Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

AML & ESG Executive Training 2025:

New Format Compliance Training Workshop on AML and ESG in Kenya

30 OCT — 01 NOV 2025

Empowering through practice

AGENDA

- ESG as the New Risk Filter for Financial Institutions
- Enhancing AML & Anti-Corruption with ESG
- ESG in Practice: Self-Assessments & Reporting
- Managing Emerging Risks: Crypto

AML Certification Centre
By Crence

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Integrating ESG into Compliance & Governance

Benedict Oduor

Senior Partner, T.M.M Partners Advocates

Brian Maera

Senior Partner, T.M.M Partners Advocates

ESG is the New Risk Filter

Objective: Understand how ESG values are reshaping compliance expectations.

What is ESG?

E (Environmental): Climate change, resource depletion, waste, pollution.

S (Social): Employee relations, diversity, human rights, community relations.

G (Governance): Board diversity, executive pay, audits, internal controls, shareholder rights.

Why is it a 'Risk Filter'?

- Identifies new risks (e.g., climate disasters, reputational damage).

- Investors and regulators now expect proactive ESG risk management.

ESG in the Kenyan Context

Why is ESG relevant for Kenyan organizations?

- Investor Attraction: Global investors prefer ESG-compliant companies.

- Market Access: Meeting international ESG standards aids exports.

- National Priorities: Aligns with Vision 2030 and sustainability goals.

- Risk Management: Avoids environmental and social crises.

Example: A Kenyan bank financing agriculture must assess water use and community impact.

ESG Strengthens AML & Anti-Corruption

Objective: Learn how ESG frameworks can strengthen due diligence.

The Core Link: Transparency – corruption thrives in secrecy.

How ESG Improves KYC/Due Diligence:

- 'Know Your Customer’s Customer' – assess suppliers’ ESG risks.

- Ultimate Beneficial Ownership (UBO) – governance clarity.

- Reputational Risk – poor ESG = higher compliance risk.

AML Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

ESG Red Flags in AML

Scenario: Your bank is onboarding a new manufacturing client.

Identify possible ESG 'red flags':

Environmental: No environmental management plan, pollution fines.

Social: Poor worker safety, land disputes.

Governance: Complex ownership, reluctance to share ESG data.

Key Local & International ESG Legislation

Kenyan Framework:

- Constitution of Kenya (2010): Articles 42 & 43 on environment and social rights.

- Climate Change Act (2016): National and county-level climate action.

- CBK Climate Disclosure Frameworks,

The Nairobi Securities Exchange (NSE) has launched its Environmental, Social and Governance (ESG) Disclosures Guidance Manual. By issuing these guidelines, the NSE aims at improving and standardizing ESG information reported by listed companies in Kenya.

International Developments:

- EU SFDR: Disclose sustainability risks.

- EU CSRD: Mandates ESG reporting for global companies.

- UK & US: Moving toward mandatory climate disclosures.

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

ESG in Practice – Reporting & Self-Assessment

Objective: Discover practical tools for aligning ESG with regulations.

Common Reporting Frameworks:

- GRI: Global standard for sustainability reporting.

- SASB: Industry-specific, financially material ESG issues.

- TCFD: Climate-related risk and opportunity disclosures.

Key Indicators:

- Environmental: Emissions, water, energy use.

- Social: Diversity, injuries, community engagement.

- Governance: Independent boards, anti-corruption training.

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

How to Conduct an ESG Self-Assessment

A Simple 4-Step Approach:

1. Materiality Assessment – What matters most to stakeholders?

2. Gap Analysis – Compare current vs. desired ESG state.

3. Data Collection – Quantify and qualify your ESG performance.

4. Action Plan – Develop roadmap, set goals, assign roles.

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Hands-On Exercise: Draft Your ESG Checklist

- Task: In pairs, create a simple ESG Compliance Checklist.
- Governance: Is there a board ESG committee?
- Environmental: Do we track energy and water use?
- Social: Anti-discrimination and harassment policy?
- Reporting: Aware of EU CSRD for exports?
- → Your first step toward a formal ESG program!

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Key Takeaways

- ESG is a critical risk management and strategic tool.
- Strengthens AML through transparency and due diligence.
- Kenya’s ESG framework offers early adopters a competitive edge.
- Start small with checklists and self-assessments.
- Stay updated on international standards like CSRD.

AML Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Certification Centre
By Crence

Managing Emerging Risks: Crypto

Andrei Sribny
CEO at AML
Certification Centre

Viktor Tkatsenko
Key Expert;
Head of AML,
Citadele Bank

Core Principles of Blockchain Technology

Decentralisation

Immutability

Transparency

Consensus

Certification Centre
By Crence

Key Elements

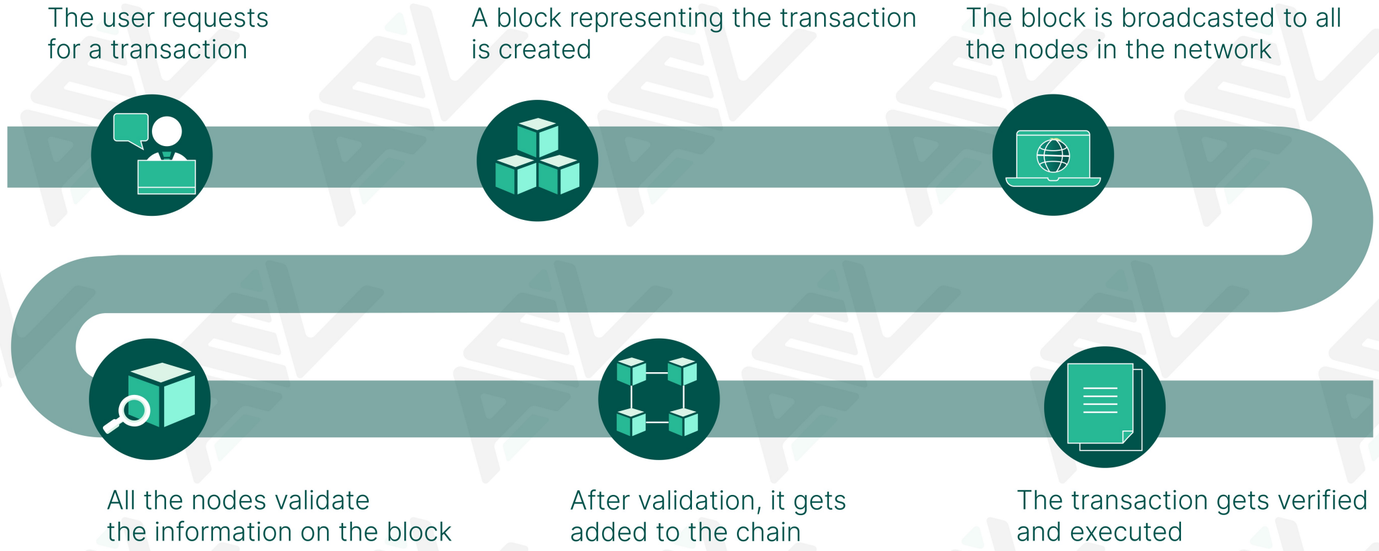
- Wallets and addresses
- Public vs private keys
- Digital signatures

Blockchain technology explained

Blockchain technology is a distributed ledger system that promotes decentralization, transparency, and data integrity.

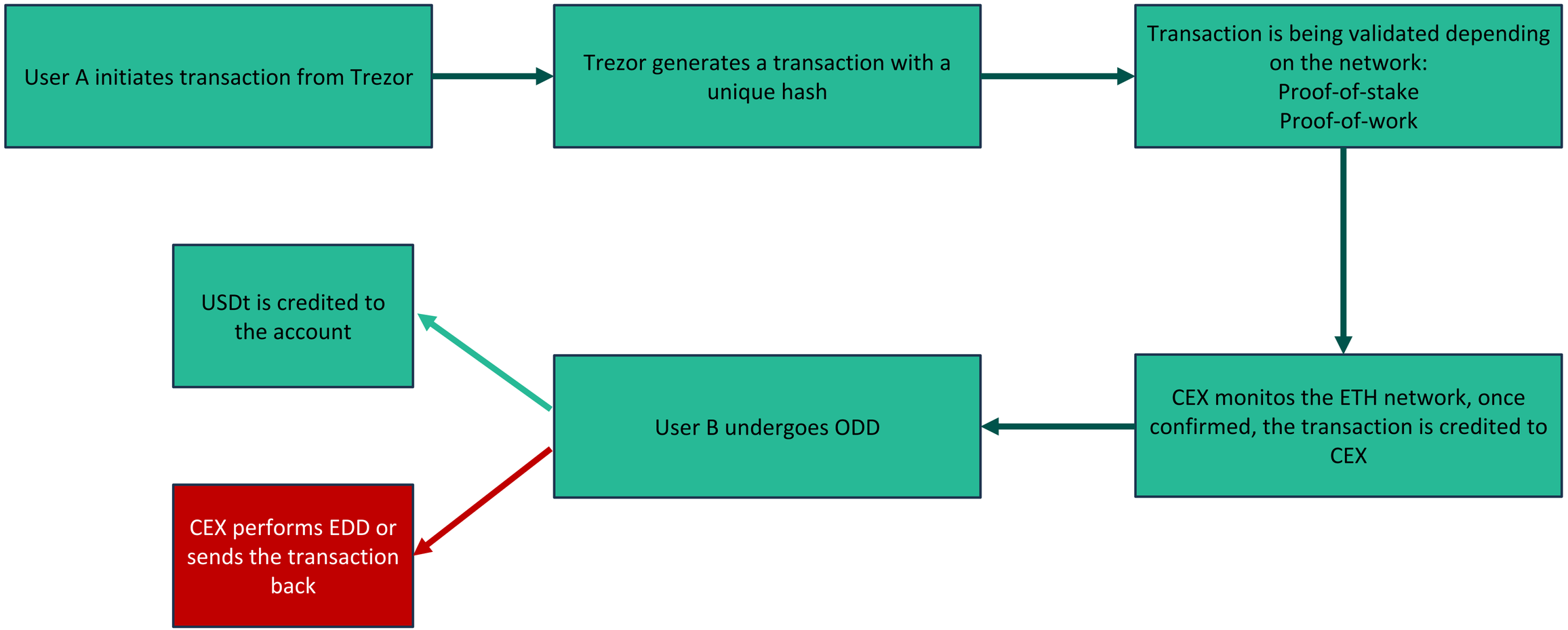
Layers of blockchain technology

How the blockchain technology works



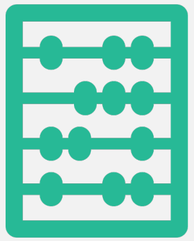
Example of a USDt Transaction

Certification Centre
By Crence



Token Mechanisms and Classification

Certification Centre
By Crence



Classification de facto:

- Technical layer
- Purpose
- Underlying value
- Utility

Problem:

Many types of different taxonomies. Often desynchronized with the regulatory landscape.

Classification MiCA

1. MiCA regulates based on how a token is used in practice i.e. functional classification

2. MiCA also looks at why a token is issued i.e. purpose:

Is it intended as a means of exchange (e.g. payments)?

Is it a store of value or stablecoin?

Is it for access to a service (i.e. utility token)?

Certification Centre
By Crence

Technical Layer

Blockchain-Native Tokens

Description: A token that is implemented on the protocol-level of a blockchain

Characteristics:
- Critical to operate the blockchain
- Integral component of the blockchain's consensus mechanism
- Part of the blockchain's incentive mechanism for block validators/other nodes

Examples: BTC (Bitcoin, Bitcoin); ETH (Ether, Etherum), STEEM (Steem, Steem)

Non-native Protocol Tokens

Description: A token that is implemented in a cryptoeconomic protocol on top of a blockchain

Characteristics:
- Integral component of the protocol's consensus mechanism
- Part of the protocol's incentive mechanism for nodes
- Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum)

Examples: REP (Decentralized Oracle Protocol, Augur)

(d)App Tokens

Description: A token that is implemented on the application-level on top of a blockchain (and potentially protocol)

Characteristics:
- Integrated within the application
- Part of the app's incentive mechanism for nodes and/or users
- Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum)

Examples: WIZ (Wisdom, Gnosis), SAFE (Safecoin, SAFE Network)

Purpose

Cryptocurrencies

Description: A token that is intended to be a "pure" cryptocurrency

Characteristics:
- Intended as a global medium of exchange
- Functions as a store of value

Examples: BTC (Bitcoin), ZEC (Zcash), KIN (Kin, Kik)

Network Tokens

Description: A token that is primarily intended to be used within a specific system (e.g. network, application)

Characteristics:
- Token has functionality within the issuers system
- Not intended as a general cryptocurrency

Examples: GNO (Gnosis), STX (Stacks, Blockstack)

Investment Tokens

Description: A token that is primarily intended as a way to passively invest in the issuing entity or underlying asset

Characteristics:
- Promises owners a share of asset value or in (future) success of the issuing entity
- No or little significant functionality

Examples: Neufund Equity Tokens (Neufund), DGX (Digix Gold, DigixDAO)

Underlying Value

Asset-backed Tokens

Description: A token that functions as a claim on an underlying asset

Characteristics:
- Allows trading via IOUs without actually having to move the underlying asset
- The issuer is responsible to hold the underlying asset
- Introduces counterparty risk

Examples: USDT (Tether USD, Tether), GOLD (GOLD, GoldMint), Ripple IOUs (Ripple)

Network Value Tokens

Description: A token that is tied to the value and development of a network

Characteristics:
- Tied to the value generated and exchanged on the network (e.g. transaction fee volume)
- Closely intertwined with key interactions of network participants

Examples: ETH (Ether, Ethereum) STEEM (Steem)

Share-like Tokens

Description: A token with share-like properties

Characteristics:
- The issuer promises token owners a share in the success of the issuing entity (e.g. dividends, profit-shares)
- May or may not come with voting-rights
- Mostly on no/weak legal basis

Examples: DGD (DigixDAO), LKK (Lykke)

Likely to be classified as a security token

Utility

Usage Tokens

Description: A token that provides access to a digital service, similar to a paid API key

Characteristics:
- Grants holders access to exclusive functionality of the service

Examples: BTC (Bitcoin), STX (Stacks, Blockstack)

Work Tokens

Description: A token that provides the right to contribute to a system

Characteristics:
- Owning Tokens is the precondition for contributing to the system
- Contributions are either incentivized with a rewards system or holders get utility from the system/decentralized organization

Examples: REP (Reputation, Augur), MKR (Maker, Maker DAO)

Hybrid Tokens

Description: A token featuring traits of both usage and work tokens

Characteristics:
- Grants access to system functionalities
- Allows owners to contribute to the system

Examples: ETH (Ether, Ethereum, after Casper), DASH (Dash)

ML typologies in Crypto-Asset Services

1. Wash trading and flash loan
2. Lliquidity manipulation
3. Synthetic KYC and fake Proof of Funds (e.g. fake USDT)
4. Cross-chain laundering and bridge exploits
5. NFT laundering and untraceable value movement

Certification Centre
By Crence

The Emerging Risk: Fake USDT

Certification Centre
By Crence

- An exchange receives what appears to be 1,000 USDT from a newly onboarded client.
- The balance updates, and the system shows confirmation...
- The token is fake.
- It uses the same symbol ('USDT'), same decimals, even identical transfer timing — but is not issued by Tether, nor backed by USD.
- How did it get past the controls?

The Crypto Compliance Challenge for Traditional Financial Institutions

Growing Reality

Traditional banks increasingly encounter customers who transact with Virtual Asset Service Providers (VASPs), creating new risk vectors without corresponding analytical capabilities

Regulatory Expectations

EU regulators (including MiCA) expect robust controls for crypto-related transactions despite limited visibility into blockchain destinations

Existing Tools Gap

Conventional SWIFT/SEPA monitoring systems were not designed to address specific risks posed by cryptocurrency transactions

Example Crypto Wallet Account Statement

Date	Type	Asset	Amount	USD Value	Transaction Hash	Description
2023-10-01	Deposit	BTC	0.05	1350	0x7a8c...d9f0	From Personal Wallet (TXN-BTC-12345)
2023-10-05	Trade	ETH	1.5	2700	0x2e4f...b7c8	Buy ETH with BTC (TradeID: ABC-6789)
2023-10-10	Withdrawal	USDT	1000	1000	0x9b1d...a3e6	To External Wallet (TXN-USDT-98765)
2023-10-15	Deposit	LTC	10	650	0x5c7a...f0b3	Received from Peer (TXN-LTC-54321)
2023-10-20	Trade	BTC	0.02	560	0x1f3h...k2m4	Sell BTC for USD (TradeID: DEF-1011)

Identifying Crypto-Related Transactions

Most traditional banks lack direct blockchain visibility but can still detect crypto activity through existing systems. Key indicators include:

- Payment references containing terms like "BTC", "ETH", "crypto", "token"
- Transfers to/from known VASP bank accounts
- Regular round-figure transactions
- Unusual transaction patterns inconsistent with customer profile
- Multiple small value transactions with similar amounts

Understanding Common Crypto Transaction Types

Exchange Activity

Customer deposits to Coinbase, Binance, Kraken showing references like "BTC purchase" or "crypto deposit"

Example: Monthly €500 transfers to Coinbase with consistent patterns

Investment Services

Larger transfers to crypto investment platforms or DeFi services

Example: €10,000 transfer to BlockFi with reference "Crypto Savings Account"

Wallet Transfers

Transfers to personal non-custodial wallets via OTC services

Example: Payment to Ramp Network with reference "ETH to Metamask"

High-Risk Crypto Transaction Indicators

Critical Red Flags Without Blockchain Analytics

- Transactions with VASPs known for weak KYC (e.g., certain non-EU exchanges, particularly those not compliant with MiCA)
- Rapidly increasing transaction volumes to crypto services
- References suggesting privacy coins or mixing services
- Transfers to P2P exchanges without regulation
- Multiple small transfers just below reporting thresholds
- Transactions with references to "tumbler", "mixer", or "anonymous"

Enhanced Due Diligence Strategies

Request Additional Information

Request blockchain transaction IDs, screenshots of exchange accounts, and purpose of crypto activity

Example: For customer sending €5,000 to Binance, request proof of destination wallet ownership

Update Customer Risk Profile

Adjust risk rating based on crypto exposure, with more frequent reviews for high-volume customers

Example: Increase monitoring frequency for customer with 40%+ transactions to crypto exchanges

Verify VASP Legitimacy

Establish internal list of approved/restricted VASPs based on their regulatory status and AML controls

Example: Maintain database noting Coinbase (MiCA-compliant) vs unregistered platforms

Implementation Roadmap for Traditional FIs

Immediate Actions (Aligned with EU regulations including MiCA)

1

- Update transaction monitoring rules with crypto-specific terms
- Train staff on common crypto transaction patterns and MiCA requirements
- Create VASP database with risk classifications based on EU guidelines

Medium-Term (3-6 months)

2

- Develop crypto-specific customer risk assessment framework, incorporating MiCA guidelines
- Implement enhanced KYC questionnaires for crypto-active customers, in line with EU standards
- Establish periodic reporting on crypto exposure for regulatory bodies

Long-Term Strategy

3

- Consider partnership with blockchain analytics vendor for enhanced EU compliance
- Develop industry information sharing protocols for cross-border cooperation
- Create specialist crypto compliance team, focusing on evolving EU regulatory landscape

Identifying High-Risk Crypto Wallet Activity

Date	Type	Asset	Amount	USD Value	Transaction Hash	Description
2023-11-03	Withdrawal	ETH	10.0	18000	0xcc1b...f2a4	To multiple external wallets (high value)
2023-11-07	Deposit	BTC	0.5	14000	0xdd2c...e3b5	From known mixing service
2023-11-12	Withdrawal	USDT	5000	5000	0xee3d...d4c6	To unregulated gambling platform
2023-11-18	Deposit	LTC	50	3250	0xff4e...a5d7	Rapid deposit from unknown source
2023-11-19	Withdrawal	LTC	49.5	3217	0x015f...b6e8	Immediate withdrawal post-deposit

Identifying Risky Crypto-Exchange Transactions: Public Intelligence Sources

Regulatory Registers

- Consult FATF guidance on crypto-asset service providers.
- Check national regulators’ registers for licensed vs. unlicensed exchanges.

Media & Enforcement Alerts

- Track news and crypto publications for breach reports or investigations.
- Subscribe to law-enforcement bulletins highlighting VASPs under scrutiny.

Industry Watchlists

- Ingest public lists from blockchain-monitoring vendors’ blogs.
- Monitor GitHub repositories by transparency initiatives (e.g., exchange risk ratings).

Community Intelligence

- Scan forums (Reddit, Telegram) for user complaints about fraud or withdrawal issues.
- Leverage social-listening tools to flag negative sentiment around exchanges.

Monitoring Fiat On/Off-Ramp Activity

Beneficiary Tagging

Automatically match payment references, IBANs, and SWIFT codes against your VASP watchlist. Flag transfers whose remittance text contains keywords like “Binance,” “Coinbase,” “WMX,” “zakupy BTC,” etc.

Velocity and Volume Patterns

Alert on sudden outbound spikes to the same beneficiary—e.g., a three-fold increase month-over-month. Identify structuring: a series of sub-threshold transfers (e.g., ten €900 payments just under a €1,000 review limit).

Round-Figure and Sequential Amounts

Watch for “round” transfers (€5,000, $10,000) that often coincide with entry or exit points on exchanges. Detect sequential increments (e.g., €1,000 today, €2,000 tomorrow, €3,000 next day) as layering attempts.

Cross-Channel Correlation

Compare ATM or point-of-sale cash withdrawals following a crypto-bound transfer—indicative of immediate cash-out strategies. Link inbound SEPA or Faster Payments followed within hours by an outbound SWIFT to an exchange.

Open-Source Tools and Databases

Sanctions & PEP Databases

Regularly consult consolidated lists (OFAC, EU, HMT, UN) via CSV or API feeds. Cross-check customer identities and identified Virtual Asset Service Providers (VASPs) against these lists for sanction and politically exposed person (PEP) hits.

Block Explorers & Address Registries

When customers provide transaction hashes, manually verify destination addresses on public block explorers (e.g., Etherscan, Blockchair). Utilise publicly maintained address-label repositories to identify if an address is linked to known mixers, gambling platforms, or illicit entities.

GitHub-Hosted VASP Lists

Integrate community-driven repositories that catalogue exchange bank details and associated risk scores. These lists can be periodically imported into payment processing rules engines to flag high-risk transactions from specific VASPs.

Crypto Enforcement Networks

Participate in working groups (e.g., Wolfsberg Group) and regional Financial Intelligence Unit (FIU)-led crypto forums that facilitate the sharing of illicit VASP lists. Access open-source threat reports (e.g., Europol's Virtual Currencies reports) for emerging trends and intelligence.

BNP Paribas: Reference-Based Screening and EDD

Reference-Based Screening

Built a watch-list of known crypto exchange account identifiers (e.g., IBANs, SWIFT codes, payment references) and fed these into its existing sanctions and PEP-screening engine.

Transaction Monitoring Rules

Configured transaction-monitoring rules to flag any outbound transfer whose beneficiary reference contains an exchange name or wallet tag.

Enhanced Due Diligence (EDD)

Triggered enhanced due diligence (EDD) for retail customers sending over €3,000 per month to such beneficiaries, requiring source-of-fund documentation and a brief purpose-of-transfer questionnaire.

Santander: Dynamic Risk Scoring by Exchange

1

VASP Taxonomy

Developed an internal taxonomy of over 40 crypto platforms, rating each by regulatory jurisdiction, publicly disclosed AML controls, and reported hack history.

2

Composite Risk Scoring

Assigned each outbound payment a composite risk score based on the target exchange’s profile and the customer’s historic transaction behavior.

3

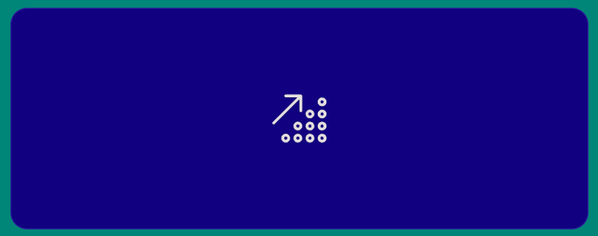
Automated Escalation

Any transfer crossing a score threshold—e.g., Tier 2 “medium-high” or above—was automatically routed for manual review by the Financial Crime team.

Citigroup: Layered Threshold Controls

Two-Person Approval

High-level alerts require a two-person approval process before execution, ensuring robust oversight.

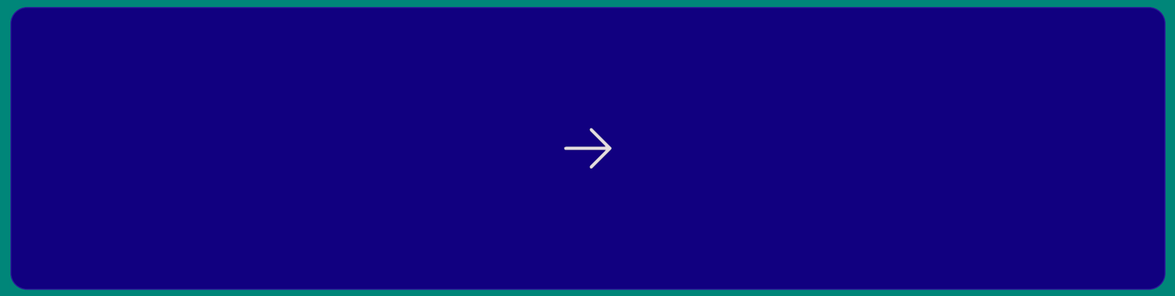


High-Level Alerts

Any single transfer above $15,000 or exhibiting unusual velocity spikes.

Mid-Level Alerts

Aggregated monthly outflows to any crypto destination exceeding $7,500.



Low-Level Alerts

Single transfers to crypto destinations over $2,500 trigger initial alerts.

Q&A Session

Certification Centre
By Crence

Thank you!

Certification Centre
By Crence