VALOORES Crypto Management System

Executive Summary

VCMS aims to offer a comprehensive solution that addresses AML/CFT compliance, transaction monitoring, and investigative needs for virtual asset service providers (VASPs), regulatory bodies, and financial institutions. The system leverages advanced blockchain analytics, geospatial intelligence, and AI-driven predictive tools to detect and prevent financial crime, specifically in the virtual assets space. This document provides an overview of the Business, Product and user requirements (BRD, PRD, URD) for the tool and is intended solely for VALOORES internal use only.

A. Business Requirements

VCMS serves a dual market, empowering both private sector entities - such as Virtual Asset Service Providers (VASPs), including exchanges, custodians, administrators, transfer services, and banks where applicable - and public sector bodies, including law enforcement and supervisory authorities, to align with regulatory standards, ensure robust compliance, and streamline investigative processes. The present document provides an outlook on the modules to be included, with the following objectives in mind:

1. **Enhanced Compliance & Customer Due Diligence:** Support institutions in meeting FATF Travel Rule requirements and maintaining global compliance standards.
2. **Robust Investigation Support:** Provide law enforcement and compliance teams with tools to identify, trace, and investigate complex financial crimes involving cryptocurrencies.
3. **Continuous Monitoring and Reporting:** Enable ongoing monitoring of transactions and patterns with automated alerts and risk-based scoring.
4. **Risk Assessment & Mitigation:** Address AML/CFT risks by assessing transactional behavior, identifying high-risk transactions, and facilitating proactive intervention.

B. Product Requirements

The following sections provide a description of each of the VCMS modules with details on the functions to be included under each module, in addition to data to be collected and trigger events.

1. Compliance Module

a. Digital KYC and Identity Verification:

The VCMS digital KYC aims at establishing identity verification and enhancing due diligence to mitigate potential risks associated with virtual assets.

Key features include:

- Integration with biometric verification tools to ensure accurate user identification, this includes but is not limited to supporting OCR capabilities for document validation.
- Verification against geospatially-tagged data to confirm identity and prevent fraud.
- Alignment with the FATF Travel Rule for cross-border compliance.

Data Points to Collect:

- **Identity Information**: Full name, date of birth, nationality, address, government ID (passport, national ID card).
- **Contact Information**: Primary email, phone number, physical address.
- **Employment & Financial Data**: Occupation, employer, annual income range, source of wealth.
- **Account Details**: Crypto wallet addresses, linked bank accounts, crypto trading accounts, IP addresses.

Data Points to Verify:

- **Government-Issued ID**: Verify name, date of birth, and photo against official documents.
- **Biometric Verification**: Face recognition or fingerprint validation (especially for high-risk clients).
- **Source of Funds/Wealth**: Cross-check income and assets based on transaction size.

- **Location Verification**: Real-time geolocation at account creation and during high-risk transactions.

Trigger Points (List is not exhaustive):

- **High-Value Transactions**: Above a specified threshold (e.g., $10,000 in crypto assets) triggers enhanced due diligence.
- **Geographic Risk**: Accounts opened or accessed from high-risk regions as per FATF guidelines require additional checks.
- **Multiple Wallets**: Multiple wallet addresses linked to one customer, or significant wallet details changes within a short period of time, or multiple wallets operating from the same IP address. From a continuous monitoring perspective, frequent IP changes or changes within a short period of time.

Functional Requirements for KYC triggers:

Automatically prompt KYC review upon:

- New user registration or wallet addition.
- Unusual transaction patterns or high-value transfers.
- Changes in risk assessment due to altered user behavior.

b. Transaction Monitoring and Risk Analysis:

The objective is to track and assess transactions to identify suspicious patterns associated with AML/CFT regulations.

Key Features include:

- Monitoring across multiple blockchain networks.
- Scenario-based alert triggers for rapid cross-chain transactions, high-value transfers, and wallet tumbling activities.
- Risk scoring based on transaction patterns and user behavior analysis.

Data Points to Track:

- **Transaction Volume**: Amount and frequency of transactions; round numbers and unusually large or small sums.
- **Transaction Type**: Crypto-to-crypto, crypto-to-fiat, or fiat-to-crypto exchanges.
- **Source & Destination**: Origin and destination wallets; especially if they involve privacy coins, mixing services, or high-risk exchanges.

- **Location**: Cross-border or jurisdiction-specific transfers on top of geolocation data.
- **Timestamp**: Time of each transaction to detect rapid or high-frequency transactions.
- **Analysis of patterns & trends**: typologies, patterns and trends analysis based on historical data.

Monitoring Scenarios and Trigger Points (List is not Exhaustive):

- **High-Risk Countries**: Transactions involving entities or wallets in jurisdictions with known AML/CFT deficiencies (leverage the FATF countries risk matrix).
- **Volume Anomalies**: Transactions that exceed typical customer behavior or sudden spikes in transaction volume.
- **Round-Sum Transactions**: Repeated transactions in round sums (e.g. exactly 1 BTC) can indicate structuring or layering.
- **Rapid Transactions Below Threshold**: Small, rapid transfers below reporting limits could indicate evasion techniques.
- **Mixing and Tumbler Services**: Transactions routed through mixing or tumbling services that obscure crypto asset origin.

Automated Alerts:

- **Velocity Alerts**: Set triggers for unusually fast transactions in succession.
- **Counterparty Monitoring**: Alerts for funds sent to or received from known high-risk wallets or addresses associated with darknet markets.
- **Flagged IP Addresses**: Alerts when users access accounts from flagged IPs or VPNs, which could indicate identity obfuscation.

c. Customer Risk Assessment (CRA)

In accordance with FATF recommendations:

Assign risk levels to customers based on data-driven criteria, allowing for tailored monitoring and due diligence.

Risk Factors and Data Points:

- **Geographic Risk (Geographic Origin & destination)**: Assign scores based on customer country and transaction locations (low, medium, or high risk).

- **Transaction Behavior**: Frequent use of privacy coins, transactions with foreign VASPs, rapid deposits and withdrawals.
- **Source of Wealth & Funds**: Income level, employment status, business activity, and legitimacy of income sources.
- **Association with High-Risk Entities**: Connections to high-risk VASPs, decentralized exchanges, or accounts with criminal records.
- **Wallet history** and previous red flags or sanctions lists

Risk Matrix Allocation (Baseline Logic):

- **Low-Risk**: Individuals with low transaction volumes, residing in low-risk regions, and demonstrating consistent, low-risk behavior.
- **Medium-Risk**: Customers with moderate transaction volumes or involvement with moderate-risk jurisdictions.
- **High-Risk**: Individuals using high-risk VASPs, engaging in high-volume or complex crypto activity, or residing in regions with high AML risk.

Risk Level Adjustments:

- **Behavioral Changes**: Automatic escalation if significant deviations in transaction patterns are detected.
- **Periodic Review**: Quarterly or bi-annual review for medium-risk customers, annual for low-risk, and monthly for high-risk.
- **Override and Manual Review**: Allow compliance officers to adjust risk levels based on additional intelligence or subjective factors.

d. Screening Requirements

Objective: Real-time screening against sanctions lists, PEPs, and other high-risk identifiers. Regular screening for sanctions, PEPs, and adverse media to prevent engagement with high-risk or prohibited individuals. Customizable alerting rules based on organization’s risk appetite and evolving regulations

Data Points for Screening:

- **Identity Details**: Full name, aliases, birthdate, nationality, wallet addresses and unique identifiers.

- **PEP Status**: Politically exposed persons and close associates, with status updated frequently.
- **Sanctions Lists**: Real-time screening against global sanctions, including OFAC, EU, and UN lists.
- **Adverse Media**: Continuous monitoring of news and online sources for links to criminal activity or financial crime.

Screening Triggers:

- **New Account Creation**: Full KYC and wallet addresses screening upon initial registration and before any transaction approval.
- **Newly Linked Wallets**: Any new wallet address added to a customer's account triggers additional screening.
- **Regulatory List Updates**: Automatic retroactive screening when updates to sanctions or PEP lists occur.
- **Periodic Rescreening**: At set intervals (e.g., quarterly for high-risk customers) and on an ad-hoc basis based on risk assessment changes.

Automated Rules for Screening:

- **Name Matching and Fuzzy Logic**: Automated matching with fuzzy logic to detect variations in customer names.
- **Transaction-Based Screening**: Alert on transactions with counterparties that are sanctioned or linked to high-risk activities.
- **Cross-Chain Screening**: Wallet addresses that interact across multiple blockchains are flagged for increased scrutiny.

2. Investigative Module

Objectives: The main objective of the Investigation Module is to enable collaboration and facilitate data sharing between VASPs and government entities for a unified compliance framework and an advanced approach to suspicious activities and financial crime risks.

Prioritization & Key Features: Notwithstanding the detailed project planning to be set by the development team, the Investigation module should ideally follow the following sequence:

- **Blockchain Data Extraction** from the open source and establishing an offline environment for data storage that would eventually serve the purpose of transaction and pattern analysis.
- **Launch of the Dashboard** - a bird's eye view into the open source data downloaded and treated in real-time. The visualization may take into consideration aspects such as but not limited to the number of transactions, volume, velocity, currencies, inflows and outflows etc.
- **Deployment of the Advanced Knowledge Graph**- The knowledge graph aims at providing users with an interactive visualization of the links between wallets on the same or cross-chain. The visualization may take into consideration aspects such as but not limited to transaction hashes, wallet addresses, transaction timestamps, a multi dimensional visual of transactional flows while also flagging high-risk wallets.
- Parallel Phase: **Development and Integration of the Centralized KYC Database**. This phase is contingent upon VASPs adopting the compliance module mentioned herein so that KYC data starts being aggregated in a pooling format in a centralized database. The idea is to provide a tiered access to this database whereas Law Enforcement and other regulatory agencies are generally given a broader view of the wallet/transaction details than a VASP. The key benefit from a VASP perspective is to be able to query wallets according to their riskiness level, that is built on the backend of the database following a risk matrix similar to the one described in the compliance module. The key benefit for Law Enforcement and other regulatory agencies is strengthening oversight, identifying suspicious behavior of natural persons, which solves for the anonymity often claimed to be the highest risk when it comes to cryptocurrencies.

C. User Requirements

1. User Types and Permissions (Role- Based Classification)

- **Compliance Officers**: Full access to compliance tools, transaction monitoring, KYC management, and reporting.

- **Investigators**: Access to investigational tools, blockchain analytics, geospatial intelligence, and case management.
- **Regulators and Auditors**: Read-only access to records, compliance reports, transaction history, and audit logs.
- **Administrators**: Control over user access, system configuration, and regulatory setting adjustments.

2. Non-functional Requirements

- **Scalability**: Support high transaction volumes and multi-currency operations.
- **Data Security**: End-to-end encryption, role-based access, and audit trails.
- **Interoperability**: Seamless integration with third-party tools and external databases.
- **Performance**: Real-time processing and low-latency alerts.

Audit Trail and Reporting

- Record all KYC verifications, CRA decisions, screening results, and transaction alerts.
- Generate regulatory reports (e.g., Suspicious Activity Reports) for transactions and customers flagged for high risk.

Data Security and Privacy Controls

- Encryption for all customer information and transaction data.
- Access controls for sensitive data, with role-based permissions.

Case Management

Built-in case management system for tracking investigations, tagging entities, and reporting to regulatory bodies.