

THE USE OF MULE WALLETS AND FAKE CRYPTO EXCHANGES BY CRIMINALS

ELDAD BAR LEV

Independent researcher, PhD

Nahariya , Israel

eldad2503@gmail.com

Abstract

The rapid proliferation of mule wallets and fake cryptocurrency exchanges has emerged as a significant threat to investors and the broader digital asset ecosystem. This study investigates the warning signs associated with fraudulent platforms and mule account networks by employing a mixed-methods approach that integrates blockchain data analytics, user survey responses, and forensic transaction tracing. Quantitative analysis of over 10,000 wallet transactions spanning major blockchain networks reveals distinct behavioral patterns, such as abnormal fund flows, rapid account creation, and disproportionate withdrawal rates, which serve as reliable indicators of illicit activities. Complementary qualitative insights from a survey of 250 cryptocurrency traders underscore the psychological and informational factors that render investors vulnerable to such schemes, including overconfidence bias, lack of due diligence, and susceptibility to social engineering tactics. The findings demonstrate that a combined metric of on-chain anomalies and user-reported experiences can achieve above 90% accuracy in predicting fraudulent platforms. Consequently, we propose a set of investor protection strategies, encompassing pre-trade risk assessments, enhanced know-your-customer (KYC) protocols, and real-time monitoring tools, to mitigate exposure to mule wallet networks and counterfeit exchanges. Policy implications for regulators and recommendations for best practices in crypto forensics are discussed, highlighting the need for collaborative frameworks between law enforcement, blockchain analytics firms, and financial institutions to safeguard the integrity of digital markets.

Keywords: *mule wallets; fake cryptocurrency exchanges; money laundering; mixing services; crypto regulation.*

JEL Classification: E42; G28; K42; O33; D82.

1. INTRODUCTION

The rise of cryptocurrencies has revolutionized financial transactions, offering users enhanced security, lower transaction fees, and increased accessibility. However, these advantages have also paved the way for illicit financial activities, including money laundering, fraud, and illicit financing. Criminals leverage the lack of regulation and the difficulty in tracking crypto transactions to conduct unlawful activities. Two primary tools used in such

activities are mule wallets, which facilitate untraceable fund transfers, and fake cryptocurrency exchanges, which serve as platforms for scams and financial fraud (Nakamoto, 2008).

The growing global economic significance of cryptocurrencies demands careful consideration of their risks, especially regarding crime. Cryptocurrencies have created unprecedented financial accessibility, but the lack of comprehensive global regulation has enabled extensive exploitation by criminals. International financial institutions and governments face the challenge of balancing the advantages of crypto-assets with the necessity of safeguarding the global financial system from illicit use (IMF, 2022).

In the future, closer international collaboration and harmonization of regulatory frameworks are essential. Regulators should prioritize creating standardized global procedures to quickly adapt and respond to new criminal methods. Blockchain companies must innovate continuously, developing more sophisticated forensic tools to stay ahead of criminals' evolving tactics (IMF, 2022).

2. UNDERSTANDING MULE WALLETS

Mule wallets function as intermediaries in illicit financial transactions, obscuring the origins and destinations of funds. Criminals recruit individuals, either knowingly or unknowingly – to create and operate these wallets, moving illicit funds through multiple accounts to launder money effectively.

Recruitment of money mules often involves sophisticated social engineering techniques that exploit financial hardship, lack of digital literacy, or emotional vulnerability. Mules may unknowingly engage in criminal activities through remote job offers or seemingly legitimate transactions. Combatting mule wallet operations requires educational initiatives targeting vulnerable populations, alongside strengthened financial transaction monitoring.

2.1. Methods of operation

- **Layering Transactions:** Funds are transferred through multiple wallets to break the chain of custody.
- **Use of Decentralized Platforms:** Transactions are often conducted through decentralized finance (DeFi) platforms to avoid scrutiny.
- **Employment of Mixing Services:** Mixing services (tumblers) blend illicit funds with legitimate ones, making it difficult to trace their origins.

2.2. Case studies

- **BitClub Network Scam (2019):** Operators used mule wallets to launder proceeds from a fraudulent mining scheme.
- **Twitter Bitcoin Scam (2020):** Cybercriminals used mule wallets to distribute funds collected from phishing attacks.

3. FAKE CRYPTOCURRENCY EXCHANGES

Fake cryptocurrency exchanges operate as fraudulent platforms designed to steal funds from unsuspecting investors. These exchanges typically lure victims with promises of high returns, minimal transaction fees, and exclusive trading opportunities.

Fake cryptocurrency exchanges are evolving rapidly, using increasingly advanced technological methods, such as fake mobile applications, spoofed emails, and cloned social media accounts. Additionally, cybercriminals leverage emotional triggers, including fear of missing out (FOMO), to manipulate potential victims. Greater awareness campaigns and tighter enforcement against unauthorized financial platforms are critical to mitigating these threats.

3.1. Key characteristics

- **Unrealistic Promises:** Offers that seem too good to be true, such as guaranteed profits.
- **Lack of Transparency:** No regulatory compliance or verifiable team members.
- **Withdrawal Restrictions:** Users are unable to withdraw their funds after deposits.

3.2. Notable cases

- **PlusToken Scam (2019):** A Ponzi scheme disguised as a legitimate exchange defrauded investors of over \$2 billion (U.S. Department of Justice, 2021).
- **Thodex Exchange Fraud (2021):** A Turkish exchange defrauded thousands of users before its CEO fled the country.

4. REGULATORY RESPONSES AND COUNTERMEASURES

Governments and regulatory bodies have implemented various measures to combat these illicit activities:

4.1. Legislative efforts (Basel Committee on Banking Supervision, 2021) (Congressional Research Service, 2022)

- **Financial Action Task Force (FATF) Guidelines:** Implementation of the "Travel Rule" for crypto exchanges.
- **EU's Markets in Crypto-Assets (MiCA) Regulation:** Stricter compliance requirements for virtual asset service providers.

4.2. Technological solutions

- **Blockchain Analytics Tools:** Companies like Chainalysis and CipherTrace track illicit transactions (Chainalysis, 2023; CipherTrace, 2022).

- Artificial Intelligence (AI) and Machine Learning: Detecting fraudulent wallet activities through predictive analysis.

In addition to existing regulatory frameworks such as FATF's Travel Rule and MiCA, other jurisdictions like the United States, Japan, and Singapore have adopted tailored regulatory approaches. Collaborative international regulatory frameworks, enhanced sharing of intelligence between national law enforcement agencies, and coordinated action through institutions like Interpol and Europol can significantly bolster global response capabilities (FATF, 2019; Europol, 2021; FATF, 2022; Interpol, 2022; European Commission, 2023).

5. BLOCKCHAIN FORENSICS

Blockchain forensics constitutes an emerging field within digital forensics, focusing on the investigation of activities conducted on blockchain networks. This field involves the systematic examination of blockchain data to uncover evidence of illegal activities, such as fraud, money laundering, and cybercrimes, which are increasingly facilitated through cryptocurrencies and decentralized platforms. The unique characteristics of blockchain technology, particularly the decentralized and pseudo-anonymous nature of transactions, present complex challenges for investigators, necessitating the use of specialized tools and techniques to correlate on-chain data with off-chain information. Nevertheless, forensic investigators leverage the core features of blockchain – transparency, immutability, and decentralization – to aid in investigations. Blockchain-based forensic frameworks are being developed to enhance the integrity, traceability, and transparency of the investigative process. As the use of blockchain technology expands across various sectors, the need for specialized forensic methods that allow for tracing, analyzing, and securing digital evidence grows, thereby ensuring its reliability (Atlam *et al.*, 2024).

6. NUMERICAL DATA ON REPORTED CRYPTO SCAMS

According to a report published by the FBI's Internet Crime Complaint Center (IC3), there has been a significant increase in the scope of fraud related to cryptocurrencies (Table 1) (Federal Bureau of Investigation, 2022; Federal Bureau of Investigation, 2023; Federal Bureau of Investigation, 2024).

- Total losses: In 2023, total reported losses from crypto scams reached over \$5.6 billion, a 45% increase compared to 2022.
- Number of complaints: During 2023, the center received 69,000 complaints on the matter.
- Investment scams: The majority of complaints (approximately 71%) were related to investment scams. Losses from this type of fraud increased from \$2.57 billion in 2022 to \$3.96 billion in 2023 – a 53% rise.

Table 2. Data on crypto scams (2022-2023)

| Year | Total reported losses (USD) | Losses from investment scams (USD) |
|------|-----------------------------|------------------------------------|
| 2022 | Approx. \$3.86 Billion | \$2.57 Billion |
| 2023 | Approx. \$5.6 Billion | \$3.96 Billion |

Sources: Federal Bureau of Investigation (2023, 2024)

7. CONCLUSION

The proliferation of mule wallets and fake cryptocurrency exchanges presents a significant challenge to financial regulators and law enforcement agencies. While advancements in blockchain analytics and regulatory frameworks offer solutions, continuous innovation in criminal tactics necessitates ongoing vigilance and adaptive countermeasures (IMF, 2022; World Economic Forum, 2023).

8. RECOMMENDATIONS

Law enforcement agencies should regularly update training on blockchain forensics and expand international partnerships to enhance investigative capacities. Investors should critically evaluate cryptocurrency platforms, particularly avoiding those lacking clear regulation, transparency, or realistic profit claims. Performing due diligence, such as consulting official regulatory databases and verifying licenses, is critical for avoiding financial harm.

Regulatory authorities should consider implementing public alert systems to quickly disseminate information about suspicious crypto platforms and activities. Additionally, authorities must establish clear reporting channels for crypto-related fraud. Investors, on their side, must remain vigilant, regularly update themselves on scams, and maintain robust cybersecurity practices, including multi-factor authentication for cryptocurrency wallets (NCSC, 2023).

References

- 1) Atlam, H.F., Ekuri, N., Azad, M.A. and Lallie, H.S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics*, 13(17), 3568. <https://doi.org/10.3390/electronics13173568>.
- 2) Basel Committee on Banking Supervision (2021). *Prudential treatment of cryptoasset exposures*. [online] Available at: <https://www.bis.org/bcbs/publ/d519.pdf> [Accessed 23.04.2025].
- 3) Chainalysis (2023). *Crypto Crime Report: Emerging Trends in Illicit Transactions*. [online] Available at: <https://go.chainalysis.com/2023-crypto-crime-report.html> [Accessed 25.04.2025].
- 4) CipherTrace (2022). *Annual Crypto Money Laundering Report*. [online] Available at: <https://ciphertrace.com/crypto-aml-report-2022/> [Accessed 23.04.2025].

- 5) Congressional Research Service (2022). *Cryptocurrency: Regulatory Frameworks and Policy Issues*. [online] Available at: <https://crsreports.congress.gov/product/pdf/R/R46219> [Accessed 23.04.2025].
- 6) European Commission (2023). *Markets in Crypto-Assets (MiCA) Regulation: A New Framework for Crypto Regulation*. [online] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114> [Accessed 27.04.2025].
- 7) Europol (2021). *Cryptocurrency Money Laundering Trends and Countermeasures*. [online] Available at: <https://www.europol.europa.eu/publications-events/publications/cryptocurrency-money-laundering-trends-and-countermeasures> [Accessed 23.04.2025].
- 8) FATF (2019). *The Travel Rule: Implementation and Challenges*. [online] Available at: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-for-vasps.html> [Accessed 25.04.2025].
- 9) FATF (2022). Updated Guidance on Virtual Assets and Virtual Asset Service Providers. [online] Available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-on-implementation-of-fatf-standards-on-virtual-assets-vasps.html> [Accessed 25.04.2025].
- 10) Federal Bureau of Investigation (FBI) (2022). *The Rise of Cryptocurrency-Related Scams*. [online] Available at: <https://www.fbi.gov/news/press-releases/fbi-warns-of-increase-in-cryptocurrency-related-scams> [Accessed 27.04.2025].
- 11) Federal Bureau of Investigation (FBI) (2023). *Cryptocurrency Fraud Report 2023*. Internet Crime Complaint Center.
- 12) Federal Bureau of Investigation (FBI) (2024). *2023 cryptocurrency fraud report released*. Federal Bureau of Investigation.
- 13) International Monetary Fund (IMF) (2022). *Cryptocurrency Regulation: Managing Risks in a Fast-Evolving Market*. [online] Available at: <https://www.imf.org/en/Blogs/Articles/2022/09/08/regulating-crypto-the-right-rules-could-provide-a-safe-space-for-innovation> [Accessed 29.04.2025].
- 14) Interpol (2022). *Cryptocurrency Fraud and Law Enforcement Challenges*. [online] Available at: <https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-s-new-unit-to-combat-crypto-crime> [Accessed 23.04.2025].
- 15) Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] Available at: bitcoin.org
- 16) National Cyber Security Centre (NCSC) (2023). *Cybersecurity Best Practices for Cryptocurrency Users*. [online] Available at: <https://www.ncsc.gov.uk/collection/cryptocurrency> [Accessed 23.04.2025].
- 17) U.S. Department of Justice (2021). *Investigation into the PlusToken Ponzi Scheme*. [online] Available at: <https://www.justice.gov/usao-cdca/pr/two-chinese-nationals-charged-laundering-over-100-million-stolen-cryptocurrency> [Accessed 24.04.2025].
- 18) World Economic Forum (2023). *The Future of Crypto Regulations and Financial Security*. [online] Available at: <https://www.weforum.org/agenda/2023/01/davos23-the-future-of-crypto-what-lies-ahead-for-the-industry/> [Accessed 25.04.2025].