



The FATF QUANTUM Leap

Transforming Compliance Standards

The VALOORES Blueprint Crafting Compliance & Investigation Excellence

Transformer les Normes de Conformité

Le Plan VALOORES pour Créer l'Excellence en Matière de Conformité et d'Enquête

Cryptocurrencies and digital assets are reshaping markets across industries. As financial services adapt, regulatory frameworks align with FATF's risk mitigation guidance. VALOORES offers its Crypto Management System (VCMS), providing institutional stakeholders a secure, compliant platform that enhances asset protection and operational confidence in a volatile market.

By seamlessly integrating cutting-edge risk mitigation protocols and robust security measures, VCMS not only shields against emerging threats but also pioneers a new era in digital asset management.

Les crypto-monnaies et actifs numériques redéfinissent les marchés. Face à cette évolution, les cadres réglementaires s'alignent sur les recommandations de la FATF. VALOORES propose son système de gestion des crypto-actifs (VCMS), offrant une plateforme sécurisée et conforme, renforçant la protection des actifs et la confiance dans un marché volatile.

En intégrant de manière transparente des protocoles d'atténuation des risques et des mesures de sécurité robustes, VCMS protège non seulement contre les menaces émergentes, mais ouvre également une nouvelle ère dans le domaine de gestion des actifs numériques.



Table of Contents

Table des Matières

Introduction	3	Introduction	3
Chapter 1: VCMS At the Forefront of FATF Compliance In the Realm of Virtual Assets	5	Chapitre 1: VCMS à la pointe de la conformité au GAFI dans le domaine des actifs virtuels	5
A. Definition of Virtual Assets and VASPs	5	A. Définition des actifs virtuels et des VASP	5
B. The Risk-Based Approach (RBA) for VAs and VASPs	6	B. L'approche basée sur les risques (RBA) pour les VA et les VASP	6
C. Ongoing Guidance and Compliance Reviews	6	C. Examens continus des orientations et de la conformité	6
D. Country-Level Compliance Requirements	7	D. Exigences de conformité au niveau national	7
E. The FATF Travel Rule	7	E. La règle de voyage du GAFI	7
F. Beyond Recommendation 15	8	F. Au-delà de la recommandation 15	8
1. FATF Recommendations for VASPs	8	1. Recommandations du GAFI pour les VASP	8
2. FATF Recommendations for Law Enforcement Agencies	11	2. Recommandations du GAFI à l'intention des organismes chargés de l'application de la loi	11
Chapter 2: VCMS Compliance Capabilities	13	Chapitre 2: Capacités de conformité VCMS	13
A. Crypto Digital KYC Solution implementation	13	A. Implémentation de la solution Crypto Digital KYC	13
1. VCMS: A Comprehensive Digital KYC Solution for Cryptocurrency Compliance	13	1. VCMS: une solution KYC numérique complète pour la conformité des crypto-monnaies	13
2. Core Features of VCMS Digital KYC and Identity Verification	13	2. Fonctionnalités principales du KYC numérique VCMS et de la vérification d'identité	13
3. Data Collection and Verification Points	14	3. Points de collecte et de vérification des données	14
4. Automated Trigger Points for Enhanced KYC Monitoring	15	4. Points de déclenchement automatisés pour une surveillance KYC améliorée	15
B. Wallet Name Matching System (WNMS)	16	B. Système de correspondance de noms de portefeuille (WNMS)	16
C. Crypto Risk Based Approach (CRBA)	17	C. Approche basée sur les risques cryptographiques (CRBA)	17
1. Cryptocurrency Transaction Analysis in the Risk Matrix:	17	1. Analyse des transactions de crypto-monnaie dans la matrice des risques:	17
2. Cryptocurrency Tracking in Case Relative Risk:	18	2. Suivi des crypto-monnaies en cas de risque relatif:	18
D. Crypto Rules and Transaction Monitoring	19	D. Règles de cryptographie et surveillance des transactions	19

1. Implementing the Travel rule based on FATF rec. 15	19	1. Mise en œuvre de la règle de voyage basée sur la rec. 15	19
2. Transaction Monitoring Location Base	20	2. Base de localisation de surveillance des transactions	20
3. Same Transaction Amount Monitoring	21	3. Surveillance du même montant de transaction	21
Chapter 3: VCMS role in Crypto investigations	22	Chapitre 3: Rôle du VCMS dans les enquêtes Crypto	22
A. Location Intelligence	22	A. Intelligence de localisation	22
B. VCMS Value Proposition	23	B. Valeur Ajoutée de VCMS	23
1. Visibility	23	1. Visibilité	23
2. Data Correlation with Multiple Data Sources	23	2. Corrélation des données avec plusieurs sources de données	23
3. Offline System	23	3. Système Offline	23
4. Friendly Graphical User Interface	24	4. Interface utilisateur graphique conviviale	24
5. Technology, Big Data, and AI	24	5. Technologie, Big Data et IA	24
6. Navigating in Time	24	6. Naviguer dans le temps	24
C. VCMS's Role in combating Crimes Using Cryptocurrencies	25	C. Le rôle de VCMS dans la lutte contre les crimes utilisant les crypto-monnaies	25
1. Tracking Crypto Wallet Devices Using Geospatial Technology	25	1. Suivi des Wallet Addresses cryptographiques à l'aide de la technologie géospatiale	25
2. Dynamic Knowledge Graph for Tracking Crypto Transactions	25	2. Graphique dynamique pour le suivi des transactions cryptographiques	25
3. Identifying Wallet Owners through Geospatial Data Correlation	26	3. Identification des propriétaires de Wallets grâce à la corrélation de données géospatiales	26
4. Financial Crime Links and Points of Interest (POI) Circles	26	4. Liens sur la criminalité financière et les points d'intérêt (POI)	26
5. Location-Based Authentication for Enhanced Security	26	5. Authentification basée sur la localisation pour une sécurité renforcée	26
6. Risk Analysis and Anomaly Detection through Geospatial Data	27	6. Analyse des risques et détection des anomalies grâce aux données géospatiales	27
Conclusion	28	Conclusion	28

Introduction

In an era of unprecedented digital transformation and financial interconnectivity, the integration of cryptocurrencies and digital assets into the global financial infrastructure presents both strategic opportunities and complex regulatory imperatives. Financial institutions, regulatory authorities, and Virtual Asset Service Providers (VASPs) face mounting pressure to implement robust Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) frameworks that meet evolving international standards.

The Financial Action Task Force (FATF), as the preeminent global authority on financial compliance, continues to shape the regulatory landscape through comprehensive governance frameworks. With a legacy spanning three decades, FATF's evolving mandate has established industry-leading standards for combating financial crime, adapting its protocols to address the sophisticated challenges presented by the digital asset ecosystem. This dynamic regulatory environment demands innovative solutions that can adapt to emerging threats while maintaining operational efficiency.

Introduction

À l'ère de la transformation numérique et de l'interconnectivité financière mondiale, l'intégration des cryptomonnaies et des actifs numériques dans les infrastructures financières internationales offre des opportunités stratégiques tout en posant des défis réglementaires complexes. Les institutions financières, les régulateurs et les fournisseurs de services d'actifs virtuels (VASP) doivent relever le défi croissant de déployer des cadres robustes de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT), alignés sur des normes internationales en constante évolution.

Le Groupe d'action financière (GAFI), en tant qu'autorité mondiale de référence en matière de conformité financière, continue d'influencer le cadre réglementaire international à travers des standards de gouvernance rigoureux. Fort d'un mandat de plus de trois décennies, le GAFI a établi des normes avancées pour lutter contre la criminalité financière, en adaptant continuellement ses protocoles pour répondre aux défis complexes posés par l'écosystème des actifs numériques. Cet environnement réglementaire en constante évolution nécessite des solutions technologiques innovantes, capables de s'adapter aux menaces émergentes tout en garantissant une efficacité opérationnelle optimale.

VALOORES delivers enterprise-grade solutions designed to meet FATF's complex compliance requirements, enabling organizations to achieve operational excellence while maintaining the highest standards of security and transparency. Through our integrated suite of solutions—VCMS, VCMS, and VFDS—we empower stakeholders across financial services, virtual asset operations, and law enforcement sectors to enhance their compliance frameworks, strengthen resilience against financial threats, and establish sustainable trust through systematically compliant operations. Our comprehensive approach ensures institutions remain at the forefront of regulatory compliance while optimizing their operational capabilities in an increasingly complex financial landscape.

VALOORES propose des solutions d'entreprise avancées répondant aux exigences de conformité rigoureuses du GAFI, permettant aux organisations d'atteindre l'excellence opérationnelle tout en respectant les normes les plus élevées de sécurité et de transparence. Grâce à notre suite intégrée (VCMS, VCIS et VFDS), nous offrons aux parties prenantes des services financiers, aux opérateurs d'actifs virtuels et aux autorités de régulation des outils pour renforcer leurs cadres de conformité, accroître leur résilience face aux menaces financières et instaurer une confiance durable grâce à une conformité systématique. Notre approche holistique garantit aux institutions de demeurer à la pointe des exigences réglementaires tout en optimisant leurs capacités opérationnelles dans un environnement financier complexe et en constante évolution.



Chapter 1: VCMS At the Forefront of FATF Compliance In the Realm of Virtual Assets

In response to the growth of digital assets, the FATF updated its recommendations in October 2018 to include financial activities related to virtual assets. This crucial expansion provided specific definitions for "virtual assets" (VAs) and "virtual asset service providers" (VASPs), establishing a framework to address the AML and CFT challenges unique to this sector.

A. Definition of Virtual Assets and VASPs

Virtual assets are defined as digital representations of value that can be traded or transferred electronically and used for payment or investment. These assets do not cover digital forms of fiat currencies, securities, or other financial assets addressed by existing FATF standards. A "virtual asset service provider" encompasses entities facilitating transactions involving virtual assets, such as exchanges, transfers, safekeeping, and financial services related to virtual asset offerings. These cover the following VASPs categories:

1. Exchange between virtual assets and fiat currencies;
2. Exchange between one or more forms of virtual assets;

Chapitre 1: VCMS à la pointe de la conformité au GAFI dans le domaine des actifs virtuels

Face à l'essor des actifs numériques, le GAFI a actualisé ses recommandations en octobre 2018 pour englober les activités financières liées aux actifs virtuels. Cette mise à jour stratégique a introduit des définitions précises des « actifs virtuels » (VA) et des « fournisseurs de services d'actifs virtuels » (VASP), posant ainsi les bases d'un cadre réglementaire adapté aux défis spécifiques de la lutte contre le blanchiment d'argent (AML ou AML) et le financement du terrorisme (CFT) dans ce secteur en pleine évolution.

A. Définition des actifs virtuels et des VASP

Les actifs virtuels désignent des représentations numériques de valeur pouvant être échangées ou transférées électroniquement, utilisées à des fins de paiement ou d'investissement. Ils excluent les formes numériques de monnaies fiduciaires, de titres ou d'autres instruments financiers déjà régis par les normes existantes du GAFI. Un VASP englobe les entités qui facilitent les opérations impliquant des actifs virtuels, telles que les échanges, les transferts, la garde et les services financiers liés aux offres d'actifs numériques. Les VASP se classent dans les catégories suivantes:

1. Conversion entre actifs virtuels et monnaies fiduciaires;
2. Conversion entre différentes formes d'actifs virtuels;

3. Transfer of virtual assets; and
4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
5. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

B. The Risk-Based Approach (RBA) for VAs and VASPs

In 2019, FATF issued an Interpretive Note to Recommendation 15, focusing on a risk-based approach (RBA) for virtual assets. This approach requires VASPs to assess and address AML/CFT risks according to the unique nature of virtual assets. VASPs must undergo robust monitoring, licensing, and preventive procedures, including customer due diligence, recordkeeping, and suspicious activity reporting.

C. Ongoing Guidance and Compliance Reviews

FATF's continuous updates, including guidance on digital identity verification (March 2020), and the release of Red Flag Indicators for VAs (September 2020), have underscored the organization's commitment to adaptive regulatory standards. FATF's two-year review of revised VA standards in July 2021 reinforced the need for clear protocols for assessing, understanding, and mitigating risks in the virtual asset space.

3. Transfert d'actifs virtuels;
4. Garde et/ou administration d'actifs virtuels ou des instruments permettant leur contrôle;
5. Participation et fourniture de services financiers liés à l'émission ou à la vente d'actifs virtuels.

B. L'approche basée sur les risques (RBA) pour les VA et les VASP

En 2019, le GAFI a publié une note sur la Recommandation 15, introduisant une approche basée sur les risques (RBA) pour les actifs virtuels. Elle oblige les fournisseurs de services d'actifs virtuels (VASP) à évaluer et gérer les risques LBC/CFT spécifiques aux actifs numériques. Les VASP doivent respecter des protocoles stricts de surveillance, d'octroi de licences, de contrôle, de diligence raisonnable (CDD), de conservation des enregistrements et de déclaration des transactions suspectes.

C. Examens continus des orientations et de la conformité

Les mises à jour régulières du GAFI, comme les directives sur la vérification d'identité numérique (mars 2020) et les indicateurs d'alerte pour les actifs virtuels (septembre 2020), montrent l'engagement de l'organisation à adapter ses normes. L'examen biennal des normes révisées sur les actifs virtuels en juillet 2021 a souligné l'importance de protocoles clairs pour gérer les risques spécifiques aux actifs numériques, insistant sur une approche proactive pour ce secteur émergent.

D. Country-Level Compliance Requirements

The FATF mandates that countries evaluate ML/TF risks within their jurisdictions and ensure that VASPs actively implement measures proportional to these risks. Competent authorities must work with VASPs to evaluate services, products, customer profiles, and geographical influences. This alignment ensures that VASPs effectively identify and mitigate risks and promotes consistent adherence to global standards.

Through these comprehensive guidelines, the FATF has solidified its position in overseeing the integrity of digital asset ecosystems. At VALOORES, we are dedicated to supporting organizations in their journey toward FATF compliance, offering tools that enhance the resilience and security of the financial network across traditional and virtual domains. Our mission is to bridge the gap between compliance and operational efficiency, ensuring our clients are equipped to thrive in an increasingly regulated digital landscape.

E. The FATF Travel Rule

The FATF Travel Rule, part of Recommendation 15 on New Technologies, mandates that Virtual Asset Service Providers (VASPs) gather and share specific identifying information on

D. Exigences de conformité au niveau national

Le GAFI exige des États qu'ils évaluent rigoureusement les risques de blanchiment de capitaux et de financement du terrorisme (BC/FT) dans leurs juridictions, et veille à ce que les VASP appliquent des mesures adaptées aux menaces identifiées. Les autorités collaborent avec les VASP pour analyser services, produits, profils clients et facteurs géographiques, assurant ainsi une gestion efficace des risques et une conformité aux normes internationales.

Grâce à ces directives exhaustives, le GAFI renforce son rôle central dans la préservation de l'intégrité des écosystèmes d'actifs numériques. Chez VALOORES, nous accompagnons les organisations dans leur parcours de conformité en proposant des solutions avancées qui renforcent la résilience et la sécurité des réseaux financiers, tant traditionnels que numériques. Notre mission est de concilier conformité réglementaire et excellence opérationnelle, garantissant à nos clients une compétitivité optimale dans un environnement numérique hautement régulé.

E. La règle de voyage du GAFI

La règle de voyage du GAFI, intégrée dans la Recommandation 15 relative aux nouvelles technologies, impose aux VASP l'obligation de collecter et de partager des informations d'identification détaillées sur l'initiateur et le bénéficiaire des transactions d'actifs virtuels dépassant un certain seuil. Cette exigence

the originator and beneficiary of virtual asset transactions above a certain threshold. This requirement mirrors the standards applied to wire transfers in traditional finance, aiming to increase transparency and prevent misuse of virtual assets in money laundering and terrorist financing. VASPs must collect, verify, and securely transmit essential information such as the name, account number, and geographical address or national ID number of both the sender and receiver. Additionally, VASPs are required to ensure secure data handling to protect customer information and maintain regulatory compliance across jurisdictions. By adhering to the Travel Rule, VASPs support global AML/CFT objectives and contribute to a safer, more transparent financial environment.

F. Beyond Recommendation 15

1. FATF Recommendations for VASPs

VCMS ensures that VASPs comply with FATF's comprehensive Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) standards by supporting key recommendations relevant to private sector compliance. Through automated tools, advanced data analytics, and machine learning, VCMS addresses the following FATF standards:

s'aligne sur les normes applicables aux virements électroniques dans le secteur financier traditionnel, visant à renforcer la transparence et à prévenir l'utilisation abusive des actifs virtuels pour le BC/FT. Les VASP doivent collecter, vérifier et transmettre de manière sécurisée des informations clés telles que le nom, le numéro de compte, l'adresse géographique ou le numéro d'identification national des parties impliquées etc. Par ailleurs, les VASP sont responsables de garantir la sécurité des données, afin de protéger les informations clients et d'assurer la conformité avec les exigences réglementaires à travers toutes les juridictions. En se conformant à la règle de voyage, les VASP contribuent activement aux objectifs mondiaux de LBC/CFT, favorisant ainsi un environnement financier plus sécurisé et transparent.

F. Au-delà de la recommandation 15

1. Recommandations du GAFI pour les VASP

VCMS assure la conformité des VASP aux exigences complètes du GAFI en matière de LBC/CFT, en alignant ses fonctionnalités avec les recommandations stratégiques pertinentes pour le secteur privé. Grâce à l'intégration de technologies avancées telles que l'automatisation des processus, l'analyse de données et le "Machine Learning", VCMS répond de manière proactive aux normes du GAFI, garantissant ainsi une gestion rigoureuse des risques et une conformité optimale:

Recommendation 10: Customer Due Diligence (CDD)

VCMS strengthens Customer Due Diligence (CDD) practices by automating the verification and ongoing monitoring of customer information, ensuring compliance with AML/CFT standards. Key data such as customer identity, transaction history, risk level, and beneficial ownership is rigorously assessed to enable VASPs and financial institutions to identify and monitor customer risks continuously, particularly for higher-risk clients.

Recommendation 12: Politically Exposed Persons (PEPs)

VCMS includes a dedicated module for identifying and monitoring politically exposed persons (PEPs), including domestic, foreign, and international individuals with prominent public functions. Real-time monitoring and periodic screenings ensure heightened due diligence, enabling VASPs to address risk effectively and in accordance with FATF's requirements.

Recommendation 16: Wire Transfers

VCMS aligns with FATF's standards on transparency for wire transfers, ensuring VASPs trace the origin and beneficiaries of transactions, including crypto-to-crypto and crypto-to-fiat transfers.

Recommandation 10: Due Diligence Client (CDD)

VCMS optimise les pratiques de diligence raisonnable envers la clientèle (CDD) en automatisant la vérification initiale et la surveillance continue des informations client, assurant ainsi une conformité totale aux normes LBC/CFT. Les données critiques, telles que l'identité du client, l'historique des transactions, le profil de risque, sont scrupuleusement analysées pour permettre aux VASP et aux institutions financières d'identifier et de surveiller de manière proactive les risques associés à chaque client, en particulier ceux présentant un risque élevé.

Recommandation 12: Personnes politiquement exposées (PEP)

VCMS intègre un module spécifique pour l'identification et la surveillance des PEP, couvrant les individus nationaux, étrangers et internationaux occupant des fonctions publiques de haut niveau. Grâce à une surveillance en temps réel et à des contrôles réguliers, le système assure une diligence raisonnable renforcée, permettant aux VASP de gérer de manière optimale les risques associés aux PEP, tout en garantissant la conformité aux exigences strictes du GAFI.

Recommandation 16: Virements électroniques

VCMS s'aligne sur les normes du GAFI en matière de transparence pour les virements électroniques, garantissant que les VASP retracent l'origine et les bénéficiaires des transactions, y compris les transferts crypto-crypto et crypto-fiat.

Recommendation 20: Suspicious Transaction Reporting

By integrating advanced analytics and anomaly detection, VCMS flags unusual or high-risk transactions that may indicate potential money laundering or terrorist financing activities. The system automatically generates reports for suspicious transactions, facilitating timely investigation and reporting to Financial Intelligence Units (FIUs) as required by FATF guidelines.

Recommendation 24: Transparency and Beneficial Ownership of Legal Persons

VCMS allows VASPs to track beneficial ownership details, providing transparency across ownership chains. This enables institutions to comply with FATF's standards on identifying ultimate beneficial owners, especially for transactions involving complex ownership structures, ensuring accountability and fostering trust within the virtual asset sector.

Recommendation 35: International Cooperation

VCMS is designed to support cross-border cooperation by facilitating secure data sharing among VASPs, financial institutions, and relevant authorities. This compatibility with international AML/CFT standards enables seamless collaboration across jurisdictions, reinforcing FATF's call for global cooperation in the fight against financial crime.

Recommandation 20: Déclaration des transactions suspectes

Grâce à des analyses avancées et des mécanismes de détection des anomalies, VCMS identifie et signale proactivement les transactions suspectes ou à haut risque liées aux activités ML/TF. Le système génère automatiquement des rapports, facilitant les enquêtes et assurant des déclarations en temps réel aux cellules de renseignement financier (FIU), conformément aux normes du GAFI.

Recommandation 24: Transparence et propriété effective des personnes morales

VCMS permet aux VASP de suivre précisément la propriété effective, garantissant la conformité avec les normes du GAFI sur l'identification des bénéficiaires ultimes, notamment pour les structures de propriété complexes. Cela renforce la transparence, la responsabilité et la confiance dans le secteur des actifs virtuels.

Recommandation 35: Coopération internationale

VCMS est conçu pour optimiser la coopération transfrontalière en permettant le partage sécurisé de données entre les VASP, les institutions financières et les autorités compétentes. En conformité avec les normes internationales en matière de LBC/CFT, cette solution favorise une collaboration fluide entre les juridictions, soutenant ainsi l'appel du GAFI à une coopération mondiale renforcée dans la lutte contre la criminalité financière.

2. FATF Recommendations for Law Enforcement Agencies

VCMS is equally equipped to empower public sector entities such as law enforcement and regulatory bodies in conducting investigations and enforcing compliance within the digital asset ecosystem. It offers investigative capabilities aligned with FATF recommendations, ensuring that agencies can tackle illicit financial activities effectively:

Recommendation 30: Responsibilities of Law Enforcement and Investigative Authorities

Through VCMS, law enforcement agencies have access to tools that support their responsibility to investigate money laundering and terrorist financing within the AML/CFT framework.

Recommendation 31: Powers of Law Enforcement and Investigative Authorities

VCMS enables law enforcement to leverage advanced investigative techniques necessary for financial crime investigations. These include undercover operations, intercepting communications, controlled deliveries, and access to critical data on account holders.

2. Recommandations du GAFI à l'intention des organismes chargés de l'application de la loi

VCMS permet aux autorités publiques de mener des enquêtes approfondies et d'assurer la conformité dans l'écosystème des actifs numériques. Avec des fonctionnalités d'investigation avancées, il aide à lutter contre les activités financières illicites et renforce la surveillance réglementaire, conformément aux recommandations du GAFI:

Recommandation 30: Responsabilités des autorités chargées de l'application de la loi et des enquêtes

Grâce au VCMS, les organismes chargés de l'application de la loi ont accès à des outils qui soutiennent leur responsabilité d'enquêter sur le blanchiment d'argent et le financement du terrorisme dans le cadre de la LBC/CFT.

Recommandation 31: Pouvoirs des autorités chargées de l'application de la loi et des enquêtes

VCMS fournit aux forces de l'ordre des outils d'enquête de pointe, essentiels pour mener des investigations sur la criminalité financière. Cela inclut des techniques avancées telles que l'infiltration d'opérations, l'interception de communications, les livraisons contrôlées, ainsi que l'accès sécurisé aux données critiques des titulaires de comptes, permettant ainsi une analyse approfondie et une action ciblée.

Recommendation 32: Cash Couriers and Virtual Assets

VCMS provides mechanisms to monitor large cryptocurrency movements that may bypass traditional financial systems, addressing FATF's focus on detecting illicit cross-border transfers. This feature assists law enforcement in jurisdictions with significant informal value transfer activities, ensuring oversight over cross-border currency transport and cryptocurrency transfers.

Why VCMS?

By aligning with FATF standards, VCMS provides a comprehensive compliance and investigation solution for both private VASPs and public sector law enforcement. Its design addresses key FATF recommendations that foster a transparent, secure, and accountable digital asset ecosystem. Through VCMS, VALOORES equips entities with the tools needed to meet evolving AML/CFT obligations, mitigate financial crime risks, and support international cooperation across the virtual asset landscape.



Recommandation 32: Passeurs de fonds et actifs virtuels

VCMS intègre des mécanismes de surveillance avancés pour détecter les flux substantiels de crypto-monnaies, en particulier ceux échappant aux canaux financiers traditionnels. Cette fonctionnalité répond aux priorités du GAFI concernant la détection des transferts transfrontaliers illicites, en facilitant la surveillance des mouvements transnationaux de crypto-monnaies et de devises, notamment dans les juridictions présentant des volumes élevés de transferts informels de valeur.

Pourquoi VCMS ?

En conformité avec les standards du GAFI, VCMS offre une solution intégrée de conformité et d'enquête, adaptée aux besoins des VASP du secteur privé ainsi que des autorités publiques chargées de l'application de la loi. Conçu pour répondre aux recommandations clés du GAFI, VCMS soutient la création d'un écosystème d'actifs numériques transparent, sécurisé et responsable. Grâce à cette plateforme, VALOORES dote les entités d'outils efficaces pour se conformer aux exigences en matière de (LAB/CFT), minimiser les risques liés à la criminalité financière et faciliter la coopération transnationale dans l'écosystème des actifs virtuels.

Chapter 2: VCMS Compliance Capabilities

A. Crypto Digital KYC Solution implementation

1. VCMS: A Comprehensive Digital KYC Solution for Cryptocurrency Compliance

VALOORES' Virtual Compliance Management System (VCMS) is designed to support government agencies, financial institutions, and regulatory bodies in upholding FATF-compliant cryptocurrency KYC protocols. The VCMS platform uses advanced biometrics technology to verify and authenticate user identities, thereby safeguarding virtual asset transactions from potential risks. VCMS integrates a robust suite of KYC features to ensure accurate identity verification, streamline due diligence, and enhance the overall compliance process for virtual assets.

2. Core Features of VCMS Digital KYC and Identity Verification *Advanced Biometric and Document Verification*

VCMS utilizes state-of-the-art identity verification methods to ensure secure, reliable identification. This process helps verify user authenticity seamlessly while enhancing compliance with global standards.

Chapitre 2: Capacités de conformité VCMS

A. Implémentation de la solution Crypto Digital KYC

1. VCMS: une solution KYC numérique complète pour la conformité des crypto-monnaies

Le VCMS de VALOORES aide les agences gouvernementales, institutions financières et régulateurs à respecter les protocoles KYC sur les crypto-monnaies, conformément aux exigences du GAFI. La plateforme utilise des technologies biométriques avancées pour authentifier les utilisateurs, renforçant ainsi la sécurité des transactions. Avec une suite complète de fonctionnalités KYC, VCMS garantit une vérification rigoureuse des identités et facilite la conformité réglementaire pour les actifs virtuels.

2. Fonctionnalités principales du KYC numérique VCMS et de la vérification d'identité

Vérification biométrique et documentaire avancée

VCMS déploie des techniques avancées de vérification d'identité pour assurer une identification sécurisée et fiable des utilisateurs. Ce processus garantit l'authenticité des individus de manière fluide, tout en optimisant la conformité avec les normes internationales en vigueur.

Geospatial Verification

VCMS incorporates location-based checks, enabling enhanced user verification and adding a powerful layer of fraud protection to safeguard transactions.

Cross-Border Compliance

Aligned with FATF's Travel Rule, VCMS supports international compliance requirements, making cross-border transactions transparent and secure.

3. Data Collection and Verification Points

Identity and Contact Information

VCMS collects essential identifying information such as user details, residence data, and contact channels to establish a solid identity profile for each individual, supporting secure onboarding and account management.

Employment & Financial Information

Key data related to a user's professional background and financial standing provides insights into transaction legitimacy, ensuring compliance with industry standards.

Account Activity Insights

VCMS gathers basic account and transaction details, including identifiers that link users to specific accounts, to foster transparency and traceability in digital asset interactions.

Vérification géospatiale

VCMS utilise des contrôles géospatiaux avancés pour renforcer la validation des utilisateurs et sécuriser les transactions contre la fraude.

Conformité transfrontalière

Conforme à la règle de voyage du GAFI, VCMS assure la transparence et la sécurité des transactions transfrontalières.

3. Points de collecte et de vérification des données

Identité et coordonnées

VCMS collecte des données essentielles, incluant les informations personnelles, l'adresse et les contacts, pour créer un profil d'identité solide, assurant une intégration sécurisée et une gestion optimale des comptes.

Emploi et informations financières

Les informations clés relatives à l'historique professionnel et à la situation financière d'un utilisateur permettent d'évaluer la légitimité des transactions, assurant ainsi la conformité avec les exigences réglementaires et les standards sectoriels.

Informations sur l'activité du compte

VCMS centralise les informations essentielles des comptes et des transactions, y compris les identifiants associés aux utilisateurs et à leurs comptes, afin de garantir une transparence optimale et une traçabilité exhaustive des interactions au sein de l'écosystème des actifs numériques.

Identity Confirmation

VCMS employs verification measures to confirm identity details against official records and uses biometric validation tools to enhance user authenticity, particularly for higher-risk accounts. Geographic data is also assessed to support location-based verification.

4. Automated Trigger Points for Enhanced KYC Monitoring

High-Value Transactions

VCMS automatically initiates enhanced monitoring for transactions above a defined threshold to mitigate risks associated with large transfers.

Geographic Risk Indicators

Accounts accessed from regions associated with heightened risk are subject to additional compliance checks, helping to reinforce secure operations.

Account Behavior and Anomaly Detection

VCMS continuously monitors for unusual activity patterns, including multiple or frequent account adjustments, ensuring a responsive and proactive approach to user risk.

Confirmation d'identité

VCMS déploie des protocoles de vérification rigoureux pour valider les informations d'identité en les confrontant aux documents officiels, tout en intégrant des solutions biométriques avancées pour renforcer l'authenticité des utilisateurs, notamment pour les comptes à risque élevé. En outre, le système évalue les données géospatiales afin de faciliter une vérification conforme basée sur la localisation.

4. Points de déclenchement automatisés pour une surveillance KYC améliorée

Transactions de grande valeur

VCMS déclenche automatiquement un niveau de surveillance renforcée pour toutes les transactions dépassant un seuil prédéfini, permettant ainsi de gérer efficacement les risques associés aux transferts de valeur significatifs.

Indicateurs de risque géographique

Les comptes situés dans des zones géographiques à risque élevé sont soumis à des contrôles de conformité supplémentaires, assurant une gestion proactive de la sécurité des transactions.

Comportement du compte et détection des anomalies

VCMS assure une surveillance continue des comportements inhabituels, y compris des modifications fréquentes ou multiples des comptes, garantissant ainsi une réponse immédiate et préventive face aux risques potentiels liés aux utilisateurs.

B. Wallet Name Matching System (WNMS)

Our matching system is engineered to simultaneously match names and wallets, constituting a multitask matching system that operates on intricate and advanced criteria. This capability enables our solution to adopt a defensive approach to money laundering by utilizing lists that can be implemented within the system to detect matching names or wallets, while also adhering to all international standards regarding crypto compliance. For example UN 1267 list which refers to the United Nations Security Council (UNSC) Consolidated List, This list is maintained by the United Nations Security and it aims to impose sanctions, such as asset freezes and travel bans, on those deemed to be involved in terrorist activities.

Another example would be the national list 1373. It established a framework for combating terrorism and called upon all UN member states to take various measures to prevent and suppress terrorist activities.

Any list or sources of data can be integrated into the solution to enhance the ability to identify all Crypto users who are considered suspicious.

B. Système de correspondance de noms de portefeuille (WNMS)

Notre système de correspondance est conçu pour effectuer simultanément des rapprochements de noms et de portefeuilles, utilisant des critères complexes et avancés pour garantir une surveillance approfondie des risques liés au blanchiment d'argent et au financement du terrorisme. Cette approche permet une détection proactive des activités illicites tout en assurant la conformité avec les normes internationales en matière de conformité cryptographique. Le système intègre des listes de contrôle telles que la liste ONU 1267, qui est mise à jour régulièrement par le Conseil de sécurité des Nations Unies. Cette liste cible les individus et entités liés à des activités terroristes, en imposant des sanctions comme le gel des actifs ou des interdictions de voyager. Grâce à cette capacité de correspondance multitâche, notre solution garantit une protection renforcée contre les risques de blanchiment d'argent et de financement du terrorisme, en s'alignant sur les standards mondiaux de sécurité financière.

N'importe quelle liste ou source de données peut être intégrée à la solution pour améliorer la capacité d'identifier tous les utilisateurs Crypto considérés comme suspects.

C. Crypto Risk Based Approach (CRBA)

Incorporating cryptocurrency into the Basic Risk Matrix and Case Relative Risk adds an extra layer of complexity and sophistication to the RBA risk-based approach in KYC.

1. Cryptocurrency Transaction Analysis in the Risk Matrix:

- In the detailed Risk Matrix, one can integrate the analysis of cryptocurrency transactions associated with an individual or entity. Cryptocurrency transactions often present unique challenges and opportunities for risk assessment. Unusual patterns, high-frequency transactions, or connections to known illicit activities in the crypto space can significantly impact the calculated risk.
- Admin users might have the capability to override the risk based on specific cryptocurrency-related findings. For instance, if an individual is involved in multiple transactions flagged for potential money laundering or fraud, the admin user could adjust the risk level accordingly.

C. Approche basée sur les risques cryptographiques (CRBA)

L'intégration de la crypto-monnaie dans la matrice de risque et l'évaluation des risques spécifiques aux cas permet d'ajouter une dimension de complexité et de sophistication à l'approche de gestion du risque basée sur le risque (RBA) dans les processus KYC.

1. Analyse des transactions de crypto-monnaie dans la matrice des risques:

- Dans une matrice de risque avancée, les transactions en crypto-monnaie liées à un individu ou une entité sont analysées avec des spécificités propres au domaine. Les comportements atypiques, la fréquence élevée des transactions et les liens potentiels avec des activités illicites compliquent l'évaluation des risques, influençant ainsi le score global.
- Les administrateurs du système peuvent ajuster dynamiquement le niveau de risque en fonction de résultats spécifiques relatifs aux transactions en crypto-monnaie. Par exemple, si un utilisateur est impliqué dans plusieurs transactions identifiées comme potentiellement suspectes, telles que des activités de blanchiment d'argent ou de fraude, le niveau de risque pourra être ajusté à la hausse, en fonction des paramètres définis.

- Clicking on the risk lookup could reveal not only traditional risk factors but also detailed insights into cryptocurrency-related risks. This might include involvement in dark web transactions, association with flagged wallet addresses, or engagement in activities linked to cryptocurrency-based scams.

2. Cryptocurrency Tracking in Case Relative Risk:

- The VCMS Tool can extend its capabilities by incorporating cryptocurrency-related information to identify potential risks. Individuals who might seem harmless based on conventional indicators could be flagged if their cryptocurrency transactions align with suspicious patterns.
- The VCMS could raise a relative risk alert if someone is found to have engaged in cryptocurrency transactions linked to known criminal activities or has received funds from a wallet associated with illicit practices. This approach allows for a more nuanced and targeted identification of risks, especially when dealing with cases involving cryptocurrency-related crimes.

- L'analyse de risque révèle non seulement les facteurs traditionnels, mais aussi des éléments spécifiques aux crypto-monnaies, tels que l'implication dans des transactions sur le dark web, les liens avec des wallets suspects ou la participation à des escroqueries crypto. Cette approche renforce la surveillance et permet une gestion proactive des risques liés aux actifs numériques.

2. Suivi des crypto-monnaies en cas de risque relatif:

- L'outil VCMS peut étendre ses fonctionnalités en intégrant des données relatives aux crypto-monnaies, permettant ainsi l'identification proactive des risques potentiels. Les entités apparemment conformes sur la base de critères traditionnels peuvent être signalées si leurs transactions en crypto-monnaies présentent des aspects anormaux ou suspectés, facilitant ainsi la détection de risques cachés.
- Le VCMS est conçu pour générer une alerte de risque contextualisée lorsqu'une personne est impliquée dans des transactions de crypto-monnaies associées à des activités criminelles identifiées ou reçoit des fonds provenant d'un wallet lié à des pratiques illicites. Cette méthodologie permet une identification plus précise et ciblée des risques, en particulier dans les cas impliquant des infractions liées aux crypto-monnaies.

By integrating cryptocurrency analysis into the risk matrices, KYC processes become more comprehensive and adaptive to the evolving landscape of financial transactions, providing a more effective means of identifying and mitigating potential risks associated with individuals or entities.

D. Crypto Rules and Transaction Monitoring

Our solution operates on a framework of dynamic rules specifically customized for cryptocurrency transactions. These rules are meticulously implemented across one or more blockchain ledger databases, forming the backbone of our system's capability to identify suspicious activity. When triggered, these rules generate alerts that are meticulously analyzed, taking into account transaction specifics and the historical data associated with the relevant wallet. This meticulous analysis ensures that any potential risks or illicit behavior are thoroughly investigated, allowing for swift and effective response measures to be taken.

1. Implementing the Travel rule based on FATF rec. 15

In the context of cryptocurrencies, the Travel Rule requires VASPs to exchange specific customer information (such as name, address, and account number) for transactions exceeding a certain threshold.

L'intégration de l'analyse des crypto-monnaies dans les matrices de risques optimise les processus KYC en offrant une approche plus holistique, adaptée à l'évolution rapide des transactions financières. Cela permet une identification proactive et une atténuation des risques potentiels liés aux individus ou entités, renforçant ainsi la gestion du risque dans un environnement financier dynamique.

D. Règles de cryptographie et surveillance des transactions

Notre solution repose sur un cadre de règles dynamiques spécifiquement adaptées aux transactions en crypto-monnaies, intégrées dans une ou plusieurs bases de données de registres blockchain. Ce mécanisme constitue la base de notre capacité à détecter les activités suspectes. Lorsqu'une règle est déclenchée, une alerte est générée et analysée en profondeur, prenant en compte les caractéristiques de la transaction et l'historique des données associées au portefeuille concerné. Cette analyse détaillée assure une évaluation rigoureuse des risques potentiels ou des comportements illicites, facilitant une réponse rapide et appropriée.

1. Mise en œuvre de la règle de voyage basée sur la rec. 15

Dans le cadre des crypto-monnaies, la règle de voyage impose aux VASP de transmettre des informations client spécifiques (notamment le nom, l'adresse et le numéro de compte) pour les transactions dépassant un seuil prédéfini.

This information is transmitted securely between the originating VASP (the sender's provider) and the beneficiary VASP (the recipient's provider) to facilitate compliance with AML/CFT regulations.

Based on Recommendation 15, the Travel Rule aims to enhance transparency and traceability in cryptocurrency transactions, thereby mitigating the risk of illicit activities such as money laundering and terrorist financing within the virtual asset space.

2. Transaction Monitoring Location Base

Many financial institutions continue to rely on IP addresses to verify a user's location, even though this method is vulnerable to spoofing and is not very effective. However, by implementing VCMS and VCMS, which include a real-time and historical risk engine and patterns of behavior in correlation with geospatial data, suspicious activities and high risk acts can be detected by identifying the country of residence, country of work, nationality, other nationality, secondary resident country, country of registration, country of incorporation, parent registration company and others.

Ces données sont échangées de manière sécurisée entre le VASP émetteur (prestataire de l'expéditeur) et le VASP récepteur (prestataire du destinataire), garantissant ainsi la conformité avec les exigences de la réglementation AML/CFT. Conformément à la recommandation 15 du GAFI, la Travel Rule renforce la transparence et la traçabilité des transactions en crypto-monnaie, contribuant à atténuer les risques d'activités illicites telles que le blanchiment d'argent et le financement du terrorisme dans l'écosystème des actifs virtuels.

2. Base de localisation de surveillance des transactions

Malgré l'utilisation courante des adresses IP pour vérifier la localisation des utilisateurs, cette méthode reste vulnérable à l'usurpation d'identité et présente des limites en matière d'efficacité. L'intégration de VCMS, incluant un moteur de gestion du risque en temps réel et historique ainsi que des modèles comportementaux analysant les données géospatiales, permet d'identifier et de corréler les risques potentiels. En croisant des informations détaillées telles que le pays de résidence, le pays de travail, la nationalité, la nationalité secondaire, le pays d'enregistrement, le pays de constitution, ainsi que la société d'enregistrement mère, VCMS assure une détection précise des activités suspectes et des comportements à haut risque.

3. Same Transaction Amount Monitoring

Sometimes, suspicious or illegal activities can go unnoticed when a certain amount of money is transferred periodically, appearing as a normal pattern. However, with VCMS, such transaction processes can be compared against several parameters, such as the income and social class of the sender based on our solution's classification, as well as the recipient's identity and location, in order to identify potential fraudulent or illegal activity.

Exchange Locations & Amounts Records

The increasing use of faster payment methods and digital acceleration has created an environment that fraudsters and cybercriminals can exploit. For instance, they may attempt to make multiple transactions from a single account located in different, distant locations within a short period of time. However, VCMS utilizes the ledger database to identify patterns and track changes in customer behavior by examining the scope of generated alerts over a specific period. This solution can also help locate the accurate site of the account owner and stop any suspicious activity as soon as it is detected.

3. Surveillance du même montant de transaction

VCMS permet d'analyser les transactions périodiques, qui peuvent sembler normales mais cacher des activités suspectes, en croisant plusieurs paramètres. Ces paramètres incluent le revenu et la catégorie sociale de l'expéditeur, basés sur la classification de notre solution, ainsi que l'identité et la localisation du destinataire. Cette approche permet de détecter efficacement des comportements frauduleux ou illicites potentiels.

Emplacements d'échange et enregistrements de montants

L'essor des méthodes de paiement rapides et de l'accélération numérique a créé des opportunités pour les fraudeurs et cybercriminels. Ces derniers peuvent, par exemple, tenter d'effectuer plusieurs transactions depuis un seul compte situé à des emplacements géographiquement éloignés en un temps réduit. Cependant, VCMS permet également de localiser précisément le propriétaire du compte et d'interrompre toute activité frauduleuse dès son identification.

Chapter 3: VCMS role in Crypto investigations

A. Location Intelligence

In today's world, billions of devices are connected to the Internet of Things, granting executives and decision-makers unparalleled access to business data, including a plethora of geospatial information. Geo-Smart Location enables the visualization and analysis of vast volumes of data in a location-specific context, empowering holistic planning, prediction, and problem-solving. By viewing all pertinent data in the context of location, whether on a smart map, app, or dashboard, unique insights can be gleaned.

Geospatial data combines location information (usually coordinates on the earth), and often also temporal information, the time or life span at which the location and attributes exist. There are many benefits to using geospatial data for cyber security. With geospatial data, cyber threat data can be captured, including, for example, the location of attacks, the number of attacks, the proportion, dates, types, and various other factors.

Chapitre 3: Rôle du VCMS dans les enquêtes Crypto

A. Intelligence de localisation

Dans le contexte actuel, où des milliards d'appareils sont interconnectés via l'Internet des objets, les dirigeants et décideurs bénéficient d'un accès sans précédent aux données d'entreprise, y compris à des informations géospatiales critiques. Geo-Smart Location permet la visualisation et l'analyse de volumes massifs de données dans un cadre géospatial spécifique, facilitant ainsi la planification, les prévisions et la résolution de problèmes de manière intégrée. En présentant ces données sur des dashboards, des informations stratégiques peuvent être extraites.

Les données géospatiales combinent des informations de localisation (généralement sous forme de coordonnées géographiques) et des informations temporelles, telles que l'heure ou la durée pendant laquelle un emplacement et ses attributs sont pertinents. Dans le domaine de la cybersécurité, l'utilisation des données géospatiales permet de capturer des informations critiques sur les cybermenaces, y compris la localisation des attaques, leur fréquence, leur proportion, les dates, les types d'attaques, et d'autres paramètres essentiels à la gestion des risques.

B. VCMS Value Proposition

1. Visibility

VCMS provides unparalleled "Global Visibility" by offering data insights beyond borders. The software manages a vast amount of data.

2. Data Correlation with Multiple Data Sources

A key feature of VCMS is Data Correlation with Multiple Data Sources integrating telecom data (CDR & SDR), tracking device data and other consolidation sources. This comprehensive approach allows investigators to establish connections and patterns across diverse datasets, facilitating a holistic understanding of criminal activities.

3. Offline System

VCMS ensures security and accessibility with its "Offline System," operating as a standalone server without the need for an internet connection. This feature is crucial for sensitive investigations, allowing law enforcement to maintain control over access to critical crime and geospatial data.

B. Valeur Ajoutée de VCMS

1. Visibilité

VCMS offre une "visibilité globale" inégalée en offrant des informations sur les données au-delà des frontières.

2. Corrélation des données avec plusieurs sources de données

Le VCMS excelle dans la corrélation de données provenant de diverses sources, telles que les télécommunications (CDR et SDR) et le suivi des appareils. Cette approche permet aux enquêteurs de détecter des relations et des schémas, optimisant l'analyse des activités criminelles pour une compréhension plus précise.

3. Système Offline

Le VCMS garantit sécurité et accessibilité grâce à son fonctionnement offline, opérant comme un serveur autonome sans besoin de connexion Internet. Cette caractéristique clé est cruciale pour les enquêtes sensibles, offrant aux autorités un contrôle total sur l'accès aux données criminelles et géospatiales, tout en préservant leur confidentialité et leur intégrité.



4. Friendly Graphical User Interface

VCMS prioritizes user experience with a Friendly Graphical User Interface that synchronizes different platforms among agencies. The software offers different data modules in one suite, eliminating the need for technical skills. This user-friendly design promotes efficient collaboration and information sharing among investigators, ensuring that agencies can seamlessly work together to analyze geospatial data and combat various crime types.

5. Technology, Big Data, and AI

VCMS integrates cutting-edge technology, big data, and AI handling both structured and unstructured data. The software efficiently ingests large amounts of data in measurable time, executing queries and scenarios in seconds.

6. Navigating in Time

VCMS introduces the innovative feature of Navigating in Time, facilitating backward and forward investigation. Investigators can understand the past, analyze the present, and predict the future. This temporal navigation enhances the software's capabilities to provide a dynamic and comprehensive view of criminal activities over time, empowering investigators to make informed decisions based on historical context and future trends.

4. Interface utilisateur graphique conviviale

Le VCMS optimise l'expérience utilisateur grâce à une interface graphique intuitive qui assure la synchronisation fluide des différentes plateformes au sein des agences. Le logiciel intègre plusieurs modules de données dans une suite unifiée, éliminant ainsi la nécessité de compétences techniques spécialisées. Cette architecture simplifiée facilite une collaboration efficace et le partage d'informations entre les enquêteurs.

5. Technologie, Big Data et IA

Le VCMS intègre des technologies avancées, Big Data et IA pour traiter efficacement les données structurées et non structurées. Il permet l'ingestion rapide de volumes massifs de données, exécutant des requêtes et des analyses complexes en quelques secondes, garantissant ainsi une performance optimale et une réactivité immédiate dans le traitement des informations.

6. Naviguer dans le temps

Le VCMS intègre la fonctionnalité avancée de Navigation temporelle, permettant aux enquêteurs d'effectuer des analyses rétroactives et prospectives. Cette capacité optimise l'examen des événements passés, l'analyse des données actuelles et la prévision des tendances futures. Grâce à cette approche, la solution offre une vue dynamique, facilitant ainsi des prises de décisions stratégiques fondées sur des données historiques et des projections à venir.

C. VCMS's Role in combating Crimes Using Cryptocurrencies

Enhancing Cryptocurrency Crime Detection with VCMS Geospatial Capabilities:

1. Tracking Crypto Wallet Devices Using Geospatial Technology

VCMS empowers law enforcement to track devices associated with crypto wallets through device IDs stored in its Digital Know Your Customer (DKYC) database. DKYC contains detailed personal and technical information on wallet owners, enabling real-time monitoring of device activities and uncovering links with individuals flagged as high-risk or criminally affiliated.

2. Dynamic Knowledge Graph for Tracking Crypto Transactions

VCMS employs a dynamic knowledge graph that monitors cryptocurrency transactions across blockchain ledgers. This graph visually maps relationships and flows of crypto assets, aiding in the detection of funds movement across wallets and exchanges, including cross-chain transfers. By correlating wallet addresses with individuals or entities using DKYC, VCMS provides law enforcement with enhanced tracking and transparency of crypto transactions.

C. Le rôle de VCMS dans la lutte contre les crimes utilisant les crypto-monnaies

Amélioration de la détection des crimes liés aux cryptomonnaies grâce aux capacités géospatiales du VCMS:

1. Suivi des Wallet Addresses cryptographiques à l'aide de la technologie géospatiale

Le VCMS permet aux autorités de suivre les appareils associés aux portefeuilles cryptographiques en utilisant les identifiants d'appareil stockés dans sa base de données Digital Know Your Customer (DKYC). Cette base de données contient des informations techniques et personnelles détaillées sur les détenteurs de wallets, facilitant ainsi une surveillance en temps réel des activités des appareils et l'identification de connexions avec des individus à haut risque ou impliqués dans des activités criminelles.

2. Graphique dynamique pour le suivi des transactions cryptographiques

Le VCMS exploite un graphique dynamique pour analyser les transactions de crypto-monnaies sur la blockchain. Ce graphique trace les flux d'actifs entre wallets et plateformes d'échange, y compris les transferts inter-chaînes. En associant les wallet adresses aux identités via DKYC, VCMS renforce la traçabilité et la transparence des transactions, offrant ainsi aux forces de l'ordre une capacité améliorée de suivi des activités crypto.

3. Identifying Wallet Owners through Geospatial Data Correlation

Using AI, VCMS links wallet addresses to owners in specific regions by correlating geospatial data with online ledger information. This includes automatically linking device IDs with wallet addresses, which is saved in the KYC database, enhancing identification accuracy. The AI engine further analyzes user behavior, activities, and connections within the crypto ecosystem, supporting law enforcement's efforts to monitor suspicious activity.

4. Financial Crime Links and Points of Interest (POI) Circles

By combining machine learning with Geo-Smart analytics, VCMS establishes a network of individuals and financial associations. This spatial analysis allows law enforcement to visualize connections between transactions, individuals, and POIs, providing context and rapidly identifying new relationships. This real-time analysis supports quick, proactive decision-making around suspicious activity.

5. Location-Based Authentication for Enhanced Security

VCMS uses location-based authentication to verify transaction origin by analyzing the physical location against pre-authorized areas.

3. Identification des propriétaires de Wallets grâce à la corrélation de données géospatiales

Grâce à l'intelligence artificielle, VCMS associe les adresses de portefeuille aux propriétaires géolocalisés en corrélant les données géospatiales avec les informations du blockchain. Cela inclut l'association automatique des identifiants d'appareil aux wallet adresses, stockées dans la base de données KYC, optimisant ainsi l'exactitude des identifications. Le moteur d'IA analyse en outre les comportements, activités et relations des utilisateurs au sein de l'écosystème crypto, renforçant ainsi les capacités des forces de l'ordre à surveiller et détecter les activités suspectes.

4. Liens sur la criminalité financière et les points d'intérêt (POI)

En intégrant l'apprentissage automatique avec l'analyse Geo-Smart, VCMS crée un réseau dynamique d'individus et d'associations financières. Cette approche spatiale permet aux forces de l'ordre de visualiser les connexions entre les transactions, les acteurs impliqués et les points d'intérêt, offrant ainsi un contexte précis et facilitant l'identification rapide de nouvelles relations. L'analyse en temps réel optimise la prise de décision proactive et éclairée sur les activités suspectes.

5. Authentification basée sur la localisation pour une sécurité renforcée

VCMS intègre l'authentification géospatiale pour valider l'origine des transactions en comparant la localisation physique à des

If a transaction occurs outside expected zones, the system triggers security responses or alerts, helping prevent unauthorized access or fraud. This geospatial check adds a robust layer of defense by scrutinizing real-time data for transaction integrity.

6. Risk Analysis and Anomaly Detection through Geospatial Data

By integrating geospatial data with security algorithms, VCMS discerns regular from irregular transaction patterns. Anomalies, like sudden changes in transaction location, prompt investigations or security responses to address potential fraud. This proactive detection capability allows financial institutions to react swiftly to emerging threats, minimizing security risks.

zones pré-autorisées. En cas de transaction effectuée en dehors de ces zones, le système déclenche des alertes ou des actions de sécurité, renforçant ainsi la prévention contre les accès non autorisés et la fraude. Cette vérification en temps réel garantit l'intégrité des transactions en ajoutant une couche de protection géospatiale avancée.

6. Analyse des risques et détection des anomalies grâce aux données géospatiales

En combinant des données géospatiales avec des algorithmes de sécurité avancés, VCMS identifie les patterns de transactions habituelles et anormales. Les anomalies, telles que des variations inattendues de localisation, déclenchent des enquêtes ou des mesures de sécurité ciblées pour contrer toute fraude potentielle. Cette approche proactive de détection permet aux institutions financières d'intervenir rapidement face aux menaces émergentes, réduisant ainsi les risques de sécurité.



Conclusion

The rapid evolution of cryptocurrencies has redefined financial systems worldwide, creating unique opportunities while intensifying the need for robust, regulatory-aligned solutions. This analysis underscores the urgent necessity for secure, compliant integration of cryptocurrencies within the global financial framework—an objective that aligns seamlessly with FATF standards.

Through the deployment of advanced tools such as Crypto Digital KYC, Wallet Network Monitoring Systems (WNMS), Continuous Risk-Based Authentication (CRBA), and sophisticated transaction monitoring, VCMS supports institutions and law enforcement in their commitment to global compliance standards. By enabling a thorough, secure, and scalable approach to crypto transactions, VCMS offers a compliance-driven infrastructure capable of adapting to the evolving demands of FATF guidelines, ultimately enhancing transparency, mitigating financial crime risks, and fortifying the resilience of the global financial ecosystem.

Conclusion

L'évolution rapide des crypto-monnaies transforme les systèmes financiers mondiaux, créant à la fois des opportunités et un besoin accru de solutions sécurisées et conformes. Cette analyse met en évidence l'importance cruciale d'une intégration sécurisée et conforme des crypto-monnaies dans le cadre financier international, en parfaite adéquation avec les normes du GAFI.

Grâce à des outils avancés tels que le Digital KYC, le système de surveillance de réseau de wallets, l'authentification continue basée sur les risques, et la surveillance des transactions, VCMS renforce l'engagement des institutions et des forces de l'ordre envers la conformité mondiale. Offrant une approche sécurisée et évolutive pour la gestion des transactions cryptographiques, VCMS assure une infrastructure axée sur la conformité, adaptable aux exigences changeantes des directives du GAFI, améliorant ainsi la transparence, réduisant les risques de criminalité financière et renforçant la résilience des écosystèmes financiers mondiaux.

ABOUT VALOORES

Careers
Press Release
Quotes

CONTACT US

Access Dashboards
Office Locations
E-mail

LINES OF BUSINESS

in'Banking
in'Technology
in'Insurance
in'Healthcare
in'Government

in'Analytics
in'Academy
in'Retail
in'Multimedia
Webinars

SERVICES

in'AML
in'Regulatory
in'Merch
in'IRFP
in'AI/BI
in'KYC

in'Fraud Management
in'Via
in'Consultancy
in'Profit
in'Campaign
in'IFRS9