IOCRF 2025 Conference
The 1st International Online Conference on Risk and Financial Management
17–18 June 2025 | Online
MDPI

Cryptocurrencies and AI-Enabled Organised Fraud: Emerging Risks and Countermeasures

Leo S.F. Lin, PhD
Charles Sturt University, Australia

INTRODUCTION & AIM

The convergence of cryptocurrencies and artificial intelligence (AI) has revolutionised financial systems while amplifying the sophistication of global financial crime (Ajayi et al., 2025; Johnson, 2025; Oluwaferanmi, 2025). Organised crime syndicates exploit AI tools, such as deepfakes and large language models (LLMs), alongside cryptocurrencies to execute complex fraud schemes, including romance baiting (also known as romance scams and pig-butchering), phishing-as-a-service (PhaaS), and ransomware-as-a-service (RaaS) (Bociga & Lord, 2025; Lin, 2025; Samuel, 2025). The above-mentioned schemes often target vulnerable populations, sometimes involving other different types of crimes, including human trafficking, drug trafficking, and money laundering using cryptocurrencies. This preliminary study examines the risks of AI-enabled fraud, including Generative AI (GenAI), deepfakes, and voice cloning (Lin, Aslett, Mekonnen, & Zecevic, 2024), assesses their impact, and proposes countermeasures through enhanced regulatory frameworks, data sharing, and international cooperation.

Aim: To assess the emerging risks of AI-enabled fraud activities and recommend mitigation strategies, emphasising data sharing, capacity building, international cooperation, and public-private partnerships.

METHOD

This preliminary study employs a qualitative analysis based on secondary data (Szabo & Strang, 1997) from recent reports, including the INTERPOL Global Financial Fraud Assessment (2024) and a SAS global survey (2025). Due to resource and time constraints, this study does not involve primary data collection; the analysis was limited to existing literature. The data sources, primarily self-reported surveys, may be subject to response bias or limited sample sizes, which could affect generalizability; therefore, this is an experimental project.

The methodology includes an analysis of current academic and industry-reported studies on AI-enabled fraud, cryptocurrency scams, and human trafficking, as well as other fraudulent activities. This study also proposes a probabilistic risk model to estimate the likelihood and impact of AI-enabled fraud crimes, with a focus on network analysis and the adoption of generative AI for improved fraud detection outcomes.

A proposed risk model was developed to quantify the probability of fraud detection failure (P_{fail}) based on technological sophistication and regulatory gaps:

$$P_{\text{fail}} = \frac{w_1 \cdot S_{\text{AI}} + w_2 \cdot S_{\text{crypto}} + w_3 \cdot G_{\text{reg}}}{R_{\text{det}} + R_{\text{coop}}}$$

where:

- S_{AI}: Sophistication of AI tools (e.g., deepfakes, LLMs) [0-1 scale]
- S_{crypto}: Anonymity level of cryptocurrency transactions [0-1 scale]
- G_{reg}: Regulatory gaps [0-1 scale]
- R_{det}: Detection capability of agencies [0-1 scale]
- R_{coop}: Level of international cooperation [0-1 scale]
- w_1, w_2, w_3: Weights reflecting relative impact (e.g., 0.4, 0.4, 0.2)

Disclaimer: This model is hypothetical, and its parameters are derived from self-reported secondary data, which may introduce biases. Empirical validation with real-world data is essential to ensure accuracy and reliability.

RESULTS & DISCUSSION

The SAS global survey (2025) reports that 98% of government agencies experienced AI-enabled fraud, based on self-reported survey data, which may not fully represent all agencies (SAS, 2025). Additionally, 70% of respondents reported an increase in AI-enabled fraud over the past five years, with financial losses averaging 16% of agency budgets, both figures derived from self-reported data (SAS, 2025).

RESULTS & DISCUSSION (cont.)

Deepfake-related fraud in the fintech sector increased by approximately 700% from 2023 to 2024; however, this figure may be specific to certain fintech segments or regions (SAS, 2025). Sumsub (2023) reports a 245% increase in global deepfake fraud, indicating significant but variable growth across various contexts. TRM Labs (2025) reported a 456% increase in generative AI-enabled scams from May 2024 to April 2025, accompanied by a fourfold rise in deepfake cases (TRM Labs, 2025). Deepfakes account for 7% of total fraud attempts in the crypto sector (Sumsub, 2023).

Romance baiting (romance scams and pig-butchering), often linked to human trafficking, has expanded in Southeast Asia, Africa, and Latin America, facilitated by anonymous cryptocurrency transactions (TRM Labs, 2025).

Table 1: Fraud Statistics (2025)

Metric	Value	Source
Agencies affected by AI fraud	98%	SAS, 2025
Increase in AI fraud (last 5 years)	70%	SAS, 2025
Budget loss due to fraud	16%	SAS, 2025
Deepfake fraud increase (2023-2024)	700%	SAS, 2025
Global deepfake fraud increase	245%	Sumsub, 2023
Deepfake fraud in crypto sector	7%	Sumsub, 2023
GenAI-enabled scam increase (May 2024-April 2025)	456%	TRM Labs, 2025
Deepfake case increase	4x	TRM Labs, 2025

Using the proposed risk model for illustrative purposes, with values $S_{\text{AI}} = 0.8$, $S_{\text{crypto}} = 0.9$, $G_{\text{reg}} = 0.7$, $R_{\text{det}} = 0.5$, $R_{\text{coop}} = 0.4$, $w_1 = 0.4$, $w_2 = 0.4$, $w_3 = 0.2$, the probability of detection failure is:

$$P_{\text{fail}} = \frac{0.4 \cdot 0.8 + 0.4 \cdot 0.9 + 0.2 \cdot 0.7}{0.5 + 0.4} = \frac{0.32 + 0.36 + 0.14}{0.9} = 0.911$$

This 91.1% probability of detection failure, calculated using parameters informed by self-reported secondary data and author-estimated weights, illustrates the formidable challenges in detecting sophisticated AI-driven and cryptocurrency-based fraud, pending empirical validation with real-world data.

Discussion: The high underscores the impact of regulatory gaps and constraints on international cooperation. AI-enabled fraud exploits emotional manipulation, posing detection challenges that require advanced AI countermeasures. The reliance on self-reported, secondary data introduces potential biases, such as over- or under-reporting, which limits generalizability. Since this is a preliminary study, the purpose is to develop an initial research agenda.

CONCLUSION

AI-enabled cryptocurrency fraud, including romance baiting and deepfake scams, poses a significant global threat exacerbated by human trafficking and anonymous transactions. Current detection capabilities are inadequate, with a high hypothetical probability of failure due to technological sophistication and regulatory gaps. Governments and financial institutions must adopt advanced AI-driven defences and enhance consumer education to mitigate these risks effectively.

FUTURE WORK / REFERENCES

In the future, this research should empirically validate the risk model, develop AI-based detection tools, and collaborate with law enforcement and industry for real-world testing. Additionally, it should conduct primary data collection to strengthen future analyses and facilitate international cooperation through public-private partnerships.

References:

Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. SSRN.
Bociga, D., & Lord, N. (2025). Artificial intelligence and the organisation and control of fraud. CrimRxiv.
INTERPOL. (2024). Global financial fraud assessment. https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technol
Johnson, B. (2025). AI and blockchain for AML: A policy and technology convergence to combat crypto-enabled financial crimes. [No URL provided]
Lin, L. S. (2025). Examining the role of deepfake technology in organised fraud: Legal, security, and governance challenges. Frontiers in Law, 4, 6–17.
Oluwaferanmi, A. (2025). Financial crime in the digital age: Comparative analysis of AML strategies using blockchain and AI in emerging and advanced markets.
Samuel, B. M. (2025). Exposing the impact of GenAI for cybercrime: An investigation into the dark side.
SAS. (2025). Trust and transparency: Combating fraud to maximise public program efficiency. https://www.bigdatawire.com/this-just-in/sass-new-study-highlights-consumer-concerns-over-generative-ai-in-fraud/
Sumsub. (2023). Deepfake phishing statistics. https://fintechnews.sg/110619/regtech/identity-fraud-surges-in-scale-and-sophistication-with-apacs-financial-services-becoming-a-prime
Sumsub. (2024). Global deepfake incidents surge tenfold from 2022 to 2023. https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/
Sumsub. (2024). Deepfake cases surge in countries holding 2024 elections. https://sumsub.com/newsroom/deepfake-cases-surge-in-countries-holding-2024-elections-sumsub-research-shows/
TRM Labs. (2025). AI-enabled fraud: How scammers are exploiting generative AI. https://www.trmlabs.com/resources/blog/ai-enabled-fraud-how-scammers-are-exploiting-generative-ai
TRM Labs. (2025). Mission: Impossible and the growing threat of AI-enabled crime. https://www.trmlabs.com/resources/blog/mission-impossible-and-the-growing-threat-of-ai-enabled-crime