Global Blockchain Business Council (GBBC) USA: The US Department of Treasury Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets

About GBBC

Global Blockchain Business Council (GBBC) is the trusted non-profit association for the blockchain, digital assets, and emerging technology community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 284 Ambassadors across 124 jurisdictions and disciplines. GBBC USA is the U.S.-focused entity.

GBBC furthers adoption of blockchain and emerging technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chain, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), GBBC Giving, GBBC USA, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC)

DISCLAIMER: please note, the responses to this request for comment represent the views of a subset of GBBC's 500+ institutional members which include traditional corporations as well as blockchain and crypto focused organizations who participate in the GBBC USA Policy working group. If there are any questions related to specific responses, please reach out to info@gbbc.io.

General Remarks

GBBC USA welcomes the opportunity to respond to the US Treasury Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets. We appreciate Treasury's engagement with industry stakeholders to date and its commitment to advancing a clear, proportionate, and innovation-friendly legislation and regulatory framework for digital assets in the United States.

This response reflects the consolidated feedback of a subset of GBBC's 500+ institutional members. Participants included representatives from regulated financial institutions, blockchain and digital asset exchanges, technology providers, legal advisors, and other members of GBBC's diverse global network.

GBBC USA supports the Treasury's core objectives and strongly believes that the regulatory framework must enable innovation, competitiveness, and sustainable growth for firms building in the United States. Without a clear, coordinated, and proportionate approach, there is a risk that well-intentioned requirements could inadvertently raise barriers to entry, fragment oversight, and diminish the U.S.'s ability to attract and retain digital asset innovation.

GBBC USA stands ready to work with policymakers, regulators, and industry to help develop a market structure framework that is clear, workable, proportionate, and internationally competitive.

1. **In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem? What key trends in illicit finance risks have financial institutions observed in the digital asset ecosystem?**

Some of the most significant illicit finance risks in the digital asset ecosystem stem from the increasing sophistication of cross-chain obfuscation. Criminal actors now routinely chain together Decentralized Exchange (DEX) swaps, bridges, and instant coin-swap services to move assets across networks at speed, often fragmenting flows (fan-out) and later reconverging them (fan-in) to frustrate investigative tracing. Mixers remain in use, but more commonly as a single layer within longer laundering sequences. State-linked groups and organized scam operators have become adept at quickly exiting freeze-prone stablecoins into native assets, then shifting to high-liquidity networks such as major L2s. Meanwhile, smaller terrorist-finance and fraud campaigns continue to rely on BTC and USDT, often revealing themselves through gas-fee financing patterns, small native-coin transfers from affiliated wallets that enable downstream transactions.

Financial institutions consistently highlight three converging trends in illicit finance risk. First, the overall volume and complexity of multichain laundering have increased dramatically. Second, criminals willingly incur significant transaction costs across dozens of swaps and bridges purely to complicate investigations. Third, risk monitoring that only examines the inbound asset or chain frequently misses illicit links a few hops back on other networks. As a result, effective defenses now require cross-chain-aware analytics, automated bridge tracing, and the use of targeted heuristics to speed triage and sharpen focus.

Practical detection and mitigation approaches include:

- Cross-chain tracing across assets and networks two to three hops back, supported by automated virtual value-transfer mapping through bridges.

- Pattern weighting to identify rapid multi-hop routes, structured fan-outs/fan-ins, stablecoin-to-native rotations, and unusually high cumulative fees with no commercial rationale.

- Wallet clustering through gas-fee financing signals that link otherwise separate addresses to the same operators.

- Expanded monitoring coverage to capture activity on new chains, L2s, long-tail tokens, and coin-swap venues, supported by standardized queries and law-enforcement referral playbooks.

Mixers and tumblers, while technically capable of enabling privacy, are still primarily deployed for illicit finance. Regulators should avoid blanket bans that risk chilling innovation or penalizing legitimate users. Instead, policy should narrowly target illicit operations by requiring custodial mixers that exercise discretion over flows to register with FinCEN, implement AML programs, and block sanctioned entities. Blockchain analytics already neutralize many of the associated risks by:

- Identifying mixer entry and exit points even when internal flows are obscured.
- Scoring wallet risk based on mixer interactions—such as mixer-first funding or repeated use—to distinguish intent.
- Triggering enhanced due diligence and automated SAR filings when high-risk mixer behavior is detected, particularly around fund velocity and timing.
- Supporting law enforcement by tracing downstream funds to exchanges and service providers subject to subpoenas.
- Preserving privacy-enhancing innovation by supervising behavior, not outlawing technology.

Another critical trend is the industrialization of scams, particularly pig-butchering schemes. These operations combine social engineering, chain-hopping, layered payments, trafficking-enabled labor, and Telegram-based marketplaces such as Huione or Xinbi, often with mixers layered in to avoid detection. Fraud schemes also exploit the historical absence of beneficiary verification in digital asset transactions—specifically, the fact that, without Travel Rule compliance and pre-transaction authorization mechanisms in place, beneficiary institutions have not traditionally verified whether the beneficiary information provided by the originator corresponds to the actual recipient. Losses typically occur before warning signs are visible. Victims face limited recourse: there are no rapid-reporting channels, cross-border hurdles delay enforcement, and many state and local agencies lack the training or technical tools to handle crypto cases.

Overlapping jurisdiction across federal, state, and local bodies further fragments victim support.

The FBI's 2024 Internet Crime Report corroborates these international findings, documenting $5.8 billion in reported losses tied to cryptocurrency investment fraud, an increase of nearly 50% year-over-year.[1] Its "Operation Level Up" further revealed the industrialization of pig-butchering schemes: more than 4,000 victims were proactively identified, three-quarters of whom were unaware they were being defrauded, with estimated prevented losses exceeding $285 million.

Since 2024, the use of stablecoins by illicit actors has accelerated sharply, with most on-chain illicit finance now occurring in stablecoins, especially USDT on the Tron network. Their appeal lies in high liquidity, low fees, and speed, which criminals exploit for layering and obfuscation. Illicit actors, including DPRK hackers, terrorist financiers, and drug traffickers, routinely pair stablecoin flows with anonymity-enhancing tools, dormant VASP accounts, mixers, and cross-chain bridges to complicate detection.[2]

The DPRK continues to represent the most acute risk. In 2025, it carried out the single largest digital asset theft to date, stealing $1.46 billion from ByBit through social engineering and malicious code manipulation. Laundering involved both unregistered service proviers and a vast network of wallets (35 Bitcoin and 125,000 Ethereum addresses), demonstrating increasingly complex transaction patterns. Only 3.8% of stolen funds were recovered, underscoring persistent weaknesses in asset recovery, public-private information sharing, and cross-border cooperation.

Financial institutions also confront broader laundering networks that use digital assets to move value across jurisdictions and reinvest in criminal enterprises. FATF members highlighted cases where funds were swapped for cash equivalents or redirected into illicit businesses. Alongside this, links between digital assets, gambling platforms, and unlicensed gaming operators are emerging as key vulnerabilities, particularly where oversight is weak or absent.

[1] FBI Internet Crime Report
[2] FATF Targeted Update 2025

Terrorist organisations such as ISIL and Al-Qaeda continue to test digital assets as a fundraising and transfer mechanism. While traditional channels (cash, hawala, MVTS) remain dominant, digital assets are valued for anonymity, diversification, and rapid cross-border transfer. This diversification trend is significant: even limited adoption signals an evolution in terrorist financing tactics that institutions and regulators must monitor closely.

Stablecoin issuer models present both vulnerabilities and potential mitigants. Some issuers embed programmable features into smart contracts that allow freezing or blocking transactions, and others apply monitoring of tokens in circulation. Yet these measures vary by issuer and depend on actionable intelligence from authorities, limiting their reliability. Market participants emphasized the need for combining issuer-level controls with advanced blockchain analytics, real-time attribution, and intermediary oversight to strengthen systemic defenses.

Another vulnerability worth mentioning is that created by blockchain's immediate, irreversible settlement characteristics, which invert the traditional finance risk model. In conventional financial systems, authorization precedes settlement, creating a critical window for compliance verification and risk assessment. Blockchain based transactions, however, have no built-in pre-transaction authorization mechanics: transactions are settled instantly and irreversibly without requiring prior verification or consent from relevant parties. This architectural difference creates a structural mismatch where institutions must perform compliance checks after funds have irreversibly moved, undermining decades of established risk management principles.

Finally, DeFi remains a regulatory blind spot. Around half of advanced jurisdictions now require certain DeFi arrangements to register as virtual assets service providers when creators or operators retain control or significant influence. Still, most struggle to identify entities that meet this threshold, and few enforcement actions have been taken. This gap leaves decentralized protocols vulnerable to misuse for laundering, layering, and cross-chain obfuscation with little supervisory recourse.

2. What innovative or novel methods, techniques, or strategies related to APIs are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to APIs?

Financial institutions increasingly use advanced API-based strategies to detect and mitigate illicit finance risks in digital assets, integrating AI-driven analytics, real-time transaction monitoring, and automated identity verification into compliance workflows. These API innovations help automate suspicious activity detection, streamline KYC/AML, and facilitate rapid cross-system data sharing between blockchain analytics tools and internal systems.

Innovative API-Based methods include:

- APIs enable automated checks against global sanction lists, monitor accounts for unusual patterns, flag high-risk cross-border transfers, and provide instant risk scoring using blockchain analytics outputs.
- KYC and digital identity APIs now utilize biometrics, liveness-detection, and multi-database cross-checking to thwart synthetic identities and deepfake fraud, reducing onboarding risk for exchanges and custodians.
- API calls to blockchain analytics platforms allow institutions to perform on-chain transaction tracing, link wallet addresses to illicit activities, and run behavioral analytics for DeFi usage.
- RegTech APIs automate regulatory updates, adapting compliance logic to evolving jurisdictional requirements without code redeployments.
- Some institutions develop API connectors to secure cloud-based data, creating “modular compliance layers” — enabling region-specific flows for KYC, reporting, and access controls.
- APIs allow institutions to transmit originator and beneficiary information in compliance with Travel Rule regulations and to exchange authorization messages ahead of transaction settlement. This allows institutions to assess counterparty risk and engage in an authorization process ahead of settlement.

Risks, benefits, challenges, and potential safeguards related to APIs

APIs can introduce serious risks, the most prominent being the potential exposure of sensitive data, unauthorized access by threat actors, and an expanded attack surface for cybercriminals to exploit. Such vulnerabilities — often stemming from poor API design, lack of proper access controls, or outdated security protocols—can lead to data breaches, theft, and disruptions to business operations.

The primary challenges revolve around ensuring secure integration between platforms, staying compliant with privacy regulations such as GDPR, and maintaining up-to-date safeguards as regulatory frameworks and threat landscapes evolve. Keeping APIs aligned with quickly changing compliance requirements can strain developer and legal teams. Despite these challenges, the benefits of APIs for compliance automation, risk detection, and business agility remain significant.

To address these risks, strong safeguards are essential. These include implementing robust authentication and access controls, encrypting all API communications, regularly auditing code and system configurations, monitoring API usage for abnormal behaviors, and ensuring privacy-preserving data handling (such as zero-knowledge proofs or off-chain storage of personally identifiable information). Modular API logic and policy engines can help organizations adapt controls on a jurisdiction-by-jurisdiction basis, while ongoing legal reviews and incident response planning further lower risk.

a. *What factors do financial institutions consider when deciding whether to employ APIs for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use APIs for these purposes, what specific compliance functions do/will APIs support? For financial institutions that decided not to use APIs, please provide additional details on the rationale for that decision.*

Financial institutions weigh a range of factors when deciding whether to implement APIs for AML/CFT and sanctions compliance. Considerations typically include the institution's existing technology infrastructure, regulatory requirements for their market, the scale and velocity of their transaction activity, perceived risk exposure, data privacy concerns, and the available expertise to securely manage API integrations. Institutions also assess how APIs align with their organizational governance policies,

cost implications, and the potential to automate time-consuming compliance tasks such as customer due diligence, beneficial ownership verification, sanctions screening, and suspicious activity reporting.

For those that adopt APIs, specific compliance functions supported include real-time transaction monitoring, automated screening and reporting against AML and CFT typologies, sanctions database checks, KYC onboarding, Travel Rule information exchange, pre-transaction authorization flows, ongoing customer risk profiling, audit trails, fraud detection, and multi-jurisdictional policy enforcement. APIs also allow institutions to integrate multiple data inputs for consolidated customer views, making it easier to assign and track risk scores while keeping up with global regulatory standards.

Institutions that choose not to use APIs often cite concerns about cybersecurity risks, the complexity of securely integrating APIs with legacy systems, fears over data breaches, and uncertainty regarding regulatory acceptance or supervision of API-driven solutions. In some cases, the costs and resource requirements to overhaul existing compliance platforms may outweigh the perceived benefits. These organizations may prefer to maintain tried-and-tested manual or batch-based processes, especially in environments where regulatory standards are evolving slowly or where strict data localization laws impede external data sharing.

Ultimately, the decision hinges on a careful balance of regulatory requirements, operational efficiency, risk management capabilities, and the institution's readiness to meet governance and security standards in a rapidly changing compliance landscape.

b. How are financial institutions using API tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of API tools with other existing or previous tools used for similar purposes.

Financial institutions are using API tools for AML/CFT and sanctions compliance in several ways: as pilots alongside legacy tools during transition or regulatory sandboxes, to augment the capabilities of existing rules-based and batch systems, or increasingly as replacements for older, slower, and less adaptable compliance technologies. During initial adoption phases, many organizations deploy API-based compliance engines in

parallel with traditional batch-processing tools, facilitating side-by-side testing and validation before a complete migration. Others use APIs to integrate and augment legacy tools — enabling real-time, automated risk screening, transaction monitoring, and reporting while maintaining established core systems for backup or redundancy.

Compared to older manual or batch systems, API-based solutions vastly increase speed and automation. APIs enable instant transaction screening, combine internal and third-party data feeds for richer risk analysis, and drastically reduce both false positives and compliance cycle times. Whereas traditional tools were prone to delays, errors, and resource constraints, API tools deliver real-time monitoring, seamless integration with third-party identity/sanctions lists, and easy scaling for growing transaction volumes. Modern systems also make it easier to keep up with regulatory changes through modular updates.

Effectiveness studies and industry feedback indicate that API tools provide superior accuracy, richer contextual data, improved customer onboarding/KYC, and overall higher efficiency. They reduce compliance failures, regulatory fines, and operational costs by replacing manual reviews with automated, auditable decision-making. Legacy tools still serve value in massive batch processing for high-volume, low-risk environments, but are less flexible and effective at adapting to new risk patterns or regulatory demands.

In summary, APIs now serve as the backbone of cutting-edge compliance programs — either augmenting or supplanting traditional approaches — yielding faster, more scalable, and more accurate AML, CFT, and sanctions screening across the digital asset ecosystem.

c. *Are there regulatory, legislative, supervisory, or operational obstacles to using APIs to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.*

US financial institutions face distinct regulatory, legislative, supervisory, and operational barriers directly linked to the evolving regulatory landscape and federal expectations.

From a regulatory and legislative perspective, the patchwork of state and federal regimes for digital assets creates uncertainty — especially around licensing, recordkeeping responsibilities, and cross-border data sharing through APIs. Treasury guidance, Executive Order 14178, and recent reports from the President's Working Group all underscore that current statutory definitions and the Bank Secrecy Act (BSA) have not fully kept pace with technological advancement, leaving ambiguity as to whether automated, API-driven monitoring tools fulfill existing AML/CFT and sanctions requirements consistently across centralized and decentralized finance. This uncertainty particularly impacts areas like the Travel Rule, reporting format requirements, and how real-time data access fits with established regulatory expectations.

On the supervisory front, there is inconsistent examiner familiarity with API-based architectures — leading to mixed signals about auditability expectations, API endpoint security, and the acceptability of automation in suspicious activity reporting. Operationally, integrating APIs with legacy core banking or compliance systems can be costly and fraught with technical challenges, including maintaining up-to-date sanctions lists and ensuring robust privacy, authentication, and cyber protections across API endpoints.

To address these issues, Treasury should:

- Issue clear, harmonized guidance on the use of APIs in AML/CFT and sanctions compliance, particularly in digital asset environments, to resolve ambiguities and foster innovation while protecting against illicit finance.
- Facilitate interagency collaboration and examiner education to help ensure supervisory consistency and to clarify security and record retention standards for API-based compliance.
- Promote technical standards and interoperability protocols for APIs (including the creation of a coherent data sharing schema), supporting modularity and secure integration with both legacy and emerging digital asset platforms.
- Engage with federal and state stakeholders as well as international financial regulators to clarify data localization and cross-border API compliance obligations,

simplifying the global compliance landscape for US institutions engaged in digital assets.

By implementing these recommendations, Treasury can help to reduce regulatory friction, increase security and effectiveness in digital asset compliance, and support the broader federal policy aim of responsible US digital asset innovation and leadership.

d. What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of APIs for detecting illicit finance involving digital assets?

The U.S. government should take several targeted steps to facilitate effective, risk-based adoption of APIs for detecting illicit finance involving digital assets.

First, it should issue clear and harmonized regulatory guidance outlining expectations for API-driven transaction monitoring, suspicious activity reporting, and sanctions screening, tailored to both centralized and decentralized finance environments. This would resolve current ambiguity within the Bank Secrecy Act (BSA), Travel Rule, and related anti-money laundering (AML)/countering the financing of terrorism (CFT) obligations, making it clear how automated, interoperable API solutions can meet compliance requirements.

Second, the government should prioritize modernization and clarification of examiner and supervisory protocols. This includes training for supervisors and examiners to ensure consistent review and audit of API implementations, and fostering collaboration between regulators and private industry to identify gaps and emerging best practices, especially in cross-border scenarios where disparate rules may impede effective data sharing.

Third, technical standards for API security, access control, authentication, and privacy should be developed and endorsed, possibly via NIST or sectoral efforts under Treasury's leadership. These standards should promote robust encryption, real-time monitoring, data localization safeguards, modular compliance layers, and secure cloud infrastructure, enabling financial institutions to integrate APIs while maintaining operational resilience.

Fourth, coordination with international standard-setting bodies, and active U.S. engagement in cross-border regulatory harmonization, will help streamline compliance for global digital asset operations and ensure interoperability of API solutions. This includes updating AML/CFT frameworks for DeFi, stablecoins, and emerging protocols, and leveraging existing partnerships with FATF, FSB, and industry forums to advance consistent global standards.

Finally, the U.S. government should maintain ongoing stakeholder consultation — such as the current RFI process under the GENIUS Act and Executive Order 14178 — to surface obstacles, support pilot programs and regulatory sandboxes, and adapt its approach in line with technological innovation and evolving illicit finance threats.

These steps will facilitate responsible adoption, increase transparency and effectiveness in financial crime detection, and promote innovation and competitiveness within the U.S. digital asset compliance landscape.

e. Treasury will evaluate APIs and consider their impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

Treasury's evaluation under the GENIUS Act should focus on how APIs can deliver scalable, effective, and risk-based compliance while addressing cost, privacy, cybersecurity, and operational considerations in the digital asset ecosystem. It is helpful to look at two industry solutions that are directly pertinent to addressing the GENIUS Act research factors Treasury will use to evaluate APIs and their impact on digital asset compliance.

For example, a crypto-native market surveillance company provides agentic-based compliance platforms with AI-powered trade surveillance, transaction monitoring, sanctions screening, and real-time detection and reporting. Their solutions are designed to enhance effectiveness by providing automated, scalable compliance functions for exchanges, stablecoin issuers, custodians, and financial institutions. The company emphasizes market integrity, operational efficiency, rapid suspicious activity identification, and compliance with evolving federal and state regulatory mandates — including those introduced under the GENIUS Act. Their technology incorporates extensive privacy and cybersecurity safeguards, multi-venue monitoring, and can be

configured to provide the real-time reporting and certifications that GENIUS Act compliance requires.

Another platform offers unified pre-transaction authorization, automated Travel Rule compliance, counterparty screening, real-time decisioning, and secure data exchange across a global open network of regulated financial institutions and virtual assets service providers. They directly address privacy and cybersecurity factors by employing bank-grade encryption, data segregation, real-time vulnerability checks, and SOC2 compliance. The platform supports effectiveness (accurate, scalable compliance and risk mitigation), interoperability (cross-jurisdictional operations), and regulatory adaptability — allowing institutions to comply with both U.S. and global Travel Rule requirements.

Both solutions offer detailed audit trails, operational resilience, and compliance automation — all core criteria within the GENIUS Act framework. They also feature robust reporting and risk analytics, helping address Treasury's concerns about operational challenges, cost-effectiveness, data privacy, cybersecurity, and real-world compliance effectiveness for digital assets.

As just two real-world examples among several, the adoption and technical capabilities of both solutions directly align with the GENIUS Act's assessment factors for evaluating how APIs can support risk-based, effective, and secure compliance programs in the digital asset ecosystem. GBBC recently published 101 Real World Blockchain Use Cases Handbook with Section IV focusing on finance and compliance solutions (please see use cases #20-31).[3]

[3] GBBC's 101 Real-World Blockchain Use Cases Handbook 2025

3. **What innovative or novel methods, techniques, or strategies related to AI are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to AI? Please describe the use of AI to conduct analysis of transactional data, including transactions that occur on blockchains, and to identify complex illicit financial networks, as well as key lessons learned from use of AI in this context.**

Financial institutions are increasingly deploying artificial intelligence (AI) to detect illicit activity and mitigate illicit finance risks involving digital assets, leveraging machine learning, graph analytics, natural language processing, and behavioral pattern recognition. These innovations have rapidly advanced beyond traditional rule-based compliance systems.

Innovative AI Methods and Strategies

- AI-powered models analyze blockchain transaction patterns, simulating end-to-end money laundering scenarios and adapting to evolving criminal tactics.
- Machine learning tools are tuned for behavioral analysis, identifying abnormal movements across decentralized exchanges, mixers, and nested accounts that may indicate layering or obfuscation attempts.
- Graph-based AI systems map connections among wallets, exchanges, and off-chain actors to uncover complex, multi-jurisdictional illicit networks that would evade simple heuristic checks.
- Deep learning approaches flag synthetic identities, deepfake-driven fraud, and cross-asset laundering through transaction, biometric, and media analysis.
- Natural language processing automates adverse media and sanctions screening in real time, improving the speed and depth of compliance investigations.
- Simulation techniques train AI on synthetic but realistic financial crime patterns, improving adaptability to new typologies.

- Agentic Trust frameworks are also emerging as a next-generation capability for performing counterparty due diligence. These systems replace static Wolfsberg style due diligence questionnaires with behavior-based, real-time counterparty assessment, prioritizing evidence-backed decision-making and reducing manual review time.

Real-World Industry Examples

Several existing industry solutions offer innovative, AI-driven solutions directly relevant to detecting illicit activity and mitigating illicit finance risks involving digital assets:

- apply advanced AI and machine learning to real-time transaction monitoring, trade surveillance, and automated detection of market manipulation, layering, and money laundering typologies.
- use behavioral analytics, natural language processing, and agentic AI approaches to identify complex illicit financial networks across both centralized and decentralized venues.
- integrate graph analytics to map relationships among wallets, exchanges, and counterparties, enabling rapid detection of suspicious flows and compliance with global regulatory obligations.
- enhance traditional counterparty due diligence through sophisticated AI-powered analysis of network behavior and transaction patterns. A set of specialized agents monitors Travel Rule interaction quality and timeliness, network transaction velocity, counterparty network integrity, sanctions/AML responsiveness, and divergences between self-reported and observed behavior. The system provides actionable A-F risk ratings while maintaining the complex analytical capabilities compliance officers require.
- deploy sophisticated AI-powered blockchain analytics—including network graphing, machine learning, and real-time anomaly detection—to trace complex illicit financial flows and uncover hidden criminal networks.
- enable interactive investigation of cross-chain transactions, sanctions screening, and multi-venue monitoring for banks, exchanges, and policy makers.

AI Analysis of Transactional Data and Network Detection

AI models analyze massive transactional datasets, including on-chain transfers and off-chain metadata, to identify money laundering strategies, mixer usage, and nested account behaviors with greater speed and accuracy than legacy systems. Advanced graph analytics reveal connections between seemingly unrelated wallets, uncovering collusion, clustering, and coordinated illicit network activity. Finally, natural language processing and behavioral AI modules are used for real-time adverse media screening, contextual enrichment, and continuous risk scoring.

Risks, Benefits, Challenges, and Safeguards

Benefits of using AI include real-time, scalable detection of illicit patterns and networks, significant reduction in compliance workload, and improved detection accuracy. In addition, AI can provide enhanced regulatory adaptability and operational efficiency across international jurisdictions.

However, the risks and challenges are very real and include:

- Data privacy and cybersecurity vulnerabilities in AI model ingestion and outputs; adversarial risks through model poisoning or manipulation.
- Biased or incomplete training data can create disparate impacts, and model drift can degrade performance over time.
- Requirement for continuous model updating, explainability, and auditable processes to meet regulatory scrutiny and ensure fairness.

Safeguards should include the deployment of multi-layer encryption, advanced access controls, model validity monitoring, and hybrid human-AI review processes. Furthermore, ongoing algorithm audits, stakeholder collaboration, and adherence to sectoral and international compliance standards will be necessary.

Key Takeaways

1. AI excels at identifying complex patterns and networks but cannot fully replace human intuition for ambiguous or novel cases. Hybrid approaches — where AI flags

and human experts review critical cases — produce the most trustworthy, effective compliance outcomes.

2. Quality and diversity of data are key to trustworthy AI; continuous updates and real-world feedback dramatically improve system performance. Regular retraining of models with real-world and synthetic financial crime data improves system adaptability and resilience.

3. AI systems require ongoing adaptation to shifting criminal tactics and regulatory change, making flexibility and explainability paramount for sustainable compliance.

4. Cross-industry standards, ongoing regulatory engagement, and modular architecture are vital for sustainable and secure AI adoption in digital asset compliance.

In summary, the use of AI in digital asset compliance — especially for analyzing transactional data and mapping illicit networks — yields transformative gains in effectiveness and efficiency, as long as risks are managed through robust governance, technical safeguards, and continuous human involvement.

a. What factors do financial institutions consider when deciding whether to employ AI for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use AI for these purposes, what specific compliance functions does/will AI support? For financial institutions that decided not to use AI, please provide additional details on the rationale for that decision.

When deciding whether to employ AI for AML/CFT and sanctions compliance, financial institutions consider factors that broadly mirror those assessed for APIs—such as regulatory clarity, cost, data privacy, cybersecurity requirements, organizational readiness, scalability of existing systems, and risk profiles. Unique aspects in the AI context include model transparency/explainability, algorithmic bias, governance frameworks, and human oversight requirements.

Factors Considered for AI Adoption

- **Regulatory and legal certainty**: Firms need clear guidance on how AI-driven decisions are audited, justified, and align with risk-based expectations, especially amidst evolving regulations and examiner expectations.
- **Transparency and explainability**: The ability to demonstrate how AI models reach decisions (explainable AI) is critical for regulator and auditor confidence, and mitigating compliance risk.
- **Operational efficiency and effectiveness**: AI's automation, real-time analytics, and ability to process large volumes can reduce false positives, costs, and manual workload.
- **Cybersecurity and data privacy obligations**: Sensitive transactional and customer data, regulatory reporting, and cross-jurisdictional privacy regimes require robust data protection for AI use.
- **Organizational readiness and governance**: Institutions assess skills, technology infrastructure, and whether comprehensive governance frameworks are in place, including model validation and oversight.

For financial institutions that use or plan to use AI for these purposes, AI supports the following compliance functions:

- Transaction monitoring and risk scoring (real-time detection, anomaly analysis, pattern recognition).
- Sanctions screening, watchlist matching, adverse media and PEP checks (using NLP and advanced matching algorithms).
- Customer and counterparty due diligence, onboarding, perpetual KYC, and identity fraud prevention.
- Alert adjudication, case investigation, compliance reporting, and automated filing.
- Network analysis (graph analytics to identify illicit financial networks or coordinated market abuse).

For financial institutions that decided not to use AI, their rationales include, but are not limited to:

- Some institutions avoid AI due to concerns about opaque "black box" decisions, inadequate internal frameworks, or model validation difficulties.
- High investment needed to build, monitor, and integrate AI into existing systems; difficulty retrofitting legacy infrastructure.
- Risk of data breach, model manipulation, and insufficient regulatory clarity for algorithmic decisions, especially for sanctions/AML obligations in multi-jurisdictional environments.
- Some legacy processes are viewed as adequate or lower risk, especially where transaction volume and complexity are less pronounced.

How This Differs From API Adoption

In addition to all the considerations noted for APIs — such as integration, regulatory change adaptation, and interoperability — AI adoption places greater emphasis on model governance, explainability, data bias, regulatory scrutiny over automated decision-making, and human-machine collaboration.

APIs are typically viewed as connectors or automation layers integrating tools and rule engines, while AI is the "decision engine" itself, requiring new forms of risk management and transparency. For APIs, technical integration, endpoint security, and scalability are the principal concerns; for AI, model oversight, fairness, legal certainty, and ethical management are critical points.

b. How are financial institutions using AI tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of AI tools with other previous or existing tools used for similar purposes.

AI is increasingly used to augment, test, or replace legacy compliance tools, delivering marked improvements in detection, adaptability, efficiency, and cost over previous manual and rules-based methods. The transformation is most pronounced where transaction complexity, volume, and regulatory pressure are highest.

Financial institutions currently deploy AI tools in AML/CFT and sanctions compliance in three main patterns: as pilots in testing phases alongside legacy solutions, as augmentation to existing rules-based or manual systems, and increasingly as replacements for traditional tools in advanced compliance programs. Many institutions start by integrating AI to enhance alert triage and transaction analytics within legacy platforms, often running side-by-side testing to compare accuracy, speed, and scalability. As confidence in AI's risk detection grows, some financial institutions are fully replacing older systems with adaptive, agentic AI models, allowing real-time pattern recognition, dynamic risk scoring, and superior network analysis capabilities for complex typologies and cross-border threats.

Compared with previous and legacy compliance tools, AI-driven platforms yield several advantages: much higher accuracy and efficiency in identifying suspicious activity, with reductions in false positives and manual review workloads by 35–55% relative to rules-based software; ability to adapt quickly to emerging money laundering and sanctions evasion tactics; unified analysis across fragmented datasets and jurisdictions; and significant operational cost savings. Agentic AI models resolve fuzzy matches, dynamically interpret ambiguous customer data, and provide real-time explanations and audit trails, far surpassing deterministic logic or scripted batch processing in both flexibility and outcome quality.

Legacy systems, while valued for their consistency in low-risk batch screening, have proven insufficient in meeting advanced regulatory demands and handling volumes/complexity of modern digital asset markets. Augmentation — though helpful — rarely achieves full risk-based compliance, prompting many leading institutions to invest in full AI transformation for more strategic, audit-ready, and adaptive financial crime prevention.

In summary, financial institutions are steadily moving toward full AI-driven compliance for AML/CFT and sanctions, finding marked improvements in detection, workflow efficiency, and regulatory responsiveness, especially as transaction complexity, digital asset adoption, and global regulatory pressures escalate.

c. Are there regulatory, legislative, supervisory, or operational obstacles to using AI to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Many foundational compliance barriers and recommendations overlap for APIs and AI — such as privacy, cybersecurity, regulatory clarity, and data governance. But AI introduces additional complexity, scrutiny, and risk around transparency, fairness, ethical oversight, and algorithmic accountability that are not part of API-focused compliance, making its adoption a more multifaceted regulatory and operational challenge.

Regulatory, legislative, supervisory, or operational obstacles to using AI (distinct from APIs)

- AI-Specific Challenges: AI poses unique risks around model transparency ("black box" decision-making), algorithmic bias, explainability, and governance that do not exist with APIs. Regulators usually have more concerns about how AI models reach conclusions, their fairness, and whether decisions can be justified in audits or legal proceedings. APIs typically function as connectors or data pipelines, making integration and security their primary regulatory challenges.
- Data Quality and Model Integrity: AI adoption requires constant validation of training data to avoid bias, model drift, and manipulation ("model poisoning"), whereas APIs focus more on secure transmission, access control, and endpoint integrity.
- Human Oversight: Effective AI deployments need continual human-machine collaboration to mitigate automation errors — a governance oversight less emphasized with API-based data or workflow integrations

Recommendations related to identified obstacles

- Both API and AI use demand strict privacy protection, robust cybersecurity, ongoing government-industry dialogue, and harmonization of global compliance standards.
- Both call for clearer guidelines and more consistent examiner protocols to support innovation and risk mitigation. For AI specifically, AML/CFT standards and examiner

protocols should be harmonized across borders and asset classes, promoting interoperable and privacy-compliant AI models.

- Issue clear government guidance on AI model transparency, auditability, allowable use cases, and acceptable outcomes in financial crime detection.
- Support technical advances in privacy, cybersecurity, and adversarial resilience in AI-driven compliance platforms.
- Promulgate best practices for AI governance, bias monitoring, and human-machine review — all supported by interdisciplinary workforce training and collaboration between government, technologists, and compliance professionals.

d. What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of AI for detecting illicit finance involving digital assets?

The U.S. government should focus on guidance for AI transparency/auditability, technical standards for bias and security, interdisciplinary capacity building, sandbox experimentation, stakeholder engagement, and international regulatory harmonization. These steps directly address the distinct risks and operational needs of AI adoption in digital asset AML/CFT, extending far beyond the requirements for API frameworks and enabling responsible, innovation-driven financial crime prevention. The U.S. government should take several unique steps to facilitate the effective, risk-based adoption of AI for detecting illicit finance involving digital assets, beyond the measures needed for APIs.

Actions for AI Risk-Based Adoption

- Publish explicit standards for AI transparency and explainability: Issue regulatory guidance detailing audit requirements, model documentation, and required levels of interpretability so financial institutions can deploy AI with confidence under examiner review. Rather than relying on prescriptive technical rules that can quickly become obsolete, such a framework should be principles-based and emphasize outcomes and governance processes that ensure AI operates effectively, fairly, and transparently.

- Advance standards for AI model governance and bias management: Support frameworks for continuous bias testing, adversarial attack resilience, and model validation that go beyond basic technical audits — helping institutions ensure fair, accurate decisions in AML/CFT and sanctions compliance. Validation should also address model drift and performance degradation over time, with more rigorous testing required for AI systems making high-consequence determinations.
- Promote interdisciplinary training and certification: Fund professional development programs combining AI, compliance, law, and cyber skills to cultivate the human expertise needed for ethical and effective oversight of machine learning in critical financial systems.
- Accelerate regulatory sandboxes and innovation pilots: Provide venues for collaborative testing and policy shaping, enabling financial institutions and regulators to assess AI effectiveness, risk, and compliance in realistic scenarios before market rollout. Sandboxes could also support testing of privacy-preserving AI techniques that enhance detection capabilities while protecting legitimate customer privacy.
- Encourage industry-regulator dialogue and best practice sharing: Facilitate regular cross-sector consultation to keep regulations, risk frameworks, ethical standards, and industry practice aligned with technological advancement and emerging threats.
- Lead global harmonization efforts for AI compliance: Drive the creation of international standards — especially around privacy, cross-border data, and audit protocols — so AI systems used for digital asset compliance are interoperable, effective, and trustworthy worldwide.

These steps, especially around transparency, bias, governance, training, innovation, and harmonization, are critical for responsible AI adoption in digital asset compliance and go much further than what is needed for APIs, due to AI's complexity, risk profile, and regulatory sensitivity.

e. Treasury will evaluate AI and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

The factual risks, benefits, and recommendations have been addressed in detail in earlier answers. However, when Treasury evaluates AI adoption for illicit finance detection under the GENIUS Act, it will likely need to frame its evaluation based on the specific research factors in the Act: effectiveness, cost, privacy and cybersecurity risks, operational impact, and other risk-based considerations. Here is the information pertinent to each factor for AI in digital asset compliance:

Effectiveness

AI enables real-time, scalable detection of complex illicit activity through advanced analytics, machine learning, natural language processing, and graph/network analysis. It can identify hidden money laundering typologies, adapt rapidly to shifting threats, and deliver higher accuracy with lower false positives than traditional rules-based approaches. Financial institutions using AI report improvements in speed, pattern detection, and the ability to uncover multi-jurisdictional illicit financial networks.

Cost

While AI can reduce manual workload and long-term costs through automation and higher detection accuracy, initial implementation costs are substantial, encompassing software investment, model training, integration with core systems, and workforce upskilling. Ongoing costs involve model maintenance, governance, monitoring, and periodic validation to ensure compliance with new regulatory standards and changing fraud tactics.

Privacy and Cybersecurity Risks

AI models require access to large volumes of sensitive data, making them targets for cyberattacks, model poisoning, or adversarial manipulation. Strong safeguards are essential, including encryption, access control, privacy-preserving protocols, and regular vulnerability testing. Data privacy compliance is also a challenge, as AI-driven analytics must remain consistent with cross-border regulations like the GDPR and CCPA, necessitating modular controls and transparency frameworks.

Operational Impact and Challenges

Operationally, AI adoption may disrupt legacy risk management and require new governance structures to ensure model explainability, fairness, and accountability. Challenges include integration with existing workflows, securing sufficient, diverse data for model training, aligning with varying examiner expectations, and maintaining up-to-date documentation and audit trails. Many financial institutions are still in the process of building the talent and governance necessary to oversee AI-driven compliance responsibly.

Additional Risk-Based Considerations

AI introduces unique regulatory and ethical risks around transparency ("black box" decision-making), bias, and fairness. Regulatory agencies, guided by the GENIUS Act, should clarify audit expectations, standardize model validation, and encourage human-in-the-loop review for high-stakes compliance determinations. Multistakeholder dialogue, regulatory sandboxes for AI piloting, international harmonization, and robust technical and privacy standards are all recommended steps to ensure safe, effective, and trusted AI deployment for financial crime detection.

4. **What innovative or novel methods, techniques, or strategies related to digital identity verification are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to digital identity verification? Please describe the portable digital identity credentialing tools in use and how such tools are being used.**

U.S. financial institutions use a mix of AI-powered KYC, biometrics, and document verification; they are piloting portable digital wallet tools, but full adoption is limited by evolving federal and state regulations, interoperability standards, and privacy/cyber concerns. Some innovations cannot be deployed if they conflict with NIST, federal, or state-level standards, especially around biometrics and credential interoperability.

American financial institutions use innovative digital identity verification techniques — including AI-driven biometrics, advanced document authentication, and portable digital identity credentialing tools — to support AML, CFT, and sanctions compliance for digital

assets. AI is leveraged for real-time liveness detection, facial/voice/behavioral biometrics, anti-deepfake measures, and automated risk profiling to rapidly onboard and monitor users. Blockchain-based digital identity models create tamperproof audit trails and enable privacy-protecting, cross-jurisdictional verification.

Portable digital identity credentialing tools — like mobile driver's licenses (mDLs) and digital wallets with reusable verifiable credentials—are gaining traction in the U.S. These wallets store government-issued IDs and KYC results, and allow users to selectively disclose identity attributes across banks, exchanges, and payment platforms. Some DeFi platforms and crypto apps are piloting credentialing frameworks that embed identity checks into smart contracts, enforcing KYC before transactions execute.

The Transaction Authorization Protocol - an open messaging standard widely adopted for Travel Rule compliance and pre-transaction authorization processes - enables selective disclosure and proof-of-relationship mechanisms. TAIP-10 integrates IVMS-101 standard into TAP messages, while TAIP-11 permits inclusion of LEIs to unambiguously identify institutional participants. TAIP-12 provides hashed participant names to verify identities without exposing full personal data.

GLEIF with its technical partner is bringing the LEI identity standard onchain, which unlocks critical capabilities for realizing tokenized finance at scale:

- Stablecoin issuers can prove their legal identity at the contract level, ensuring regulators, markets, and users can distinguish between genuine, reserve-backed stablecoins and fraudulent imitations.
- Asset issuers and smart contract applications can unlock seamless compliance with regulations across different jurisdictions, such as Europe's Markets in CryptoAssets Regulation (MiCA), the U.S. Financial Data Transparency Act (FDTA), and the Financial Action Task Force (FATF) requirements.
- Custodians and Virtual Asset Service Providers (VASPs) can verify that receiving addresses meet FATF Travel Rule requirements without exposing customer data. In this model, GLEIF provides verifiable Legal Entity Identifier (vLEI) credentials, which serve as trusted digital identity attestations. These are then anchored onchain as Cross-Chain Identities (CCIDs) using Chainlink's infrastructure. Custodians and VASPs can reference and verify these credentials through Chainlink's Automated

Compliance Engine (ACE), allowing FATF Travel Rule compliance checks without revealing customer data.

- Enables unique, verifiable identification of counterparty institutions linked to wallet addresses, supporting counterparty risk assessment and accurate routing of required Travel Rule information to the correct legal entity.
- Facilitates secure, standardized transmission of legal entity credentials to satisfy Travel Rule requirements efficiently and consistently across jurisdictions.
- Banks and asset managers can issue tokenized assets with verifiable provenance throughout the asset's lifecycle.
- Enterprises can restore control of compromised contracts using role-based recovery mechanisms.
- Regulators can supervise transactions with assurance of compliance while also preserving user privacy.
- Trading venues can restrict participation to verified entities through onchain credential checks.
- Investors and institutions can confirm the legal ownership of specific wallets with ease.

Used in America:

- mDLs and digital identity wallets from vendors that align with the NIST Identity Assurance Level (IAL) standards are increasingly used, particularly for onboarding and KYC refreshing.
- Modular eKYC solutions with biometric and document verification have broad deployment, as do AI-driven identity fraud detection tools.
- Select pilot programs in DeFi leverage portable credentials and smart contract integrations for transaction-level KYC.

Not usable in America (due to regulatory limitations):

- European-centric digital ID frameworks like the EUDI Wallet, some blockchain/DID identifiers, and W3C global credentials may be excluded from U.S. government use if they don't meet current federal standards (e.g., NIST IAL2).

- Solutions relying on facial recognition or certain biometrics may be prohibited or restricted for federal agencies and affected by proposed biometric moratoriums, depending on legislation and privacy concerns.
- Many portable digital credentialing solutions that bypass in-person or document checks might not be recognized for compliance purposes due to American rules demanding robust multi-factor, real-world identity proofing.

a. *What factors do financial institutions consider when deciding whether to employ digital identity verification for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use digital identity verification for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use digital identity verification, please provide additional details on the rationale for that decision.*

Financial institutions decide whether to use digital identity verification by asking four practical questions: (1) Will it meet supervisory expectations for "reliable, independent" identification? (2) Can the identity be strongly bound to a device or channel so the right person is the one transacting? (3) Are the resulting records auditable across borders and retention-compliant? (4) Does it interoperate with sanctions screening, Travel Rule workflows, and existing KYC/KYB vendors at acceptable latency and cost? Firms also test coverage for thin-file customers and businesses, the strength of fraud defenses (liveness, device and telco signals, duplicate detection), and privacy posture under data-minimization and data-transfer rules. Increasingly, they evaluate privacy-preserving options, especially zero-knowledge proofs (ZKPs), that let them prove required facts without over-sharing personal data.

When adopted, digital identity supports the full compliance lifecycle. At onboarding, it verifies customers and beneficial owners, improves entity resolution for sanctions and adverse-media screening, and seeds risk scoring and segmentation. During the relationship, it enables timely refreshes and event-driven reviews, and it powers pre-transaction controls on fast, irreversible rails (for example, stablecoin withdrawals or L2 transfers) so counterparties can be cleared before funds move. ZKPs enhance these controls without weakening them: a user (or their credential issuer) can prove "not on a sanctions list," "resident in an allowed jurisdiction," "over 18," or "verified by a

supervised KYC provider in the last N days" without revealing the underlying PII. Financial institutions can exchange ZKP attestations that Travel Rule data were collected and matched, or that a wallet belongs to a "KYC-cleared set," while retaining the ability to unmask details under lawful order. Properly engineered, this reduces cross-border data friction and breach surface area, complies with GDPR requirements, yet preserves an auditable trail (proof timestamps, issuer identity, circuit version, and revocation status).

Some institutions delay or limit digital identity, or ZKPs specifically, when prerequisites are not yet in place. Typical blockers include thin or unreliable data sources in target markets; uncertainty about whether ZKP attestations alone satisfy statutory "collection and retention" duties; immature interoperability across credential schemas, revocation methods, and proof formats; and operational readiness gaps for credential issuance, revocation, circuit management, and audit.

Additionally, regulatory definitions of identity remain rigid — requiring fixed attributes such as legal name, address, and government-issued documents—and often mandate the transmission and storage of full records rather than privacy-preserving attestations. Similarly, record-keeping rules typically require centralized retention of personal data for extended periods, discouraging decentralized or privacy-minimizing architectures. Limited regulatory acceptance of delegated customer due diligence (CDD) — where one entity relies on another's verified credential or cryptographic proof — also hinders scalable, cross-platform reuse of KYC checks. In those settings, firms retain traditional documentary KYC or hybrid models while piloting digital identity and ZKP-based selective disclosure in narrow, high-impact flows (for example, sanctions negative-match proofs for high-risk withdrawals or Travel Rule collection proofs).

Where institutions proceed, clear guardrails make the difference between a pilot and a production-grade control. They establish supervised trust anchors with liability and real-time revocation; define freshness windows for proofs and enforce revocation checks; minimize correlation through one-time proofs and pair-wise pseudonyms; keep immutable logs of verification events; and maintain documented unmasking procedures for lawful orders. They treat ZKPs as an augmentation of conventional KYC: the underlying identity data remain with a supervised issuer, day-to-day screening relies on proofs, and unmasking occurs only when required. This approach aligns with

risk-based expectations, strengthens AML/CFT and sanctions outcomes, and fits the privacy and interoperability constraints of modern, cross-border compliance.

b. How are financial institutions using digital identity verification tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of digital identity tools with other existing or previous tools used for similar purposes.

Financial institutions are using digital identity verification to augment — not replace — their existing AML/CFT and sanctions stacks. In practice, digital ID tools are layered alongside KYC/KYB/CIP and ongoing monitoring to improve how firms answer three core questions at onboarding and throughout the relationship: does the person exist (identity resolution), are the source records trustworthy (from reliable relationships), and is the session actually them (secure channel/device binding). This "establish–authenticate–authorize" model strengthens CDD and ties assets and activity to a verified party, aligning with FATF's digital identity guidance on using reliable, independent sources within a risk-based approach.

Effectiveness improves further when institutions treat CDD as an ongoing process, refreshing customer profiles, updating beneficial ownership, and risk-segmenting populations to trigger EDD for higher-risk customers, sectors, jurisdictions, or digital-asset activity. This continuous KYC/KYB/CDD cycle is a regulator-recognized cornerstone that supports sanctions screening (e.g., nationality, residence, counterparty jurisdictions), PEP handling, and source-/destination-of-funds assessments. Relative to prior, static KYC programs, these digital identity workflows deliver richer data for sanctions filtering and suspicious activity monitoring, and create clearer audit trails for supervisors.

Overall, compared with earlier, single-source KYC, modern digital identity verification is more effective because it (1) triangulates across trusted, reliable sources; (2) binds identity to secure channels/devices; and (3) supports continuous CDD with risk-based refreshes.

c. Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Regulatory and legislative: U.S. requirements already extend to many digital-asset services through the Bank Secrecy Act and related AML/FCC obligations, but application is still uneven where obligations turn on the specific "activities and practices" of a provider (e.g., when a digital-asset business is an MSB and thus BSA-covered). Federal authorities have reiterated that facts and circumstances drive registrations and duties, yet comprehensive application to digital-asset services "has not yet been reached" in the U.S. This creates ambiguity for web-native and decentralized models, even as Executive Order 14067 and Treasury's action plan seek to address sector risks. Internationally, FATF's risk-based standards set the baseline, but jurisdictions differ in how they implement digital-identity and AML expectations, complicating cross-border operations and supervision.

Supervisory: Examiners are accustomed to bank-style controls and records; assessing on-chain programs, decentralized governance, and modern identity credentials (e.g., DIDs/VCs) can be inconsistent. At the same time, FATF has emphasized that AML/CFT effectiveness, not mere technical compliance, should be the benchmark, and that financial inclusion and integrity are mutually reinforcing. Supervisory practices must therefore evolve to evaluate digital-identity controls, risk scoring, and monitoring in web-native environments on a risk-based basis, not by analogy alone.

Operational: Fragmented data-access rules and cross-jurisdictional constraints make it hard to share or verify identity data while meeting reporting duties (e.g., SARs) and law-enforcement requests. Reliance on traditional, centralized identity systems introduces single-points-of-failure and concentration risk; conversely, decentralized identity (self-sovereign identity using DIDs/VCs) is still maturing in issuance, revocation, and governance. Firms also face de-risking pressures: growing FCC obligations can push providers to exit higher-perceived-risk customers, sectors, or markets, undermining inclusion and, paradoxically, the traceability benefits that digital rails and digital identity can provide.

Recommendations: First, anchor policy to FATF's risk-based approach and clarify obligations by activity: specify when and how digital-asset services (centralized or

decentralized) assume full AML/CFT duties, so controls can be engineered at the right layer. Second, modernize supervision to focus on effectiveness: publish examiner guidance that recognizes digital identity as the entry point to CDD/CIP, and that evaluates risk scoring, ongoing monitoring, and sanctions screening in web-native contexts. Third, promote interoperable, privacy-preserving digital identity: encourage adoption of DIDs/VCs, with clear trust anchors, revocation, and verification processes, so institutions can prove what is required while limiting over-collection of PII. Fourth, strengthen public-private collaboration and international coordination so data-access, reporting, and cross-border investigations can function in real time. Finally, support the responsible use of blockchain tracing and analytics to leverage the auditability and transparency of distributed ledgers — turning the technology's inherent attributes into stronger AML/KYC outcomes while mitigating de-risking by bringing more activity onto traceable, compliant rails.

d. What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets?

Create a federal sandbox that lets agencies and regulated firms pilot privacy-preserving digital-ID approaches alongside payment innovations (including self-hosted wallets and payment stablecoins) to surface governance, technical, and supervisory standards before at-scale deployment. The brief explicitly recommends a public-private sandbox to inform future standards, reduce improper-payment and fraud pain points, and maximize digital-ID deployment.[4]

Anchor adoption to NIST SP 800-63-4 and other standards in the federated architecture. Use the updated federal digital-identity guideline as the baseline for assurance, authentication, and lifecycle management, and encourage a federated "trust layer" (issuers, verifiers, relying parties) so private and public actors can interoperate without centralizing all personal data.

Mandate interoperability and verifiable-credential support. Direct agencies to accept (and vendors to issue/verify) W3C-style verifiable credentials and eIDAS-aligned wallets where feasible, to enable portable, auditable proofs of identity and attributes that work across jurisdictions and sectors. The brief emphasizes international moves toward

[4] Atlantic Council

harmonization and pilots around wallet-based credentials; U.S. policy should mirror that emphasis on interoperability.

Codify privacy protections (data minimization, portability, redress) while requiring "integrated verification" across agencies and their private partners to shrink ID-based fraud vectors, U.S. guidance should require both privacy safeguards and joined-up verification.

Institutionalize cross-agency and law-enforcement information sharing. Establish regular, structured exchanges on emerging fraud/abuse patterns and early-warning indicators tied to digital IDs used in benefits and payments, so that signals feed both prevention and investigations. The brief calls for periodic engagement and information-sharing strategies to keep pace with evolving threats.

Fund pilots that combine digital ID with modern payment rails. Sponsor R&D and pilots for a "federated technology stack" that integrates digital identity with novel payment solutions (including stablecoins), with clear guardrails and measurement of fraud-reduction and inclusion outcomes. This is highlighted as a near-term opportunity for the U.S. to advance standards and practice.

Promote international alignment — use MOUs and standards cooperation (as the EU and Japan have done) to ease cross-border recognition of trusted IDs and verification flows that accompany digital-asset transfers. Success in the EU and Japan is coming from (1) clear governance with a federated trust layer, (2) wallet/credential interoperability, and (3) targeted pilots that balance privacy with fraud reduction. Translating those lessons to U.S. digital-asset contexts through a sandbox, standards conformance, VC/eIDAS-style interoperability, integrated verification, and structured public-private collaboration—would enable risk-based digital-ID verification that both protects civil liberties and strengthens illicit-finance detection on faster, programmable rails.

e. Treasury will evaluate digital identity verification and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

Financial Data Transparency Act (FTDA) was enacted as Title LVIII of the FY23 NDAA (P.L. 117–263). The FDTA as enacted amends subtitle A of the Financial Stability Act of 2010 (Financial Stability Act) by adding a new section 124, which directs the Agencies jointly to issue regulations establishing data standards for (1) certain collections of information reported to each Agency by financial entities under the jurisdiction of the Agency, and (2) the data collected from the Agencies on behalf of the Financial Stability Oversight Council (FSOC). The term "data standard" is defined by the statute as a standard that specifies rules by which data is described and recorded, and its core is a legal entity identifier.

Treasury should consider incorporating statutory language on the use of identifiers to promote efficiency and transparency. This alignment with the FDTA would be beneficial because the FDTA statute mandates two sets of rulemakings: first, the joint rulemaking for the financial agencies to establish the data standard/identifier (released August 2024), and second, a series of individual agency-specific rulemakings that apply the final data standard to their information collections. With the Treasury as party to the August 2024 rule, incorporating references to the LEI/vLEI or the FDTA's common identifier/data standard language into the market structure legislation will give both agencies direction on the intersection between the legislation and the FDTA. This would also give digital market participants clarity from the start on whether they may be expected to provide an identifier as part of their registration. As it relates to digital assets, the LEI can be implemented for the identification of crypto and virtual asset service providers, digital asset and stablecoin issuers, and more generally entities that participate in crypto markets, for example, stablecoin custody service providers.

5. **What innovative or novel methods, techniques, or strategies related to blockchain technology and monitoring are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to blockchain technology and monitoring? Please describe how financial institutions are integrating information from blockchain analytics with off-chain data and mention any key challenges associated with using blockchain analytics (e.g., obfuscation tools and methods that can complicate tracing and assessing confidence in attribution or complexities inherent in cluster analysis).**

Pre-transaction authorization protocols like TAP (the Transaction Authorization Protocol) are increasingly used to counter some of the above mentioned risks posed by the immediate and irreversible nature of settlement in blockchain based transactions. Travel Rule compliant pre-transaction authorization processes introduce a fundamental architectural shift with implications extending far beyond Bank Secrecy Act compliance into sanctions enforcement, fraud prevention, and consumer protection. This innovation addresses multiple regulatory objectives simultaneously through a single infrastructure layer. Specifically, it allows institutions to tie blockchain transactions to real world identities (through exchanged Travel Rule information) before settlement. This allows institutions to:

- Perform sanctions screening and risk assessment against OFAC lists and other sanctions databases before blockchain transaction execution. This timing proves essential for sanctions enforcement because once a transaction settles on-chain, preventing sanctioned parties from accessing the funds becomes operationally complex if not impossible.

- Enhance fraud controls through pre-transaction verification of beneficiary name. Institutions are able to collaborate on exchanging information about the parties to a transaction and verify that the intended beneficiary of the transaction (as declared by the originator) is the actual recipient of funds.

a. *What factors do financial institutions consider when deciding whether to employ blockchain technology and monitoring for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use blockchain technology and monitoring for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use blockchain technology and monitoring, please provide additional details on the rationale for that decision.*

When evaluating whether to employ blockchain technology for AML/CFT and sanctions compliance, financial institutions weigh several factors: the effectiveness of available tools, the ability to integrate with existing compliance systems, the readiness of supervisory authorities to interpret blockchain evidence, and the regulatory expectations imposed by new legislation. Increasingly, these decisions are shaped by statutory frameworks such as the GENIUS Act, which applies comprehensive financial surveillance requirements to stablecoin issuers and mandates unprecedented technical capabilities for real-time transaction monitoring and enforcement. While sanctions prohibitions apply to U.S. persons regardless, GENIUS extends those obligations directly to payment stablecoin issuers (PPSIs) and requires them to implement programs comparable to those of traditional financial institutions, even at the token level.

For institutions that adopt blockchain monitoring, the technology supports a wide range of compliance functions. Modern compliance architectures combine identity verification, sanctions screening, and behavioral transaction analytics into unified platforms that operate in real time across both centralized and decentralized ecosystems. These systems are capable of:

- Flagging high-risk jurisdictions, sanctioned counterparties, and cross-chain laundering patterns before settlement occurs;
- Employing dynamic risk scoring and AI that reduces false positives and strengthens detection accuracy;
- Monitoring on-chain events and counterparties associated with potential illicit finance, including proceeds from exploits or scams moving between decentralized and centralized platforms;

- Maintaining immutable, auditable logs that support supervisory review and enforcement

The effectiveness of such systems ultimately depends on institutional investigative capacity, the ability of compliance teams to evaluate alerts, prioritize cases, and act on findings in a timely manner. Equally, supervisory bodies must be equipped to interpret on-chain evidence and evaluate the adequacy of institutions' controls.

New tools could include mandatory blockchain analytics with flexible and configurable risk rules that allow for dynamic and real-time behavioral-pattern detection requirements for crypto native players and banks to flag illicit financial activities; statutory data-sharing between private forensics and law enforcement; and designated legal obligations for tracing scam-connected addresses automatically and filing the suspicious activities reports.

Blockchain analytics can be deployed proactively to disrupt these networks by:

- Mapping scam funds flows across wallets, exchanges, and mixers to reveal laundering pathways.
- Detecting behavioral signatures such as repeated small deposits from multiple victims, rapid wallet churn, and ties to known scam clusters.
- Flagging high-risk wallets so exchanges and banks can block transfers, freeze funds, or file SARs before perpetrators off-ramp their proceeds.

Key regulatory requirements to the digital asset intermediaries such as exchanges, custodians, and wallet providers with the capacity to control customer funds or effect transactions should include:

- Explicitly applying the BSA to digital asset platforms, requiring know-your-customer (KYC), travel rule, customer due diligence, suspicious activity reporting, and transaction monitoring.
- Mandating robust, auditable recordkeeping, even for transactions involving unhosted or cross-border wallets, while respecting lawful privacy practices.

- Supporting the adoption of blockchain analytics and dynamic, risk-based compliance technology to proactively identify and stem illicit flows.
- Facilitating coordinated information sharing between regulators, law enforcement, and industry, with safeguards against overreach or privacy violations.

Institutions that choose not to adopt blockchain monitoring typically cite the scale and complexity of on-chain data, the lack of clear supervisory standards, or insufficient investigative resources to meaningfully act on alerts. However, the trend is clear: the greatest risks arise not from blockchain itself but from how criminals exploit liquidity, obfuscation tools, and regulatory blind spots. Financial institutions that invest in cross-chain analytics, behavior-based monitoring, and proactive alignment with GENIUS-style obligations are better positioned to detect multichain laundering, enforce sanctions compliance at scale, and keep pace with increasingly professionalized illicit actors.

b. How are financial institutions using blockchain technology and monitoring tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of blockchain technology and monitoring tools with other existing or previous tools used for similar purposes.

Financial institutions are increasingly using blockchain technology and monitoring tools not as a wholesale replacement for existing compliance infrastructures, but as an augmentation that addresses blind spots in traditional systems. In practice, this means deploying blockchain analytics in parallel with legacy transaction monitoring, sanctions screening, and KYC systems. While some institutions remain in a testing phase, the prevailing trend is toward integrating blockchain monitoring to strengthen real-time oversight, improve detection accuracy, and reduce reliance on after-the-fact reconciliation processes.

It is important to emphasize that blockchain analytics are not the same as blockchain technology itself. Blockchain technology is the underlying market infrastructure: decentralized, cryptographically secured ledgers (e.g., Bitcoin, Ethereum, Solana) that record transactions immutably and transparently. Blockchain analytics, by contrast, are off-chain applications built on top of that infrastructure. They do not alter or extend the

blockchain; instead, they ingest, index, and analyze publicly available blockchain data (sometimes enriched with proprietary inputs) to provide risk scoring, wallet clustering, transaction tracing, and monitoring capabilities. Most of these platforms are built using Web2 infrastructure (databases, APIs, and machine learning engines) to process blockchain data at scale. They are best described as Web3-adjacent: while not themselves decentralized protocols, they analyze and interpret Web3/blockchain activity, making it actionable for compliance teams. In this sense, blockchain analytics are not blockchain technology, but tools that leverage blockchain data to deliver compliance insights.

Distributed ledger technology (DLT) offers distinct compliance advantages over conventional infrastructure. Its immutable record provides tamper-resistant audit trails that can be independently verified, unlike siloed financial databases that require reconciliation across intermediaries. The granularity of blockchain data allows financial institutions to trace the full journey of funds, including indirect exposures, offering visibility that surpasses what is available in traditional payment networks.

Blockchain monitoring also enables real-time, pre-transaction compliance checks. This proactive capacity is especially valuable for stablecoin transactions and cross-border digital asset transfers, where speed and irreversibility heighten risks. By integrating blockchain analytics into compliance workflows, institutions can not only detect but also prevent illicit activity before it enters the financial system.

Given the transparent yet permissionless nature of blockchain-based assets, financial institutions and regulators are beginning to recognize that a new paradigm is required - one that goes beyond traditional Know-Your-Customer (KYC) and Know-Your-Transaction (KYT) frameworks. A Know-Your-Ecosystem (KYE) model introduces a more holistic approach to risk management, tailored to the unique dynamics of digital asset markets. Under this model, regulators could require:

- Ecosystem-wide risk assessments: obligating stablecoin issuers and other intermediaries to map and monitor key participants in their operational environment, including custodians, validators, liquidity providers, and on/off-ramp service providers.

- Counterparty due diligence requirements: mandating rigorous vetting of service providers, liquidity sources, and operational partners to mitigate compliance, operational, and reputational risks.
- Real-time intelligence and threat monitoring: ensuring that issuers leverage advanced analytics and intelligence tools to proactively detect illicit flows, anomalous trading behaviors, or emerging threats across their ecosystems.
- Threshold-based alerting and escalation protocols: requiring issuers to set predefined risk thresholds, implement early-warning indicators, and establish real-time response mechanisms when ecosystem-wide risks are detected.

KYE extends KYC or KYT to reflect the interdependencies and systemic risks inherent in permissionless blockchain environments. By embedding this broader perspective, financial institutions can more effectively manage ecosystem-level vulnerabilities that traditional frameworks alone are ill-suited to capture.

The novel risks in this ecosystem stem from the design and usage of public, permissionless blockchains. As highlighted in the Risk Mitigation Framework (RMF)[5], these include:

- Private key management risks: digital assets depend on cryptographic keys, and loss or compromise can mean permanent loss of funds.
- Information security and technology risks: smart contract exploits, consensus attacks, and cryptographic vulnerabilities specific to blockchain systems.
- Decentralized governance risks: limited accountability mechanisms, reliance on dispersed governance processes, and the absence of traditional SLAs.
- Enhanced financial crime risks: pseudonymity and transaction irreversibility make illicit activity harder to reverse once executed.
- Legal and regulatory uncertainty: smart contract enforceability, decentralized custody arrangements, and unclear accountability.

[5] Risk Mitigation Framework (RMF)

Blockchain analytics help mitigate some of these risks by enabling better traceability, faster detection, and more effective law enforcement collaboration. They complement existing compliance systems by providing visibility into the permissionless environment, where legacy tools alone are insufficient.

Taken together, financial institutions view blockchain analytics as a powerful augmentation to existing AML/CFT and sanctions compliance architectures. They do not replace legacy monitoring, but they fill critical gaps by shifting compliance from post-transaction reporting to proactive prevention, an evolution increasingly seen as essential to addressing the sophistication of illicit finance in digital assets.

c. Are there regulatory, legislative, supervisory, or operational obstacles to using blockchain technology and monitoring to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

Digital asset market participants, depending on their business model and activities conducted, are often required to follow extensive federal requirements including Bank Secrecy Act (BSA) obligations for Money Services Businesses (31 U.S.C. 5311 et seq and 31 CFR Chapter X), FinCEN's Travel Rule requirements (31 CFR 1010.410(f)), OFAC sanctions screening and comprehensive due diligence programs, Suspicious Activity Report (SAR) filing with enhanced virtual asset context, and customer due diligence (CDD) and enhanced due diligence (EDD) programs that often exceed traditional finance standards.

These rules were designed for cash-based or historical banking systems, so they do not always "map over" to digital assets, where the technological differences in how the systems operate can create massive challenges. For example, there is industry confusion on the Travel Rule[6], and we have seen global regulators in the UK, UAE, Canada, Hong Kong, Singapore, Japan, EU, and many more countries specifically "call out' problems with the Travel Rule and provide their own updated guidance/requirements (i.e., Transfer of Funds Regulation in EU). In particular, when implementing Travel Rule in digital asset transactions, it is essential to recognise the importance of pre-transaction compliance and implementation of authorization processes that precede settlement. As explained throughout this response,

[6] What is the Crypto Travel Rule? The FATF Crypto Travel Rule, Explained.

pre-transaction authorization supports multiple regulatory objectives simultaneously, including sanctions enforcement, consumer protection, and fraud prevention, making it an indispensable standard for risk management in digital asset transactions.

Furthermore, there is no question that with more digital asset market participants being subject to the BSA, BSA Modernization is essential. FinCEN has been working on this proposal for years and historically, it has included updating IT infrastructure, enhancing data analysis capabilities, and streamlining the BSA E-Filing System. Going forward, however, it should also include revisions needed to reflect the technological differences of digital assets and the massive improvements to AML/CFT that crypto offers regulators and law enforcement, as further explained below.

At the international level, the Financial Action Task Force (FATF)[7] sets global AML standards for digital assets through Recommendations 15 and 16[8], including the Travel Rule[9]. FATF has also prioritized fraud prevention by requiring beneficiary verification before execution. The Basel Committee offers additional prudential guidance for crypto-asset exposures.

At the federal level, FinCEN's 2019 guidance confirms that Bank Secrecy Act (BSA) obligations apply to virtual currencies. U.S. banking regulators (OCC, FDIC, and the Federal Reserve) supervise crypto-related banking activity, recently clarifying risk management and BSA/AML expectations for digital asset safekeeping. The CFTC and SEC regulate derivatives and securities markets, respectively, while OFAC enforces sanctions compliance, including for digital asset transactions.

At the state level, regimes like New York's BitLicense and state money transmitter licensing laws impose additional AML requirements, with oversight by state financial regulators and attorneys general. Collectively, these frameworks aim to mitigate illicit finance risks across the digital asset ecosystem.

[7] Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers

[8] FATF updates Standards on Recommendation 16 on Payment Transparency

[9] Best Practices Travel Rule Supervision

Across these touchpoints, expectations can diverge on unhosted-wallet treatment, Travel Rule exceptions, and acceptable vendor models, driving compliance inconsistency and, at times, forum shopping. Operationally, the industry still lacks common, machine-readable standards for exchanging compliance data: Travel Rule payloads, chain-aware sanctions identifiers (including contract addresses), and cross-chain risk signals. Talent remains scarce, particularly investigators fluent in multi-chain analysis, and there is limited model-risk guidance for analytics that cluster wallets, score counterparties, and link virtual value transfers. Even when funds are traced, asset recovery suffers from slow cross-border processes, uneven token-level freeze authorities, and inconsistent evidentiary standards.

According to RMF, legal risks when utilizing public blockchains are driven primarily by uncertainties in how laws, regulations, and contractual obligations are enforced. Three legal and regulatory risk themes stand out in public permissionless blockchain use:

- The absence of an attributable counterparty, due to decentralized or pseudonymous governance and no SLAs, can leave users without a legally recognized entity for recourse when failures or disputes occur, driving legal uncertainty, adoption barriers, and enforcement gaps. Mitigate by establishing clearer governance frameworks and escalation paths, performing legal/governance due diligence to identify contractable ancillary counterparties, maintaining transparent records of protocol changes, monitoring governance activity, and documenting controls for regulators.

- Smart-contract “contractual rights/obligations failure” arises when complex code or insufficient legal review produces on-chain behavior that diverges from parties’ intent, with immutability impeding correction—leading to asset loss, stalled processes, disputes, and reputational harm. Mitigate with standardized, audited templates; multidisciplinary pre-deployment audits; upgrade-enabled designs and vetted libraries; continuous monitoring against expected logic; and failover plans for pausing, migrating assets, notifying stakeholders, and pursuing legal remedies.

- A third risk - processing/execution failure in client-facing flows stems from the irreversibility of public-chain transfers, where small user or technical errors cause permanent losses and consumer-protection scrutiny. Mitigate through strict transaction-format standards and reference UI code, dual approval or strong

confirmations for high-value transfers, embedded data-quality checks and anomaly alerts, and defined corrective playbooks (e.g., pause/freeze hooks where available, off-chain remediation or insurance where contractual, and timely customer notice).

d. What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of blockchain technology and monitoring for detecting illicit finance involving digital assets?

US Government should take the following steps:

- Expand the definition of "financial institution" to cover a broader array of digital asset market participants (e.g., DeFi protocol operators with control, DAOs that perform custodial functions, wallet providers with asset control), thereby firmly bringing them under BSA jurisdiction.
- Expand FinCEN's authority to mandate more detailed information gathering, for example, at the wallet or transaction level, develop and broaden KYC compliance practices, to contemporary concepts such as Know-Your-Wallet or Know-Your-Transaction. In doing so, enabling authorities and reporting entities to leverage insights and intelligence offered by blockchain analytics data. Additionally, impose minimum behavioral detection standards and require information sharing on high-risk wallets or entities.
- Grant explicit authority to FinCEN over mixers, tumblers, and other anonymity-enhancing tools where there is a substantial nexus to illicit finance — but require any restriction be targeted and subject to oversight to protect lawful innovation and civil liberties.
- Promote international cooperation for cross-border investigations, AML/CFT standards cross borders and synchronized sanction/enforcement actions.

Regulators could explicitly require platforms to implement scam prevention measures, such as customer warnings and account freezes, and enhance authorities to facilitate asset recovery for victims.

Existing tools include: FinCEN SAR mandates, OFAC sanctions, DOJ enforcement requests to exchanges for KYC on scam funds, and blockchain analytics to flag scam

wallet flows and trigger alerts/SARs. The U.S. government should use its existing powers under the BSA and Section 314(b) of the USA PATRIOT Act to provide updated guidance affirming that beneficiary verification and pre-transaction fraud detection are essential elements of a risk-based AML framework. In parallel, agencies should promote tools that enable real-time fraud prevention and create clear mechanisms for victim restitution and recovery.

6. **What innovative or novel methods, techniques, or strategies related to any other innovative technologies such as cryptographic protocols and other privacy-enhancing tools, cloud-based solutions, on-chain compliance tools, oracles, or new verification tools for smart contracts are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to these other innovative technologies?**

Financial institutions increasingly integrate cloud-hosted compliance systems with blockchain monitoring platforms through API-based data exchanges. These cloud-native solutions enable scalable transaction analysis and real-time suspicious activity flagging across exchanges, custodians, and stablecoin issuers. On-chain compliance tools, including embedded compliance "hooks" in smart contracts, automate AML checks by enforcing predefined policies before asset transfers occur.

Treasury can spur compliance innovation by supporting regulatory technology pilots (e.g., on-chain KYC attestations, privacy-preserving compliance protocols, interoperable messaging layers for Travel Rule compliance, and network-level sanctions screening) that facilitate auditability, reporting, and cross-border verifiability while minimizing data exposure. Public/private partnerships should encourage industry adoption of interoperable standards for identity, reporting, and asset provenance. Finally, regulators could also create safe harbors or streamlined pathways for projects that successfully implement such compliance-enhancing tools. Regulations can incentivize regulated actors to adopt on-chain analytics tools and interoperable travel-rule infrastructure. It can promote blockchain-based KYC credentials, mandated risk intelligence sharing, and support open standards for traceability. These steps bolster compliance across the digital ecosystem and traditional finance.