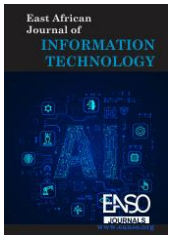

East African Journal of Information Technology
eajit.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Online Fraud and Cryptocurrency in Tanzania: Legal Issues Surrounding Cyber Scams

Herbert Ndimbo[1*] *& Dr. Advocate Anne Malipula, PhD*[1]

[1] Ruaha Catholic University, P. O. Box 774, Iringa, Tanzania.
[*] Author for Correspondence Email: hndimbo2015@gmail.com

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

Date Published:

18 August 2025

Keywords:

Anti-Money Laundering Act 2006, Electronic Transactions Act 2015, Cybercrimes Act 2015, cryptocurrency-related fraud, phishing scams, Ponzi schemes, Cyber Scams, Online Fraud.

ABSTRACT

Over the past decade, Tanzania has experienced significant digital transformation driven by increased internet access, mobile technology, and digital financial services. This growth has created fertile ground for innovations like blockchain and cryptocurrencies. Popular digital currencies such as Bitcoin and Ethereum are now used locally for investment, remittances, and transactions, promoting financial inclusion and modernisation. However, these benefits are accompanied by rising risks, particularly online fraud. Criminal activities such as Ponzi schemes, phishing scams, fraudulent Initial Coin Offerings (ICOs), and ransomware attacks have increased, exploiting limited public awareness and weak institutional oversight. Tanzanian law enforcement and regulatory bodies often lack the technical expertise and jurisdictional reach to respond effectively, leaving victims vulnerable and eroding trust in digital finance. This paper examines the legal and regulatory challenges posed by cryptocurrency-related fraud in Tanzania. It analyses key domestic laws, including the Cybercrimes Act 2015, Electronic Transactions Act 2015, and Anti-Money Laundering Act 2006. While these laws address cybercrime broadly, they lack specific provisions related to cryptocurrencies, such as clear definitions, asset tracing mechanisms, and cross-border cooperation tools. Drawing on Tanzanian case studies, legal literature, and international examples from countries like the UK and Japan, the study identifies legal gaps and highlights successful regulatory strategies abroad, including crypto exchange licensing, Know Your Customer (KYC) rules, and public education campaigns. The paper concludes by recommending comprehensive reforms to strengthen Tanzania's legal framework, enhance regulatory oversight, promote public awareness, and develop cross-border enforcement strategies to protect the integrity of the country's digital financial ecosystem.

APA CITATION

Ndimbo, H. & Malipula, A. A. (2025). Online Fraud and Cryptocurrency in Tanzania: Legal Issues Surrounding Cyber Scams. *East African Journal of Information Technology*, *8*(1), 411-418. https://doi.org/10.37284/eajit.8.1.3504.

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

CHICAGO CITATION

Ndimbo, Herbert and Advocate Anne Malipula. "Online Fraud and Cryptocurrency in Tanzania: Legal Issues Surrounding Cyber Scams". *East African Journal of Information Technology* 8 (1), 411-418. https://doi.org/10.37284/eajit.8.1.3504.

HARVARD CITATION

Ndimbo, H. & Malipula, A. A. (2025) "Online Fraud and Cryptocurrency in Tanzania: Legal Issues Surrounding Cyber Scams", *East African Journal of Information Technology*, 8(1), pp. 411-418. doi: 10.37284/eajit.8.1.3504.

IEEE CITATION

H. Ndimbo & A. A. Malipula "Online Fraud and Cryptocurrency in Tanzania: Legal Issues Surrounding Cyber Scams", *EAJIT*, vol. 8, no. 1, pp. 411-418, Aug. 2025.

MLA CITATION

Ndimbo, Herbert & Advocate Anne Malipula. "Online Fraud and Cryptocurrency in Tanzania: Legal Issues Surrounding Cyber Scams". *East African Journal of Information Technology*, Vol. 8, no. 1, Aug. 2025, pp. 411-418, doi:10.37284/eajit.8.1.3504.

INTRODUCTION

Online fraud, particularly in the realm of cryptocurrency, has become an increasingly significant concern in the global digital landscape. In Tanzania, the rise of cryptocurrency-related scams has mirrored global trends, with individuals and organisations becoming victims of cyber fraud. These scams often exploit the anonymity and global reach of digital currencies, leaving the legal system struggling to keep pace with new and evolving criminal activities.

Cryptocurrency, initially celebrated for its decentralised nature and potential for financial empowerment, has also become a vehicle for malicious actors to perpetuate fraudulent activities. In Tanzania, where the regulatory framework for cryptocurrencies is still developing, the rise of cyber scams presents an urgent need for comprehensive legal solutions and awareness[1].

This colloquium will explore the legal issues surrounding online fraud and cryptocurrency scams in Tanzania, examining current laws, gaps in enforcement, and the challenges faced by victims, law enforcement, and regulatory authorities. By examining the context of cyber scams and their impact on Tanzania's digital economy, we will seek to understand how the country's legal system can be better equipped to address this growing issue.

Definition and Terms

Definition and Types of Online Fraud (e.g., Ponzi schemes, phishing, fake ICOs)

The range of online fraud in Tanzania includes:

Ponzi schemes: These scams involve fraudulent investment schemes that promise high returns with little to no risk. Early investors are paid with the funds of new investors, but the scheme eventually collapses when it can no longer attract new investors. Cryptocurrency investments are a common vehicle for Ponzi schemes because of the anonymity and ease of transferring funds[2].

Phishing: Fraudsters attempt to steal users' private keys or login credentials through deceptive emails, fake websites, or social engineering tactics. These phishing attacks often target cryptocurrency holders or exchanges to gain unauthorised access to wallets or funds.

Fake Initial Coin Offerings (ICOs): ICOs are fundraising mechanisms for new cryptocurrency projects, where investors exchange fiat currency or other cryptocurrencies for new tokens. However, many fraudsters run fake ICOs, promising

[1]Chale, E. (2021). Cyber fraud and cryptocurrency scams: Legal challenges in Tanzania's digital economy. Dar es Salaam University Press.

[2]Boehme, K., & Jackson, R. (2020). Ponzi schemes and cryptocurrency: A study of fraud in the digital age. Oxford University Press.

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

significant returns but disappearing with the funds once the offering is complete[3].

Ransomware and hacking: Cybercriminals may use ransomware to lock a victim's system or steal sensitive data, demanding cryptocurrency payments as ransom. In addition, hackers target cryptocurrency exchanges or individual wallets to steal assets[4].

Growth of Cryptocurrency Usage in Tanzania and Its Implications

Cryptocurrency use in Tanzania has grown through platforms like peer-to-peer trading and remittance services, with a growing interest in decentralized finance (DeFi). The expansion of cryptocurrency use presents significant opportunities for financial inclusion, especially among people without access to traditional banking systems. However, it also poses risks, particularly in an environment where users may not fully understand the technology or its risks. Additionally, the lack of clear regulation has made it easy for malicious actors to exploit the system, leaving users vulnerable to scams.

Specific Examples of High-profile Scams or Frauds in Tanzania

Providing a few real-life examples of cryptocurrency scams in Tanzania will help underscore the urgency of addressing the issue. These could include:

The rise of unlicensed cryptocurrency trading platforms: These platforms promise high returns but are eventually revealed to be fraudulent operations.

Scams involving fake investment opportunities: For example, fraudulent companies may claim to offer cryptocurrency mining services or promise high-yield investment opportunities that ultimately turn out to be Ponzi schemes.

Fake ICOs and Initial Exchange Offerings (IEOs): Mention how certain projects have come under scrutiny after being exposed as fraudulent, resulting in significant financial losses for Tanzanians[5].

Audience

This colloquium is relevant to a wide range of audiences, including but not limited to:

Legal Professionals: Lawyers, judges, and legal scholars interested in the intersection of technology and law, particularly in the area of cybercrime, cryptocurrency, and online fraud.

Government Regulators and Policymakers: Tanzanian officials involved in the development of digital policy, financial regulations, and cybersecurity.

Financial Institutions and Digital Payment Service Providers: Banks, payment systems, and fintech companies that deal with cryptocurrencies and are affected by online fraud.

Academics and Researchers: Scholars researching cybercrime, digital currency regulation, and Tanzanian legal frameworks for emerging technologies.

Public and Private Sector Stakeholders: Entrepreneurs, businesses, and individuals who are either victims or potential targets of cryptocurrency fraud.

Law Enforcement: Police and other investigative bodies tasked with tackling cybercrime and digital fraud in Tanzania.

[3]Smith, J. T., & Patel, A. R. (2019). Fraudulent fundraising: The rise of fake initial coin offerings (ICOs) and their impact on investors. Cambridge University Press

[4]https://www.blockchainintelligence.com/prevent-crypto-fraud accessed 15 February 2025.

[5]Mwita, J. A., & Sanya, P. M. (2022). Cryptocurrency scams in Tanzania: A critical analysis of fake ICOs and IEOs. Journal of Digital Economy and Cybersecurity, 14(3), 45–67.

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

Relevance of the Topic

The topic of online fraud and cryptocurrency is highly relevant in the context of Tanzania's growing digital economy and the increasing usage of cryptocurrencies like Bitcoin, Ethereum, and others. As more Tanzanians engage in online transactions and cryptocurrency investments, they become more susceptible to scams such as Ponzi schemes, fake initial coin offerings (ICOs), and phishing attacks.

Tanzania, like many African nations, faces unique challenges related to cybersecurity and digital finance. While the country has made significant strides in mobile banking and digital payments, it remains vulnerable to the risks posed by the unregulated cryptocurrency market. Furthermore, the legal framework for addressing online fraud related to digital currencies is still in its infancy, and there is a pressing need for legislative action to protect citizens, businesses, and financial institutions from these fraudulent activities[6].

The colloquium will highlight the need for clearer regulatory measures and legal frameworks, with a focus on establishing consumer protections, increasing awareness, and fostering collaboration among stakeholders to combat cyber fraud. The topic also underscores the importance of developing specialised law enforcement capabilities to handle cybercrime and digital **fraud cases in Tanzania.**

Overview of the Rise of Cryptocurrency in Tanzania

Cryptocurrency has gained global attention for its decentralised nature, providing a digital alternative to traditional banking systems. In Tanzania, the adoption of cryptocurrencies such as Bitcoin, Ethereum, and various altcoins has grown steadily in recent years. This trend is largely driven by their potential to enable faster and cheaper cross-border transactions, reduce reliance on traditional financial intermediaries, and offer access to financial services for the underbanked and unbanked populations. With many Tanzanians lacking access to conventional banking infrastructure, digital currencies present a promising solution for financial inclusion.

The Tanzanian government and citizens alike have shown growing interest in leveraging these technologies for investment, remittances, and everyday transactions. Startups, tech-savvy youth, and informal traders are increasingly engaging with cryptocurrency markets. However, alongside these opportunities lie significant challenges. The absence of a comprehensive regulatory framework has created an environment where fraudulent schemes such as Ponzi operations, phishing scams, and fake Initial Coin Offerings (ICOs) can flourish.

Online fraud targeting unsuspecting investors has increased, exploiting limited public awareness and the lack of institutional oversight. Many victims have no legal recourse due to gaps in the law and the technical limitations of enforcement agencies. This undermines trust in digital financial systems and poses risks to economic stability.

As cryptocurrency continues to evolve in Tanzania, there is a growing need for clear legal definitions, regulatory guidance, and public education. Strengthening institutional capacity and enacting targeted policies will be critical to ensuring that the benefits of digital currencies can be realised without exposing the population to undue harm[7].

BRIEF DISCUSSION ON THE RELATIONSHIP BETWEEN ONLINE FRAUD AND CRYPTOCURRENCY

The rise of cryptocurrency has brought with it not only financial innovation but also a troubling increase in online fraud. In Tanzania and other emerging markets, the rapid adoption of digital

[6]Mwanza, M. F., & Kinyanjui, L. W. (2023). Regulating cryptocurrency: The legal and economic challenges of online fraud in emerging markets. African Journal of Cybersecurity and Law, 8(2), 89–112

[7]idem

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

currencies like Bitcoin and Ethereum has been accompanied by a surge in scams exploiting both technological complexity and public unfamiliarity. Common forms of crypto-related fraud include Ponzi schemes, phishing attacks, fake Initial Coin Offerings (ICOs), and misleading investment opportunities. These schemes often promise high returns with minimal risk, preying on individuals who may lack digital literacy or awareness of financial fraud tactics.

Fraudsters benefit from the perceived anonymity and decentralised nature of cryptocurrencies, making it difficult for victims and authorities to trace transactions or identify perpetrators. In Tanzania, where regulatory oversight is still evolving, there are limited legal tools to protect victims or pursue justice. Existing laws often do not explicitly address digital assets, and law enforcement agencies may lack the technical expertise needed to investigate crypto-related crimes effectively.

This lack of regulation and enforcement capacity creates a fertile ground for abuse, weakening public trust in the broader digital financial ecosystem. As more Tanzanians engage with cryptocurrency for investment or remittance purposes, the need to understand and address crypto-enabled fraud becomes increasingly urgent.

The relationship between online fraud and cryptocurrency in Tanzania underscores the importance of proactive legal reform, capacity building, and public education. Developing a clear regulatory framework that defines digital currencies and establishes mechanisms for asset recovery and international cooperation is essential to safeguard users and promote safe digital innovation.

THE IMPORTANCE OF ADDRESSING LEGAL ISSUES RELATED TO CYBER SCAMS

As cyber scams related to cryptocurrencies increase, Tanzania's legal system faces challenges in developing laws that adequately address these threats. The lack of legal clarity and regulatory frameworks leaves many victims of online fraud without recourse. Therefore, it is essential to discuss the urgent need for legal reforms and to explore how the country's legal system can be improved to combat these issues effectively[8].

Current Legal Framework in Tanzania

Overview of Tanzania's current laws concerning cybercrime and online fraud

Tanzania's legal framework regarding online fraud is generally underdeveloped in terms of cryptocurrency-specific regulation. However, several existing laws address broader issues of cybercrime and fraud:

The Cybercrimes Act, 2015[9]: This act addresses cybercrimes such as hacking, identity theft, and online fraud, but it does not specifically target cryptocurrency-related issues. It serves as a foundation for cybercrime legislation but lacks the necessary focus on the unique nature of cryptocurrency fraud.

The Electronic Transactions Act, 2015[10]: This act focuses on electronic contracts, signatures, and transactions, which may touch on cryptocurrency use but does not provide comprehensive guidance for cryptocurrency trading or fraud.

The Anti-Money Laundering Act, 2006[11]: While not specifically targeting cryptocurrency fraud, this act may indirectly apply to cryptocurrency scams, especially when fraudulent activities involve money laundering.

[8]idem
[9]Cybercrimes Act, Cap. 13 (2015). United Republic of Tanzania.
[10]Electronic Transactions Act, 2015
[11]Anti-Money Laundering Act 2006, Cap 25

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

Analysis of Existing Financial and Digital Regulations Related to Cryptocurrency

There is no dedicated regulatory framework for cryptocurrencies in Tanzania, leading to regulatory uncertainty. Cryptocurrencies are not officially recognised as legal tender, and there is limited oversight over digital assets. The lack of clear guidelines means that individuals and institutions engaging in cryptocurrency transactions face significant risks, as the legal protections are insufficient.

Limitations of the Current Legal System in Addressing Online Fraud

The Tanzanian legal system is ill-equipped to handle cryptocurrency scams effectively. Gaps include:

Lack of expertise in cryptocurrency regulations among law enforcement and legal practitioners.

Absence of clear consumer protection laws specific to cryptocurrency users.

Difficulty in enforcing digital asset-related crimes, especially with cross-border transactions and anonymous actors.

Limited collaboration between international authorities to track down crypto criminals, given the decentralised nature of cryptocurrencies.

Challenges in Addressing Online Fraud and Cryptocurrency Scams

Legal Gaps and Challenges in Enforcement

The lack of specialised legal frameworks in Tanzania means that existing laws are often insufficient to comprehensively address the growing threat of cryptocurrency-related fraud. Most current statutes were designed to regulate traditional financial systems and general cybercrime, leaving a significant gap in the regulation of digital assets. The unique features of blockchain technology—such as decentralisation, pseudonymity, and irreversible transactions—create additional challenges for enforcement and legal interpretation. Criminals can easily exploit these features to operate anonymously, making it difficult to trace illicit activities or recover stolen assets. Furthermore, the borderless nature of cryptocurrency transactions means that many fraudulent schemes are executed from outside Tanzania, raising complex issues of international jurisdiction. Without treaties or cooperation agreements with other countries, Tanzanian authorities struggle to investigate, apprehend, or prosecute perpetrators based abroad. This legal and procedural disconnect severely limits the country's ability to protect its citizens from sophisticated and cross-border digital financial crimes[12].

Lack of Consumer Protection Mechanisms

Consumers involved in cryptocurrency transactions are often left vulnerable and unprotected, with little to no clear legal recourse if they become victims of fraud. Unlike traditional financial systems, where regulations and consumer protection mechanisms are well established, the cryptocurrency ecosystem in Tanzania and many other jurisdictions—operates in a largely unregulated space. This lack of oversight means that when scams, thefts, or fraudulent schemes occur, victims may find it difficult to trace perpetrators, recover lost assets, or pursue legal action. The absence of formal safeguards increases the risk of financial loss and undermines public confidence in digital financial innovations[13].

[12]https://www.tcra.go.tz/cryptocurrency accessed 15 February 2025.

[13] Mwanza, M. F., & Kinyanjui, L. W. (2023). *Regulating cryptocurrency: The legal and economic challenges of online fraud in emerging markets*. **African Journal of Cybersecurity and Law**, 8(2), 89–112.

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

Jurisdictional Issues and International Cooperation in Cybercrime Cases

Due to the borderless nature of cryptocurrencies, enforcement becomes more challenging when fraudsters operate from different countries. Without international treaties or agreements on cybercrime, Tanzania's ability to investigate and prosecute fraud is limited.

Proposals for Reform

Recommendations for improving legal and regulatory frameworks

Some key proposals could include:

Establishing clear cryptocurrency regulations: Developing a comprehensive legal framework that explicitly addresses the use, trading, and fraud prevention of cryptocurrencies.

Consumer protection laws: Enforce stronger protections for cryptocurrency users, including mandatory disclosures and transparency for cryptocurrency service providers.

Increased collaboration with international regulatory bodies: Tanzania should work with international bodies like the Financial Action Task Force (FATF) to adopt global best practices for cryptocurrency regulation and fraud prevention.

Regulation of cryptocurrency exchanges: Introducing mandatory licensing, security standards, and periodic audits for cryptocurrency exchanges operating in Tanzania.

Public awareness campaigns: Educating Tanzanians about the risks associated with cryptocurrency investments and scams.

Best Practices from Other Countries

Countries like Japan and the UK have implemented regulatory frameworks that effectively protect consumers while allowing the cryptocurrency market to thrive. Lessons from these countries can be adapted to the Tanzanian context.

Strategies for strengthening collaboration between regulators, law enforcement, and financial institutions

Building partnerships between financial regulators, law enforcement, and the private sector is crucial for developing a multi-faceted approach to combat cryptocurrency fraud. Establishing task forces or working groups focused on cryptocurrency crimes could foster better communication and coordination.

CONCLUSION

In summary, the rise of cryptocurrency has led to a surge in cyber scams in Tanzania. While the country has existing laws that address cybercrime, these are insufficient for dealing with the nuances of cryptocurrency-related fraud. To tackle this issue, Tanzania needs clear regulations, stronger consumer protections, and greater international cooperation.

Emphasis on the need for proactive and responsive legal measures

The legal system must proactively adapt to the changing landscape of digital finance. Reforming laws and improving enforcement are critical to safeguarding the interests of Tanzanians involved in cryptocurrency transactions.

Call to action for stakeholders to collaborate in fighting online fraud and protecting consumers.

The success of any regulatory efforts will depend on the active collaboration between government agencies, financial institutions, and the public. Together, they can create a safer environment for cryptocurrency use, reducing the risk of fraud and fostering trust in digital currencies.

REFERENCES

Blockchain Intelligence. (2025, February 15). How to prevent crypto fraud. https://www.blockchainintelligence.com/prevent-crypto-fraud

Article DOI: https://doi.org/10.37284/eajit.8.1.3504

Boehme, K., & Jackson, R. (2020). Ponzi schemes and cryptocurrency: A study of fraud in the digital age. Oxford University Press.

Chale, E. (2021). Cyber fraud and cryptocurrency scams: Legal challenges in Tanzania's digital economy. Dar es Salaam University Press.

Mwanza, M. F., & Kinyanjui, L. W. (2023). Regulating cryptocurrency: The legal and economic challenges of online fraud in emerging markets. African Journal of Cybersecurity and Law, 8(2), 89–112.

Mwita, J. A., & Sanya, P. M. (2022). Cryptocurrency scams in Tanzania: A critical analysis of fake ICOs and IEOs. Journal of Digital Economy and Cybersecurity, 14(3), 45–67.

Smith, J. T., & Patel, A. R. (2019). Fraudulent fundraising: The rise of fake initial coin offerings (ICOs) and their impact on investors. Cambridge University Press.

United Republic of Tanzania. (2006). Anti-Money Laundering Act, Cap. 25. Government Printer.

United Republic of Tanzania. (2015). Cybercrimes Act, Cap. 13. Government Printer.

United Republic of Tanzania. (2015). Electronic

