March, 2025

The GLOCEPS Policy Brief

Research and Analysis in Transnational Organized Crimes Focus

Implications of the Proliferation of Virtual Currencies on Transnational Organized Crimes (TOCs) in Eastern Africa

Stephen Nduvi

Photo credit: www.fichtelegal.com

Executive Summary

The brief opines that the global proliferation of virtual currencies portends a rise in crypto-driven Transnational Organized Crimes (TOCs) risks to the Eastern Africa region if effective dissuasive measures are not implemented. The usage of cryptocurrencies globally rose by over 880% in 2020 with Kenya and Tanzania ranked 5th and 19th globally. Virtual currencies are digital forms of money that exist solely in electronic form including Cryptocurrencies, Centralized Virtual Currencies, and Central Bank Digital Currencies (CBDCs). They can take various forms depending on their use, nature, and underlying technology and are typically created, owned, and traded on digital platforms. While these innovations promote financial inclusion, they have also become enablers for TOCs. The recent pro-crypto policy directives by the Trump Administration will significantly catalyze the growth of global virtual currencies and Eastern Africa's Crypto-driven TOC activities due to the non-existence of effective dissuasive measures. The crypto-facilitated TOCs will be expedited by borderless nature of virtual currencies; jurisdictional arbitrage on virtual currencies; cybersecurity infrastructure preparedness; and linkages between regional informal and global illicit economies. The brief concludes that strengthening Eastern Africa's digital security requires a multi-pronged approach as the absence of effective measures to disrupt

combat crypto-driven TOC risks the region becoming a perpetual theater for transnational crypto cybercriminals, undermining its digital economic aspirations. Key recommendations include establishing regional cyber-defense hubs including the Nairobi Regional Blockchain Institute to undertake standardized training on crypto-induced TOCs; harmonizing national and regional frameworks to monitor crypto's dual use; strengthening cross-border intelligence sharing to disrupt TOC networks in real-time; enhancing technological capacity and cybersecurity infra-structure investment through public-private partnerships; and strengthening the use of advanced blockchain forensics for crypto-driven TOCs analysis to safeguard financial systems without stifling innovation.

Context

The 2021 Chainalysis report shows usage of cryptocurrencies globally rose by over 880% in 2020, largely driven by transactions on peer-to-peer (P2P) platforms in emerging markets. In Eastern Africa, Kenya and Tanzania are ranked 5th and 19th globally by the 2021 Global Crypto Adoption Index, with Kenyans leading the world in peer-to-peer crypto trade. The P2P platforms allow citizens to circumvent high international transaction costs, particularly in Africa. The increased growth and usage without commensurate compliance initiatives could propel crypto-related TOCs, particularly in Eastern Africa.

Photo Credit: www.nasdaq.com

The rise of virtual currencies, including cryptocurrencies and blockchain-based platforms, has revolutionized global financial systems, offering decentralized, pseudonymous, and borderless transaction capabilities. Virtual currencies are digital forms of money that exist solely in electronic form including Cryptocurrencies, Centralized Virtual Currencies, and Central Bank Digital Currencies (CBDCs). They can take various forms depending on their use, nature, and underlying technology and are typically created, owned, and traded on digital platforms. While these innovations promote financial inclusion, they have also become enablers of TOCs. Cryptocurrencies like Bitcoin and privacy coins (e.g., Monero) are increasingly used for money laundering, ransomware attacks, drug trafficking, and cybercrime due to their perceived anonymity and cross-jurisdictional fluidity. For instance, the 2021 Chainalysis report noted a 79% annual increase in global cryptocurrency-based money laundering, with TOC networks exploiting regulatory asymmetries between nations. The lack of a unified global regulatory framework exacerbates this challenge, as criminals exploit jurisdictions with weak oversight. The Financial Action Task Force (FATF) requires nations to adopt its "Travel Rule" for crypto exchanges, but compliance remains inconsistent, creating loopholes for TOC networks to exploit.

TOCs in the Eastern Africa region could escalate due to the growth of global virtual currencies being catalyzed by the recent pro-crypto policy directives by the Trump administration. In January 2025, his administration's Executive Order overtly rescinded both President Biden's order on ensuring the responsible Development of Virtual currencies and the Treasury's July 2022 Framework for International

Engagement on Virtual currencies, which were the two cornerstones of previous United States (U.S.) crypto policy. In March 2025, Trump named five cryptocurrencies including Bitcoin, Ethereum, XRP, Solana, and Cardano for his proposed Crypto Strategic Reserve, leading to a positive virtual currencies market panic globally. The total cryptocurrency market rose by about 10%, or more than $300 billion, in hours since Trump's announcement. The new order could catalyze activities in Crypto TOC due to the nonexistence of clear policies on how Trump's proposed reserve would work in practice.

Eastern Africa, a region grappling with porous borders, political instability, and underdeveloped financial governance, is uniquely susceptible to crypto-facilitated TOC. The region's rapid adoption of mobile money (e.g., M-Pesa in Kenya) reflects a tech-savvy population but also highlights systemic vulnerabilities. Cryptocurrencies are increasingly used to launder proceeds from illicit activities such as wildlife trafficking, piracy, and terrorism financing. For example, Al-Shabaab, a Somalia-based terrorist group, has reportedly used Bitcoin to bypass traditional banking sanctions and receive funds from diaspora supporters. The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) has flagged weak anti-money laundering (AML) controls in member states, including Kenya and Tanzania, as a critical risk. Furthermore, the absence of harmonized regional regulations allows criminals to exploit jurisdictional arbitrage moving illicit funds through countries with lax crypto laws, such as Uganda, which lacks comprehensive crypto oversight.

Kenya's progressive stance on digital innovation as a regional fintech hub contrasts with its fragmented regulatory environment. While the Central Bank of Kenya (CBK) has warned against cryptocurrencies, its 2022 Financial Stability Report acknowledged their growing use in informal cross-border trade, complicating AML efforts. Crypto scams and Ponzi schemes, such as the 2021 "Dashcoin" fraud, have siphoned millions from unsuspecting citizens, illustrating the dual threat of consumer harm and organized crime. In Tanzania despite the Bank of Tanzania's 2019 ban on cryptocurrencies, peer-to-peer (P2P) trading persists due to high remittance demands. This underground market provides TOC networks with untraceable channels for moving funds. Tanzania's gold smuggling networks, which the UN estimates generate $1.3 billion annually, are increasingly linked to crypto payments, evading traditional banking scrutiny. In Somalia, the collapse of state institutions and reliance on hawala systems have made Somalia a hotspot for crypto-enabled terrorism financing. Al-Shabaab's use of crypto

wallets to solicit donations via social media underscores the intersection of technology and instability. The UN Monitoring Group reports indicate that crypto donations are laundered through Kenyan and Ethiopian exchanges, exploiting weak regional oversight.

Equally, high youth unemployment, poverty, and low digital literacy in Eastern Africa create a fertile ground for recruitment into cybercrime including illicit trade in virtual currencies. Organized groups co-opt tech-savvy individuals through financial incentives, particularly in urban hubs like Nairobi and Kampala. For example, "Yahoo Boys" networks in Uganda and Tanzania engage in romance scams and identity theft, targeting victims in Europe and North America. These socioeconomic dynamics are exacerbated by state priorities focusing on physical security over digital threats, leaving systemic vulnerabilities unaddressed.

Key Issues

The following key issues are bound to influence the growth of virtual currencies and their linkage to TOCs in the Eastern Africa region.

The borderless nature of virtual currencies

Enforcing TOC compliance on virtual currencies will be disrupted by the borderless nature of virtual currencies as this complicates tracking of cross-border flows. The disruption would demand coordinated international cooperation and intelligence sharing to disrupt TOC networks. While international cooperation frameworks like the Financial Action Task Force (FATF) provide guidelines, inconsistent enforcement of the Travel Rule that requires crypto exchanges to share transaction data allows TOCs to exploit jurisdictional loopholes. Similarly, asymmetry in the ability of states to apply advanced technology in intelligence sharing on the trading of cryptocurrency could impede real-time

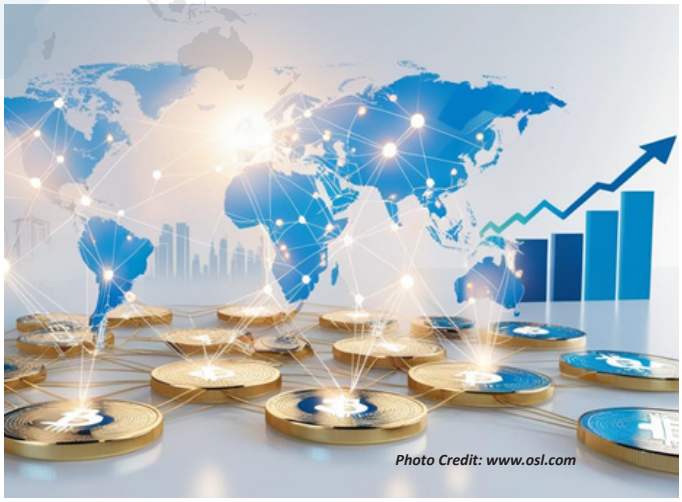


Photo Credit: www.osl.com

cooperation among countries in combatting illicit trade in crypto. The United States-led sanctions under the 2020 Executive Order on Combating Criminal Use of Cryptocurrencies targeted mixers like Tornado Cash, but Eastern African states lacked access to real-time blockchain analytics tools used by Western agencies, creating intelligence disproportionality. TOCs leverage Decentralized Exchanges (DEXs) in inadequately regulated regions to launder proceeds from drug trafficking or wildlife crime, especially where no binding multilateral agreements exist.

Compounding the international cooperation deficits is the lack of mandates by Eastern Africa's regional bodies including the Eastern African Police Chiefs Cooperation Organization (EAPCCO), to harmonize crypto-related crime responses. Nascent crypto regulatory framework at the regional level hinders regional investigations as it excludes some countries including Ethiopia from collaboration with Interpol's Cybercrime Directorate. Similarly, limited cross-border data-sharing protocols impede Kenya's Financial Reporting Centre (FRC) from tracing crypto transactions linked to Al-Shabaab financing.

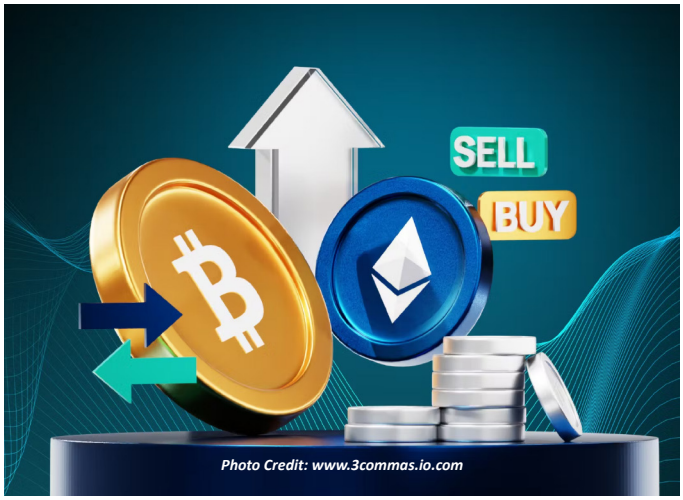
Exacerbating regional efforts in the management of borderless virtual currencies is the fragmentation of capacity-building initiatives such as the U.S.-funded

Africa Cryptocurrency Initiative. This leaves national agencies reliant on outdated anti-money laundering tools ill-suited for blockchain forensics. As such the Eastern African states face acute shortages of specialized cybersecurity personnel and forensic tools. According to a 2023 INTERPOL report, fewer than 20% of regional law enforcement agencies have dedicated cybercrime units and most of them lack advanced data analytics capabilities. This hampers sharing real-time data and threat detection on suspicious transactions on crypto-currency. For instance, delays in sharing real-time data on suspicious transactions allowed a 2022 ransomware attack on Tanzania's national grid to escalate unchecked.

Jurisdictional arbitrage on virtual currencies

There exists global divergence on how different jurisdictions regulate the mobility of virtual currencies. This situation would complicate the management of the mobility of borderless virtual currencies. The European Union (EU) Markets in Crypto-Assets (MiCA) framework versus China's crypto ban create safe havens for TOCs. The region-specific regulation indifference is likely to attract illicit actors in the virtual currencies to use illicit proceeds in investing in the cryptocurrency trade. Eastern African states like Uganda, with no crypto-specific laws, attract illicit actors seeking to convert drug proceeds into stable coins via Peer-to-Peer (P2P) platforms. Without alignment with global standards, TOCs exploit regulatory arbitrage, using the Eastern Africa region as a transit hub for moving illicit funds to offshore exchanges in Dubai or Seychelles. The vacuum in global crypto norms led to Trump's 2020 Executive Order emphasizing U.S. leadership in shaping global crypto norms by pressuring nations to adopt stringent AML laws or face exclusion from dollar-dominated markets.

Regional inconsistencies in legal and regulatory frameworks to regulating virtual currencies offer a key barrier to securing virtual currencies thus presenting safe havens for the currencies' illicit trade. The East African Community (EAC) is yet to adopt a unified approach leading to regional fragmentation in regulating crypto. While Kenya and Rwanda have enacted progressive cybercrime laws (e.g., Kenya's Computer Misuse and Cybercrimes Act, 2018, and Rwanda's 2023 Digital Asset Policy that proposes regional collaboration), harmonization with neighbors remains limited allowing crypto-facilitated smuggling of counter-feit pharmaceuticals and arms to persist. Transnational criminals exploit jurisdictional gaps, such as operating servers in countries with lax regulations (e.g., Somalia's underdeveloped cyber

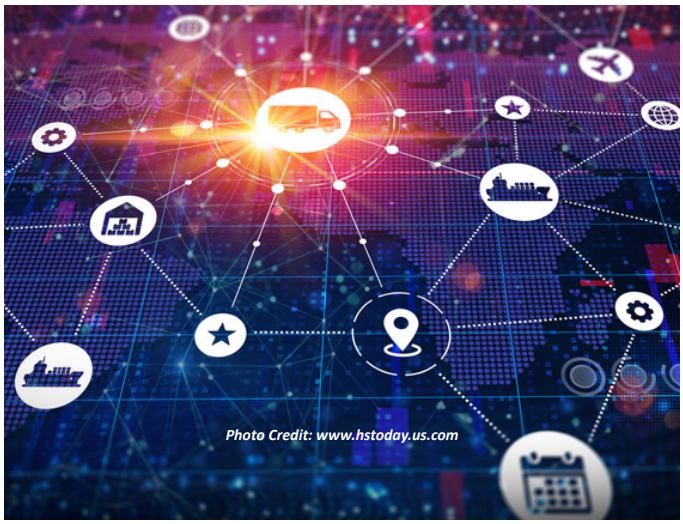


laws) to target victims regionally. Additionally, limited adoption of the African Union's Malabo Convention on Cybersecurity, ratified by only 8 of 14 Eastern African states, undermines collective action. This fragmentation enables crime networks to evade prosecution, relocate operations, and leverage corrupt officials to bypass scrutiny. While Kenya regulates crypto as a digital asset, Tanzania has banned its unlicensed exchanges. This contradiction enables TOCs to route transactions through jurisdictions with slack oversight. For instance, Tanzanian mobile money platforms can be used to cash out Bitcoin linked to ivory trafficking.

Cybersecurity infrastructure preparedness

Global inequalities in technological advancement and the capacity to embrace Artificial Intelligence (AI) tools in combating crypto-facilitated illicit trade would make the Eastern African region vulnerable to crypto-driven TOCs. The regions' disparity in technological capacity and cyber-security preparedness in combatting illicit trade and threats to virtual currencies would make the Eastern Africa region a haven for crypto-TOCs. Advanced blockchain analytics tools including Chainalysis or Elliptic, are highly concentrated in the Global North, leaving Eastern African law enforcement dependent on external support. In 2020 when a U.S. Executive Order prioritized disrupting crypto-enabled ransomware networks, African cybersecurity infrastructure and agencies remained exposed due to a lack of access to threat intelligence on groups like Conti or REvil, which target regional critical infrastructure. For instance, a 2023 ransomware attack on Kenya's eCitizen portal demanded payment in Monero, a privacy coin untraceable by local authorities. The region's cybersecurity preparedness is further impaired by weak global partnerships, like the UN's Countering Cyber-Enabled Organized Crime Initiative, which remains underfunded, perpetuating reliance on reactive rather than proactive measures.

Inadequate technological and cybersecurity infrastructure capacities offer acute shortages of specialized cybersecurity personnel and forensic tools that impede the efficiency of Eastern Africa's cybersecurity agencies in real-time combating of crypto-jacking or phishing schemes used to fund crypto TOCs. A 2023 INTERPOL report noted that less than 20% of regional law enforcement agencies have dedicated cybercrime units and most of them lack advanced data analytics capabilities with limited intra-agency collaboration to facilitate real-time threat detection. For instance, delays in sharing real-time data on suspicious transactions allowed a 2022 ransomware attack on Tanzania's national grid to escalate unchecked. These challenges deepen



the regional vulnerabilities to virtual currencies' illicit trade. For instance, in Somalia, crypto wallets linked to Al-Shabaab are repeatedly hosted on platforms beyond the jurisdiction of the Horn of Africa's Cyber Response Unit. Ethiopia's proposed National Blockchain Institute, faces delays due to budgetary constraints, while cybercrime laws in Djibouti and South Sudan lack provisions for seizing crypto assets. Without intensifying national efforts to combat and disrupt illicit crypto trade, virtual currencies TOCs will continue to exploit weak information technology governance controls.

Photo Credit: www.ifcreview.com

Regional and global informal illicit economies

Virtual currencies progressively intersect with informal economies, complicating efforts to distinguish legitimate remittances from illicit finance. Regional informal and global illicit economies provide a haven for transnational virtual currencies illicit trade. Generally, TOCs adapt by shifting to jurisdictions with lax regulations. Weak traditional financial surveillance of the region's informal economies and the existence of global illicit economies for cryptocurrencies compounded by the borderless nature of virtual currencies would propel and enable criminal networks to bypass traditional financial surveillance systems. Globally, darknet marketplaces and decentralized platforms enable TOCs to trade narcotics, arms, and counterfeit goods using crypto, eluding traditional financial surveillance. Venezuela's gold-smuggling networks and Eastern African TOCs exploit globalization's loopholes including weak regulations, corrupt officials, and high demand for "clean" gold to launder conflict minerals, evade sanctions, and fund instability. While Uganda produces less than 1 tonne of gold annually, reports indicate that it exported a $2.2 billion value of gold in 2022 a discrepancy suggesting massive laundering of foreign gold, including Venezuelan supplies. In 2023, a United Nations report noted that Tanzanian gold exports to the United Arab Emirates (UAE) surged despite limited mining activity, mirroring patterns seen in Uganda. Venezuelan gold may exploit these routes to evade U.S. sanctions.

In Eastern Africa, Kenyan informal traders convert crypto to cash via mobile money platforms, masking proceeds from wildlife trafficking while Tanzania's porous borders and artisanal gold trade facilitate traffickers using crypto to pay Afghan heroin suppliers along the Southern Route, evading export controls and taxation. The complexity of enforcing compliance illustrates how global regulatory gaps enable regional criminal convergence. Somalia's hawala networks which were traditionally cash-based currently integrate crypto to facilitate remittances from the diaspora, creating channels co-opted by militants for moving


Photo Credit: www.businessdailyafrica.com

funds undetected. The Al-Shabaab employs crypto to receive donations and launder ransom payments, exploiting Kenya's under-regulated P2P exchanges like Local Bitcoins to convert virtual currencies into mobile money (e.g., M-Pesa). The dilemma of criminalizing cross-border trade in crypto outright due to its role in financial inclusion is complicated by a lack of harmonized frameworks in the region to monitor crypto's dual use. The weak oversight allows TOCs to thrive perpetuating jurisdictional arbitrage on virtual currencies misuse. For instance, Uganda's unregulated P2P markets attract traffickers seeking to launder proceeds through Dubai-based exchanges.

Conclusion

The intersection of virtual currencies and TOCs in Eastern Africa underscores an urgent need for adaptive governance. The future of TOCs in the Eastern Africa region could increase due to the growth of global virtual currencies being catalyzed by the recent pro-crypto policy directives by the Trump administration. The global proliferation of virtual currencies poses prevalent TOC risks to Eastern Africa if effective dissuasive measures are not implemented. Strengthening Eastern Africa's digital security demands a multi-pronged approach as the absence of effective measures to disrupt and combat crypto-driven TOC risks the region becoming a perpetual playground for transnational cybercriminals, undermining its digital economic aspirations. Strategic initiatives lie in harmonizing national and regional frameworks to monitor crypto's dual use; strengthening coordinated international cooperation and intelligence sharing through artificial-enabled surveillance tools to disrupt TOC networks in real-time; enhancing technological capacity and cybersecurity infrastructure investment through public-private partnerships; and strengthening adaption of risk-based regulations and use of advanced blockchain forensics for crypto-driven TOC analysis to safeguard financial systems without stifling innovation.


Photo Credit: www.portfolio-adviser.com

Recommendations

The Ministry of ICT and Digital Economy, Kenya should;

a) establish regional cyber-defense hubs including the Nairobi Regional Blockchain Institute to undertake standardized training on crypto-induced TOCs dissuasive and combative measures;

b) lobby regional parliaments to amend cybersecurity laws to allow the lawful seizure of crypto–driven TOCs investments and assets;

c) collaborate with relevant policy actors nationally and regionally to lobby harmonizing national and regional frameworks under the East African Community (EAC) and IGAD frameworks to monitor crypto's dual use;

d) lobby Eastern Africa's regional bodies including the Eastern African Police Chiefs Organization (EAPCO), to harmonize crypto-related crime responses;

e) lobby for ratification and adoption of the African Union's Malabo Convention on Cybersecurity by all 14 Eastern African states and enforce states' compliance with a regional and global crypto regulatory framework to promote collaboration in regional investigations through Interpol's Cybercrime Directorate;

f) strengthen coordinated international cooperation and intelligence sharing through artificial-enabled surveillance tools to disrupt TOC networks in real-time;

g) enhance technological capacity and cybersecurity infrastructure investment through public-private partnerships;

h) partner with the Central Bank of Kenya (CBK) to integrate AI-driven fraud detection into M-Pesa and mandate real-time reporting of crypto transactions exceeding $10,000;

i) lobby regional and global partnerships to strengthen funding for the UN's Countering Cyber-Enabled Organized Crime Initiative, for proactive measures on cybersecurity threats;

j) invest in localized cybersecurity training programs like Rwanda's Africa Digital Policy Institute to build human capital on crypto-driven TOCs; and

k) leverage emerging technologies to adopt AI-driven fraud detection, risk-based regulations, and the use of advanced blockchain forensics for crypto-driven TOC analysis to safeguard financial systems without stifling innovation.

THE GLOBAL CENTRE FOR POLICY AND STRATEGY
(GLOCEPS)
Research | Knowledge | Influence
Off Kiambu Road, Nairobi Kenya
P.O. Box 27023-00100,Nairobi.
Telephone: 0112401331
Email: info@gloceps.org
Web: www.gloceps.org