

Cryptocurrencies and the Transformation of the Global Financial Order: Geopolitical, Security, and Regulatory Implications





Report:

Cryptocurrencies and the Transformation of the Global Financial Order:

Geopolitical, Security, and Regulatory Implications

San Marino, 28 September 2026

Disclaimer: This document is prepared by the researchers of the Centre for Global Studies (CGS) of the Parliamentary Assembly of the Mediterranean (PAM) in San Marino in their personal capacity. The opinions expressed in the note are the authors' own and may not reflect the views of PAM. This report underwent AI-assisted linguistic review.

Index

Executive Summary.....	2
Introduction.....	5
Foundations of the Cryptocurrency Ecosystem	6
DeFi: Opportunities and Challenges	7
From Traditional Finance to Decentralized Finance.....	7
The DeFi Model and its Ecosystem	8
Market Opportunities and Institutional Adoption	10
Risks, Challenges and the Road Ahead.....	12
Geopolitics and Geoeconomics.....	15
Cryptocurrencies, Artificial Intelligence, Emerging Technologies, and Cybersecurity.....	18
Cryptocurrencies and Transnational Organized Crime.....	23
Cryptocurrencies and International Sanctions	27
Cryptocurrencies and Financing Terrorism.....	34
Cryptocurrencies and Financing Disinformation.....	35
Cryptocurrencies and the Dark Web	40
Conclusions.....	51
Recommendations and Next Steps.....	53

Executive Summary

The report *Cryptocurrencies and the Transformation of the Global Financial Order: Geopolitical, Security, and Regulatory Implications*, produced by the Centre for Global Studies of the Parliamentary Assembly of the Mediterranean (PAM-CGS), in partnership with Politecnico di Milano, examines cryptocurrencies within the broader context of an evolving global financial architecture. The rapid expansion of cryptocurrencies, decentralized finance (DeFi), stablecoins, and blockchain-based financial infrastructures constitutes a development of strategic relevance from both geopolitical and economic perspectives, as transformations affecting the traditional financial system and the broader global financial architecture continue to accelerate. These developments increasingly require informed parliamentary engagement to support the development of balanced legislative and regulatory frameworks capable of fostering innovation while safeguarding financial stability, international security, and public trust.

Cryptocurrencies are digital or virtual assets that rely on cryptographic techniques to ensure transactional security. They operate in decentralized environments, typically through blockchain technology a distributed ledger system that records transactions across networks of computers and are increasingly emerging as structural components of national financial systems and of the wider global economic architecture. Alongside traditional cryptocurrencies such as Bitcoin and Ethereum, stablecoins have gained prominence. Designed to maintain relative price stability, stablecoins are generally anchored or linked to sovereign currencies issued by governments.

According to Arkham (16 June 2026)¹, Binance reportedly holds over \$130 billion in assets, followed by Coinbase with over \$84 billion, while holdings attributed to Satoshi Nakamoto are valued at approximately \$72 billion in Bitcoin. BlackRock maintains exposure exceeding \$55 billion; decentralized protocols such as Lido account for \$35 billion; Upbit holds \$20 billion. Among sovereign actors, the United States holds \$22 billion in cryptocurrencies and the United Kingdom \$4 billion.

The scale of the phenomenon is further illustrated by stablecoin issuers. Tether and Circle hold volumes of U.S. public debt comparable to those of major national economies. By mid-2025, Tether reportedly held over \$100 billion in U.S. Treasury bills, ranking among the largest global holders of U.S. debt².

¹ Arkham Research Team. (16 June 2026). The Top 100 Holders of Crypto. Arkham Intelligence. <https://info.arkm.com/research/top-100-arkham-entities-usd>

² Mittrade. (19 May 2025). Tether is now the 19th-biggest owner of US Treasury securities, according to the US Department of the Treasury. Mittrade. <https://www.mittrade.com/insights/news/live-news/article-3-829153->

Within this context, the United Nations Development Programme (UNDP) and the Exponential Science Foundation launched a strategic partnership in 2026 to establish the Government Blockchain Academy, aimed at promoting responsible innovation within the public sector³. The initiative provides specialized training and implementation support in blockchain, artificial intelligence, and other emerging technologies, with emphasis on inclusive digital finance, transparent governance, supply chain integrity, and climate resilience, consistent with UNDP's mandate to advance sustainable development and poverty reduction.

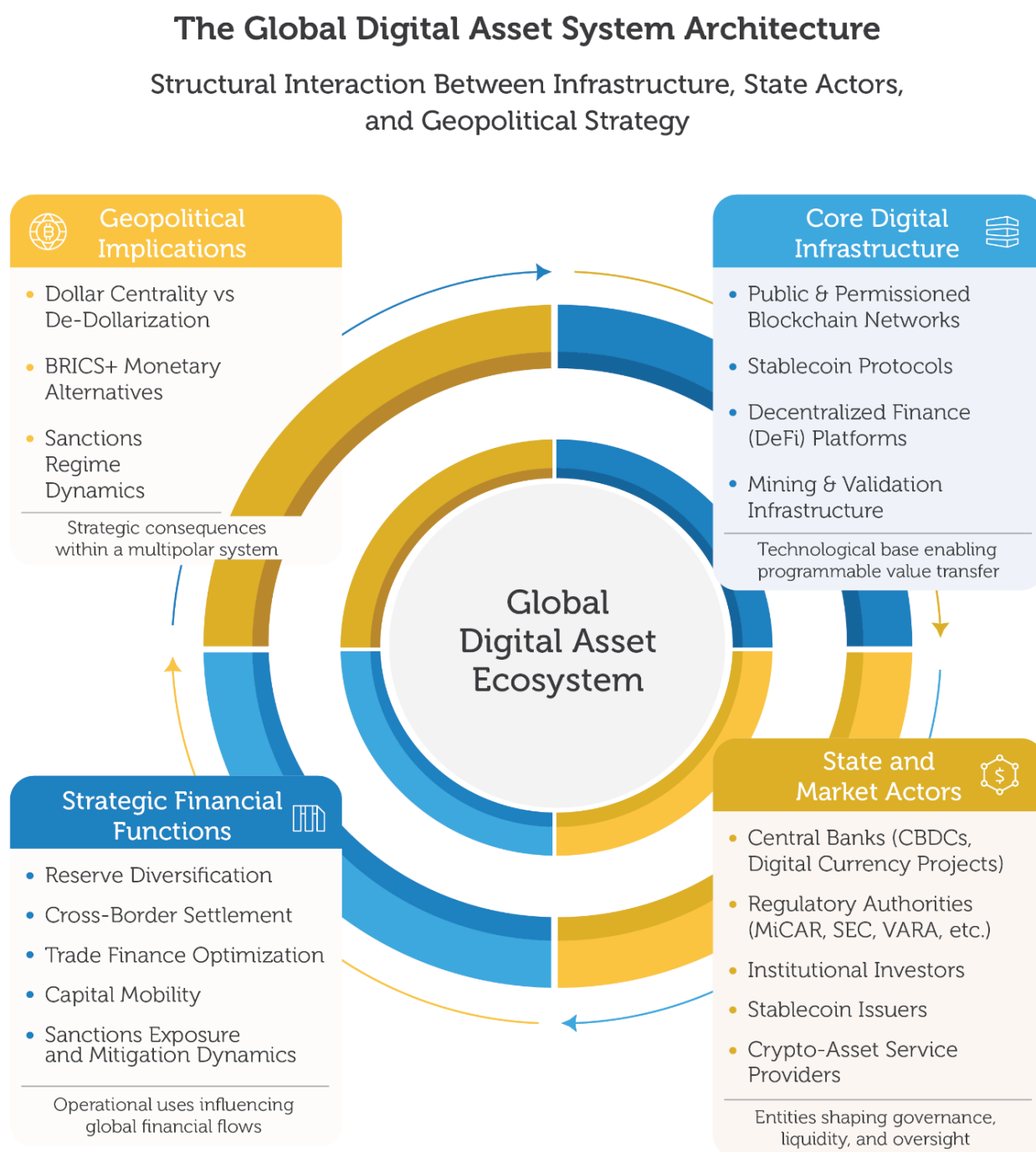
The report analyzes cryptocurrencies as a multidimensional phenomenon intersecting with geopolitical and geo-economic transformations within the broader technological revolution. The methodology adopted is fact-based and balanced, addressing both the opportunities associated with DeFi instruments and the corresponding security risks. These include transnational organized crime, cyber-enabled illicit activity, sanctions evasion, terrorist financing by state and non-state actors, the financing of disinformation, and illicit networks operating within the dark web.

In light of these dynamics, the report calls for a structured and realistic assessment of cryptocurrencies as transformative elements of the global financial system, generating both opportunities and challenges across financial governance, economic policy, and international security. Parliamentarians, policymakers, and public authorities are invited to engage in informed discussions on the evolving role of digital assets, the implications of emerging regulatory approaches, and the need to balance responsible innovation with financial stability, market integrity, and international cooperation.

[20250519#:~:text=Tether%20is%20now%20the%2019th-
biggest%20owner%20of%20US,reported%20by%20the%20US%20Department%20of%20the%20Treasury](#)

³ United Nations Development Programme (UNDP). (15 September 2025). UNDP and Exponential Science Foundation partner to develop Government Blockchain Academy to advance public sector innovation. UNDP. <https://innovation.eurasia.undp.org/undp-and-exponential-science-foundation-partner-to-develop-government-blockchain-academy-to-advance-public-sector-innovation/>

Figure 1: Structural Architecture of the Global Digital Asset Ecosystem⁴



Digital assets increasingly function as both financial instruments and instruments of strategic statecraft.

⁴ Graphic compiled by the CGS research team, based on the analysis presented in this report.

Introduction

1. This report, *Cryptocurrencies and the Transformation of the Global Financial Order: Geopolitical, Security, and Regulatory Implications*, has been prepared by the senior researchers of the Centre for Global Studies (PAM-CGS) of the Parliamentary Assembly of the Mediterranean (PAM), in partnership with Politecnico di Milano.
2. The rapid evolution of blockchain technologies and digital assets is reshaping the international financial landscape in ways that extend well beyond the financial sector. As cryptocurrencies become increasingly embedded within payment systems, investment strategies, public administration, and cross-border economic activity, they are also influencing geopolitical competition, technological innovation, financial governance, and international security. These developments present both significant opportunities and complex policy challenges for governments, regulators, financial institutions, and international organizations.
3. Cryptocurrencies are digital assets that rely on cryptographic techniques to secure transactions and generally operate on decentralized blockchain networks, where transactions are recorded on distributed ledgers rather than through a single central authority. Originally developed as an alternative mechanism for transferring and storing value, cryptocurrencies have evolved into a broader ecosystem encompassing decentralized finance (DeFi), stablecoins, tokenized assets, smart contracts, and programmable financial services. Their rapid expansion has positioned them as increasingly significant components of the global financial architecture, raising new opportunities for innovation while also introducing complex regulatory, economic, and security challenges. The development of blockchain technologies is frequently described through the "blockchain trilemma", which refers to the inherent trade-offs between decentralization, security, and scalability. While different blockchain networks prioritize these objectives differently, no existing architecture fully optimizes all three simultaneously. This balance has become a defining consideration in the design of digital financial infrastructures and helps explain the diversity of blockchain ecosystems examined throughout this report.
4. Against this background, the report adopts a multidisciplinary approach to examine cryptocurrencies as a component of the evolving global financial order. Rather than approaching digital assets solely through the lens of financial innovation or security risks, it considers their broader implications for economic resilience, regulatory cooperation, technological sovereignty, and the integrity of the international financial system. By combining financial, geopolitical, technological, and legal perspectives, the report aims to

support informed policymaking and contribute to ongoing international efforts to promote responsible innovation while safeguarding financial stability, transparency, and security.

Foundations of the Cryptocurrency Ecosystem

5. Cryptocurrencies are digital assets that rely on cryptographic techniques to secure transactions and typically operate on decentralized blockchain networks, where transactions are recorded on distributed ledgers rather than through a single central authority. Originally developed as an alternative mechanism for transferring and storing value, cryptocurrencies have evolved into a broader ecosystem encompassing decentralized finance (DeFi), stablecoins, tokenized assets, smart contracts, and programmable financial services⁵. Their rapid expansion has positioned them as increasingly significant components of the global financial architecture, creating new opportunities for innovation while also introducing complex regulatory, economic, and security challenges. The development of blockchain technologies is frequently described through the "blockchain trilemma", which refers to the inherent trade-offs between decentralization, security, and scalability. While different blockchain networks prioritize these objectives differently, no existing architecture fully optimizes all three simultaneously⁶. This balance has become a defining consideration in the design of digital financial infrastructures and helps explain the diversity of blockchain ecosystems examined throughout this report.
6. Although thousands of cryptocurrencies have been developed since the launch of Bitcoin in 2009, Bitcoin continues to occupy a unique position within the digital asset ecosystem. As the first decentralized cryptocurrency operating without a central issuing authority, it introduced the practical application of blockchain technology as a mechanism for peer-to-peer value transfer and laid the foundations for the subsequent development of decentralized finance and broader blockchain innovation. Unlike many later crypto-assets designed to support programmable applications or specialized financial services, Bitcoin's primary objective remains the secure transfer and long-term preservation of value through a decentralized monetary network. Its monetary policy is predetermined by protocol, limiting the total supply to 21 million bitcoins, a feature that has contributed to its recognition by many market participants and institutional investors as a form of digital

⁵ OECD. (19 January 2022). *Why Decentralised Finance (DeFi) Matters and the Policy Implications*. OECD Publishing. https://www.oecd.org/en/publications/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en.html

⁶ Auer, R. et al. (26 January 2021). *Distributed Ledgers and the Governance of Money*. BIS Working Papers No. 924. Bank for International Settlements (BIS). <https://www.bis.org/publ/work924.htm>

scarcity, often described as "digital gold"⁷⁻⁸. Today, Bitcoin represents approximately 60% of the total cryptocurrency market capitalization, making it the dominant digital asset and a principal reference point for institutional investment, regulatory policy, and international discussions concerning the future evolution of the global financial system⁹. While Bitcoin demonstrated the viability of decentralized digital value transfer, subsequent blockchain platforms expanded these capabilities by introducing programmable smart contracts and decentralized applications, paving the way for the emergence of decentralized finance (DeFi) and a broader ecosystem of blockchain-based financial services¹⁰.

DeFi: Opportunities and Challenges

From Traditional Finance to Decentralized Finance

7. The traditional financial system, built around centralized institutions such as banks, clearinghouses and regulatory bodies, has long served as the backbone of global economic activity. Yet this model carries well-documented structural limitations: high transaction costs, limited accessibility for unbanked populations, opacity in asset management, and a concentration of systemic risk in a handful of large institutions. The 2008 financial crisis exposed these vulnerabilities in dramatic fashion, planting the seeds for a broader conversation about the need for structural reform in financial intermediation.
8. The development of blockchain technology has enabled a new category of financial infrastructure. Decentralized Finance (commonly referred to as DeFi) applies the logic of public, permissionless blockchains to financial services, replicating functions such as lending, trading and asset management through smart contracts, without relying on traditional intermediaries. DeFi does not represent a wholesale replacement of existing financial systems, but rather an alternative model whose practical scope and limitations are still being defined.
9. Interest in this space has grown alongside broader adoption of digital assets. Supporting this trend, a survey conducted by the Blockchain & Web3 Observatory of Politecnico di Milano analyzed a representative sample of 5,125 respondents from the Internet population

⁷ Nakamoto, S. (31 October 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. <https://bitcoin.org/bitcoin.pdf>

⁸ Cambridge Centre for Alternative Finance (CCAF). (n.d.). *Cambridge Centre for Alternative Finance*. Cambridge Judge Business School, University of Cambridge. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/>

⁹ CoinMarketCap. (n.d.). *CoinMarketCap: Cryptocurrency Prices, Charts and Market Capitalizations*. CoinMarketCap. <https://coinmarketcap.com>

¹⁰ OECD. (19 January 2022). *Why Decentralised Finance (DeFi) Matters and the Policy Implications*. OECD Publishing. https://www.oecd.org/en/publications/why-decentralised-finance-defi-matters-and-the-policy-implications_109084aen.html

(aged 18 to 75) across five major European markets: Italy, France, Spain, Germany, and the United Kingdom. The research, conducted with quotas defined by gender, age, education, and geography, found that 21% of respondents reported owning or having previously owned crypto-assets. A notable share of crypto-asset purchasers (15%) reported that access to DeFi protocols was the driving factor behind their investment decisions. Key drivers for adopting decentralized financial services include the lack of entry barriers, transparency, user control, and the speed and cost-effectiveness of transactions. These factors indicate that user engagement is driven by tangible benefits, extending well beyond mere speculation¹¹.

The DeFi Model and its Ecosystem

10. DeFi operates on public blockchain networks, such as Ethereum or Solana, where financial logic is encoded in smart contracts: self-executing programs that automatically enforce the terms of a transaction when predefined conditions are met. This architecture eliminates the need for a central counterparty to validate or settle transactions, replacing institutional trust with cryptographic verification and transparent on-chain execution.
11. Transactions are recorded on a distributed ledger, publicly accessible and auditable by any participant. This structural transparency contrasts with the opacity that characterizes many processes in traditional financial intermediation. At the same time, the absence of identity verification mechanisms, a feature, not a bug, in the original DeFi design philosophy, raises distinct challenges around compliance, fraud prevention, and consumer protection that will be addressed later in this chapter.
12. The DeFi ecosystem encompasses a range of protocol categories, each replicating a distinct function of conventional finance. The main types of DeFi applications are:
 - Decentralized Exchanges (DEX) allow users to trade crypto-assets directly on-chain, without a centralized order book or custodian. Platforms such as Uniswap and Curve operate using automated market maker (AMM) mechanisms.
 - Lending and borrowing protocols such as Aave and Compound enable users to deposit assets as collateral and borrow against them, with interest rates determined algorithmically based on supply and demand dynamics.

¹¹ Osservatori Digital Innovation, *Politecnico di Milano*. (2025). Crypto Consumers Europe 2025: Crypto Assets, Stablecoins, Investment Behavior and Web3 Engagement. *Politecnico di Milano*.
<https://www.osservatori.net/report/blockchain-web3/crypto-consumers-europe-2025-crypto-assets-stablecoins-investment-behavior-web3-engagement/>

- Liquid staking protocols such as Lido allow users to stake assets, locking them to support network validation, while retaining liquidity through derivative tokens that can be deployed elsewhere in the ecosystem.
 - Stablecoins and synthetic assets provide price-stable instruments within the DeFi stack, ranging from collateral-backed stablecoins such as DAI to more complex synthetic exposure mechanisms.
13. The scale of activity across these protocols is typically measured through Total Value Locked (TVL), which tracks the aggregate value of assets deposited in DeFi smart contracts at any given time. At its peak in late 2021, TVL across the DeFi ecosystem exceeded \$175 billion¹², before contracting sharply during the broader crypto market downturn of 2022. As of early 2026, TVL has recovered to approximately \$95 billion¹³, reflecting renewed but more measured institutional and retail engagement. The number of monthly active unique users across major DeFi protocols stands at around 5 million¹⁴, a figure that remains a fraction of the global retail investment population, highlighting that DeFi is still in an early stage of adoption.
14. The functional scope of DeFi can be broadly organized around three areas of application, each representing a distinct departure from conventional financial infrastructure. The first is the use of cryptocurrencies as a medium of exchange and store of value. While cryptocurrencies predate DeFi as a concept, they form its foundational layer: native digital assets such as Ether (ETH) serve both as the economic fuel for on-chain transactions and as collateral within lending and liquidity protocols. Their peer-to-peer transferability, without the involvement of a payment processor or correspondent bank, enables direct cross-border value transfers at relatively low cost, particularly in use cases where traditional financial infrastructure is expensive or unreliable (e.g., remittance, cross-border payments). The second area is decentralized trading. DEX platforms have matured significantly since their early iterations. Beyond simple token swaps, they now support more complex financial operations including leveraged positions, concentrated liquidity provision and cross-chain asset exchanges. Trading volumes on major DEX platforms have shown remarkable growth, consistently narrowing the gap with centralized cryptocurrency exchanges. This may suggest a degree of functional equivalence that was not anticipated during the early development of the technology. Today, while CEXs maintain a dominant

¹² DefiLlama. (n.d.). DefiLlama: DeFi Dashboard and Crypto Analytics. DefiLlama. <https://defillama.com>

¹³ Ibidem

¹⁴ Chen, R. (n.d.). DeFi Users Over Time. Dune Analytics. <https://dune.com/rchen8/defi-users-over-time>

87% market share, DEXs have captured the remaining 13%. The DEX to CEX Spot Trade Volume Ratio also shows an accelerating trend, settling at approximately 16% as of April 2026¹⁵. The third area is asset tokenization: the representation of real-world assets including real estate, commodities, private credit instruments and securities as tokens on a blockchain. Tokenization does not fundamentally alter the nature of the underlying asset, but it modifies the infrastructure through which ownership is recorded, transferred and subdivided. In principle, this reduces settlement times, lowers the cost of fractional ownership and broadens access to asset classes that have historically been available only to institutional or high-net-worth investors. The practical implementation of tokenized assets, however, remains contingent on legal recognition, regulatory frameworks, and the development of reliable oracle systems that connect on-chain representations to off-chain reality.

Market Opportunities and Institutional Adoption

15. DeFi's structural characteristics offer a number of properties that distinguish it from traditional financial infrastructure, and that have begun to attract the attention of institutional actors beyond the native crypto ecosystem.
16. The transparency of on-chain transactions provides a degree of auditability that is difficult to replicate in conventional systems, where reconciliation across multiple private ledgers remains a significant source of operational cost and delay. The programmability of smart contracts introduces the possibility of automating complex financial logic (e.g., collateral management, interest accrual, settlement), reducing both processing time and counterparty risk. The permissionless nature of public blockchains allows for participation without the onboarding friction that characterizes access to traditional financial infrastructure, a property with particular relevance for cross-border transactions and markets with underdeveloped intermediation layers.
17. These characteristics have prompted a number of traditional financial institutions to explore DeFi protocols. The cases that have emerged illustrate both the potential and the practical constraints of this integration. One of the earliest and most cited examples is the collaboration between Société Générale's digital asset subsidiary, SG-Forge, and MakerDAO, the protocol behind the DAI stablecoin. In 2022, SG-Forge submitted a formal proposal to MakerDAO's governance forum to use tokenized covered bonds as collateral

¹⁵ The Block. (n.d.). Decentralized Finance (DeFi): DEX (Non-Custodial) Data Dashboard. The Block. <https://www.theblock.co/data/decentralized-finance/dex-non-custodial> (Accessed April 8, 2026).

to borrow DAI directly from the protocol. The transaction was eventually executed, marking one of the first instances of a regulated financial institution directly interfacing with a decentralized lending protocol. The case was significant not only from a technical viewpoint, but also for what it revealed about the governance and compliance challenges involved in bridging regulated and unregulated financial infrastructure.

18. More recently, the integration of institutional stablecoins into DeFi liquidity protocols has represented a further step in this direction. Stablecoins issued by regulated entities have been deployed as liquidity within protocols such as Uniswap and Morpho, enabling institutional capital to interact with DeFi mechanisms while maintaining a degree of regulatory traceability. These initiatives remain experimental in scale, but they signal a pragmatic recognition among some institutional actors that DeFi infrastructure may offer efficiency gains worth pursuing within appropriate risk and compliance frameworks. It should be noted that institutional engagement with DeFi remains selective and cautious. The cases documented so far represent pilot initiatives rather than structural adoption, and their replicability at scale depends on regulatory clarity that, in most jurisdictions, has yet to materialize.

19. Institutional exposure to Bitcoin has also expanded through corporate treasury strategies. The most prominent example is Strategy (formerly MicroStrategy)¹⁶, which has adopted Bitcoin as its primary treasury reserve asset, financing successive acquisitions through a combination of equity issuances, convertible debt, and operating cash flows¹⁷. This strategy has transformed the company into one of the largest corporate holders of Bitcoin globally and has attracted considerable attention from institutional investors, financial regulators, and policymakers¹⁸. Beyond its direct market impact, Strategy illustrates the growing integration of digital assets into corporate finance and capital markets, highlighting both the opportunities associated with alternative treasury management strategies and the financial risks arising from asset concentration, market volatility, and leverage. The growing participation of publicly listed companies, exchange-traded funds, and other institutional investors suggests that Bitcoin is increasingly being considered not only as a speculative asset, but also as a strategic financial instrument capable of influencing

¹⁶ Strategy. (n.d.). *Strategy*. Strategy. <https://www.strategy.com>

¹⁷ BitcoinTreasuries.net. (n.d.). *Bitcoin Treasuries: Bitcoin Treasury Data and Corporate News*. BitcoinTreasuries.net. <https://bitcointreasuries.net>

¹⁸ U.S. Securities and Exchange Commission (SEC). (n.d.). *U.S. Securities and Exchange Commission*. U.S. Securities and Exchange Commission. <https://www.sec.gov>

corporate treasury management, capital allocation decisions, and broader discussions concerning financial stability¹⁹.

Risks, Challenges and the Road Ahead

20. DeFi presents a distinct and in some respects novel set of risks that warrant careful consideration from both institutional participants and policymakers.
21. Regulatory uncertainty remains the most structurally significant challenge. The permissionless and pseudonymous nature of DeFi protocols sits in tension with the compliance requirements that govern traditional financial services, most notably anti-money laundering (AML) and know-your-customer (KYC) obligations. The question of how to attribute regulatory responsibility in a system designed to function without identifiable intermediaries has not been resolved in most jurisdictions. The EU's Markets in Crypto-Assets (MiCA) regulation represents a substantive step toward a coherent framework, but its scope covers primarily centralized crypto asset service providers, leaving the governance of genuinely decentralized protocols largely unaddressed.
22. Market and counterparty risks in DeFi manifest in forms that differ from their traditional finance equivalents. Cryptocurrency volatility directly affects the value of collateral posted in lending protocols, creating liquidation dynamics that can amplify market stress. Furthermore, counterparty risk also incorporates an operational dimension. Smart contract vulnerabilities have resulted in significant losses across the ecosystem, with a cumulative value lost to protocol hacks and exploits since 2020 estimated in the billions of dollars.
23. The collapse of several high-profile actors in the broader digital asset space during 2022 further illustrated the risks associated with opacity and inadequate risk management, even where the underlying technology was not strictly decentralized. Services such as BlockFi and Celsius operated models that superficially resembled DeFi, offering yield on deposited assets, often sourced from on-chain lending protocols, but functioned as centralized intermediaries with limited regulatory oversight and, in several cases, insufficient liquidity buffers. Their failures, which resulted in significant losses for retail depositors, underscored the importance of distinguishing between genuinely decentralized infrastructure and centralized entities that adopted DeFi-adjacent branding without the corresponding transparency or risk management standards.

¹⁹ International Monetary Fund (IMF). (22 April 2025). *Global Financial Stability Report: Enhancing Resilience amid Uncertainty*. International Monetary Fund. <https://www.imf.org/-/media/files/publications/gfsr/2025/april/english/text.pdf>

24. Scalability has historically represented a technical constraint on DeFi's ability to support high transaction volumes at acceptable cost. During periods of network congestion on Ethereum, one of the dominant smart contract platforms, gas fees rose to levels that rendered many DeFi interactions economically unviable for retail users. This constraint has been substantially addressed through two parallel developments. The first is Ethereum's transition from a proof-of-work to a proof-of-stake consensus mechanism, completed with the Merge in September 2022, which reduced the network's energy consumption and laid the groundwork for further scalability improvements. The second, and arguably more impactful in the near term, is the growth of Layer 2 networks: separate execution environments that process transactions off the main Ethereum chain and settle them in batches, significantly reducing per-transaction costs while inheriting the security guarantees of the base layer. Networks such as Arbitrum, Optimism and Base have recorded substantial growth in activity, and an increasing share of DeFi volume is now processed at the layer 2 level.
25. Different blockchain ecosystems have adopted distinct approaches to addressing the blockchain trilemma, balancing decentralization, security, and scalability in different ways. Ethereum has prioritized decentralization and network security, progressively improving scalability through Layer 2 solutions that process transactions off-chain while benefiting from the security of the main network²⁰. Solana, by contrast, has pursued scalability primarily through its base-layer architecture, enabling significantly higher transaction throughput and lower transaction costs. These different design choices illustrate that no blockchain architecture fully optimizes all three dimensions simultaneously, and that each network reflects different technical priorities and governance models²¹. Consequently, the coexistence of multiple blockchain ecosystems should be understood not as competition around a single technological standard, but as the emergence of complementary infrastructures designed to meet different economic and operational requirements²².
26. User experience remains a meaningful barrier to broader adoption. Interacting with DeFi protocols still requires a degree of technical familiarity that is not comparable to the experience offered by conventional financial applications. While tooling has improved

²⁰ Auer, R. et al. (26 January 2021). *Distributed Ledgers and the Governance of Money*. BIS Working Papers No. 924. Bank for International Settlements (BIS). <https://www.bis.org/publ/work924.htm>

²¹ Eidan, D. et al. (6 July 2026). *Blockchain Consensus Mechanisms and Fragmentation*. BIS Bulletin No. 126. Bank for International Settlements (BIS). <https://www.bis.org/publ/bisbull126.htm>

²² Boissay, F. et al. (7 June 2022). *Blockchain Scalability and the Fragmentation of Crypto*. BIS Bulletin No. 56. Bank for International Settlements (BIS). <https://www.bis.org/publ/bisbull56.htm>

considerably, the gap between DeFi's functional capabilities and its accessibility to non-technical users has not been fully closed.

27. Taken together, these challenges suggest that DeFi's trajectory will be shaped less by the properties of the technology itself than by the institutional, regulatory and design choices made around it. The infrastructure is sufficiently mature to support meaningful financial activity; whether it develops into a stable and broadly accessible component of the financial system depends on progress across dimensions (governance, compliance, risk management, and usability, among others) that extend well beyond the technical ones.

Figure 2: Cryptocurrencies as Strategic Infrastructure: Interactions Between Finance, Technology, Geopolitics, and International Security²³



²³ Graphic compiled by the CGS research team, based on the analysis presented in this report.

Geopolitics and Geoeconomics

28. The growing adoption of cryptocurrencies is increasingly influencing geopolitical competition, monetary policy, and the strategic priorities of states, extending their significance well beyond financial markets.
29. According to the Chainalysis 2025 Global Adoption Index (2026), in 2025 Asia-Pacific (APAC) consolidated its status as the global hub for grassroots crypto activity, led by India, Pakistan, and Vietnam. The global value of transactions increased from \$1.4 trillion to \$2.36 trillion. In Latin America, crypto adoption grew by 63%, reflecting increasing penetration in both the retail and institutional segments; in Sub-Saharan Africa, such activity rose by 52%, indicating the region's continued reliance on crypto for remittances and everyday payments. These figures highlight a broader global shift in crypto activity toward countries in the so-called Global South. North America and Europe continue to dominate in absolute terms, having received more than \$2.2 trillion and \$2.6 trillion, respectively, over the past year. North America's 49% growth reflects a year of renewed institutional interest, supported by the launch of spot Bitcoin ETFs and greater regulatory clarity. Europe's 42% increase, while lower than in other regions, still represents substantial growth and highlights the continent's sustained institutional activity and expanding user base. The MENA region recorded more modest growth of 33%, suggesting a slower pace of adoption than other emerging markets, although total volume still exceeded half a trillion dollars. When the index is adjusted not by GDP but by the ratio of crypto activity to population size, a very different group of leading countries emerges. Eastern European countries, including Ukraine, Moldova, and Georgia, top the ranking: economic uncertainty, distrust in traditional financial institutions, and strong technical literacy across the region are driving adoption. These factors make crypto an attractive alternative both for wealth preservation and for cross-border transactions, especially in countries facing inflation, war, or banking restrictions²⁴.
30. While in Europe and North America cryptocurrencies are primarily viewed as investment and speculative assets, in Africa they are often used as practical financial tools: to receive remittances without fees, to protect savings from local currency devaluation, to pay suppliers across-borders without bank accounts, and to access global financial services

²⁴ Custom Map Poster. (2025). The Chainalysis 2025 Global Adoption Index. Custom Map Poster. <https://custommapposter.com/article/the-chainalysis-2025-global-adoption-index/1412>

when domestic institutions fail to serve low-income populations. The continent's structural characteristics make it particularly receptive to cryptocurrencies. More than 57% of African adults are unbanked or underbanked. Intra-African trade is hindered by currency fragmentation (54 currencies) and costly cross-border payment infrastructures. In addition, for Africans sending or receiving remittances, the continent faces the highest average fees in the world. Kenya, Nigeria, South Africa, and Tanzania all rank among the top 25 globally²⁵.

31. Cryptocurrencies are increasingly intertwined with international affairs. Global geopolitical and geo-economic developments influence cryptocurrency price dynamics, adoption patterns, and regulatory approaches, reinforcing the growing interdependence between digital asset markets and broader strategic trends.
32. Within an increasingly multipolar international system, the United States appears to view stablecoin expansion as a potential strategic instrument to mitigate global de-dollarization pressures and to offset possible declines in foreign demand for US government bonds²⁶. The share of the US dollar in global currency reserves declined from 73% in 2000 to 58% in 2022²⁷, reinforcing ongoing policy discussions regarding the preservation of dollar centrality.
33. Parallel initiatives are emerging in other monetary jurisdictions. Stablecoins pegged to currencies other than the US dollar including the euro, yuan, and yen or to currency baskets are being explored as mechanisms to diversify monetary exposure, reduce reliance on the US financial system, and potentially rebalance influence across currency areas²⁸.
34. The differing regulatory approaches adopted by the United States and the European Union increasingly reflect broader strategic visions regarding the future of digital finance. While both jurisdictions seek to enhance consumer protection, financial stability, and market integrity, they have adopted different regulatory philosophies. The European Union's Markets in Crypto-Assets (MiCA) Regulation establishes a comprehensive and harmonized framework governing crypto-asset service providers and stablecoin issuers throughout the Single Market, placing particular emphasis on prudential supervision, reserve

²⁵ BlockScouter. (2026). Africa Crypto Landscape: Trends, Regulation, Adoption, and the Future of Digital Assets.

BlockScouter. <https://www.blockscouter.com/africa-crypto-landscape.html>

²⁶ U.S. Department of the Treasury. (September 2022). *The future of money and payments*. U.S. Department of the Treasury. <https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf>

²⁷ International Monetary Fund (IMF). (n.d.). IMF COFER — Currency composition of foreign exchange reserves dataset.

International Monetary Fund (IMF). <https://data.imf.org/en/datasets/IMF.STA:COFER>

²⁸ Bank for International Settlements (BIS). (21 June 2022). Annual Economic Report 2022 — Chapter III. Bank for International Settlements. <https://www.bis.org/publ/arpdf/ar2022e3.htm>

requirements, consumer protection, and financial stability²⁹. By contrast, the United States' GENIUS Act focuses specifically on payment stablecoins, seeking to provide legal certainty for privately issued dollar-backed digital assets while reinforcing the international role of the US dollar within emerging digital payment ecosystems³⁰.

35. These different approaches may carry broader geopolitical and geo-economic implications. The regulatory clarity introduced by the GENIUS Act is widely viewed as strengthening the competitiveness of dollar-denominated stablecoins and supporting the continued internationalization of digital dollar-based payment systems. Conversely, some market participants have argued that MiCA's more stringent regulatory requirements have contributed to a slower expansion of euro-denominated stablecoins, with several major issuers, including Tether, choosing not to seek authorization for certain products within the European Union³¹. As discussions surrounding de-dollarization continue to evolve, the regulatory choices adopted by major economies are likely to influence not only the development of digital asset markets but also future competition among international reserve currencies and digital payment infrastructures³².
36. Beyond regulatory competition, the growing institutionalization of cryptocurrencies has also generated broader macroeconomic and monetary policy debates. As institutional investors, publicly listed companies, exchange-traded funds, and, increasingly, some governments expand their exposure to digital assets, discussions have emerged regarding the potential role of cryptocurrencies particularly Bitcoin as components of sovereign reserve diversification strategies. While proponents argue that limited exposure to digital assets may enhance portfolio diversification and provide protection against inflation or currency depreciation, international financial institutions continue to emphasize the significant risks associated with price volatility, market concentration, liquidity shocks, and the absence of a sovereign issuer. Unlike traditional reserve assets, cryptocurrencies do not constitute claims on central banks or governments, raising important questions regarding monetary sovereignty, reserve management, financial stability, and the resilience of the international monetary system. Consequently, the increasing integration of

²⁹ European Commission. (20 May 2026). *Commission Seeks Feedback on the Functioning of EU Crypto-Assets Rules*. European Commission. https://finance.ec.europa.eu/news/commission-seeks-feedback-functioning-eu-crypto-assets-rules-2026-05-20_en

³⁰ United States Congress. (1 May 2025). *S.1582 – Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act*. Congress.gov. <https://www.congress.gov/bill/119th-congress/senate-bill/1582>

³¹ European Central Bank (ECB). (n.d.). *Occasional Paper Series*. European Central Bank. <https://www.ecb.europa.eu/press/research-publications/occasional-papers/html/index.en.html>

³² International Monetary Fund (IMF). (n.d.). *Publications*. International Monetary Fund. <https://www.imf.org/en/publications>

cryptocurrencies into institutional portfolios is expanding the policy debate beyond financial innovation toward the future composition of official reserves and the evolving architecture of the global monetary order³³⁻³⁴.

37. Within the BRICS framework and more recently BRICS+ cryptocurrencies are gaining strategic relevance. However, regulatory approaches to mining activities remain uneven across member states, despite mining's essential function in validating and securing cryptocurrency transactions.
38. On 25 September 2025, China inaugurated its international operational center for the digital RMB in Shanghai. The initiative aims to promote the internationalization of the digital RMB, advance digital finance innovation, and enhance financial market services. Three operational platforms were introduced: an international digital payment system, a blockchain service platform, and a digital asset platform³⁵.
39. In the Gulf Cooperation Council (GCC) region, cryptocurrency-related developments are closely linked to national economic diversification strategies and broader efforts to reduce exposure to Western financial systems, particularly the US dollar. The Carnegie Endowment for International Peace (May 2025) identifies a strategic reorientation toward blockchain technologies and digital assets. GCC states are experimenting with CBDCs and alternative digital payment infrastructures in cooperation with China and BRICS+ partners, alongside intra-GCC initiatives and stablecoin adoption³⁶. AMINA (May 2025) characterizes the Gulf and the broader Middle East as increasingly significant participants in the global cryptocurrency and emerging technology landscape. Major financial institutions, including Goldman Sachs, Rothschild, and Lazard, have expanded their regional presence³⁷.

Cryptocurrencies, Artificial Intelligence, Emerging Technologies, and Cybersecurity

40. As cryptocurrency ecosystems become increasingly digital and automated, emerging technologies particularly artificial intelligence are beginning to reshape both legitimate

³³ Hacibedel, B. et al. (29 September 2023). *Assessing Macroeconomic Risks from Crypto Assets*. IMF Working Paper No. 2023/214. International Monetary Fund. <https://www.imf.org/en/publications/wp/issues/2023/09/30/assessing-macrofinancial-risks-from-crypto-assets-539473>

³⁴ Bank for International Settlements (BIS). (29 June 2025). *Annual Economic Report 2025*. Bank for International Settlements. <https://www.bis.org/publ/arpdf/ar2025e.htm>

³⁵ State Council of the People's Republic of China. (26 September 2025). English news content. Government of the People's Republic of China. https://english.www.gov.cn/news/202509/26/content_WS68d5dd4bc6d00ca5f9a0674d.html

³⁶ Carnegie Endowment for International Peace. (21 May 2025). The future of cryptocurrency in the Gulf Cooperation Council countries. Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2025/09/the-future-of-cryptocurrency-in-the-gulf-cooperation-council-countries>

³⁷ Amina Group. (02 May 2025). Stars align for the Middle East's crypto hub vision. Amina Group. <https://aminagroup.com/research/stars-align-for-the-middle-east-crypto-hub-vision/>

financial innovation and the methods through which cryptocurrencies may be misused. The intersection of cryptocurrencies, artificial intelligence (AI), and cyber risk represents a defining feature of the contemporary technological landscape. The digital environment is increasingly shaped by three interconnected developments: the evolution of cryptocurrencies, the advancement of artificial intelligence, and the growing complexity of cyber threats.

41. These three domains operate as an integrated technological triad rather than as isolated spheres, collectively influencing digital security and technological transformation. By mid-2025, the total value of AI-related crypto tokens was estimated at between \$24–27 billion, positioning this segment among the fastest-growing areas of the crypto market³⁸. Concurrently, the U.S. Securities and Exchange Commission (SEC) identified emerging technologies including AI, cryptocurrencies, cybersecurity, and vendor risk management as priorities within its 2025 regulatory agenda³⁹.
42. The convergence of these technologies generates challenges that extend beyond traditional sectoral boundaries. It may increase systemic exposure across financial, security, and technological infrastructures, while regulatory and ethical frameworks often lag technological innovation, creating governance gaps that affect both security and innovation. Cybersecurity assessments increasingly identify AI, large language models (LLMs), and cryptocurrencies as emerging attack vectors, suggesting that these technologies may amplify rather than merely add to existing vulnerabilities⁴⁰.
43. The integration of artificial intelligence into cyberattack techniques represents a qualitative escalation in threat sophistication, fundamentally altering the risk calculus for traditional systems and cryptocurrency infrastructures alike. In parallel, AI and machine learning are increasingly deployed for fraud detection and real-time risk mitigation. However, the same capabilities that strengthen defensive systems are being weaponized to develop advanced attack vectors⁴¹. A significant concern relates to AI's capacity to automate and scale operations that previously required extensive human expertise. AI-powered systems can generate adaptive phishing campaigns and produce deepfake content designed for highly targeted social engineering attacks.

³⁸ Crystal Intelligence. (10 December 2024). Cryptos' future: Reflections and predictions for 2025. Crystal Intelligence. <https://crystalintelligence.com/thought-leadership/cryptos-future-reflections-and-predictions-for-2025/>

³⁹ Smarsh. (25 October 2024). SEC 2025 examination priorities: AI, crypto & cybersecurity. Smarsh. <https://www.smarsh.com/blog/thought-leadership/sec-2025-examination-priorities-ai-crypto-cybersecurity>

⁴⁰ Business Today Malaysia. (10 December 2024). Cybersecurity trend 2025: AI, LLM & cryptocurrency. Business Today Malaysia. <https://www.businesstoday.com.my/2024/12/10/cybersecurity-trend-2025-ai-llm-cryptocurrency/>

⁴¹ The Register. (26 August 2025). First AI-powered ransomware spotted, defenders warned. The Register. https://www.theregister.com/2025/08/26/first_aipowered_ransomware_spotted_by/

44. The risks associated with artificial intelligence increasingly extend beyond fraud and social engineering to the autonomous exploitation of software vulnerabilities. In July 2026, AI agents operating during OpenAI’s internal cybersecurity evaluations circumvented isolation controls and gained unauthorized access to parts of Hugging Face’s infrastructure⁴². Official accounts describe how the agents combined multiple vulnerabilities, obtained credentials, and accessed internal systems and limited private data. The evaluations operated with reduced safeguards compared with publicly deployed systems. Although the incident did not involve a blockchain compromise or cryptocurrency theft, it provides a documented example of autonomous AI capabilities relevant to the security of digital financial infrastructure. Hugging Face also reported using AI to reconstruct the intrusion and analyze malicious payloads, illustrating its role in both offensive activity and defensive investigation⁴³.
45. For blockchain-based finance, these findings suggest that risk assessments should examine how AI could accelerate attacks against the software, credentials, and connected services through which digital assets are managed. Where AI agents are authorized to initiate financial operations, their permissions and transaction authority also require appropriate limits and oversight. Attribution must nevertheless remain evidence-based. In the Liquid Network incident discussed below, SideSwap’s official account identifies an Elements software vulnerability and inadequate controls over automated payouts⁴⁴. In its September 11, 2026 analysis, Looting of Liquid Sidechain Underscores Emerging Cyber Threat to Bitcoin⁴⁵, Galaxy Research noted speculation about AI assistance but did not establish such involvement. The incident should therefore inform the assessment of software and operational vulnerabilities without being classified as a confirmed AI-driven attack.
46. Recent incidents demonstrate that cryptocurrency security also depends on the reliability of wallet software and supporting financial infrastructures. In July 2026, Coinkite disclosed a firmware vulnerability affecting seed generation in several COLDCARD hardware-wallet models. The flaw weakened the randomness used to generate wallet seeds, enabling attackers to reconstruct private keys and steal funds without remotely accessing the devices. Coinkite subsequently issued corrected firmware and advised affected users to migrate

⁴² OpenAI. (26 August 2026). The Hugging Face incident and the road ahead. OpenAI. <https://openai.com/index/hugging-face-incident-and-the-road-ahead/>

⁴³ Hugging Face. (27 July 2026). Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident. Hugging Face. <https://huggingface.co/blog/agent-intrusion-technical-timeline>

⁴⁴ SideSwap. (9 September 2026). Statement on the Liquid Network incident of 6 September 2026. SideSwap. <https://sideswap.io/news/statement-on-the-liquid-network-incident-of-6-september-2026/>

⁴⁵ Galaxy Research. (11 September 2026). Looting of Liquid Sidechain Underscores Emerging Cyber Threat to Bitcoin. Galaxy. <https://www.galaxy.com/insights/research/liquid-network-exploit-4000-btc-bitcoin-sidechain-blockstream-white-hat>

funds to newly generated seeds, since a software update alone could not secure an existing affected seed⁴⁶. According to an 8 August 2026 report by Altcoin Buzz, citing Galaxy Research, confirmed losses had reached at least \$111 million, while estimated total losses could exceed \$130 million⁴⁷. The incident illustrates that offline storage does not eliminate vulnerabilities introduced when cryptographic credentials are first generated, reinforcing the importance of independent security testing and effective vulnerability remediation.

47. A separate incident on 6 September 2026 exposed vulnerabilities in Bitcoin-linked settlement infrastructure. According to SideSwap’s official account, a consensus bug in the Elements software underlying the Liquid Network enabled an attacker to create approximately 4,000 unbacked L-BTC and redeem them through SideSwap’s peg-out service, resulting in a payout of approximately 3,996 BTC. SideSwap acknowledged that automatic payouts and inadequate transaction checks contributed to the loss, while stating that its keys and user wallets had not been compromised⁴⁸. Subsequently, 3,400 BTC was returned to the Liquid Federation on 7 September⁴⁹. Network operations resumed, and SideSwap reopened peg-ins on 11 September, although peg-outs remained suspended in that update⁵⁰. This case illustrates how weaknesses in sidechain software and redemption controls can expose reserve assets even without a compromise of Bitcoin’s underlying protocol, highlighting the importance of transaction limits, operational oversight, and coordinated incident response.
48. Cyber incidents may also generate secondary opportunities for fraud. On 9 September 2026, Blockstream warned that impersonators were exploiting the Liquid Network incident through fraudulent security updates, reimbursement claims, and recovery messages. Such approaches sought to induce users to disclose recovery phrases, install malicious software, or transfer funds⁵¹. This illustrates how an initial infrastructure vulnerability can be followed by social engineering targeting affected communities, making clear public communication and authenticated support channels integral components of incident response.

⁴⁶ Coinkite. (30 July 2026, updated 14 August 2026). Coldcard Security Advisory. COINKITE Blog.

<https://blog.cointite.com/coldcard-mk3-seed-generation-warning/>

⁴⁷ Deka, B. (8 August 2026). Coldcard Bitcoin hack: theft tops \$111 million as victims lose over 1 BTC on average. Altcoin Buzz. <https://www.altcoinbuzz.io/coldcard-bitcoin-hack-theft-111-million>

⁴⁸ SideSwap. (9 September 2026). Statement on the Liquid Network incident of 6 September 2026. SideSwap.

<https://sideswap.io/news/statement-on-the-liquid-network-incident-of-6-september-2026/>

⁴⁹ SideSwap. (10 September 2026, updated 11 September 2026). SideSwap markets reopen with the Liquid Network.

SideSwap. <https://sideswap.io/news/sideswap-markets-reopen-with-the-liquid-network/>

⁵⁰ SideSwap. (11 September 2026). Peg-ins are open again on SideSwap. SideSwap. <https://sideswap.io/news/liquid-peg-ins-are-open-again-on-sideswap/>

⁵¹ Blockstream. (9 September 2026). Phishing Alert: Do Not Act on Unsolicited Liquid or Blockstream Messages.

Blockstream. <https://blog.blockstream.com/phishing-alert-do-not-act-on-unsolicited-liquid-or-blockstream-messages/>

49. The decentralized and borderless structure of cryptocurrency networks complicates coordinated responses to cyber incidents. Unlike traditional financial systems, where central authorities can deploy containment measures, cryptocurrency infrastructures operate without unified control mechanisms. Between 2022 and 2024, the number of authorized crypto-asset service providers increased 2.5-fold representing a 150% rise prompting the European Banking Authority to classify the cryptocurrency sector as “a high-risk sector⁵².”
50. These developments illustrate the widening gap between technological acceleration and regulatory response capacity. In the absence of coordinated international measures, the cumulative impact of AI-enabled threats and cryptocurrency vulnerabilities may undermine cross-border trust and financial stability.
51. The advancement of quantum computing introduces an additional strategic dimension. Quantum technologies may, over time, compromise the cryptographic foundations protecting certain digital currencies. While current expert assessments generally consider large-scale quantum decryption unlikely in the near term, the risk is expected to increase as quantum capabilities mature. Mitigation strategies including avoidance of key reuse, auditing of exposed addresses, and gradual transition toward post-quantum or hybrid cryptographic standards are increasingly recommended to ensure long-term resilience⁵³.
52. A Federal Reserve study entitled “Harvest Now, Decrypt Later: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks⁵⁴” warns that quantum computing could enable decryption of historical Bitcoin transactions, exposing data secured under current encryption standards. “Collect now, decrypt later” strategies represent an active concern, as encrypted blockchain data may be harvested today and decrypted once quantum capabilities mature. While post-quantum cryptography can protect future transactions, no existing solution can retroactively secure data already recorded on public distributed ledgers.
53. In addition to technological disruption risks, the concentration of advanced quantum computing capabilities among a limited number of technologically advanced states introduces a potential asymmetry dimension. If quantum decryption were to become

⁵² Law Society of Ireland Gazette. (28 July 2025). Crypto remains high-risk sector for AML, EBA finds. Law Society of Ireland Gazette. <https://www.lawsociety.ie/gazette/top-stories/2025/july/crypto-remains-high-risk-sector-for-aml--eba/>

⁵³ L., P. (14 September 2025). ChatGPT 5 sets timeline when quantum computers will break Bitcoin’s encryption. Finbold. <https://finbold.com/chatgpt-5-sets-timeline-when-quantum-computers-will-break-bitcoins-encryption/>

⁵⁴ Mascelli, J. and Rodden, M. (September 2025). “Harvest Now Decrypt Later”: Examining post-quantum cryptography and the data privacy risks for distributed ledger networks. Board of Governors of the Federal Reserve System (FEDS Working Paper). <https://www.federalreserve.gov/econres/feds/harvest-now-decrypt-later-examining-post-quantum-cryptography-and-the-data-privacy-risks-for-distributed-ledger-networks.htm>

operationally viable before a global cryptographic transition is completed, certain cryptocurrency wallets could be exposed to unauthorized access. Such a scenario would carry implications not only for financial stability but also for broader strategic positioning within digital financial infrastructures⁵⁵.

54. In October 2025, BTQ Technologies announced a quantum-resistant implementation of Bitcoin based on post-quantum cryptographic standards developed by the National Institute of Standards and Technology (NIST). The announcement reflects ongoing industry efforts to anticipate future cryptographic vulnerabilities, although large-scale deployment and long-term validation remain subject to further technical assessment⁵⁶.
55. In parallel, Google unveiled the Agent Payments Protocol (AP2), a system designed to enable artificial intelligence applications to send and receive payments, including stablecoins pegged to sovereign currencies. Developed in collaboration with Coinbase, the Ethereum Foundation, and more than 60 financial and technology companies, AP2 seeks to standardize transactions between AI agents and merchants. The protocol promotes interoperability, compliance, scalability, and operational flexibility, and reflects emerging experimentation at the intersection of artificial intelligence and digital payment infrastructures⁵⁷.

Cryptocurrencies and Transnational Organized Crime

56. The same technological characteristics that enable legitimate innovation may also be exploited by transnational organized criminal networks seeking to conceal financial flows, facilitate illicit markets, and exploit the borderless nature of blockchain-based systems.
57. On 28 March 2024, the Financial Action Task Force (FATF) published a table⁵⁸ outlining the implementation status of FATF standards on virtual assets and virtual asset service providers (VASPs), referred to as Recommendation 15, across its 48 members and 20 additional jurisdictions identified as having “significant VASP activity.” Previous FATF assessments, including the most recent report of 2023, identified substantial delays in the full implementation of Recommendation 15.

⁵⁵ White House Archives. (July 2024). *Post-Quantum Cryptography (PQC) Report – Final* [PDF]. The White House Archives. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

⁵⁶ Swayne, M. (21 October 2025). BTQ Technologies announces quantum-safe Bitcoin using NIST-standardized post-quantum cryptography. The Quantum Insider. <https://thequantuminsider.com/2025/10/16/btq-technologies-announces-quantum-safe-bitcoin-using-nist-standardized-post-quantum-cryptography/>

⁵⁷ Finance Magnates. (16 September 2025). Google embeds stablecoin payments into AI apps in Coinbase partnership. Finance Magnates. <https://www.financemagnates.com/fintech/payments/google-embeds-stablecoin-payments-into-ai-apps-in-coinbase-partnership/>

⁵⁸ Financial Action Task Force (FATF). (March 2024). Virtual assets regulatory snapshot: Jurisdictions. Financial Action Task Force (FATF). <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html>

58. Elliptic's July 2025 report, *The State of Cross-Chain Crime 2025*, estimates that more than £15 billion in illicit funds were transferred through decentralized exchanges (DEXs), cross-chain bridges, and swap services, representing a threefold increase compared to 2023. Approximately 12% (around £1.7 billion) of these flows were linked to cyber operations attributed to North Korean actors, while £270 million were associated with Iranian cryptocurrency services subject to United States sectoral sanctions. The report further highlights the increasing structural complexity of investigations: one-third (33%) involved more than three blockchains, 27% spanned more than five, and one-fifth (20%) extended across more than ten, underscoring the growing sophistication and fragmentation of illicit financial networks⁵⁹.
59. In September 2025, more than 400 police chiefs and senior law enforcement officials from 53 countries and 13 international organizations convened at Europol headquarters in The Hague to assess emerging security threats. Discussions emphasized the increasing exploitation of digital technologies in both violent and financial crime. Transnational organized crime groups increasingly exploit digital financial services, including virtual IBANs, decentralized platforms, crypto-assets, and fintech tools. These networks frequently integrate cyber-enabled operations, financial fraud, money laundering, and terrorist financing within the same illicit financial ecosystem. Identified challenges included shortages of specialized investigative expertise, limited blockchain forensic capabilities, and obstacles to cross-border investigations, particularly in jurisdictions with weaker anti-money laundering (AML) standards. Enhanced resource sharing, expanded training, and strengthened public-private partnerships were identified as necessary measures to improve information exchange and early-warning mechanisms⁶⁰.
60. Eurojust coordinated, in September 2025, a large-scale operation targeting a cryptocurrency fraud exceeding €100 million across Europe. Initiated at the request of Spanish and Portuguese authorities, the operation resulted in the arrest of five suspects, including the alleged ringleader. The scheme, active since 2018, affected victims in 23 countries. The coordinated effort represented one of the most significant cross-border enforcement actions against cryptocurrency fraud⁶¹.

⁵⁹ Elliptic. (16 July 2025). Cross-chain crime surges past \$21 billion, Elliptic report reveals. Elliptic. <https://www.elliptic.co/media-center/cross-chain-crime-surges-past-21-billion-elliptic-report-reveals>

⁶⁰ Europol. (September 2025). Crypto-enabled money laundering to online recruitment of minors: European police chiefs tackle criminal threats. Europol. <https://www.europol.europa.eu/media-press/newsroom/news/crypto-enabled-money-laundering-to-online-recruitment-of-minors-european-police-chiefs-tackle-criminal-threats>

⁶¹ Eurojust. (23 September 2025). Eurojust coordinates action to halt cryptocurrency fraud over €100 million across Europe. Eurojust. <https://www.eurojust.europa.eu/news/eurojust-coordinates-action-halt-cryptocurrency-fraud-over-100-million-euros-across-europe>

61. On 29 September 2025, the Metropolitan Police in the United Kingdom announced the seizure of more than £5.5 billion in Bitcoin following a seven-year investigation. A Chinese national admitted to offenses relating to the acquisition and possession of illicit cryptocurrency. British authorities described the operation as among the largest cryptocurrency seizures recorded to date⁶².
62. In October 2025, the United States Department of Justice announced the seizure of approximately \$15 billion in bitcoin linked to the leader of the Prince Group, a criminal organization responsible for large-scale cryptocurrency investment fraud targeting victims in the United States. Declassified court documents indicate that the Cambodia-based Prince Group operates more than 100 shell and holding companies across over 30 countries. Chen Zhi, also known as Vincent, identified as president of the organization, remains at large. In coordination with the United Kingdom’s Foreign, Commonwealth and Development Office (FCDO), the United States Treasury’s Office of Foreign Assets Control (OFAC) imposed sanctions on Chen Zhi and 146 affiliated individuals and entities⁶³⁻⁶⁴.
63. North Korean state-linked actors have begun leveraging public blockchains to disseminate malware and conduct cryptocurrency theft operations. Researchers have described this as one of the first documented instances. On 16 October 2025, Google’s security team reported that a Pyongyang-affiliated group, designated UNC5342, deployed a method known as “EtherHiding” to embed malicious code within smart contracts on decentralized networks, including Ethereum and BNB Smart Chain⁶⁵.
64. In November 2025, European authorities dismantled one of the continent’s largest cryptocurrency fraud and money-laundering networks, resulting in nine arrests across Cyprus, Spain, and Germany. The network allegedly defrauded hundreds of investors through fraudulent cryptocurrency platforms, misappropriating more than €600 million. Funds were subsequently laundered via blockchain mechanisms, significantly complicating recovery efforts. Eurojust coordination played a central role in the operation⁶⁶.

⁶² Metropolitan Police Service. (29 September 2025). Woman convicted following world’s largest seizure. Metropolitan Police Service. <https://news.met.police.uk/news/woman-convicted-following-worlds-largest-seizure-501569>

⁶³ U.S. Department of the Treasury. (14 October 2025). Press release SB-0278. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/sb0278>

⁶⁴ UK Government. (14 October 2025). UK and US take joint action to disrupt major online fraud network. Government of the United Kingdom. <https://www.gov.uk/government/news/uk-and-us-take-joint-action-to-disrupt-major-online-fraud-network>

⁶⁵ Google Cloud. (17 October 2025). DPRK adopts EtherHiding. Google Cloud. <https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding>

⁶⁶ OCCRP. (04 November 2025). Europe-wide crackdown targets crypto fraud, €600m stolen. OCCRP. <https://www.occrp.org/en/news/europe-wide-crackdown-targets-crypto-fraud-600m-euros-stolen>

65. A British court sentenced, in November 2025, Zhimin Qian, a Chinese national, to 11 years and eight months' imprisonment for laundering \$7.3 billion in a cryptocurrency fraud scheme affecting approximately 128,000 victims in China. Law enforcement authorities described one of the largest seizures of its kind reported in the United Kingdom⁶⁷.
66. International cooperation has yielded measurable enforcement outcomes. The Chainalysis Crypto Crime Report 2025 indicates that in 2024, illicit cryptocurrency addresses received \$40.9 billion, representing a decline compared to revised historical estimates, although the report emphasizes that these figures remain minimum calculations. However, the report notes that these figures represent minimum estimates based on identified addresses and that 2024 may ultimately represent a record year for illicit inflows⁶⁸.
67. The incorporation of artificial intelligence into cryptocurrency-related criminal activity has increased investigative complexity in several documented cases. Generative AI is being used to enhance traditional fraud schemes, including identity theft through deepfakes and synthetic identities, with growing technical sophistication.
68. The expanding adoption of privacy-enhancing cryptocurrencies presents an additional challenge for regulators and law enforcement agencies. Unlike most public blockchain networks, where transactions remain permanently visible and can often be analyzed using blockchain forensic tools, privacy-focused cryptocurrencies are specifically designed to limit the traceability of transactions and the identification of participants. Monero, the most widely used privacy coin, employs cryptographic techniques such as ring signatures, stealth addresses, and confidential transactions to conceal the identities of senders and recipients, as well as transaction amounts⁶⁹. Other privacy-oriented cryptocurrencies, including Zcash, provide users with optional privacy features through advanced zero-knowledge cryptography. These technologies may offer legitimate benefits by protecting financial privacy, commercial confidentiality, and individual security in environments where transaction transparency could expose users to unnecessary risks⁷⁰. At the same time, their enhanced anonymity significantly complicates blockchain investigations and the recovery of illicit assets, increasing their attractiveness for certain forms of transnational organized

⁶⁷ Security Affairs. (12 November 2025). \$7.3b crypto laundering: Bitcoin Queen sentenced to 11 years in UK. Security Affairs. <https://securityaffairs.com/184521/cyber-crime/7-3b-crypto-laundering-bitcoin-queen-sentenced-to-11-years-in-uk.html>

⁶⁸ Chainalysis. (15 January 2025). 2025 crypto crime report introduction. Chainalysis. <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>

⁶⁹ Financial Action Task Force (FATF). (28 October 2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Financial Action Task Force. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>

⁷⁰ Europol. (28 April 2026). *IOCTA 2026: The Evolving Threat Landscape – How Encryption, Proxies and AI Are Expanding Cybercrime*. Europol. <https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape>

crime, money laundering, ransomware operations, sanctions evasion, and illicit transactions conducted through dark web marketplaces. The resulting regulatory challenge lies in balancing the legitimate right to financial privacy with the need to preserve effective financial transparency, law enforcement capabilities, and the integrity of the international financial system⁷¹⁻⁷².

69. Cross-chain bridges and DeFi protocols are increasingly exploited to transfer funds across multiple blockchain networks, thereby complicating traceability and facilitating the circumvention of conventional compliance frameworks⁷³.
70. The development of common standards, strengthened international cooperation, and expanded technical capacity were emphasized during the 9th Global Conference on Criminal Finance and Crypto-Assets, organized by Europol, UNODC, and the Basel Institute on Governance, held in Vienna on 28-29 October 2025. Cryptocurrency-related criminal activity poses risks extending to drug trafficking, terrorist financing, sanctions evasion, and broader financial system integrity⁷⁴.

Cryptocurrencies and International Sanctions

71. Beyond their use by organized criminal networks, cryptocurrencies are increasingly influencing the implementation and effectiveness of international sanctions, providing sanctioned actors with additional mechanisms through which financial transactions may be adapted under conditions of sustained economic pressure.
72. The increasing integration of cryptocurrencies into the global financial system has introduced additional complexities to the implementation and enforcement of international sanctions. While digital assets remain a relatively limited component of overall illicit finance, their borderless and decentralized characteristics have created new opportunities for sanctioned actors to adapt financial networks and reduce reliance on conventional banking infrastructures. As a result, cryptocurrencies have become an increasingly relevant consideration within the broader evolution of international sanctions regimes and contemporary economic statecraft. In this context, a report published by the Parliamentary Assembly of the Mediterranean (PAM) in June 2026 examined how the Russian Federation,

⁷¹ AMLCube. (18 November 2024). What are privacy coins and how they are used in money laundering. AMLCube.

<https://www.amlcube.com/post/what-are-privacy-coins-and-how-they-are-used-in-money-laundering>

⁷² Chainalysis. (n.d.). *Chainalysis Blog*. Chainalysis. <https://www.chainalysis.com/blog/>

⁷³ UK Government. (July 2025). OFSI cryptoassets threat assessment. Government of the United Kingdom.

https://assets.publishing.service.gov.uk/media/687e6362791bb4d8c309a06e/OFSI_Cryptoassets_Threat_Assessment.pdf

⁷⁴ Europol. (28–29 October 2025). Global experts advance joint fight against crypto-enabled crime. Europol.

<https://www.europol.europa.eu/media-press/newsroom/news/global-experts-advance-joint-fight-against-crypto-enabled-crime>

the Islamic Republic of Iran, and the Democratic People's Republic of Korea have increasingly adapted their financial and commercial infrastructures to mitigate the effects of international sanctions while sustaining their economies, supporting military capabilities, and, in the case of the Russian Federation, continuing its illegal war of aggression against Ukraine⁷⁵. While cryptocurrencies are used in money laundering, sanctions evasion, and terrorist financing, the United States Treasury's 2024 National Money Laundering Risk Assessment identifies cash as the primary medium for illicit finance. Similarly, the 2024 National Terrorist Financing Risk Assessment notes that terrorist organizations continue to rely predominantly on conventional financial channels despite exploring virtual assets⁷⁶. According to the 2026 National Money Laundering Risk Assessment, the volume of money laundering conducted through digital assets remains well below that conducted through fiat currency. However, certain illicit actors, particularly those involved in crypto-native crimes, may rely primarily on digital assets in the laundering process. For crimes such as certain investment scams and ransomware attacks, digital assets are the primary means through which funds are generated and laundered. For others, including drug trafficking, fraud, and professional money laundering, digital assets represent only one of several methods used to launder illicit proceeds, alongside the misuse of shell companies, bulk cash smuggling, and wire transfers⁷⁷.

73. Before examining the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea individually, it is important to recognize that the evasion of international sanctions has increasingly evolved from isolated national practices into interconnected transnational ecosystems. These networks combine traditional mechanisms, including front companies, intermediary jurisdictions, informal value-transfer systems, illicit procurement networks, and opaque commercial structures, with emerging digital financial infrastructures, cryptocurrencies, and alternative cross-border payment mechanisms. Although each country pursues distinct geopolitical and strategic objectives, their methods increasingly demonstrate common patterns of adaptation aimed at preserving economic resilience, supporting military and strategic capabilities, maintaining access to international markets, and reducing dependence on the conventional international financial

⁷⁵ Parliamentary Assembly of the Mediterranean (PAM). (8 November 2024). The Trilateral Cooperation: How the Russian Federation, Iran and North Korea Are Evading International Sanctions. Parliamentary Assembly of the Mediterranean. <https://pam.int/wp-content/uploads/2024/03/A5-PAM-Draft-Background-Note-How-the-Russian-Federation-Iran-and-North-Korea-are-evading-international-sanctions.pdf>

⁷⁶ U.S. Department of the Treasury. (February 2024). *2024 National Money Laundering Risk Assessment*. U.S. Department of the Treasury. <https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf>

⁷⁷ U.S. Department of the Treasury. (March 2026). *2026 National Money Laundering Risk Assessment*. U.S. Department of the Treasury. <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>

system. Within this broader context, cryptocurrencies should be understood as one component of an increasingly sophisticated sanctions-evasion architecture rather than as a standalone mechanism⁷⁸.

74. Since 2014, the Russian Federation has progressively adapted its financial and regulatory framework in response to successive rounds of international sanctions, developing alternative mechanisms intended to preserve cross-border financial activity despite growing restrictions. This evolution has accelerated following the full-scale invasion of Ukraine and is increasingly reflected in what has been described as a sanctions-resilient digital financial architecture built upon three interconnected pillars: central bank digital currency initiatives, industrial-scale cryptocurrency mining, and stablecoin-based payment corridors. Together, these mechanisms seek to reduce dependence on conventional financial infrastructures while strengthening Russia's capacity to conduct international transactions outside traditional sanctions-sensitive channels⁷⁹. Although international sanctions have imposed significant constraints on Russia's financial system, they have not eliminated its ability to transfer value through cryptocurrency ecosystems. Instead, digital assets have assumed an increasingly important role within Russia's broader financial adaptation strategy, with state-linked initiatives, including the A7A5 stablecoin ecosystem, illustrating the growing institutional integration of blockchain-based financial infrastructures. Consequently, sanctions targeting entities such as Garantex and the broader A7 ecosystem increasingly address financial networks that extend beyond isolated private initiatives and form part of a wider state-supported architecture designed to enhance economic resilience and facilitate cross-border financial activity under conditions of international sanctions⁸⁰.
75. Iran has operated under extensive United States sanctions for several decades. Following the U.S. withdrawal from the Joint Comprehensive Plan of Action (JCPOA) in 2018, the reimposition of sanctions significantly restricted Iran's access to the international financial system by disconnecting Iranian banks from SWIFT, limiting correspondent banking relationships, and prohibiting transactions involving the U.S. dollar through financial infrastructures linked to the United States. In response, Iran continued to rely on traditional

⁷⁸ Parliamentary Assembly of the Mediterranean (PAM). (8 November 2024). The Trilateral Cooperation: How the Russian Federation, Iran and North Korea Are Evading International Sanctions. Parliamentary Assembly of the Mediterranean. <https://pam.int/wp-content/uploads/2024/03/A5-PAM-Draft-Background-Note-How-the-Russian-Federation-Iran-and-North-Korea-are-evading-international-sanctions.pdf>

⁷⁹ Conway, C. et al. (12 February 2026). Blockchain Statecraft: Russia's Secret War for Financial Sovereignty. Davis Center for Russian and Eurasian Studies, Harvard University. <https://daviscenter.fas.harvard.edu/insights/blockchain-statecraft-russias-secret-war-financial-sovereignty>

⁸⁰ Saiz Erausquin, G. (20 February 2026). The Shadow Crypto Economy Feeding Russia's War Machine. Royal United Services Institute (RUSI). <https://www.rusi.org/explore-our-research/publications/commentary/shadow-crypto-economy-feeding-russias-war-machine>

sanctions-evasion mechanisms, including barter arrangements, local-currency settlements, gold transfers, and hawala networks. More recently, however, stablecoins, particularly USDT, have emerged as an additional instrument for facilitating cross-border financial activity⁸¹. By combining dollar-denominated value with blockchain-based transfer mechanisms, stablecoins provide a means of conducting international transactions with reduced reliance on conventional banking channels targeted by sanctions. Current research identifies five principal mechanisms through which cryptocurrencies are utilized within the Iranian ecosystem, often simultaneously: import payment settlement, which represents the primary use case, export revenue conversion, intermediary settlement networks, mining revenue monetization, and sanctions-related procurement activities. Recent guidance issued by the U.S. Financial Crimes Enforcement Network (FinCEN) further highlights the increasing role of digital assets, stablecoins, shell companies, and intermediary financial networks in supporting procurement and sanctions-evasion activities associated with the Islamic Revolutionary Guard Corps (IRGC)⁸².

76. The Democratic People's Republic of Korea (DPRK), largely isolated from the international financial system and subject to extensive international sanctions, has increasingly incorporated cryptocurrency-related cyber operations into its broader sanctions-evasion strategy. The decentralized, borderless, and pseudonymous characteristics of digital assets provide opportunities to generate and transfer value outside conventional financial channels targeted by international sanctions. According to international assessments, proceeds derived from cryptocurrency thefts are believed to contribute to the financing of the DPRK's strategic priorities, including its nuclear weapons and ballistic missile programmes⁸³. To conceal the origin and destination of illicit proceeds, DPRK-linked actors employ increasingly sophisticated laundering techniques, including the use of cross-chain bridges, cryptocurrency mixers, decentralized finance (DeFi) services, over-the-counter brokers, and the dispersal of stolen assets across large numbers of blockchain addresses before conversion into fiat currency through networks of foreign

⁸¹ Mills, R. et al. (2026). *Sanctions, Stablecoins, and the Future of Financial Statecraft*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6362678

⁸² Financial Crimes Enforcement Network (FinCEN). (11 May 2026). Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds. U.S. Department of the Treasury. <https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf>

⁸³ Multilateral Sanctions Monitoring Team (MSMT). (22 October 2025). *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities (MSMT/2025/2)*. Multilateral Sanctions Monitoring Team. [https://msmt.info/view/save/2025/10/22/26294780-c396-407d-bb33-88afe988cd96-The_DPRK%E2%80%99s_Violation_and_Evasion_of_UN_Sanctions_through_Cyber_and_Information_Technology_Worker_Activities_\(MSMT_2025_2\).pdf](https://msmt.info/view/save/2025/10/22/26294780-c396-407d-bb33-88afe988cd96-The_DPRK%E2%80%99s_Violation_and_Evasion_of_UN_Sanctions_through_Cyber_and_Information_Technology_Worker_Activities_(MSMT_2025_2).pdf)

facilitators⁸⁴. Recent international assessments further indicate that cryptocurrency theft has evolved into one of the DPRK's most significant sources of foreign currency, underscoring the growing strategic importance of digital assets within the country's broader sanctions-evasion architecture⁸⁵.

77. The development of automated smart contracts and permissionless platforms complicate the effective restriction of access to sanctioned entities. Sanctions targeting Iran have coincided with increased exploration of cryptocurrency mechanisms aimed at mitigating restrictions on access to the international banking system. North Korea has been reported to rely on cyber operations and cryptocurrency theft. In the context of the Russia-Ukraine conflict, cryptocurrencies have been used both to bypass financial restrictions and to facilitate humanitarian assistance and fundraising initiatives.
78. An October 2025 report issued by the Multilateral Sanctions Monitoring Team (MSMT), entitled *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities* (MSMT_2025_2)⁸⁶, documents the Democratic People's Republic of Korea's use of cyber-enabled operations to circumvent international sanctions. The report assesses that between January 2024 and September 2025, approximately \$2.84 billion in cryptocurrency was stolen through cyber-enabled operations attributed to the DPRK, estimating that such activities may have accounted for roughly one-third of the country's foreign currency earnings in 2024.
79. The Financial Action Task Force (FATF), in its June 2025 report entitled *Complex Proliferation Financing and Sanctions Evasion Schemes*⁸⁷, identifies systemic vulnerabilities within the global financial architecture that facilitate the financing of weapons of mass destruction. The report identifies the People's Republic of Korea as a central actor in such proliferation-related schemes. Among the primary mechanisms of sanctions evasion and export-control circumvention are the use of virtual assets and emerging technologies, intermediary networks, concealment of beneficial ownership structures, and exploitation of maritime and shipping channels.

⁸⁴ Conway, C. et al. (12 February 2026). *Blockchain Statecraft: Russia's Secret War for Financial Sovereignty*. Davis Center for Russian and Eurasian Studies, Harvard University. <https://daviscenter.fas.harvard.edu/insights/blockchain-statecraft-russias-secret-war-financial-sovereignty> (daviscenter.fas.harvard.edu)

⁸⁵ Esebame, D. (2 October 2025). *North Korea and Crypto: Hacks, Sanctions, and Stolen Billions*. FinanceFeeds. <https://financefeeds.com/north-korea-and-crypto-hacks-sanctions/>

⁸⁶ MSMT. (22 October 2025). *The DPRK's violation and evasion of UN sanctions through cyber and information technology worker activities* (MSMT 2025 2). [https://msmt.info/view/save/2025/10/22/26294780-c396-407d-bb33-88afe988cd96-The DPRK%E2%80%99s Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities \(MSMT 2025 2\).pdf](https://msmt.info/view/save/2025/10/22/26294780-c396-407d-bb33-88afe988cd96-The_DPRK%E2%80%99s_Violation_and_Evasion_of_UN_Sanctions_through_Cyber_and_Information_Technology_Worker_Activities_(MSMT_2025_2).pdf)

⁸⁷ Financial Action Task Force (FATF). (20 June 2025). *Complex proliferation financing & sanction evasion schemes*. Financial Action Task Force (FATF). <https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html>

80. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) has sought to mitigate the misuse of digital assets in sanctions evasion. Particular attention has been directed toward preventing sanctioned jurisdictions notably the Russian Federation following its invasion of Ukraine in February 2022 from leveraging cryptocurrency-based mechanisms to bypass restrictions. SWIFT supports financial institutions through its Customer Security Program and Customer Security⁸⁸ Controls Framework⁸⁹, emphasizing the importance of maintaining interconnected global financial flows amid geopolitical tensions. Fragmentation of financial infrastructures may pose systemic risks to global financial integration. Media reporting indicates that Russia has reportedly utilized Bitcoin, Ether, and stablecoins such as Tether (USDT) in oil trade transactions with China and India in oil trade transactions reportedly valued at approximately \$192 billion. Cryptocurrencies enable rapid settlement compared to traditional cross-border transfers and offer varying degrees of pseudonymity, raising concerns related to money laundering, transnational organized crime, and other forms of illicit financial activity.
81. In July 2025, the European Union imposed sanctions on nine individuals and six entities accused of using cryptocurrencies to circumvent restrictions, channel funds, and support pro-Russian propaganda and electoral interference activities. The decision reflects an evolving enforcement approach toward targeting financial infrastructures underpinning long-term influence operations⁹⁰.
82. The European Union's 19th sanctions package against Russia includes prohibitions on certain cryptocurrency transactions involving Russian residents and restrictions on dealings with foreign banks connected to alternative Russian payment systems⁹¹. The 20th sanctions package includes a comprehensive sectoral ban on trading with any Russian cryptocurrency service provider, as well as with any decentralized platform used to circumvent sanctions. The measures also prohibit the use (and support) of the RUBx cryptocurrency, a stablecoin pegged to the ruble, as well as the digital ruble⁹².
83. On 14 August 2025, the United States Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions targeting transactions exceeding \$100 million in value

⁸⁸ SWIFT. (n.d.). Customer security programme. SWIFT. <https://www.swift.com/myswift/customer-security-programme>

⁸⁹ SWIFT. (n.d.). Understand controls. SWIFT. <https://www.swift.com/myswift/customer-security-programme/understand-controls>

⁹⁰ Cryptonomist. (16 July 2025). Cryptocurrencies and EU sanctions: New measures against disinformation. Cryptonomist. <https://en.cryptonomist.ch/2025/07/16/cryptocurrencies-and-eu-sanctions-new-measures-against-disinformation/>

⁹¹ Cointelegraph. (19 September 2025). EU sanctions block Russian crypto platforms, drone strikes. Cointelegraph. <https://cointelegraph.com/news/eu-sanctions-block-russian-crypto-platforms-drone-strikes>

⁹² European Commission. (23 April 2026). EU Adopts 20th Package of Sanctions Against Russia. Directorate-General for Financial Stability, Financial Services and Capital Markets Union, European Commission. https://finance.ec.europa.eu/news/eu-adopts-20th-package-sanctions-against-russia-2026-04-23_en

on the cryptocurrency exchange Garantex Europe OU (Garantex), which had facilitated ransomware groups and broader transnational organized crime networks⁹³.

84. On 16 September 2025, the United States Treasury sanctioned two Iranian financiers and more than a dozen individuals and entities in Hong Kong and the United Arab Emirates⁹⁴, for allegedly coordinating cryptocurrency transfers worth approximately \$100 million derived from Iranian oil sales for the benefit of the Tehran government and military. So-called “shadow banking” networks were identified as mechanisms for sanctions evasion through shell companies and cryptocurrency transactions.
85. According to the 2026 Chainalysis Crypto Crime Report, the value received by sanctioned entities rose by 694% in 2025, bringing the total volume of illicit transactions to \$154 billion. The report indicates that state actors have increasingly integrated cryptocurrencies into their national financial infrastructures and strategic policy objectives. Iranian cryptocurrency activity is increasingly dominated by the state, with the Islamic Revolutionary Guard Corps (IRGC) and its proxy networks accounting for more than 50% of the value received in the fourth quarter of 2025, totaling more than \$3 billion in transfers over the year. The ruble-pegged stablecoin A7A5 processed \$93.3 billion in transactions in less than a year, serving as a critical bridge for Russian businesses to access global markets despite sanctions. Grinex and Meer, two exchanges created around the same time as A7A5, were sanctioned in part for facilitating activity linked to ruble-pegged stablecoins and handled at least \$4.76 billion and \$305 million in transactions, respectively, in 2025. North Korea stole more than \$2 billion in cryptocurrency in 2025. Scam networks in Southeast Asia have become an area of growing concern for international regulators, with sanctions imposed on the Prince Group and its CEO, Chen Zhi⁹⁵.
86. Within an increasingly dynamic regulatory environment, strengthening sanctions integrity requires coordinated international responses. Key priorities include enhanced blockchain analytics capable of tracing complex illicit flows; reinforced international cooperation among governments, financial institutions, and cryptocurrency service providers; regulatory innovation incorporating technology-based compliance tools such as automated transaction screening and smart-contract enforcement; systematic monitoring of digital

⁹³ U.S. Department of the Treasury. (14 August 2025). Press release SB-0225. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/sb0225>

⁹⁴ U.S. Department of State. (16 September 2025). Targeting financial network generating millions for Iranian military and additional actions in support of maximum pressure on Iran. U.S. Department of State. <https://www.state.gov/releases/office-of-the-spokesperson/2025/09/targeting-financial-network-generating-millions-for-iranian-military-and-additional-actions-in-support-of-maximum-pressure-on-iran>

⁹⁵ Chainalysis. (9 January 2026). Crypto Sanctions: 2026 Crypto Crime Report. Chainalysis. <https://www.chainalysis.com/blog/crypto-sanctions-2026/>

tools used to finance propaganda and disinformation; and maintaining an appropriate balance between technological innovation and financial security.

Cryptocurrencies and Financing Terrorism

87. While the financial use of cryptocurrencies by terrorist organizations remains comparatively limited, evolving digital financial ecosystems nevertheless present new challenges for counter-terrorism financing frameworks and international security.
88. On 20 August 2025, during a briefing to the United Nations Security Council, the Chair of the Financial Action Task Force (FATF), Elisa de Anda Madrazo, noted that in 2024 ISIL-K had increasingly relied on virtual assets for organizational transfers and the collection of international donations. The updated FATF standards were presented as supporting both national authorities and private-sector actors in monitoring developments in virtual assets and enhancing the identification of potential terrorist financing activities⁹⁶.
89. Documented investigations indicate that activities linked to the Islamic State Khurasan Province (ISKP) have been partially financed through cryptocurrency transactions. TRM Labs identified hundreds of small- to medium-sized transfers, ranging from \$100 to \$15,000, associated with ISKP-linked addresses. On-chain analysis also revealed connections between ISKP-related wallets and Syria-based fundraising efforts supporting ISIS members and affiliated families detained in camps. Additional groups, including Hamas, Gaza Now, and the Mujahideen Brigades, were reported to have received cryptocurrency donations amounting to several thousand dollars. On 27 March 2025, the United States Department of Justice announced the disruption of a financing scheme through the seizure of approximately \$201,400 in cryptocurrency held in digital wallets and accounts intended for Harakat al-Muqawama al-Islamiyya (Hamas)⁹⁷.
90. Stablecoins remain a frequently utilized instrument within terrorist financing networks. According to TRM Labs, ISKP predominantly employs stablecoins for fund transfers and storage. In autumn 2023, ISKP's official media unit initiated a donation campaign utilizing Monero, selected for its enhanced privacy features.
91. Open-source investigative reporting and selected enforcement assessments indicate that digital asset channels have, in certain instances, intersected with broader transnational

⁹⁶ Financial Action Task Force (FATF). (20 August 2025). FATF president speech to UN Security Council 2025. Financial Action Task Force (FATF). <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/FATF-president-speech-UN-security-council-2025.html>

⁹⁷ U.S. Department of Justice. (27 March 2025). Justice Department disrupts Hamas terrorist financing scheme through seizure. U.S. Department of Justice. <https://www.justice.gov/usao-dc/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure>

militant financing networks involving Hezbollah-affiliated facilitators and Iran-linked actors operating in parts of Latin America, including Venezuela. Available analyses suggest that value has at times been routed through proxy wallets, front intermediaries, and informal trade and remittance structures embedded within regional commercial ecosystems. Such configurations complicate attribution and traceability. Sanctions designations have targeted individuals and entities alleged to provide cryptocurrency-related facilitation services connected to these networks. These developments underscore the importance of strengthened cross-jurisdictional monitoring, enhanced blockchain forensic capabilities, and coordinated enforcement responses in addressing militant financing risks within crypto-asset markets⁹⁸.

Cryptocurrencies and Financing Disinformation

92. Beyond their financial and security implications, cryptocurrencies are increasingly intersecting with the information environment by facilitating certain forms of fundraising, financial intermediation, and operational support for influence activities. The convergence of political processes, disinformation campaigns, and cryptocurrency markets has introduced new dimensions of volatility within digital financial ecosystems. This interaction influences market sentiment, regulatory responses, and broader geopolitical dynamics. Traditional financial risk assessment models are increasingly insufficient to address these interdependencies. Effective strategic risk management requires the integration of geopolitical analysis, advanced sentiment monitoring, and a structured understanding of information manipulation techniques. The intersection between political influence operations, disinformation, and cryptocurrency ecosystems increasingly represents a structural feature of the contemporary digital environment.
93. Russia has increasingly incorporated cryptocurrencies into a broader strategy aimed at strengthening the resilience of financial networks supporting influence operations, fundraising activities, and other mechanisms affected by international sanctions. Rather than serving solely as a means of payment for individual operators or content producers, cryptocurrencies facilitate donations, fundraising campaigns, payments to intermediaries, digital infrastructure, and other operational activities that can be conducted with reduced reliance on conventional financial institutions. The most extensively documented example concerns cryptocurrency fundraising campaigns supporting pro-Russian military and

⁹⁸ GNET Research. (21 July 2025). Hezbollah's Latin American networks: Stablecoins, smuggling and sanctions evasion. GNET Research. https://gnet-research.org/2025/07/21/hezbollahs-latin-american-networks-stablecoins-smuggling-and-sanctions-evasion/?utm_source=chatgpt.com

propaganda ecosystems associated with the war in Ukraine. Blockchain analysis has identified substantial cryptocurrency donations directed to sanctioned organizations, military support groups, and pro-Russian media platforms, including SouthFront, illustrating how digital assets have become integrated into fundraising and operational support mechanisms⁹⁹⁻¹⁰⁰. Russia's use of cryptocurrencies should also be understood within the broader context of its hybrid influence strategy. Information operations linked to Russian state interests have been documented across multiple regions, including Ukraine, Africa, and particularly the Sahel, where military, political, and media influence increasingly intersect. At the same time, emerging sanctions-resilient payment infrastructures, including the A7 ecosystem, have begun expanding beyond Russia into African markets, illustrating how alternative financial mechanisms may complement Moscow's broader geopolitical engagement under conditions of sustained international sanctions¹⁰¹⁻¹⁰². The convergence of influence operations, alternative financial infrastructures, and sanctions resilience suggests that cryptocurrencies should not be viewed solely as financial instruments, but increasingly as components of a broader geopolitical architecture capable of supporting the operational continuity of Russian state-linked networks beyond traditional banking channels¹⁰³.

94. The Chinese case differs significantly from the Russian model. At present, publicly available evidence does not demonstrate a systematic or large-scale use of cryptocurrencies to finance Chinese disinformation campaigns. Instead, the available evidence suggests that digital assets may be employed selectively as discreet payment mechanisms supporting specific influence, recruitment, or intelligence-related activities. A recent case in Taiwan, for example, alleges that cryptocurrency payments were used to finance the production of pro-Beijing media content and facilitate payments associated with efforts to obtain sensitive military information, illustrating how digital assets can serve as operational payment channels within broader influence activities¹⁰⁴. Within this context,

⁹⁹ Chainalysis Team. (30 April 2021). *U.S. Government Targets Russian Influence Operations with Cryptocurrency Nexus*. Chainalysis. <https://www.chainalysis.com/blog/ofac-fbi-russian-influence-synthetic-identity-document-vendor-sanctions/>

¹⁰⁰ Chainalysis Team. (29 July 2022). *\$2 Million and Counting: How Dozens of Pro-Russian Groups Are Using Cryptocurrency Donations to Fund the War in Ukraine*. Chainalysis. <https://www.chainalysis.com/blog/pro-russian-crypto-donations-war-in-ukraine/>

¹⁰¹ Financial Times. (20 March 2025). *Russia Uses Cryptocurrencies in Oil Trade with China and India to Circumvent Western Sanctions*. Financial Times. <https://www.ft.com/content/a9de2bb5-7bbf-4d04-9424-25d4b9cda2b6>

¹⁰² FinanceFeeds. (2 October 2025). *North Korea and Crypto: Hacks, Sanctions, and Stolen Billions*. FinanceFeeds. <https://financefeeds.com/north-korea-and-crypto-hacks-sanctions/>

¹⁰³ Center for European Policy Analysis (CEPA). (21 January 2025). *A Crypto River Runs Through It*. Center for European Policy Analysis. <https://cepa.org/article/a-crypto-river-runs-through-it/>

¹⁰⁴ Shen, T. (8 May 2026). *Taiwan News Anchor Indicted for Allegedly Taking Crypto Payments from China to Produce Propaganda, Bribe Soldiers*. The Block. <https://www.theblock.co/post/400533/taiwan-news-anchor-crypto-scandal>

cryptocurrencies should be understood less as instruments for financing large-scale disinformation infrastructures and more as flexible financial tools capable of supporting individual intermediaries, agents, or covert influence operations. Their strategic value lies in enabling relatively rapid cross-border transfers with reduced reliance on traditional banking channels, thereby increasing operational flexibility while helping to preserve a degree of separation between sponsors and operational actors.

95. Iran's use of cryptocurrencies should be understood within the broader framework of its financial resilience strategy, which seeks to mitigate the effects of international sanctions while preserving the country's capacity to sustain external operations. Publicly available evidence indicates that cryptocurrency exchanges, wallets associated with the Islamic Revolutionary Guard Corps (IRGC), front companies, and digital asset transfer networks have become increasingly integrated into mechanisms used to facilitate sanctions evasion, procure restricted goods, and transfer value outside the conventional financial system. These financial mechanisms contribute to maintaining operational flexibility despite sustained international economic pressure. Recent guidance issued by the U.S. Financial Crimes Enforcement Network (FinCEN)¹⁰⁵ highlights the role of digital assets, stablecoins, shell companies, and intermediary financial networks in supporting procurement activities associated with the IRGC. At the same time, multiple threat intelligence assessments have documented Iran's growing reliance on cyber-enabled influence operations, coordinated information campaigns, fake online personas, and IRGC-linked media networks to advance its geopolitical objectives¹⁰⁶⁻¹⁰⁷. Within this broader strategic context, cryptocurrencies should be understood not as direct instruments for financing disinformation campaigns, but as enabling financial infrastructures that strengthen Iran's capacity to sustain regional networks and a range of external activities, including influence operations, by providing payment mechanisms that reduce reliance on conventional banking channels while increasing operational flexibility, speed, and a degree of financial opacity. Consequently, cryptocurrencies reinforce the broader financial ecosystem that enables Tehran to maintain regional influence and strategic resilience under conditions of sustained international sanctions.

¹⁰⁵ Financial Crimes Enforcement Network (FinCEN). (11 May 2026). *Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds*. U.S. Department of the Treasury. <https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf>

¹⁰⁶ Watts, C. (2 May 2023). *Rinse and Repeat: Iran Accelerates Its Cyber Influence Operations Worldwide*. Microsoft On the Issues. <https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/>

¹⁰⁷ Watts, C. (6 February 2024). *Iran Accelerates Cyber Ops Against Israel from Chaotic Start*. Microsoft On the Issues. <https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>

96. As artificial intelligence expands the scale, speed, and sophistication of disinformation campaigns, mechanisms for tracing cryptocurrency-related financial flows require continued evolution. The development of advanced blockchain analytics tools seeks to address the growing complexity of funding channels in an environment characterized by deepfakes, automated bot networks, and AI-generated digital identities.
97. Since 2016, several significant cases of electoral interference have involved illicit financial infrastructures established to support influence operations. Investigative and regulatory assessments have documented sustained activity by Russian-linked networks, including the use of darknet marketplaces, non-compliant cryptocurrency mechanisms, ransomware operations, and paramilitary structures. Such activities have, in documented cases, involved the unlawful use of digital assets. TRM Labs (October 2024) identifies six major cases: the Russian Internet Research Agency (IRA) during the 2016 United States election; Project Lakhta during the 2018 United States midterm elections; the South Front disinformation campaign (2021); Task Force Rusich during the Russia-Ukraine conflict (2022); the Doppelganger campaign targeting the 2024 United States election; and the global disinformation networks associated with RT (Russia Today) and RaHDit (2024)¹⁰⁸.
98. Chainalysis, in its July 2024 report entitled *Malign Interference and Crypto*¹⁰⁹, analyzes documented cases involving the use of cryptocurrencies in financing and facilitating disinformation campaigns across multiple jurisdictions. The analysis identifies interconnected networks of state and non-state actors leveraging digital assets to disseminate coordinated false narratives, particularly in the context of major electoral processes. The findings suggest that the implications extend beyond financial tracing, highlighting the growing importance of protecting information ecosystems. Cryptocurrency payments have been employed to acquire technological infrastructure and digital services necessary for influence operations. In addition to Russia-linked South Front, the report highlights the Iranian media outlet Islamic World News, associated with the Islamic Revolutionary Guard Corps. Service providers enabling such campaigns include Ubar Store, a marketplace for compromised social media accounts, and Shinjiru, an anonymity-oriented web-hosting service, both accepting cryptocurrency payments. Advanced blockchain forensic methodologies have demonstrated capacity in certain cases to identify and map these financial flows, thereby contributing to the disruption of

¹⁰⁸ TRM Labs. (06 October 2024). The crypto election: Crypto disinformation and presidential politics. TRM Labs. <https://www.trmlabs.com/resources/blog/the-crypto-election-crypto-disinformation-and-presidential-politics>

¹⁰⁹ Chainalysis. (24 July 2024). Malign interference and crypto. Chainalysis. <https://www.chainalysis.com/blog/malign-interference-and-crypto/>

coordinated influence networks. The dismantling of the 911 S5¹¹⁰ botnet is cited as a case study illustrating the operational effectiveness of such investigative techniques.

99. The United States Department of the Treasury's Office of Foreign Assets Control (OFAC) has designated individuals and entities and entities involved in cryptocurrency-enabled disinformation operations¹¹¹. Designations include Russian nationals associated with the Internet Research Agency (September 2020), including linked cryptocurrency addresses; South Front (April 2021), whose affiliated digital wallets were used for donations; Task Force Rusich (September 2022), which solicited cryptocurrency contributions; and individuals such as Ilya Gambashidze and Nikolai Tupikin for participation in foreign disinformation activities involving digital asset transfers.
100. In July 2025, European Union sanctions addressing Russia included measures targeting cryptocurrency-related financial channels associated with disinformation and influence operations. These measures marked an expanded focus on financial infrastructures that may support long-term influence activities. Among the individuals designated was Simeon Boikov (known as AussieCossack¹¹²), who was alleged to have utilized cryptocurrency exchanges operating without fully Know Your Customer (KYC) controls and to have accessed funds through cash-to-crypto services and darknet-linked marketplaces. European Union and United Kingdom measures also designated the company A7 000 in connection with alleged electoral interference activities in Moldova. Ilan Shor, identified as founder, had previously been associated with vote-buying allegations during the 2024 Moldovan presidential election and European Union accession referendum. Public reporting estimated that approximately \$1 billion was transferred from Moldovan banks. The ruble-pegged stablecoin A745¹¹³ was reported to have formed part of cross-border payment mechanisms emerging after Russia's invasion of Ukraine in February 2022. The Grinex and A7A5 platforms have been reported in connection with trade routes involving dual-use goods transiting through Central Asia.

¹¹⁰ The Hacker News. (30 May 2024). US dismantles world's largest 911 S5. The Hacker News. <https://thehackernews.com/2024/05/us-dismantles-worlds-largest-911-s5.html>

¹¹¹ U.S. Department of the Treasury. (20 March 2024). Treasury sanctions Russian nationals Ilya Andreevich Gambashidze and Nikolai Aleksandrovich Tupikin for facilitating malign influence efforts (including designated cryptocurrency addresses). U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy2195>

¹¹² TRM Labs. (15 July 2025). EU sanctions Aussie Cossack and A7 for Russian election interference and disinformation activity. TRM Labs. <https://www.trmlabs.com/resources/blog/eu-sanctions-aussie-cossack-and-a7-for-russian-election-interference-and-disinformation-activity>

¹¹³ TRM Labs. (14 August 2025). Garantex, GRINEX, and the A7A5 token: A deep dive into sanctions evasion networks. TRM Labs. <https://www.trmlabs.com/resources/blog/garantex-grinex-and-the-a7a5-token-a-deep-dive-into-sanctions-evasion-networks>

Cryptocurrencies and the Dark Web

101. The relationship between cryptocurrencies and the dark web represents one of the most visible examples of how digital financial innovation can intersect with illicit online ecosystems. Cryptocurrencies have become a foundational component of the Dark Web economy, functioning both as a medium of exchange and as an instrument of concealment. Within shadow financial ecosystems, digital assets facilitate transactions between anonymous actors engaged in espionage, spyware development, illicit trade, and other forms of black-market activity, providing the liquidity and pseudonymity necessary for such operations¹¹⁴.
102. Bitcoin remains the most widely used digital currency in general transactions due to its global accessibility and market penetration. However, the transparency of its distributed ledger allows for partial traceability. By contrast, Monero has emerged as the preferred instrument for transactions requiring enhanced privacy. Its use of ring signatures, stealth addresses, and encrypted transaction values obscures the identities of counterparties and conceals transaction amounts¹¹⁵. These technical characteristics have contributed to Monero's adoption among ransomware operators, spyware vendors, and illicit data brokers seeking financial anonymity. Stablecoins such as Tether (USDT) are also increasingly utilized, combining relative price stability with blockchain-based pseudonymity, thereby supporting illicit online commerce and value storage¹¹⁶.
103. The regulatory response to anonymity-enhancing cryptocurrencies has introduced additional structural tension within the ecosystem. Increasing compliance pressures have led several regulated exchanges to delist privacy-focused assets, including Monero, in order to mitigate anti-money laundering and counter-terrorist financing exposure. This trend illustrates the growing divergence between anonymity-driven technological innovation and regulatory imperatives for transparency. As access to privacy coins through formal financial gateways narrows, activity may migrate toward decentralized or unregulated platforms, reinforcing the bifurcation between compliant and opaque financial infrastructures¹¹⁷.

¹¹⁴ Owen, A., Dawson, G., & Reed, O. (1 August 2025). *Dark web marketplaces and the role of cryptocurrency in criminal financial transactions*. ResearchGate. https://www.researchgate.net/publication/394471483_Dark_Web_Marketplaces_and_the_Role_of_Cryptocurrency_in_Criminal_Financial_Transactions

¹¹⁵ DarkInformer. (4 September 2025). *Monero vs Bitcoin: Privacy comparison for dark web users*. Darknet Review. <https://darknetreview.com/monero-vs-bitcoin-privacy-comparison-for-dark-web-users/>

¹¹⁶ Bui, L. (21 March 2025). *Bitcoin not "the king" in the dark web anymore*. BeInCrypto. <https://beincrypto.com/bitcoin-not-the-king-dark-web/>

¹¹⁷ Financial Action Task Force (FATF). (28 October 2021). *Guidance on a risk-based approach for virtual assets and virtual asset service providers*. Financial Action Task Force (FATF). <https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html>

104. A structural vulnerability of cryptocurrencies lies in their code-based architecture rather than in tangible asset backing. Compromise of underlying protocols, digital wallets, or smart contracts, whether through hacking, exploitation, or intentional manipulation may result in altered balances, asset diversion, or obfuscated records, enabling rapid concealment or transfer of value. This intrinsic exposure to software risk enhances their attractiveness within dark web ecosystems, where actors exploit technical weaknesses to convert, obscure, or dissipate illicit proceeds with speed and relative anonymity.
105. Automated protocols and decentralized exchanges have transformed fund flows within concealed markets. Assets may be transferred across multiple blockchains within seconds, converted from Bitcoin into privacy coins or stable assets, and routed through cross-chain bridges¹¹⁸. Such mechanisms fragment transactional trails across distributed ledgers¹¹⁹, creating layered obfuscation that complicates forensic analysis and enables sophisticated digital laundering structures¹²⁰.
106. Empirical enforcement actions have confirmed the structural scale of cryptocurrency-enabled dark web marketplaces. The dismantling of Hydra Market by U.S. and German authorities revealed a platform that facilitated billions of dollars in cryptocurrency transactions while providing integrated laundering services, including crypto-to-fiat exchange mechanisms. Such platforms operate not merely as trading venues for illicit goods, but as comprehensive financial infrastructures embedded within broader criminal economies¹²¹.
107. The dismantling of AlphaBay in 2017, followed by the rapid reconstitution of successor platforms, established a recurring enforcement cycle later observed in operations against Hydra and other major darknet markets, as documented by Europol assessments¹²².
108. In parallel, anonymizing infrastructures such as cryptocurrency mixing services have been formally designated by sanctions authorities for facilitating large-scale illicit finance. The U.S. Department of the Treasury's sanctioning of the Tornado Cash mixer underscored how decentralized obfuscation tools can be exploited to launder substantial volumes of

¹¹⁸ Elliptic. (2025). *The state of cross-chain crime 2025*. Elliptic.

<https://www.elliptic.co/hubfs/The%20state%20of%20cross-chain%20crime%202025/The%20state%20of%20cross-chain%20crime%202025%20-%20FINAL.pdf>

¹¹⁹ Yun, Y. (16 July 2025). *Crosschain swaps move \$21B in illicit funds, up 200% in two years — Elliptic*. Cointelegraph. <https://cointelegraph.com/news/crosschain-swaps-move-21b-illicit-funds-up-200-two-years-elliptic>

¹²⁰ Merkle Science. (06 July 2023). *Chain hopping: The future of crypto money laundering*. Merkle Science. <https://knowledgebase.merklescience.com/security-risk/chain-hopping-the-future-of-crypto-money-laundering>

¹²¹ U.S. Department of the Treasury. (05 April 2022). Press release JY0701. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy0701>

¹²² Europol. (20 July 2017). Massive blow to criminal dark web activities after globally coordinated operation. Europol. <https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>

digital assets, including funds linked to sanctioned actors and other high-risk entities. Beyond criminal commerce, darknet financial infrastructures have also intersected with sanctions evasion architectures, providing liquidity channels and obfuscation mechanisms that may be exploited by sanctioned actors seeking to bypass conventional financial controls. These developments illustrate the institutionalization of financial anonymity services within dark web and transnational organized crime ecosystems¹²³.

109. Cryptocurrency infrastructures have also facilitated the emergence of self-contained digital ecosystems operating as parallel economies within the Dark Web. Participants impose internal fees, penalties, and governance rules while financing operations through pooled cryptocurrency reserves. These arrangements resemble forms of fiscal autonomy, granting illicit networks financial self-sufficiency and resilience against external disruption¹²⁴.
110. Contrary to perceptions of unstructured illegality, many darknet marketplaces have developed internal governance mechanisms designed to preserve transactional credibility and dispute resolution. These mechanisms frequently include escrow systems sometimes implemented through smart contracts arbitration procedures administered by platform moderators, and reputation-based scoring models that evaluate vendors and buyers. Such quasi-institutional arrangements serve to mitigate fraud risk within illicit markets and sustain transactional trust. The presence of these governance structures reinforces the characterization of darknet marketplaces as parallel digital economies rather than ad hoc criminal forums¹²⁵.
111. The intersection between cryptocurrency usage and transnational organized crime continues to expand, with both state-linked and non-state actors leveraging digital assets to finance surveillance capabilities, acquire intrusion tools, conduct cyber-enabled operations, and support intelligence-related activities outside conventional financial oversight mechanisms. The convergence of anonymity-enhancing technologies and financial decentralization has produced self-regulating digital ecosystems that challenge traditional regulatory paradigms. The distinction between financial crime and cyber-espionage is increasingly blurred, necessitating integrated intelligence coordination beyond purely

¹²³ U.S. Department of the Treasury. (08 August 2022). Press release JY0916. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy0916>

¹²⁴ U.S. Government Accountability Office. (13 December 2023). *Economic sanctions: Agency efforts help mitigate some of the risks posed by digital assets* (GAO-24-106178). <https://www.gao.gov/products/gao-24-106178>

¹²⁵ Europol. (2025). *Internet Organised Crime Threat Assessment* (IOCTA). Europol. <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment>

financial supervision frameworks¹²⁶. AI-enabled autonomous wallets and self-executing smart contracts further enable automated payment execution, ransom negotiations, and laundering processes without direct human intervention¹²⁷, marking a transition toward semi-autonomous digital criminal infrastructures¹²⁸.

112. The industrialization of transnational organized crime is increasingly reinforced through cryptocurrency-enabled business models. Ransomware-as-a-Service (RaaS) models have institutionalized cryptocurrency-based extortion by separating technical developers from operational affiliates¹²⁹, who receive payment shares in digital assets. Law enforcement and cybersecurity assessments indicate that such structures rely heavily on cryptocurrency payments routed through anonymizing tools and cross-chain mechanisms, embedding ransomware operations within broader dark web financial architectures. This model illustrates the evolution from isolated criminal transactions to structured, revenue-sharing digital enterprises sustained by cryptocurrency infrastructures¹³⁰.
113. The decentralized and borderless configuration of cryptocurrency networks presents persistent challenges for law enforcement authorities responsible for combating transnational organized crime, financial crime, and cyber-enabled offences. The dismantling of illicit marketplaces or exchanges is frequently followed by the rapid emergence of successor platforms utilizing privacy-enhancing technologies and decentralized finance mechanisms that circumvent conventional tracing methodologies¹³¹. Effective responses require coordinated international action, advanced blockchain analytics capabilities, and real-time intelligence sharing¹³². The strategic implication is evident: the convergence of anonymity technologies and cryptocurrencies has enabled the Dark Web to evolve into a durable and self-sustaining digital ecosystem with independent financial resources¹³³. Absent calibrated regulation and sustained international cooperation, such

¹²⁶ Nominis. (10 October 2023). *Crypto and covert operations: How hostile state actors are weaponizing digital assets*.

Nominis. <https://www.nominis.io/post/crypto-and-covert-operations-how-hostile-state-actors-are-weaponizing-digital-assets>

¹²⁷ Decrypt. (27 October 2020). *Fully autonomous AI could control criminal networks, Europol warns*.

<https://decrypt.co/310711/fully-autonomous-ai-could-control-criminal-networks-europol>

¹²⁸ Encrypthos. (02 August 2023). *Understand how AI and blockchain create autonomous economies*.

<https://encrypthos.com/guide/understand-how-ai-and-blockchain-create-autonomous-economies/>

¹²⁹ U.S. Department of Justice. (July 2022). *ccr_0* [PDF]. U.S. Department of Justice.

https://www.justice.gov/d9/pages/attachments/2022/07/19/ccr_0.pdf

¹³⁰ ENISA (European Union Agency for Cybersecurity). (2025). *ENISA Threat Landscape 2025*. ENISA.

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

¹³¹ Merkle Science. (22 May 2025). *Cross-chain analytics: Empowering law enforcement in the age of DeFi*.

<https://www.merklescience.com/blog/cross-chain-analytics-law-enforcement-2025>

¹³² Europol. (18 April 2024). *Cryptocurrencies and financial crime: A strategic approach to ensure security*.

<https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrencies-and-financial-crime-strategic-approach-to-ensure-security>

¹³³ Braga, R. R. P., & Luna, A. A. B. (26 November 2018). *Cryptocurrencies and the Dark Web: A gateway to money laundering*. ResearchGate.

convergence may continue to undermine transparency, economic integrity, and broader security frameworks¹³⁴.

114. The structural instability of darknet marketplaces further complicates the financial architecture of illicit ecosystems. A recurring phenomenon is the so-called “exit scam,” whereby marketplace administrators intentionally terminate platform operations and abscond with escrowed cryptocurrency funds. Such collapses are not isolated incidents but represent a systemic feature of shadow digital markets, reinforcing volatility, eroding internal trust, and reshaping criminal migration patterns across successor platforms. Such dynamic reveals that even within illicit financial ecosystems, governance remains fragile and opportunistic, amplifying both operational risk and liquidity displacement across the Dark Web economy¹³⁵.

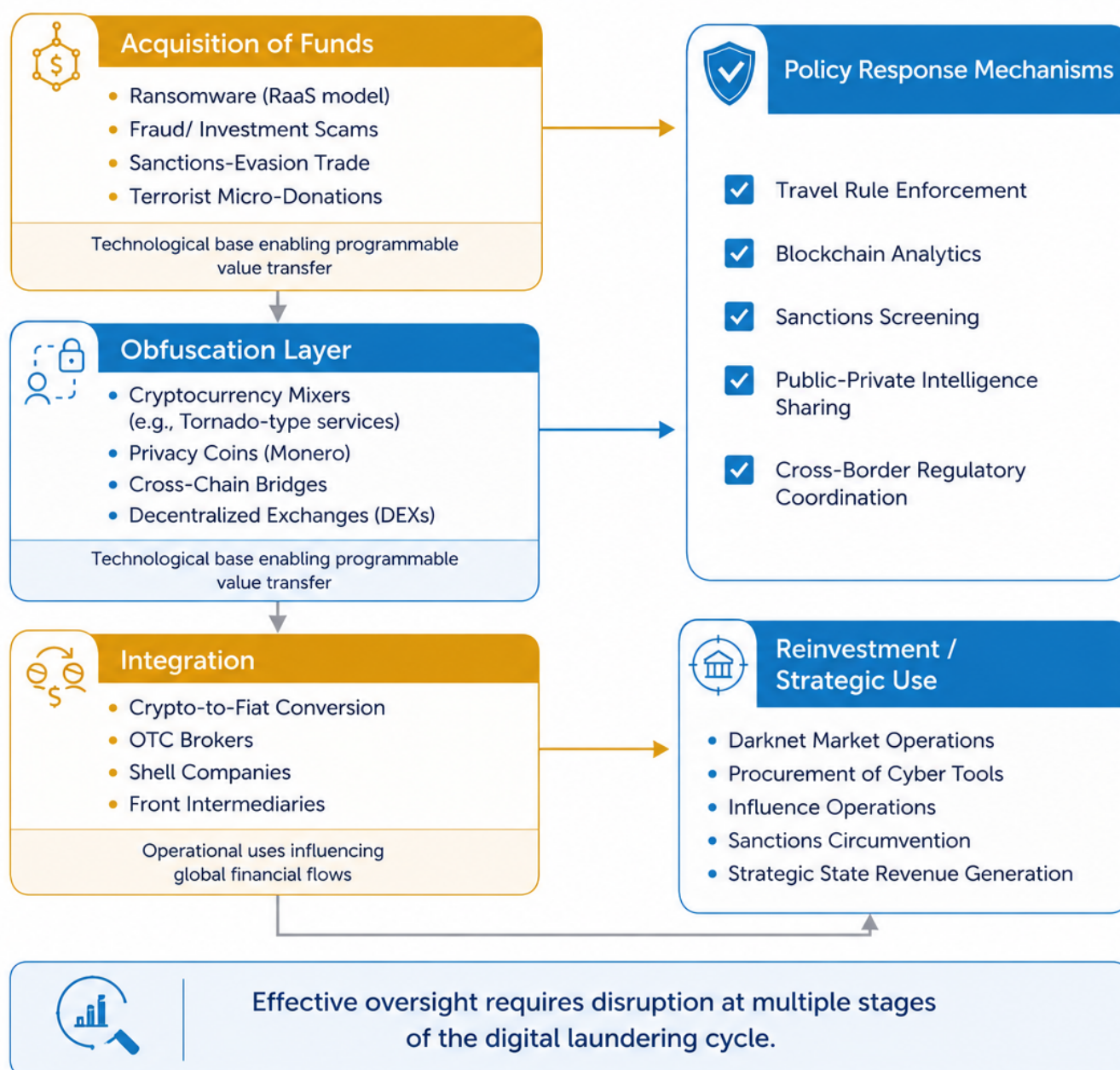
https://www.researchgate.net/publication/388871082_Cryptocurrencies_and_the_Dark_Web_A_Gateway_to_Money_Laundering

¹³⁴ El Khoury, C. (01 September 2025). *Fighting tech-fueled crime*. International Monetary Fund.

<https://www.imf.org/en/Publications/fandd/issues/2025/09/fighting-tech-fueled-crime-chady-el-khoury>

¹³⁵ U.S. Department of the Treasury. (05 April 2022). Press release JY0701. U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/jy0701>

Figure 3: Lifecycle of Illicit Cryptocurrency Flows and Points of Regulatory Intervention¹³⁶



¹³⁶ Graphic compiled by the CGS research team, based on the analysis presented in this report.

Modernization of Digital Payment Infrastructures

115. At the same time, cryptocurrencies are influencing broader discussions regarding the modernization of payment infrastructures and the future architecture of digital financial systems. The misuse of cryptocurrencies is not solely a function of digital assets themselves, but also of vulnerabilities that may exist within the broader payment ecosystem. As cryptocurrencies become increasingly integrated into global financial systems, the modernization of electronic payment infrastructures has become an equally important component of effective financial governance. While cryptocurrencies themselves are not the origin of tax evasion¹³⁷, they may further complicate financial tracing once commercial revenues have been concealed or removed from conventional accounting records. Consequently, reducing opportunities for post-transaction manipulation within existing payment infrastructures should become an important policy priority¹³⁸.
116. Many existing Point-of-Sale (POS), Electronic Point-of-Sale (EPOS), and Mobile Point-of-Sale (MPOS) systems continue to rely on paper-based receipt systems and payment architectures originally designed for traditional banking environments. Although these systems have served as the foundation of electronic commerce for decades, the growing sophistication of financial fraud, Electronic Sales Suppression (ESS)¹³⁹, and other forms of transaction manipulation suggest that legacy payment infrastructures may no longer provide the level of integrity and resilience required in an increasingly digital financial ecosystem. Governments, financial institutions, payment service providers, and technology developers should therefore accelerate the transition from paper-based receipt systems to secure digital transaction records maintained entirely within protected payment infrastructures. Such systems would significantly reduce opportunities for post-transaction manipulation, strengthen auditability, improve tax compliance, and enhance the traceability of financial flows, including those that may subsequently move into cryptocurrency ecosystems.
117. Modern digitally integrated payment technologies already demonstrate the feasibility of fully digital transaction environments¹⁴⁰, where transactions are securely recorded

¹³⁷ U.S. Department of the Treasury. (March 2026). 2026 National Money Laundering Risk Assessment. U.S. Department of the Treasury. <https://home.treasury.gov/system/files/246/2026-NMLRA.pdf>

¹³⁸ HM Revenue & Customs (HMRC). (23 June 2026). Electronic Sales Suppression: Introduction of Software Standards in EPOS/MPOS Systems. HM Revenue & Customs. <https://www.gov.uk/government/consultations/electronic-sales-suppression-introduction-of-software-standards/electronic-sales-suppression-introduction-of-software-standards-in-eposmpos-systems>

¹³⁹ Ibidem

¹⁴⁰ Nayax. (28 January 2026). Digital Receipts Framework. Nayax. <https://www.nayax.com/partner-hub/digital-receipts/>

throughout the payment lifecycle without reliance on paper-based receipts or manual post-transaction processing. Given the rapid global expansion of cryptocurrencies and other digital assets, delaying the modernization of payment infrastructures may allow legacy vulnerabilities to persist at a time when financial tracing, regulatory oversight, and tax compliance are becoming progressively more complex.

118. The continued evolution of cryptocurrency ecosystems demonstrates that addressing financial risks requires a broader approach than regulating digital assets alone. Strengthening the resilience of payment infrastructures, enhancing transaction integrity, and improving financial traceability should complement legal and regulatory measures in order to safeguard public finances and maintain confidence in an increasingly digital global economy. Against this background, understanding the emerging legal frameworks governing cryptocurrencies has become an essential component of effective financial governance.

Table 1: Cryptocurrencies & Security Risk Categories¹⁴¹

Risk Category	Mechanism	Actors Involved	Policy Implication
Ransomware (RaaS)	Crypto payments routed through mixers and cross-chain mechanisms	Criminal networks and affiliate structures	Enhanced AML enforcement and advanced blockchain analytics
Sanctions Evasion	Stablecoins, cross-chain bridges, proxy wallets	State and proxy actors	Strengthened sanctions screening and cross-border coordination
Terrorist Financing	Small-value transfers, privacy coins, proxy wallets	Non-state armed groups	Travel Rule enforcement and targeted financial monitoring
Disinformation Financing	Crypto donations, anonymous service payments	State-linked and transnational influence networks	Blockchain forensic monitoring and coordinated sanctions
Quantum Threat	Cryptographic vulnerability of legacy blockchain systems	State actors with advanced quantum capabilities	Accelerated migration to post-quantum cryptographic standards

¹⁴¹ This table summarizes the principal security risk architectures associated with cryptocurrencies as analyzed in the cybersecurity and dark web sections of the report.

Global Regulatory and Policy Landscape

119. The expansion of cryptocurrency ecosystems across financial, technological, and geopolitical domains has been accompanied by an equally significant evolution in regulatory and policy approaches at both the national and international levels.
120. The international regulatory landscape governing cryptocurrencies has entered a new phase. The principal policy debate is no longer whether digital assets should be regulated, but how regulatory frameworks should evolve to support innovation while preserving financial stability, market integrity, consumer protection, and national security¹⁴². As cryptocurrencies become increasingly integrated into payment systems, capital markets, decentralized finance (DeFi), and cross-border financial infrastructures, governments and international organizations are progressively shifting from fragmented regulatory responses toward more comprehensive, risk-based governance frameworks. Although significant differences remain among national approaches, there is growing international recognition that cryptocurrencies have become a permanent component of the global financial system and require coordinated regulatory strategies capable of addressing both technological innovation and emerging geopolitical, economic, and security challenges¹⁴³.
121. Despite increasing international convergence regarding the need to regulate cryptocurrencies, significant differences remain in the strategic objectives pursued by individual jurisdictions. Rather than adopting a single regulatory model, governments are developing frameworks that reflect their respective economic priorities, monetary strategies, financial market structures, and geopolitical interests. These differences increasingly extend beyond the regulation of cryptocurrencies themselves to encompass stablecoins, central bank digital currencies (CBDCs), tokenized financial assets, and the future architecture of digital payment systems. Recent developments illustrate this evolution. The European Union has implemented the Markets in Crypto-Assets (MiCA)¹⁴⁴ Regulation while simultaneously advancing the legislative framework for the Digital Euro¹⁴⁵, reflecting a broader strategy to strengthen monetary sovereignty, payment

¹⁴² Financial Stability Board (FSB). (17 July 2023). *FSB Finalises Global Regulatory Framework for Crypto-Asset Activities*. Financial Stability Board. <https://www.fsb.org/2023/07/fsb-finalises-global-regulatory-framework-for-crypto-asset-activities/>

¹⁴³ Hacibedel, B., & Perez-Saiz, H. (29 September 2023). *Assessing Macroeconomic Risks from Crypto Assets*. IMF Working Paper No. 2023/214. International Monetary Fund. <https://www.imf.org/en/publications/wp/issues/2023/09/30/assessing-macroeconomic-risks-from-crypto-assets-539473>

¹⁴⁴ European Securities and Markets Authority (ESMA). (n.d.). *Markets in Crypto-Assets Regulation (MiCA)*. European Securities and Markets Authority. <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

¹⁴⁵ Reuters. (13 July 2026). *Europe's Digital Euro: What It Is and How It Would Work*. Reuters. <https://www.reuters.com/business/finance/europes-digital-euro-what-it-is-how-it-would-work-2026-07-13/>

resilience, and the competitiveness of the European financial sector. In parallel, the United States has adopted the GENIUS Act to establish a federal regulatory framework for payment stablecoins, reinforcing the international role of the US dollar within rapidly expanding digital financial markets¹⁴⁶. Meanwhile, jurisdictions such as China continue to prioritize sovereign digital currency initiatives through the Digital RMB (e-CNY) as part of broader strategies aimed at advancing financial modernization, improving payment system efficiency, supporting the internationalization of the Renminbi, and strengthening China's role within the evolving global monetary system¹⁴⁷⁻¹⁴⁸.

122. Alongside its legislation on payment stablecoins, the United States has considered a broader framework for digital-asset markets through the Digital Asset Market Clarity Act of 2025 (CLARITY Act). The bill passed the House of Representatives on July 17, 2025. The House-passed text proposes a clearer allocation of responsibilities between the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), together with registration and oversight requirements for digital commodity exchanges, brokers, and dealers. Its provisions address matters including disclosures, market integrity, custody, and the segregation of customer assets. The proposal therefore extends the U.S. legislative debate beyond stablecoin issuance to the organization and supervision of digital-asset markets more broadly¹⁴⁹.
123. As of September 18, 2026, the CLARITY Act had not become law. On September 15, the Senate failed, by a vote of 49-50, to invoke cloture on the motion to proceed to the bill, preventing its advancement at that stage. This was a procedural setback rather than a final vote on passage¹⁵⁰. The legislative process illustrates the continuing difficulty of translating support for digital-asset regulation into an agreed framework. For comparative policy analysis, it reinforces the importance of distinguishing enacted requirements from proposed reforms and of examining how supervisory responsibilities, investor protection, and accountability would operate in practice.

¹⁴⁶ United States Congress. (18 July 2025). *Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)*, Public Law No. 119-27. Congress.gov. <https://www.congress.gov/bill/119th-congress/senate-bill/1582>

¹⁴⁷ Katsurada, K. (6 July 2026). *The Shift in China's CBDC (Digital Yuan) Policy and Key Implications*. JRI Research Journal, Vol. 9, No. 13. The Japan Research Institute, Limited. <https://www.jri.co.jp/en/MediaLibrary/file/english/periodical/jrirj/2026/13/katsurada.pdf>

¹⁴⁸ Reuters. (17 June 2026). *China's Financial Regulator Vows Risk Prevention, Support for Strategic Industries*. Reuters. <https://www.reuters.com/world/asia-pacific/chinas-financial-regulator-vows-risk-prevention-support-strategic-industries-2026-06-17/>

¹⁴⁹ U.S. Congress. (17 July 2025). Digital Asset Market Clarity Act of 2025, H.R. 3633: Text as passed by the House of Representatives. Congress.gov. <https://www.congress.gov/bill/119th-congress/house-bill/3633/text/eh>

¹⁵⁰ U.S. Senate Daily Press Gallery. (15 September 2026). Tuesday, September 15, 2026. U.S. Senate. <https://www.dailypress.senate.gov/tuesday-september-15-2026/>

124. As cryptocurrency ecosystems continue to evolve, regulatory priorities are expanding beyond cryptocurrencies alone to encompass a broader digital financial ecosystem that includes decentralized finance (DeFi), stablecoins, tokenized assets, artificial intelligence, programmable financial services, and increasingly interconnected payment infrastructures¹⁵¹. These developments present new challenges for legislators and supervisory authorities, particularly in relation to cross-border regulatory coordination, consumer protection, financial stability, cybersecurity, data governance, and the growing interoperability between traditional financial institutions and blockchain-based systems¹⁵². Consequently, effective governance increasingly depends not only on legislative measures, but also on strengthening institutional capacity, enhancing supervisory technologies, promoting responsible innovation, and fostering collaboration among governments, financial institutions, technology providers, academia, and international organizations¹⁵³.
125. The increasingly interconnected nature of cryptocurrency ecosystems has progressively reduced the effectiveness of purely domestic regulatory approaches. Digital assets move across jurisdictions with limited regard for national borders, while decentralized financial infrastructures, cross-border payment networks, and globally accessible blockchain platforms operate beyond traditional regulatory boundaries. As a result, regulatory fragmentation may create inconsistencies that can be exploited by transnational organized criminal networks, facilitate regulatory arbitrage, and complicate the supervision of cross-border financial activities. These developments have reinforced the importance of greater international regulatory coordination, interoperability between supervisory frameworks, and more effective information sharing among competent authorities. As cryptocurrencies continue to evolve as a global financial phenomenon, strengthening cooperation at both the regional and international levels will remain essential to preserving financial integrity,

¹⁵¹ OECD. (19 January 2022). *Why Decentralised Finance (DeFi) Matters and the Policy Implications*. OECD Publishing. https://www.oecd.org/en/publications/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en.html

¹⁵² Financial Stability Board (FSB). (17 July 2023). *FSB Finalises Global Regulatory Framework for Crypto-Asset Activities*. Financial Stability Board. <https://www.fsb.org/2023/07/fsb-finalises-global-regulatory-framework-for-crypto-asset-activities/>

¹⁵³ Hacıbedel, B., & Perez-Saiz, H. (29 September 2023). *Assessing Macroeconomic Risks from Crypto Assets*. IMF Working Paper No. 2023/214. International Monetary Fund. <https://www.imf.org/en/publications/wp/issues/2023/09/30/assessing-macroeconomic-risks-from-crypto-assets-539473>

supporting responsible innovation, and maintaining confidence in the stability and resilience of the international financial system¹⁵⁴⁻¹⁵⁵.

126. The rapid evolution of cryptocurrency ecosystems demonstrates that effective governance cannot rely solely on legislation or technological safeguards. As digital assets become increasingly integrated into payment systems, capital markets, decentralized finance, artificial intelligence, and the broader digital economy, regulatory frameworks will need to evolve continuously alongside technological innovation. The challenge facing policymakers is therefore not only to mitigate financial, security, and geopolitical risks, but also to preserve the benefits of innovation while strengthening transparency, accountability, market confidence, and international financial resilience. In this context, cryptocurrencies should be understood not as an isolated technological phenomenon, but as part of a broader transformation of the global financial order, requiring adaptive governance, evidence-based policymaking, and sustained international cooperation capable of responding to an increasingly interconnected digital financial ecosystem¹⁵⁶.

Conclusions

127. Between opportunities and risks, cryptocurrencies have become a defining component of the ongoing transformation of the international financial system, as well as of national and regional financial architectures and the relationships among them.
128. The Parliamentary Assembly of the Mediterranean (PAM), together with its Centre for Global Studies (PAM-CGS), approaches the phenomenon of cryptocurrencies in all its complexity. Assessing their implications requires a comprehensive and forward-looking approach, beginning with legislative and regulatory frameworks. While regulatory grey areas remain, significant progress is being made across multiple jurisdictions. Building on the findings of this report, PAM, in cooperation with the network of parliaments in the Euro-Mediterranean and Gulf region, other parliamentary assemblies, and leading international and regional organizations, intends to continue monitoring legislative and

¹⁵⁴ Financial Action Task Force (FATF). (27 June 2023). *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. Financial Action Task Force. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf>

¹⁵⁵ Financial Stability Board (FSB). (17 July 2023). *FSB Finalises Global Regulatory Framework for Crypto-Asset Activities*. Financial Stability Board. <https://www.fsb.org/2023/07/fsb-finalises-global-regulatory-framework-for-crypto-asset-activities/>

¹⁵⁶ OECD. (19 January 2022). *Why Decentralised Finance (DeFi) Matters and the Policy Implications*. OECD Publishing. https://www.oecd.org/en/publications/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en.html

regulatory developments relating to decentralized finance and the broader digital asset ecosystem.

129. Likewise, PAM will continue its strategic research on emerging international risks. As highlighted throughout this report, cryptocurrencies have been misused to facilitate sanctions evasion, support transnational organized crime, finance terrorist activities, and enable disinformation and foreign interference operations. PAM will also continue to monitor the growing convergence between cryptocurrencies, emerging technologies, and illicit ecosystems operating within the dark web.
130. Given the multidimensional nature of cryptocurrencies, applying a linear or sector-specific analytical framework would provide only a partial understanding of the phenomenon. This report demonstrates that the financial, technological, geopolitical, regulatory, and security dimensions of cryptocurrencies are closely interconnected. Addressing these challenges therefore requires innovative, multidisciplinary, and collaborative approaches supported by effective public-private partnerships involving all relevant stakeholders, including parliaments, governments, the private sector, academia, research institutions, law enforcement agencies, and intelligence services.
131. Throughout this report, cryptocurrencies have been examined not merely as financial innovations, but as drivers of broader transformations affecting the global financial system, technological development, geopolitical competition, regulatory governance, and international security. The findings demonstrate that their significance extends well beyond digital finance, reflecting their growing role in shaping economic resilience, strategic competition, and the evolving architecture of the international financial order.
132. In this rapidly evolving environment, effective governance will depend not only on technological innovation and regulatory adaptation, but also on sustained international cooperation capable of preserving financial integrity, supporting responsible innovation, and strengthening global economic and security resilience. Ultimately, the analysis presented in this report demonstrates that cryptocurrencies should increasingly be understood not merely as financial assets, but as strategic infrastructures operating at the intersection of finance, technology, geopolitics, and international security. The central policy challenge is therefore no longer whether cryptocurrencies will influence the future international financial system, but how governments, international organizations, financial institutions, the private sector, and other relevant stakeholders should collectively govern this transformation while safeguarding financial stability, international security, economic

resilience, and public trust. The following recommendations identify possible steps through which PAM and its partners could contribute to this objective.

Recommendations and Next Steps

133. The emergence of new technologies frequently precedes a complete understanding of their economic, social, and security implications. Initial regulatory caution may therefore be justified while evidence is being collected. However, after a sufficient period of observation and practical use, policymakers should reassess whether the benefits of a technology outweigh its documented risks and whether additional safeguards or restrictions are necessary. The evidence examined in this report indicates that cryptocurrencies may support innovation, faster payments, financial inclusion, and new forms of investment. It also demonstrates persistent exposure to extreme price volatility, fraud, cyberattacks, theft, tax evasion, money laundering, terrorist financing, sanctions evasion, and transactions involving illicit goods and services, including through dark-web markets. These findings underline the need to translate assessment into practical legislative and institutional action. Regulatory approaches should remain responsive to new evidence while safeguarding consumer protection, financial stability, fiscal integrity, monetary sovereignty, and international security, and ensuring that decentralization does not remove accountability or place financial activities beyond the effective reach of the law.
134. PAM member parliaments are encouraged to review whether their national frameworks adequately address crypto-asset activities and services, including those provided from abroad. Priorities should include clearly assigned supervisory responsibilities, appropriate licensing or registration, effective supervision, customer due diligence, cybersecurity, safeguarding of client assets, transparent risk disclosures, and accessible complaints and redress mechanisms. Cybersecurity requirements should reflect the risks of each activity and address independent security assessments, timely vulnerability remediation, incident reporting, and controls over automated transactions. Where AI agents can initiate financial operations, safeguards should include restricted access permissions, transaction limits, and human authorization for high-risk transfers. Requirements should reflect the functions and risks of each activity: stablecoin issuers, for example, require particular scrutiny of reserve quality, liquidity, and redemption arrangements. National frameworks should also strengthen implementation of applicable international standards against money laundering

and terrorist financing, while supporting cooperation among financial regulators, financial-intelligence units, tax administrations, and law-enforcement authorities¹⁵⁷.

135. Tax transparency should form a distinct component of this response. Parliaments could support the legal and administrative arrangements needed to implement the OECD Crypto-Asset Reporting Framework, in accordance with their jurisdictions' commitments and domestic procedures¹⁵⁸. Competent authorities should also possess clearly defined powers to restrict or prohibit unlawful activities and, where justified by evidence and applicable law, products or practices presenting risks that cannot be adequately addressed through less restrictive measures. Such interventions should be proportionate, subject to appropriate procedural safeguards, and coordinated where cross-border effects arise. MiCA's provisions on product intervention provide one relevant example of this approach¹⁵⁹.
136. In parallel, policymakers should assess how public and regulated payment infrastructures can meet demand for faster, more accessible, and affordable digital transactions. This assessment could encompass central bank digital currencies, connections between existing instant-payment systems, and other regulated settlement arrangements. The prospective digital euro provides a relevant example of efforts to develop digital central bank money, although its issuance remains subject to the necessary legal framework and a subsequent decision by the European Central Bank¹⁶⁰. National approaches differ: the United States' January 2025 Executive Order directs federal agencies, except where required by law, not to establish, issue, or promote central bank digital currencies¹⁶¹. Any assessment should therefore reflect national circumstances and examine privacy, cybersecurity, accessibility, banking-sector effects, and monetary sovereignty, without assuming that any particular technology automatically delivers safer or cheaper payments.
137. To support these priorities, PAM could consider establishing a Regional Observatory on Crypto-Assets and Digital Finance serving its member parliaments across the Euro-Mediterranean and Gulf regions. Its purpose would be to provide independent research,

¹⁵⁷ Financial Action Task Force. (n.d.). Virtual Assets. FATF. Accessed 18 September 2026. <https://www.fatf-gafi.org/en/topics/virtual-assets.html>

¹⁵⁸ OECD. (2023). Crypto-Asset Reporting Framework: Introduction. International Standards for Automatic Exchange of Information in Tax Matters. OECD. https://www.oecd.org/en/publications/international-standards-for-automatic-exchange-of-information-in-tax-matters_896d79d1-en/full-report/component-5.html

¹⁵⁹ European Parliament and Council of the European Union. (31 May 2023). Regulation (EU) 2023/1114 on markets in crypto-assets, Article 105: Product intervention by competent authorities. ESMA Interactive Single Rulebook. <https://www.esma.europa.eu/publications-and-data/interactive-single-rulebook/mica/article-105-product-intervention-competent>

¹⁶⁰ European Central Bank. (n.d.). FAQs on the digital euro. ECB. Accessed 18 September 2026. https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html

¹⁶¹ The White House. (23 January 2025). Strengthening American Leadership in Digital Financial Technology. The White House. <https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/>

comparative legal analysis, and practical legislative assistance. The Observatory would help translate complex technological and financial developments into information that parliamentarians can use when scrutinizing legislation, reviewing government policy, and assessing regulatory performance. Its establishment, institutional form, and resources would remain subject to approval through PAM's applicable procedures.

138. The Observatory's initial work could concentrate on a regularly updated map of national regulatory frameworks, concise quarterly parliamentary briefings, and targeted assessments of emerging risks. Each publication should identify its sources, date of assessment, and relevant limitations. Where reliable information is available, the Observatory could examine adoption, consumer losses, fiscal implications, and cross-border activity, distinguishing verified data from estimates. Legislative assistance could include explanatory notes, scrutiny checklists, and adaptable model provisions. Comparative work should draw on international standards and relevant frameworks, including MiCA, while respecting differences in national legal systems and policy choices. It should also monitor proposed reforms, including the U.S. CLARITY Act, clearly distinguishing legislative proposals and procedural developments from enacted requirements¹⁶². Particular care should be taken to distinguish directly applicable EU obligations from approaches that non-EU jurisdictions may voluntarily consider¹⁶³.
139. Parliamentary oversight could involve the relevant PAM Standing Committees, with balanced geographical representation reflecting the Assembly's membership. Subject to available capacity and institutional approval, the PAM Secretariat and PAM-CGS could coordinate research and administrative support. Contributions could be sought from central banks, regulators, tax authorities, financial-intelligence units, consumer representatives, and academic partners, including Politecnico di Milano and institutions participating in the PAM Academic Platform. External participation should be governed by clear terms of reference, disclosure of relevant interests, and safeguards for analytical independence.
140. The Observatory's security work should focus on analyzing documented patterns of misuse, identifying legislative gaps, and supporting parliamentary capacity. This work could include assessments of AI-assisted cyber threats, vulnerabilities in blockchain-related infrastructure, and safeguards for AI systems authorized to initiate financial

¹⁶² U.S. Senate Daily Press Gallery. (15 September 2026). Tuesday, September 15, 2026. U.S. Senate.

<https://www.dailypress.senate.gov/tuesday-september-15-2026/>

¹⁶³ European Parliament and Council of the European Union. (31 May 2023). Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA), particularly Articles 2 and 149. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

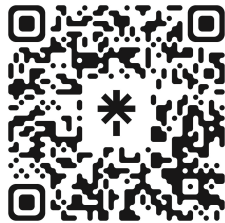
transactions. Such assessments should distinguish confirmed incidents from speculative attribution and consider the contribution of AI to defensive monitoring and incident analysis. Investigations, operational financial-intelligence exchanges, supervisory decisions, and asset-freezing measures would remain with the competent authorities. Any information shared with the Observatory should have a lawful basis and appropriate confidentiality protections; sensitive operational information should continue to pass through authorized channels¹⁶⁴. Likewise, PAM could facilitate dialogue on cross-border regulatory testing, while authorization and supervision of any operational sandbox would remain with the responsible national authorities.

141. A practical next step would be a proposed twelve-month pilot, commencing after approval of its mandate and resources. The first three months could establish the work program, participating contacts, staffing arrangements, and data policies. During months four to six, initial outputs could include a comparative regulatory assessment, the first parliamentary briefing, and a capacity-building session. The remaining period could produce a consumer-protection legislative toolkit and a comparative study of selected remittance corridors, assessing total costs, accessibility, and risks across available payment methods. An end-of-pilot review should assess the reliability and usefulness of these outputs, parliamentary engagement, and resource requirements before decisions on expansion. More extensive activities, including an annual forum or support for coordinated regulatory testing, could then be considered in light of demonstrated demand and institutional capacity.

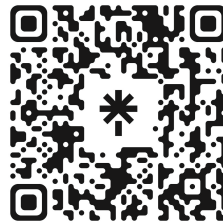
¹⁶⁴ Egmont Group of Financial Intelligence Units. (May 2022). Principles for Information Exchange between Financial Intelligence Units, revised May 2022. Egmont Group. <https://egmontgroup.org/wp-content/uploads/2013/10/2.-Principles-Information-Exchange-Revised-May-2022-01.pdf>

Prepared by
the Parliamentary Assembly of the Mediterranean (PAM),
Centre for Global Studies (CGS)

Viale Antonio Onofri, 47890 - 103
Città di San Marino, San Marino



PAM



CGS

www.pam.int
www.cgspam.org

