Cryptocurrency, Crime, And Children: Unveiling The Dark Side of Financial Technology in Child Sexual Exploitation

Fatria Harwanto[1], Artha Febriansyah[2], Nanda Irwantika[3]
[1,2,3] Faculty of Law, Sriwijaya University, Palembang, Indonesia

fatriaharwanto@fkm.unsri.ac.id

Abstract. *The paper delves into the pivotal role of financial technology, particularly cryptocurrencies, in perpetuating child sexual exploitation. It examines methods such as converting cryptocurrency to fiat, using mixers, and exploiting decentralized finance for money laundering, all of which facilitate anonymity and fund child exploitation networks. Additionally, it assesses regulatory effectiveness, considering instruments such as the UN Convention on the Rights of the Child and Indonesia's Law No. 35/2014, an amendment to Law No. 23/2002 on Child Protection, and proposes reforms to bolster child protection measures. Through stakeholder interviews, it uncovers challenges faced by law enforcement, regulators, and child protection agencies, guiding collaborative recommendations to disrupt exploitation networks and safeguard children from harm. Addressing ethical dilemmas, the paper advocates for a holistic approach that prioritizes child welfare and human rights. Moreover, it highlights concerning data from 2019, where the IWF identified 288 new dark web sites selling Child Sexual Exploitation Material (CSEM), reflecting a 238% increase from 2018. Notably, 197 of these sites exclusively accepted payment in virtual currencies, exacerbating the challenge. Emphasizing the need for action, the paper underscores the Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN (RPA), stressing the urgency to address anonymous users and transactions. In conclusion, the paper underscores the necessity for collective action to combat the misuse of financial technology in child exploitation. It advocates for regulatory reforms, increased collaboration, and ethical considerations to ensure a safer future for vulnerable children worldwide.*

Keywords: *Cryptocurrency, Crime, Child Sexual Exploitation.*

1. Introduction

Financial technology, particularly cryptocurrencies, has evolved into a double-edged sword in modern times. While these technologies provide unprecedented prospects for innovation and financial inclusion, they have also been misused for malicious reasons, especially for supporting child sexual abuse. There has been an obvious and disconcerting increase in the application of digital currencies for child pornographic transactions. The annual study from Internet Watch Foundation states that the number of new dark web sites providing child sexual exploitation material (CSEM) increased by 238% in 2019 and that a significant proportion of these sites used virtual currencies [1]. Furthermore, the global child pornography market has been estimated to be worth billions of dollars by the International Centre for Missing Child, with a significant portion of these transactions made possible by cryptocurrencies [2].

A study by the International Monetary Fund (IMF) highlighted that the rise in child trafficking in Southeast Asia is closely linked to the increase in online child pornography, including the live streaming of sexual abuse of children. This illegal industry is estimated to generate between $3 billion and $20 billion annually. Countries like Cambodia and Thailand have been identified as major sources of child pornographic material [3]. Human trafficking is a significant issue in ASEAN, with two-thirds of the estimated 40 million global victims

A. Sofian et al. (eds.), *Proceedings of the ASEAN Conference on Sexual Exploitation of Children (ACOSEC 2024)*, Advances in Social Science, Education and Humanities Research 876,
https://doi.org/10.2991/978-2-38476-325-2_4

of modern slavery located in East Asia and the Pacific. This crime, generating over $150 billion annually, disproportionately affects children, who are often trafficked for sexual exploitation and forced labor, as highlighted by the ASEAN–Australia Counter Trafficking Baseline Report.

To establish a theoretical foundation and context for this study, a comprehensive review of existing literature on cryptocurrencies, child sexual exploitation, and relevant legal frameworks will be conducted. This review will encompass academic papers, reports from organizations and studies on regulatory effectiveness. Sources will include peer-reviewed journals, books, conference proceedings, and reports from international and national agencies, as well as credible online databases. To provide detailed examples of how cryptocurrencies are used in child sexual exploitation and to illustrate the effectiveness of different regulatory approaches, the paper will include an in-depth analysis of specific cases involving cryptocurrency transactions related to child exploitation. This will involve examining court cases, law enforcement reports, and media coverage, focusing on high-profile instances where cryptocurrencies were used to fund child exploitation networks and subsequent legal proceedings.

Assessing the effectiveness of current regulatory frameworks and identifying gaps will be a key objective. This involves analyzing international and national laws, such as the UN Convention on the Rights of the Child and Indonesia's Law No. 35/2014, an amendment to Law No. 23/2002 on Child Protection, and evaluating how these laws are implemented and enforced in practice. Sources for this analysis will include legal texts, government reports, and policy papers.

2. Literature Review

Cryptocurrencies provide a high level of anonymity and decentralization, which enables the facilitation of numerous illegal operations [4]. Cryptocurrency transactions take place on decentralized networks, which makes them difficult to monitor and regulate, unlike traditional financial systems that are regulated by central authorities. Transactions are logged on a blockchain, although identities are concealed by cryptographic addresses, making them challenging to track. The ability to remain anonymous enables the occurrence of illegal actions such as money laundering, drug trafficking, and child exploitation, all while keeping the names of the users concealed [5]. Mixers, or tumblers, augment the level of anonymity in Cryptocurrency transactions.

These services combine the cash from various users, rendering it exceedingly difficult to track the source and destination of individual transactions. Mixers, by severing the connection between the sender and receiver, offer an extra level of secrecy that is frequently utilized by criminals to conceal the movement of illegal funds [6].

Studies suggest that child exploitation victims commonly suffer from severe psychological trauma, which manifests as various mental health disorders including post-traumatic stress disorder (PTSD), anxiety, and depression [7]. The use of cryptocurrency transactions, which offer anonymity, makes it difficult to identify and capture perpetrators, thus prolonging the abuse and intensifying the psychological damage caused. Moreover, the awareness that their perpetrators can act without being discovered intensifies feelings of helplessness and isolation among survivors, thereby deepening their psychological distress [8]. Anonymous cryptocurrency transactions may trap children in cycles of exploitation, especially those driven by poverty or coercion, due to the financial incentives involved [9].

The UN Convention on the Rights of the Child (CRC) is a global agreement aimed at protecting the rights and well-being of children worldwide. Established in 1989, the CRC outlines various rights for children, including protection from sexual exploitation. Article 34 requires signatory states to prevent the forced involvement of children in illegal sexual activities, prostitution, and exploitation in pornographic materials. The CRC encourages countries to create legislation and policies to safeguard children from exploitation, including addressing the misuse of financial technology in such crimes.

In Indonesia, Law No. 35/2014, an amendment of Law No. 23/2002 on Child Protection, strengthens the legal framework for protecting children from various forms of abuse and exploitation, including sexual exploitation. The law imposes strict penalties on perpetrators and obliges the state to prevent, protect, and rehabilitate victims. Indonesia has also regulated the use of cryptocurrency through the Financial Services Authority Regulation No. 13/POJK.02/2018, which aims to oversee digital financial innovations and prevent their misuse for money laundering or other illegal activities.

In 2023, CyrberTipLine received over 36.2 million reports, mostly related to suspected child sexual abuse material (CSAM) [10]. Over 35.9 million of these reports were from ESPs, who reported instances of child sexual abuse material found on their platforms. Additionally, NCMEC identified a new and alarming trend with 4,700 reports involving generative AI (GAI), which refers to a significant number of incidents where advanced AI technologies were used to create child sexual abuse material (CSAM) [11]. Specifically, this includes cases where AI generated images of fictional children in sexually explicit scenarios and deepfakes that manipulated real children's images or videos to appear sexually explicit. This trend highlights the growing misuse of AI for creating harmful and illegal content, encompassing 49,528,198 videos, 54,842,374 images, and 1,282,590 other [12].

The rapid growth of cryptocurrency technology has outpaced regulatory frameworks, leading to a fragmented global system that criminals exploit. While countries like the U.S. and Japan have strict Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, others, such as Nigeria and Russia, have weaker enforcement. Research emphasizes the need for global harmonization of regulations to reduce regulatory gaps and limit the anonymity that enables illegal activities. Law enforcement requires significant resources and advanced tools to trace transactions, and cross-border cooperation is crucial for addressing cryptocurrency-related crimes. Education and awareness are also key to preventing online exploitation and reducing risks.

3. Methodology

This study utilizes a mixed-methodologies approach, combining qualitative and quantitative research methods, to investigate the role of financial technology, specifically cryptocurrency, in enabling child sexual exploitation. Quantitative data collected through law enforcement reports, financial transactions, and research on blockchain technology is utilized to identify patterns and measure the extent of cryptocurrency misuse in child exploitation networks [13]. This method allows for

identify patterns and measure the extent of cryptocurrency misuse in child exploitation networks [14]. This method allows for obtaining in-depth information about the difficulties faced in addressing these crimes [15]. Moreover, detailed analysis of particular cases in which bitcoins were employed for child exploitation provides a comprehensive contextual understanding [16]. The study acknowledges potential limitations, including the difficulty in obtaining comprehensive data due to the anonymity of cryptocurrency transactions and the potential biases in law enforcement reports dan and research on blockchain technology. To mitigate these limitations, the research triangulates data from multiple sources and employs rigorous data validation techniques.

4. Discussion And Findings

a. Role of Financial Technology in Child Sexual Exploitation

The anonymity and decentralization of cryptocurrencies significantly improve the perpetration of child sexual exploitation. These digital currencies enable anonymous transactions, posing a challenge for law enforcement in tracking illicit activity. Bitcoin transactions are documented on a publicly accessible ledger, but the identities of the participants remain anonymous, making it difficult to trace real-world individuals involved[17]. Mixing services, also known as tumblers, and decentralized finance (DeFi)

platforms enhance the opacity of transaction trails by combining several transactions, rendering the tracing of funds exceedingly difficult [18]. DeFi systems facilitate financial operations such as lending and trading without complying to conventional Know Your Customer (KYC) and Anti-Money Laundery procedure consequently adding a further layer of complexity [19].

Comprehensive blockchain forensics and data analytics technologies such as Chainalysis, Elliptic, CipherTrace, TRM Labs, BlockSeer, BitcoinWhosWho, and Crystal Blockchain are used to improve the monitoring and tracing of cryptocurrency transactions. These tools utilize advanced algorithms to identify and analyze relationships and patterns in order to address the issues of anonymity and decentralization related to cryptocurrencies. Their purpose is to assist in the fight against criminal activity, particularly focusing on child sexual exploitation. Chainalysis offers significant transaction monitoring and investigation software that is vital for law enforcement purposes. Elliptic is a company that focuses on ensuring compliance and detecting fraud, offering help for regulatory initiatives. CipherTrace provides anti-money laundering (AML) technologies and blockchain analytics to reduce financial risks. TRM Labs offers advanced fraud detection solutions for monitoring and identifying illegal actions. BlockSeer facilitates the visualization of financial transactions within cryptocurrency networks. BitcoinWhosWho is a platform that aims to identify the owners of Bitcoin addresses in order to prevent scams. Crystal Blockchain provides real-time analytics for monitoring and examining transactions. These tools enable researchers and law enforcement to properly identify and track illegal bitcoin operations, overcoming the difficulties posed by anonymity and decentralization.

b. Child Protection Agencies

Child protection authorities emphasise the immediate necessity of addressing the misuse of financial technologies by child exploitation networks. These agencies prioritise a comprehensive strategy that integrates technical solutions and strong legislative frameworks. Organisations such as ECPAT (End Child Prostitution, Child Pornography, and Trafficking of Children for Sexual Purposes) play a vital role, particularly in the ASEAN region. ECPAT Indonesia combats child exploitation through activities such as advocating for legal reforms, providing training to law enforcement personnel, and conducting awareness campaigns. The ASEAN Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse also advocates for international collaboration and standardised rules to combat online child sexual exploitation. The Ministry of Women's Empowerment and Child Protection in Indonesia collaborates with stakeholders to strengthen child protection measures. Their attempts involve legislative improvements, public awareness, and the integration of modern technologies in order to monitor and anticipate exploitation

c. Case Studies

Case Study 1: Welcome to Video

In 2019, one of the largest child pornography websites, "Welcome to Video," was taken down by international law enforcement agencies . The site operated on the dark web and accepted Bitcoin for payments. Over a period of three years, users made over a million downloads of child exploitation material, generating significant revenue through cryptocurrency transactions. The site was able to mask the identities of its users, making it difficult for authorities to trace the transactions until sophisticated blockchain analysis tools were employed [20].

Case Study 2: Dark Scandals

The Dark Scandals case involved a website that hosted videos and images of rape and child abuse. The site operated using Bitcoin to facilitate transactions, allowing users to purchase content anonymously. The site's operator was eventually arrested, and blockchain

analysis was instrumental in tracking down the financial transactions linked to the exploitation network [21].

Case Study 3: Online Sexual Exploitation of Children (OSEC) in Philippines

The Philippines is a prominent hub for cases of online child sexual exploitation, with numerous instances including the use of cryptocurrency. Frequently, individuals involved in human trafficking are close relatives who utilise digital currencies to obtain money for the purpose of broadcasting instances of abuse in real-time. For example, children are forced to engage in sexual acts on video, and transactions are conducted using bitcoins to preserve anonymity and avoid detection. This exploitation is driven by economic deprivation and assisted by the extensive utilisation of the internet and digital platforms [22].

5. Conclusion

This study addresses the issue of child sexual exploitation facilitated by cryptocurrencies, focusing on the challenges posed by their anonymity and decentralization. While blockchain forensics can help detect transaction patterns, the complexity of the problem demands international collaboration and innovative technological solutions. Case studies from the ASEAN region, particularly in the Philippines and Thailand, highlight the use of cryptocurrencies for exploitation, emphasizing the need for cooperation between global organizations and local law enforcement. Regulatory frameworks like Indonesia's Law No. 35/2014 and the ASEAN Regional Plan of Action are vital but require ongoing improvements to keep pace with evolving digital currencies. Child protection agencies must advocate for increased funding, technological innovation, and stronger legal frameworks. A unified global approach is essential, combining advanced technology, strict regulations, and international partnerships to protect children from exploitation.

6. Acknowledgement

We would like to express our sincere appreciation to all those who have contributed to the successful completion of this research on the impact of financial technology, specifically cryptocurrencies, in facilitating the current problem of child sexual exploitation. We deeply grateful to our advisor for their consistent support, guidance, and insightful input during this endeavor. Their specialized knowledge and skills. We wish to express my gratitude for the assistance provided by family and friends, whose tolerance, comprehension, and motivation have played a crucial role in maintaining concentration. Lastly, we would like to express my gratitude to the diverse organizations and agencies whose reports and publications have supplied crucial data and context for this study. We truly appreciate and praise their dedication to combatting child sexual exploitation.

References

[1]. Internet Watch Foundation, “2019 Annual Report,” Cambridge, 2019
[2]. International Centre for Missing & Exploited Children (ICMEC), “Studies in Child Protection: Technology-Facilitated Child Sex Trafficking,” Australia, 2018.
[3]. M. Anthony, “A HIDDEN SCOURGE,” Finance Dev, vol. 55, no. 3, pp. 18–21, Nov. 2018.
[4]. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2009. Accessed: Jun. 22, 2024. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[5]. EUROPOL, “Internet Organised Crime Threat Assessment 2019,” Den Haag, 2019. Accessed: Jun. 22, 2024. [Online]. Available: https://www.europol.europa.eu/iocta/2019

[6]. S. Meiklejohn et al., “A fistful of bitcoins,” in Proceedings of the 2013 conference on Internet measurement conference, New York, NY, USA: ACM, Oct. 2013, pp. 127–140. doi: 10.1145/2504730.2504747.
[7]. D. Finkelhor, A. Shattuck, H. A. Turner, and S. L. Hamby, “The Lifetime Prevalence of Child Sexual Abuse and Sexual Assault Assessed in Late Adolescence,” Journal of Adolescent Health, vol. 55, no. 3, pp. 329–333, Sep. 2014, doi: 10.1016/j.jadohealth.2013.12.026
[8]. EUROPOL, “Internet Organised Crime Threat Assessment 2019,” Den Haag, 2019. Accessed: Jun. 22, 2024. [Online]. Available: https://www.europol.europa.eu/iocta/2019
[9]. UNICEF, “CHILD PROTECTION FROM VIOLENCE, EXPLOITATION AND ABUSE ,” Mar. 2013.
[10]. CyberTipline, “2023 CyberTipline Reports by Electronic Service Providers (ESP),” New York, 2023. Accessed: Jun. 21, 2024. [Online]. Available: https://www.missingkids.org/content/dam/missingkids/pdfs/2023-reports-by-esp.pdf
[11]. NCMEC, “2023 Our Impact,” New York, 2023. Accessed: Jun. 21, 2024. [Online]. Available: https://www.missingkids.org/content/dam/missingkids/pdfs/2023-ncmec-our-impact.pdf
[12]. CyberTipline. (2023). CyberTipline 2023 Report. New York. Retrieved from https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata
[13]. S. Foley, J. R. Karlsen, and T. J. Putniņš, “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?,” Rev Financ Stud, vol. 32, no. 5, pp. 1798–1853, May 2019, doi: 10.1093/rfs/hhz015
[14]. S. Foley, J. R. Karlsen, and T. J. Putniņš, “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?,” Rev Financ Stud, vol. 32, no. 5, pp. 1798–1853, May 2019, doi: 10.1093/rfs/hhz015
[15]. J. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches, 3rd ed. California: Sage publications, 2009.
[16]. R. K. Yin, Case study research and applications: Design and methods, 6th ed. Thousand Oaks: Sage Publications, 2018.
[17]. S. Foley, J. R. Karlsen, and T. J. Putniņš, “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?,” Rev Financ Stud, vol. 32, no. 5, pp. 1798–1853, May 2019, doi: 10.1093/rfs/hhz015.
[18]. M. Moser, R. Bohme, and D. Breuker, “An inquiry into money laundering tools in the Bitcoin ecosystem,” in 2013 APWG eCrime Researchers Summit, IEEE, Sep. 2013, pp. 1–14. doi: 10.1109/eCRS.2013.6805780.
[19]. F. Schär, “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,” Review, vol. 103, no. 2, 2021, doi: 10.20955/r.103.153-74.
[20]. US Department of Justice, “South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin,” May 2018. Accessed: Jul. 03, 2024. [Online]. Available: https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child
[21]. E. Celiksoy and K. Schwarz, “Investigation into financial transactions used in the online sexual exploitation of children,” Nottingham, Nov. 2023.
[22]. Malindog-Uy, “Philippines: Online Child Sexploitation Hotspot,” The ASEAN Post, Manila, Oct. 18, 2020.