrency payment for child sexual abuse images 'doubling every year'*. <https://www.iwf.org.uk/news-media/news/websites-offering-cryptocurrency-payment-for-child-sexual-abuse-images-doubling-every-year/>.
- ³ Bialik, C, (2006, April 18). Measuring the child-porn trade. *The Wall Street Journal*. <https://www.wsj.com/articles/SB114485422875624000>.
- ⁴ Graver, K., & Updegrave, H. (2021). *The 2021 crypto crime report*. Chainalysis, p. 63. <https://safewayconsultoria.com/wp-content/uploads/2021/09/Chainalysis-Crypto-Crime-2021.pdf>.

Human Trafficking Front is a non-profit organization with 501(c)(3) status with the IRS, committed to eliminating all forms of slavery and human trafficking, especially of women and children. Human Trafficking Front works to end these forms of exploitation by equipping professionals with best practices, empowering communities to be less vulnerable to exploitation, and promoting more effective implementation of legal and policy frameworks that address prevention and protection. Human Trafficking Front is under the leadership of Dr. Beatriz Susana Uitts, who is the author of the book, [*Sex Trafficking of Children Online: Modern Slavery in Cyberspace*](#). For further information see: www.humantraffickingfront.org.

* The Human Trafficking Front's Program, *Putting an End to the Online Sexual Exploitation of Children: Preventing Victimization and Strengthening Child Protection Systems*, is funded in part by the generous support of The Children's Trust. The Children's Trust is a dedicated source of revenue established by voter referendum to improve the lives of children and families in Miami-Dade County. The views expressed in this best-practices prevention guide are those of the author and do not necessarily reflect the opinions of funders, NGOs, or countries. Human Trafficking Front is responsible for this specialized guide and its contents. For more tools and information, check out our [Resources](#) page on our website.