VCMS Unveiling the Crypto Crime Nexus: A Deep Dive into A Money Laundering Operation Between Nigeria, Turkey & Europe

VCMS Révèle le Nexus des Crimes Crypto: Analyse Approfondie d'un Réseau de Blanchiment d'Argent Entre le Nigeria, la Turquie et l'Europe

Cryptocurrencies have transformed finance, creating both innovation and vulnerabilities. This document examines a transnational money laundering scheme using digital asset anonymity. Using VCIS, tools like geospatial intelligence and blockchain analysis trace illicit activities, link wallet addresses to real-world actors, and uncover hidden criminal networks. It highlights the challenges and need for global collaboration to combat crypto-related financial crimes.

To tackle evolving crypto-financial crimes, VCIS provides real-time insights, uncovering hidden networks and linking digital assets to illicit activities with precision.

Les crypto-monnaies ont transformé le paysage financier, créant des opportunités et des vulnérabilités. Ce document examine un cas de blanchiment d'argent transnational exploitant l'anonymat des actifs numériques. Grâce à VCIS, l'enquête utilise l'intelligence géospatiale et l'analyse de la blockchain pour retracer les flux illicites et identifier des réseaux criminels, soulignant l'importance des technologies avancées et de la collaboration internationale pour sécuriser le système financier mondial.

Pour contrer les menaces des crimes crypto-financiers, VCIS fournit des informations en temps réel, découvre des réseaux cachés et lie les actifs numériques aux activités illicites avec précision.

Table of Contents

VCIS: Illuminating and Tracking beyond the Dark Web of Global Finance and Counterintelligence in Time Travel

Unmasking Financial Crimes with Geospatial Intelligence AI and Unraveling Past Crimes, Present and Predicting Future Threats.

Combating Financial Crimes and Terrorist financing demands cutting-edge solutions in the complex landscape of digital finance and global security. VALOORES Crowd Intelligence Solution (VCIS) emerges as a beacon of innovation, leveraging geospatial intelligence and advanced analytics to unravel illicit activities. This comprehensive overview delves into VCIS's capabilities, showcasing its pivotal role in safeguarding global financial systems and national security.

Key takeaways include:

1. **Cryptocurrency Tracking**

VCIS traces the flow of digital assets, correlating movements with real-world events, predicting future transactions, and integrating blockchain data with KYC information and geospatial intelligence.

2. **Advanced Knowledge Graphs**

VCIS constructs a living map of the global financial ecosystem, correlating blockchain transactions with real-world

VCIS: Éclairer et Suivre au-delà du Dark Web de la Finance Mondiale et du Contre-Espionnage dans le Voyage dans le Temps

Démasquer les crimes financiers grâce à l'IA de renseignement géospatial et démêler les crimes passés, présents et prédire les menaces futures.

La lutte contre les crimes financiers et le financement du terrorisme exige des solutions de pointe dans le paysage complexe de la finance numérique et de la sécurité mondiale. La solution VALOORES Crowd Intelligence (VCIS) se distingue comme un modèle d'innovation, exploitant l'intelligence géospatiale et des analyses avancées pour démêler les activités illicites. Cette présentation approfondie met en lumière les capacités de VCIS, soulignant son rôle clé dans la protection des systèmes financiers mondiaux et de la sécurité nationale.

Les points clés à retenir comprennent:

1. **Suivi des crypto-monnaies**

VCIS trace les flux d'actifs numériques, relie ces mouvements à des événements du monde réel et anticipe les transactions futures. En intégrant les données blockchain aux informations KYC et à l'intelligence géospatiale, VCIS offre une analyse proactive et approfondie des activités financières.

2. **Graphiques de connaissances avancés**

VCIS élabore une cartographie dynamique de l'écosystème financier mondial, en associant les transactions blockchain à des identités et des

identities and locations, filling in knowledge gaps, and predicting future actions.

3. **Geospatial Intelligence in Global Crime Networks**

VCIS makes visible the invisible flows of illicit finance worldwide, overlaying trade flows with financial transactions, communication records, and movement patterns.

4. **Uncovering New Layers in Crypto-Money Laundering Operations**

VCIS expands investigative horizons with recursive analysis, revealing layer after layer of criminal activity, bridging seemingly unrelated activities, and identifying and neutralizing criminal adaptation in real time.

5. **The Present and the Future of Counterintelligence**

VCIS revolutionizes security with comprehensive intelligence solutions, handling unlimited geospatial data, transitioning between offline and online modes, and maintaining the highest security levels.

6. **Unlock the Power of Time-Based Insights**

VCIS performs financial time travel, reconstructing past financial ecosystems and projecting future criminal activities, creating a comprehensive Temporal Analytics view of financial crime.

emplacements réels. Il comble les lacunes informationnelles et anticipe les actions futures pour une surveillance proactive et stratégique.

3. **L'intelligence géospatiale dans les réseaux criminels mondiaux**

VCIS dévoile les flux cachés de financement illicite à l'échelle mondiale en croisant les flux commerciaux avec les transactions financières, les enregistrements de communication et les schémas de déplacement.

4. **Identifier de nouvelles dimensions dans les opérations de blanchiment d'argent liées aux crypto-actifs**

VCIS étend les investigations par une analyse récursive, révélant les strates d'activités criminelles et reliant des opérations apparemment isolées. Il détecte en temps réel les stratégies d'adaptation des réseaux criminels pour les neutraliser efficacement.

5. **Le Présent et l'avenir du contre-espionnage**

VCIS transforme la sécurité avec des solutions de renseignement intégrées, exploitant des volumes illimités de données géospatiales. Il garantit une transition fluide entre les modes en ligne et hors ligne tout en maintenant des standards de sécurité de niveau supérieur.

6. **Libérez la puissance des informations temporelles**

VCIS propose une analyse financière temporelle complète en retraçant les écosystèmes financiers passés et en anticipant les activités criminelles futures. Il offre ainsi une vision analytique approfondie de l'évolution de la criminalité financière.

7. Adaptive Security Measures

VCIS employs state-of-the-art encryption, access controls, and adaptive security protocols to ensure the highest data protection.

Clear Direction and Benefits

VCIS offers a clear path to a safer financial world by harnessing the power of geospatial smart location intelligence. It enables the tracking of Financial Crimes, crypto money laundering, and Terrorist financing activities, tracing historical criminal activities to uncover hidden networks and prevent future threats. By providing a comprehensive view of illicit financial flows, VCIS empowers decision-makers to take decisive action, safeguarding global financial systems and national security.

VCIS is not merely a tool; it is a paradigm shift in financial crime prevention. By harnessing cutting-edge technologies, VCIS empowers law enforcement and financial institutions to detect, prevent, and combat sophisticated Financial Crimes across borders. Its impact extends beyond immediate crime prevention, promising a future of enhanced transparency, security, and trust in global financial systems.

7. Mesures de sécurité adaptatives

VCIS utilise un cryptage, des contrôles d'accès et des protocoles de sécurité adaptatifs de pointe pour garantir la plus haute protection des données.

Orientation et avantages clairs

VCIS renforce la sécurité financière mondiale grâce à l'exploitation de l'intelligence géospatiale et de la localisation intelligente. Il identifie les crimes financiers, le blanchiment d'argent en cryptomonnaie et le financement du terrorisme en retraçant les activités criminelles historiques pour révéler les réseaux dissimulés et anticiper les menaces émergentes. En offrant une vue exhaustive des flux financiers illicites, VCIS permet aux décideurs de prendre des mesures stratégiques et décisives, assurant ainsi la protection des systèmes financiers mondiaux et de la sécurité nationale.

VCIS transforme la lutte contre la criminalité financière en offrant aux forces de l'ordre et aux institutions financières des outils avancés pour détecter, prévenir et contrer les crimes complexes à l'échelle mondiale. Son impact va au-delà de la prévention, favorisant un avenir de transparence, de sécurité et de confiance renforcées dans les systèmes financiers mondiaux.

Introduction

Virtual asset activities may create illicit finance vulnerabilities due to their borderless nature, decentralized structure, limited transaction transparency, hidden or undisclosed UBOs, and speed of operations. Anonymized cryptos or privacy coins further reduce transparency and obscure the source through cryptographic enhancements, thus circumventing typical Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) controls.

"Cryptocurrency has given money launderers a feature that they have dreamt of – secrecy"

Regulations continue to be insufficient, necessitating the use of further technological solutions like **VCIS**. This geospatial technology is beneficial, especially in high-tech and rapidly advancing industries such as crypto. By utilizing cutting-edge technologies, this technique enables law enforcement to more effectively monitor and control cryptocurrency operations.

With the Middle East emerging as a hotspot for cryptocurrency trading,

Introduction

Les actifs virtuels créent des vulnérabilités financières en raison de leur nature qui n'est pas limitée aux frontières, de leur structure décentralisée et de la transparence limitée des transactions. L'anonymat des cryptomonnaies et des pièces de confidentialité, renforcé par des améliorations cryptographiques, complique la traçabilité des flux financiers. Cela permet de contourner les contrôles traditionnels de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT), augmentant ainsi les risques de financement illicite.

"La crypto-monnaie a offert aux blanchisseurs d'argent une fonctionnalité qu'ils avaient toujours recherchée : la confidentialité."

Les réglementations actuelles demeurent insuffisantes, rendant nécessaires l'adoption de solutions technologiques avancées comme le **VCIS**. Cette technologie géospatiale se révèle particulièrement précieuse dans des secteurs en constante évolution, tels que la cryptographie. En intégrant des technologies de pointe, elle permet aux forces de l'ordre d'assurer une surveillance et un contrôle plus efficaces des opérations liées aux crypto-monnaies.

Le Moyen-Orient devient un centre clé pour le commerce des crypto-monnaies, avec une croissance de 500 % des transactions entre juillet 2020 et mai 2024, ce qui rend essentiel de renforcer la lutte contre le blanchiment d'argent transfrontalier. Les Émirats arabes unis, en particulier Dubaï, ont créé un

boasting a 500% increase in transactions between July 2020 and May 2024, it's imperative to address cross-border money laundering effectively.
The UAE has been harboring an encouraging environment for the growth of its crypto industry, especially with Dubai's enactment of the Virtual Assets Law and establishment of VARA. While the industry was largely unregulated a few years ago, recent legislative measures have shown the government's keenness to reduce potential financial crime risk in the nascent industry.

The surge of cryptocurrencies in the UAE has ushered in a new era of financial innovation, posing a massive challenge to regulatory authorities. Thus, we see that the UAE has made many provisions for protecting crypto assets from money laundering. But, money launderers are at a higher pace of exploiting technology for illegal activities.

In response to a rise in cases of money laundering and terrorist financing, global and national regulators are making a significant progress with relevant protection laws, but the challenge lies in identifying the red flags at the right time and the real users of the digital wallet addresses in the absence of any effective KYC or national crypto wallet database.

Digital currencies are reshaping the landscape of money where combating

environnement favorable à l'essor de l'industrie de la cryptographie, notamment grâce à l'adoption de la loi sur les actifs virtuels et à la création de la VARA. Alors que le secteur était principalement non réglementé il y a quelques années, les récentes initiatives législatives témoignent de l'engagement du gouvernement à atténuer les risques liés à la criminalité financière dans ce domaine émergent.

L'essor des crypto-monnaies aux Émirats arabes unis marque le début d'une nouvelle ère financière, tout en représentant un défi majeur pour les autorités de régulation. En réponse, les Émirats ont adopté des mesures pour protéger les actifs cryptographiques contre le blanchiment d'argent. Toutefois, les blanchisseurs d'argent exploitent de plus en plus ces technologies à des fins illégales, nécessitant ainsi une vigilance renforcée et des ajustements réglementaires.

Face à l'augmentation des cas de blanchiment d'argent et de financement du terrorisme, les régulateurs nationaux et mondiaux ont fait des progrès notables avec des législations de protection. Cependant, le véritable défi réside dans l'identification en temps réel des signaux d'alarme et des adresses réelles des utilisateurs de portefeuilles numériques, en l'absence de bases de données KYC ou de registres nationaux de portefeuilles crypto efficaces.

Les monnaies numériques transforment le paysage financier, rendant la lutte contre le

money laundering through cryptocurrency has become paramount. You find yourself at the forefront of this dynamic shift, charged with navigating the complexities of this brave new world. But fear not, for VALOORES stands as a beacon of expertise, drawing upon 35 years of unparalleled experience in the financial crime arena.

Yet, despite your best efforts, you are not ready yet! The challenge remains daunting: identifying elusive digital wallet owners and unraveling the enigma of their movements, behaviors, and connections. Enter VCIS, a pioneering solution harnessing the power of data correlation. Through an innovative fusion of blockchain databases, geospatial data, KYC protocols, digital identity verification, and call detail records (CDR), VCIS empowers you to conquer this formidable challenge.

Through VCIS we are monitoring VASPs activities and uncovering the financial crimes committed through cryptocurrencies. VCIS empowers industry players with advanced tools to monitor and investigate activities effectively, bridging the gap between regulatory provisions and real-time surveillance and investigation.
By leveraging geospatial data and correlating it with transactions through dynamic knowledge graphs, VCIS can track digital wallet activities and identify wallet address owners swiftly.

blanchiment d'argent via les cryptomonnaies essentielles. Vous êtes à l'avant-garde de cette évolution, naviguant dans ses complexités. Toutefois, avec VALOORES, vous bénéficiez d'un partenaire expert, fort de 35 années d'expérience inégalée dans le domaine de la criminalité financière.

Malgré vos efforts, le défi demeure : identifier les propriétaires de portefeuilles numériques et comprendre leurs mouvements, comportements et connexions. C'est là qu'intervient VCIS, une solution innovante qui exploite la puissance de la corrélation des données. En intégrant des bases de données blockchain, des données géospatiales, des protocoles KYC, des vérifications d'identité numérique et des enregistrements détaillés des appels (CDR), VCIS vous permet de surmonter ces défis complexes avec efficacité.

Avec VCIS, nous assurons une surveillance approfondie des activités des VASP et détectons les crimes financiers liés aux crypto-monnaies. La plateforme fournit aux acteurs du secteur des outils avancés pour mener des enquêtes et une surveillance efficaces, comblant ainsi le fossé entre la réglementation et la surveillance en temps réel. En utilisant les données géospatiales et en les corrélant avec les transactions via des graphiques de connaissances dynamiques, VCIS permet de suivre les activités des portefeuilles numériques et d'identifier rapidement les propriétaires des adresses associées.

Imagine having the power to unravel the complicated web of a money laundering scheme, spanning multiple countries and leveraging the anonymity of cryptocurrencies. This is precisely what VCIS did; through a deep dive into a real case study. As the investigation unfolds, you'll witness the crucial role played by the VASPs, operating as cryptocurrency exchange stores, in facilitating the conversion of illicit funds into fiat currency – the critical "cash-out" step that allows laundered money to be integrated into the traditional financial system. VCIS connects the dots between suspicious wallet addresses, physical devices, and individuals' movements, establishing direct links between perpetrators and their illicit financial activities. But the thrill doesn't stop there, our system's prowess extends to untangling the transnational complexities of this money laundering operation, involving multiple individuals

Imaginez avoir la capacité de démêler un réseau complexe de blanchiment d'argent, s'étendant sur plusieurs pays et exploitant l'anonymat des crypto-monnaies. C'est exactement ce que permet VCIS, à travers une étude de cas approfondie. L'enquête met en lumière le rôle clé des VASP, qui agissent en tant que plateformes d'échange de crypto-monnaies, facilitant la conversion des fonds illicites en monnaie fiduciaire – l'étape critique de « retrait » permettant d'intégrer l'argent blanchi dans le système financier traditionnel. VCIS relie les points entre les adresses de portefeuilles suspects, les appareils physiques et les mouvements des individus, établissant des liens directs entre les auteurs et leurs activités criminelles. En outre, notre technologie permet de démêler les complexités transnationales de ces opérations de blanchiment, impliquant de multiples acteurs et entités répartis sur plusieurs pays.

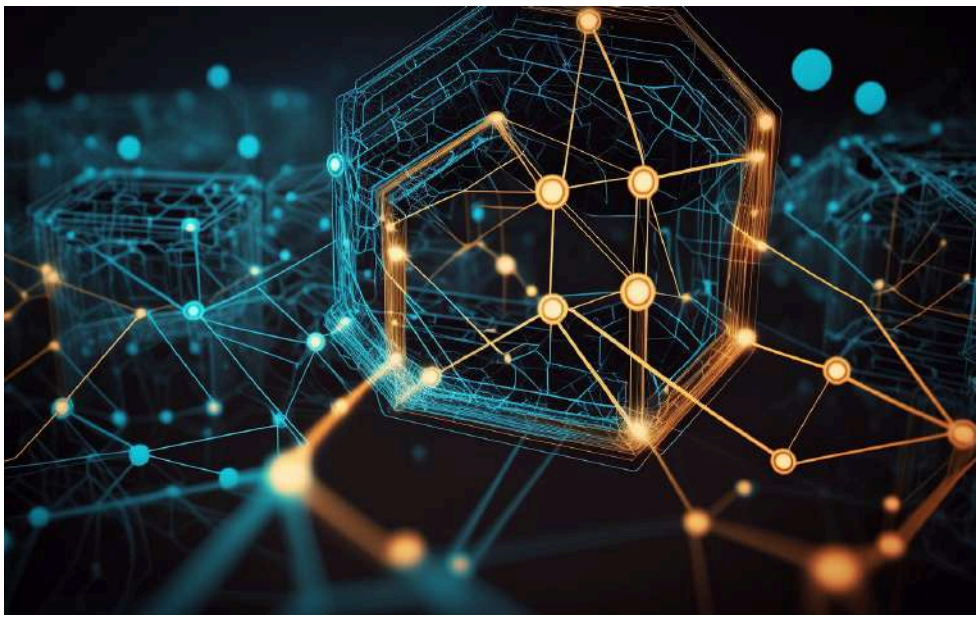
and entities across different locations, potentially spanning multiple countries.

Join us on this journey, where geospatial technology meets investigative prowess, and witness firsthand how our system empowers you to stay ahead of the curve in the ever-evolving world of financial crimes.

Through the following case study, we identified several parties using unregistered digital wallets to launder money between Europe, Turkey and Nigeria.
Brace yourself, for you are about to embark on a journey where every transaction tells a story, and every clue leads to uncovering the truth behind the flow of illicit funds. Welcome to the future of financial security. Welcome to VCIS!

Participez à cette aventure où l'innovation géospatiale se conjugue avec des capacités d'enquête avancées, et découvrez comment notre solution vous permet de maintenir une longueur d'avance face à l'évolution rapide de la criminalité financière.

Grâce à l'étude de cas suivante, nous avons identifié des entités exploitant des portefeuilles numériques non enregistrés pour faciliter le blanchiment d'argent entre l'Europe, la Turquie et le Nigeria.
Préparez-vous à explorer un processus où chaque transaction révèle des informations cruciales et chaque indice conduit à la compréhension des flux financiers illicites.
Découvrez l'avenir de la sécurité financière avec VCIS!



Story

The Nigerian law enforcement recently received critical intelligence from a European law enforcement agency concerning a digital wallet address suspected of involvement in complex money laundering activities spanning Europe, Turkey, and Nigeria. This suspected digital wallet address **TPyjXXXXXXXXXNa5** has been implicated in a series of cryptocurrency transactions on the decentralized Tron blockchain linked to drug trafficking operations and subsequent laundering activities.
According to the information provided, individuals associated with this wallet address are believed to have received substantial crypto transactions in Nigeria from a drug cartel operating between Europe and Turkey. These transactions are suspected to be part of a larger scheme involving cashing out at local exchanges in Nigeria before the illicit funds are reintegrated into the financial system, ultimately returning to Europe through undisclosed methods. One particularly notable transaction, amounting to $3.7 million, was traced to this wallet on February 11, 2024. This significant sum underscored the urgency and gravity of the situation.

Histoire

Les autorités nigérianes ont récemment reçu des informations clés d'une agence européenne de régulation concernant une adresse de portefeuille numérique, **TPyjXXXXXXXXXNa5**, suspectée d’être impliquée dans des activités complexes de blanchiment d'argent à travers l’Europe, la Turquie et le Nigeria. Cette adresse a été liée à une série de transactions en crypto-monnaies sur la blockchain décentralisée Tron, associées à des opérations de trafic de drogue et à des activités de blanchiment ultérieures.
Les informations disponibles indiquent que les individus associés à cette adresse de portefeuille ont reçu d'importantes transactions cryptographiques en provenance du Nigeria, provenant d'un cartel de la drogue opérant entre l'Europe et la Turquie. Ces transactions font probablement partie d'un schéma plus large visant à encaisser des fonds dans des bourses locales au Nigeria, avant de réintégrer ces fonds illicites dans le système financier et de les faire revenir en Europe par des méthodes non divulguées. Une transaction clé de 3,7 millions de dollars, effectuée le 11 février 2024, a mis en évidence l'ampleur et la gravité de cette opération.

In response to these findings, Nigerian law enforcement initiated a comprehensive financial investigation leveraging our cutting-edge **VCIS** platform.
The primary objectives of this investigation are to:
Uncover the identities behind the suspected money laundering operation.
Ascertain the accomplices involved.
Trace the flow of illicit funds to their final recipients and destinations.
Expose the methods employed to reintegrate laundered money back into Europe.
Pinpoint any conversion of cryptocurrencies into tangible assets within the financial system.

This case study will delve into the intricate web of financial transactions and criminal activities associated with this wallet address, shedding light on the challenges and methodologies encountered during the investigation. It highlights the critical role of advanced technological solutions VCIS in combating modern financial crimes, emphasizing the commitment to robust enforcement and international cooperation in countering illicit financial activities.

En réponse à ces découvertes, les forces de l'ordre nigérianes ont lancé une enquête financière approfondie en s'appuyant sur l'expertise avancée de la plateforme VCIS.
Les objectifs principaux de cette enquête sont les suivants:
Identifier les individus derrière l'opération présumée de blanchiment d'argent.
Vérifier les complices impliqués dans le réseau.
Tracer le flux des fonds illicites jusqu'à leurs destinataires et destinations finales.
Révéler les méthodes utilisées pour réintégrer les fonds blanchis en Europe.
Localiser toute conversion de crypto-monnaies en actifs physiques dans le système financier.

Cette étude de cas examine le réseau complexe de transactions financières et d'activités criminelles liées à cette adresse de portefeuille, mettant en évidence les défis et les méthodologies utilisés au cours de l'enquête. Elle souligne l'importance des solutions technologiques avancées, telles que VCIS, dans la lutte contre la criminalité financière moderne, tout en affirmant l'engagement en faveur d'une répression efficace et d'une coopération internationale renforcée contre les activités financières illicites.

Scenario

Chapter 1: Wallet Address Owners and the Flow of Crypto Transactions

A. Crypto Transaction Analysis

Utilizing the VCIS knowledge graph, we accurately survey the crypto transactions associated with the identified wallet address: **TPyjyXXXXXXXXXXXXNan5**

1. The initial transaction occurred at 13:42 on February 11, 2024, with 3.7 million USDT, received via the Tron blockchain. The sender was the wallet address **TUpMXXXXXXXXXXXXQo2**. Subsequently, at 17:32 on the same day, **TPy…an5** executed a transfer on the Tron blockchain to a third party, **TWzQXXXXXXXXXXXXMmjo**.

2. The second transaction occurred on February 14, 2024, at 10:35, involving the reception of 8.3 million USDT via the Tron blockchain. This transaction originated from **TCr8dXXXXXXXXXXXXyhE.** Shortly thereafter, at 13:32 on the same day, **TPy…an5** executed another transfer on the Tron blockchain to the same third party, using wallet address **TWz…mjo**.

This wallet address is registered in our VCIS DKYC (Digital Know Your Customer) database as associated with a cryptocurrency exchange store named Crystal Star, located at 16D street.

Scénario

Chapitre 1: Propriétaires d'Adresses de Portefeuille et Flux de Transactions Crypto

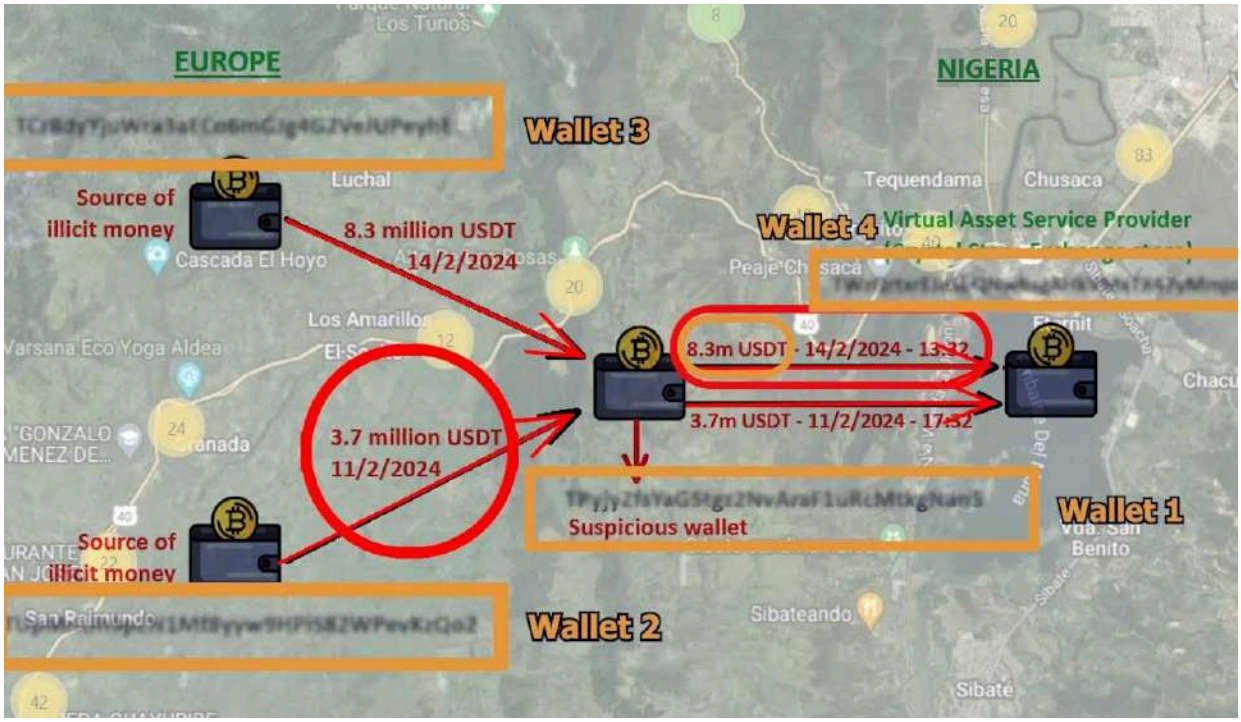
A. Analyse des transactions cryptographiques

Grâce au graphique de connaissances VCIS, nous analysons en profondeur les transactions cryptographiques liées à l'adresse de portefeuille identifiée: **TPyjyXXXXXXXXXXXXNan5**

1. La transaction initiale a eu lieu à 13h42 le 11 février 2024, avec 3,7 millions USDT, reçus via la blockchain Tron. L'expéditeur était l'adresse du portefeuille **TUpMXXXXXXXXXXXXQo2**. Par la suite, à 17h32 le même jour, **TPy...an5** effectué un transfert sur la blockchain Tron vers un tiers, **TWzQXXXXXXXXXXXXMmjo**.

La deuxième transaction a eu lieu le 14 février 2024 à 10h35, impliquant la réception de 8,3 millions USDT via la blockchain Tron, en provenance de l'adresse **TCr8dXXXXXXXXXXXXouais**. Quelques heures plus tard, à 13h32, l'adresse TPy...an5 a effectué un autre transfert sur la blockchain Tron vers le même destinataire, utilisant l'adresse du portefeuille **TWz…mjo**.

Cette adresse de portefeuille est référencée dans notre base de données VCIS DKYC (Digital Know Your Customer) comme étant associée à un échange de crypto-monnaies, Crystal Star, situé au 16D rue.



B. Common Devices at the VASP Store

In order to trace the owners or users of the wallet address **TPyjXXXXXXXXXXXXNan5**, which was used by the suspected individuals, we conducted targeted activity scans around the location of the crystal star exchange store within a 30-minute window before and after the specific date and time of each transaction originating from the suspect's wallet to the cryptocurrency exchange store's wallet **TWzQXXXXXXXXXXXXMmjo.**

Below are the screenshots capturing the details of these common devices identified during the investigative activity scans conducted around the Crystal Star store's location (6.562624,3.250005).

B. Appareils courants dans la boutique VASP

Pour identifier les propriétaires ou utilisateurs associés à l'adresse du portefeuille **TPyjXXXXXXXXXXXXNan5**, utilisée par les individus suspects, nous avons mené des analyses d'activités ciblées autour de l'emplacement de l'échange de crypto-monnaies Crystal Star. Ces analyses ont été réalisées dans une fenêtre de 30 minutes avant et après chaque transaction spécifique, depuis le portefeuille suspect vers le portefeuille de l'échange **TWzQXXXXXXXXXXXXMmjo.**

Ci-dessous, vous trouverez les captures d'écran présentant les détails des appareils identifiés lors des analyses d'activités menées autour de l'emplacement de l'échange de crypto-monnaies Crystal Star (coordonnées: 6.562624, 3.250005).

Through these activity scans, we successfully identified several devices present at the location of the Crystal Star store during each of the specified time periods. Among these devices, the following are recognized as common across both activity scans:

- Device ID 1: 12d3b9fd-7b85-4796-9c09-185f50ff9af5
- Device ID 2: ede4edef-1059-45d3-aadc-80f611a2ee77
- Device ID 3: 340c0e55-b71d-4ebe-882b-d80710ae1fd6

These transactions occurred at:

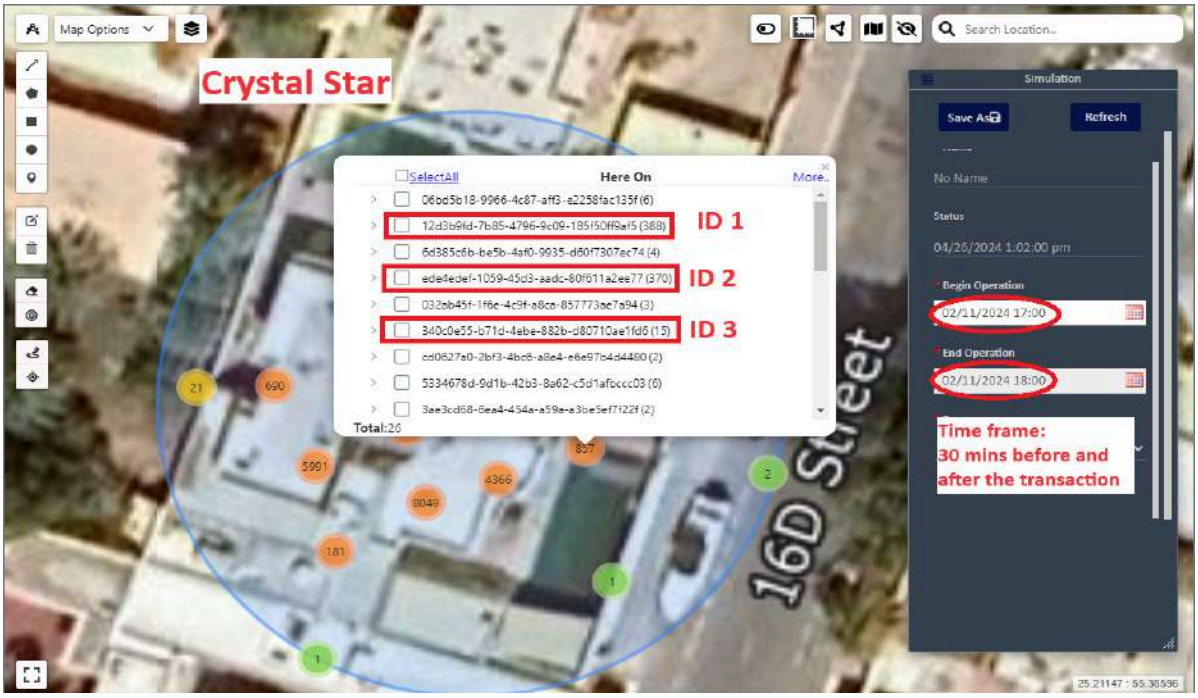
1. **17:32 on February 11, 2024**
   (AS - Crystal Star 11 Feb)

Ces analyses ont permis d'identifier plusieurs appareils présents à cet emplacement durant les périodes spécifiées. Parmi ces appareils, les suivants ont été reconnus comme communs aux deux séries d'analyses:

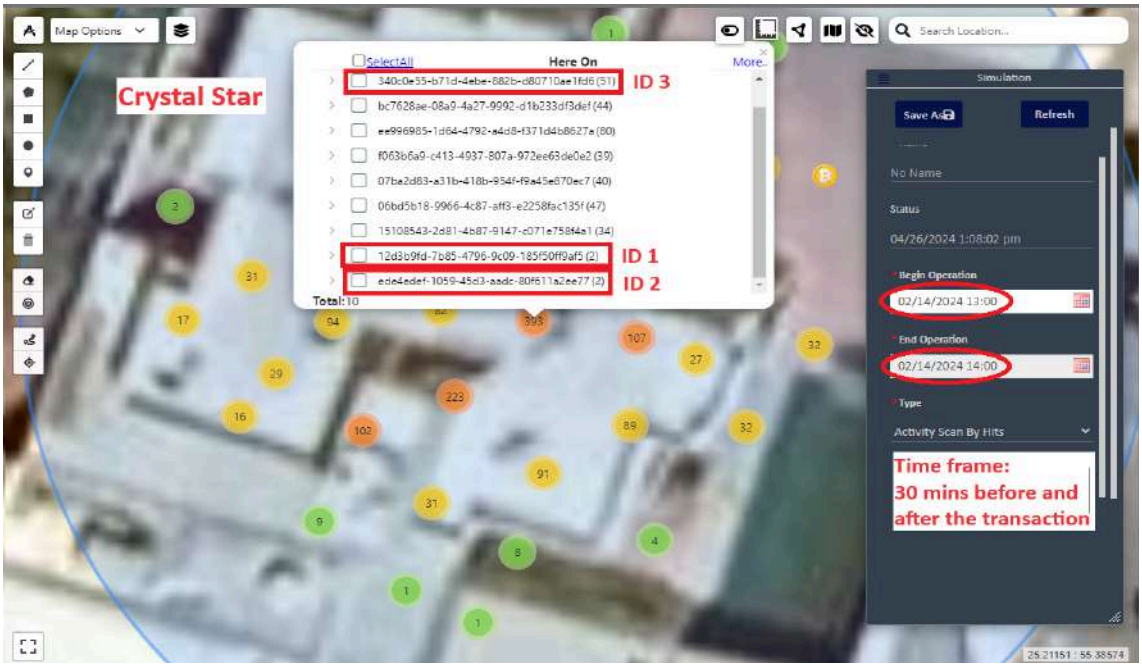
- ID de l'appareil 1: 12d3b9fd-7b85-4796-9c09-185f50ff9af5
- ID de l'appareil 2: ede4edef-1059-45d3-aadc-80f611a2ee77
- ID de l'appareil 3: 340c0e55-b71d-4ebe-882b-d80710ae1fd6

Ces transactions ont eu lieu à:

1. **17h32 le 11 février 2024**
   (AS - Étoile de cristal 11 février)



1. **13:32 on February 14, 2024**
   (AS - Crystal Star 14 Feb)



These findings contribute crucial insights into potential connections between the suspicious wallet addresses associated with the suspects and the devices detected within the proximity of the cryptocurrency exchange store during the respective transaction periods.

C. Suspicious Wallet Address Owner

Further investigation involving a Device History query **DH** for the identified three devices introduced critical insights:

1. Device ID1 and Device ID2 are attributed to the VASPs (Virtual Asset Service Providers), as their historical patterns indicate regular visits to the same location each

1. **13h32 le 14 février 2024**
   (AS - Crystal Star, 14 février)

Ces résultats fournissent des informations essentielles sur les liens potentiels entre les adresses de portefeuille suspectes associées aux individus concernés et les appareils détectés à proximité du magasin d'échange de crypto-monnaies pendant les périodes de transaction spécifiées.

C. Propriétaire d'une adresse de portefeuille suspecte

Enquête plus approfondie impliquant une requête sur l'historique de l'appareil **DH** pour les trois appareils identifiés, des informations essentielles ont été introduites:

1. Les identifiants Device ID1 et Device ID2 sont associés aux fournisseurs de services d'actifs virtuels (VASP), car leurs modèles de déplacements

day, followed by a return to their respective home location (6.562278, 3.241365). This consistent behavior suggests a routine associated with professional duties or regular business operations.
(DH - ID1 and ID2)

historiques révèlent des visites régulières au même emplacement chaque jour, suivies d'un retour systématique à leur domicile (coordonnées: 6,562278, 3,241365). Ce comportement cohérent laisse présager une routine liée à des activités professionnelles ou commerciales régulières. (DH - ID1 et ID2)

2. In contrast, Device ID3 exhibited a distinct pattern correlating with the suspected wallet address **TPyjXXXXXXXXXXXXNan5**. Device ID3 visited the Crystal Star exchange store precisely during the times when transactions totaling 12 million dollars were sent to the VASP's wallet address. This observation strongly suggests that

2. En revanche, l'appareil ID3 a présenté un comportement distinct, corrélé avec l'adresse du portefeuille suspecté **TPyjXXXXXXXXXXXXNan5**. Ce dispositif a accédé à la boutique d'échange Crystal Star précisément au moment où des transactions d'une valeur totale de 12 millions de dollars étaient effectuées vers l'adresse du portefeuille du VASP.

Device ID3 is the individual responsible for controlling the wallet address in question. They visited the exchange store to convert crypto assets into cash. *(DH - ID 3)*

Cette corrélation suggère fortement que l'appareil ID3 est lié à la gestion de l'adresse de portefeuille concernée, et qu'il a visité le magasin d'échange pour procéder à la conversion des actifs cryptographiques en liquidités. (DH - ID3)

Moreover, an in-depth examination of Device ID3's history revealed that on February 10, 2024, at 14:30, Device ID3 arrived at Lagos International Airport (6.579516, 3.326987) from Istanbul. The screenshots below show the journey of Device ID3 from Istanbul international Airport to Lagos and onwards to the B&C Dyamond Hotel & SUITES (6.528894311636171,3.215514999376401) *(DH - ID 3)*

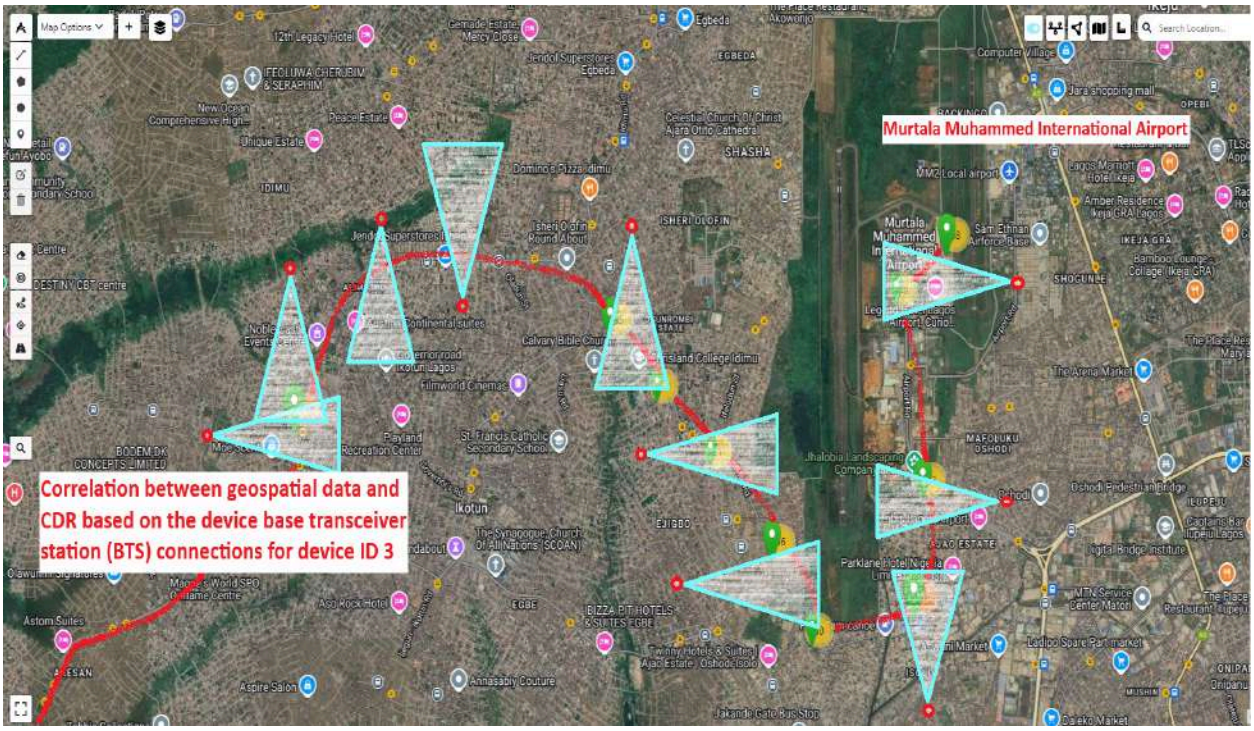
Une analyse approfondie de l'historique de l'appareil ID3 a révélé qu'il est arrivé à l'aéroport international de Lagos (6.579516, 3.326987) en provenance d'Istanbul le 10 février 2024 à 14h30. Les captures d'écran ci-dessous illustrent le trajet de l'appareil ID3, depuis l'aéroport international d'Istanbul jusqu'à Lagos, et au-delà, vers l'hôtel B&C Diamond & Suites (6.528894311636171, 3.215514999376401). (DH-ID 3)

D. Correlation between geospatial data and call detail record (CDR)

Furthermore, leveraging the correlation feature between geospatial data and CDR, we executed a query for device ID3 between Lagos International Airport and the B&C Dyamond Hotel & Suites to compare its geospatial activities on the road to its CDR activities based on the device base transceiver station (BTS) connections.

D. Corrélation entre les données géospatiales et enregistrement détaillé des appels (CDR)

En utilisant la corrélation entre les données géospatiales et les enregistrements d'appels détaillés (CDR), nous avons analysé l'appareil ID3 entre l'aéroport international de Lagos et le B&C Diamond Hotel & Suites, en comparant ses activités géospatiales avec celles des stations de base (BTS) associées.



The previous query allowed us to identify significant associations tied to ID3:

1. Device ID3 utilized a Nigerian SIM card associated with the IMSI number: 6548xxxxxxxx13453.
2. This IMSI is linked to the IMEI number: 3554xxxxxxxxx1239.

La requête précédente nous a permis d'identifier des associations significatives liées à ID3:

1. L'appareil ID3 utilisait une carte SIM nigériane associée au numéro IMSI: 6548xxxxxxxx13453.
2. Cet IMSI est lié au numéro IMEI : 3554xxxxxxxxx1239.

3. This IMSI corresponds to the phone number: +234 201 XXX XXX registered to a Turkish resident with the ID number : RG3 xxxx 70

3. Cet IMSI correspond au numéro de téléphone : +234 201 XXX XXX enregi d'un résident turc avec le numéro d'identification : RG3 xxxx70

Accumulatively, these findings corroborate the identification of the owner of the wallet address **TPyjXXXXXXXXXXXXNan5** as a Turkish individual who travels between Istanbul and Lagos. The integrated capabilities of VCIS enabled the synthesis of geospatial, CDR, blockchain database, and transactional data to uncover vital details crucial to this investigative case. Attached are relevant screenshots and data visualizations, providing comprehensive documentation of these critical findings within the investigative process.This robust analysis strengthens our understanding of the individuals and activities tied to the flow of illicit cryptocurrency transactions.

Ces résultats confirment l'identité du propriétaire de l'adresse du portefeuille **TPyjXXXXXXXXXXXXNan5** en tant qu'individu turc voyageant entre Istanbul et Lagos. Grâce aux capacités avancées de VCIS, nous avons pu intégrer et analyser les données géospatiales, les enregistrements CDR, les bases de données blockchain et les informations transactionnelles, fournissant des informations essentielles pour cette enquête. Vous trouverez ci-joint des captures d'écran et des visualisations des données pertinentes, offrant une documentation complète de ces conclusions cruciales pour l'investigation. Cette analyse approfondie renforce notre compréhension des individus et des activités impliquées dans les flux de transactions cryptographiques illicites.

Chapter 2: Suspects and their Suspicious Activities

Continuing our investigation, we employed advanced queries and analyses within the VCIS tool to uncover the suspicious activities of the identified suspects, focusing on Device ID3.

A. Co-Traveler Query

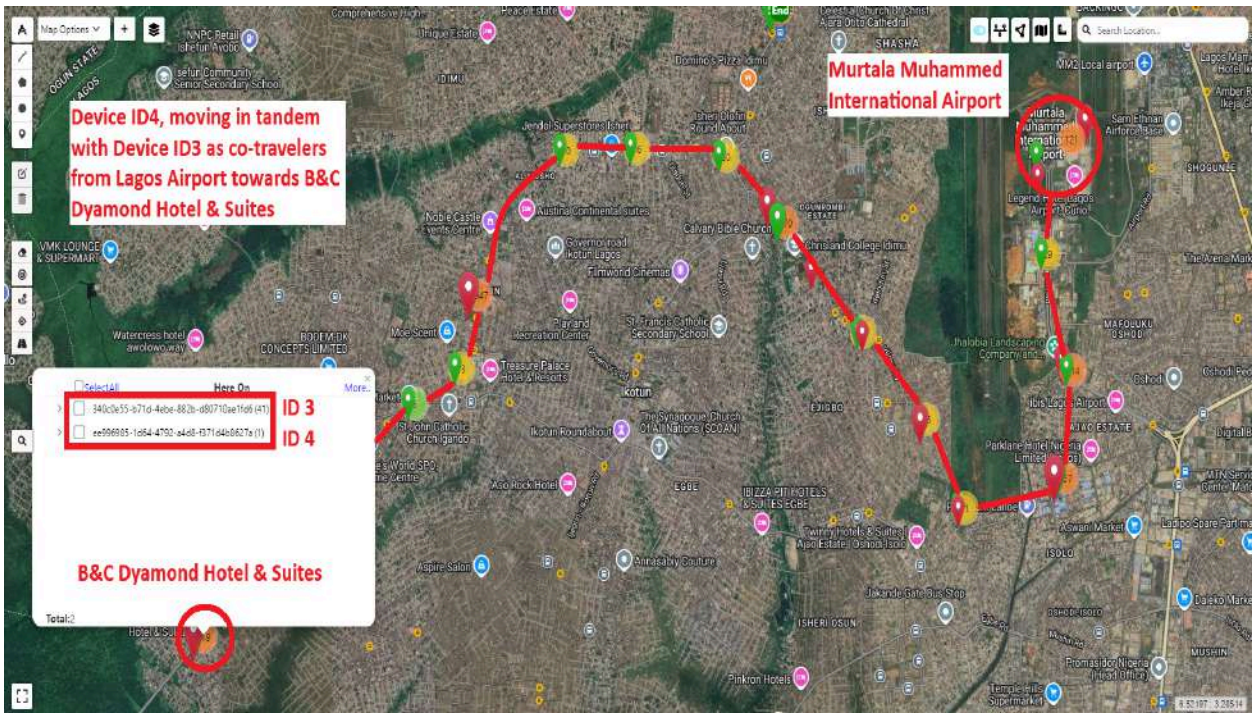
Applying a co-traveler query for Device ID3 from Lagos Airport to "B&C Dyamond Hotel & Suites" revealed the presence of a new device, Device ID4, which moved in tandem with Device ID3 during this journey. The screenshot detailing this co-traveler scenario provides critical evidence of their association.

Chapitre 2: Suspects et leurs activités suspectes

Dans le cadre de notre enquête continue, nous avons utilisé des requêtes et des analyses approfondies au sein de la plateforme VCIS pour examiner les activités suspectes des individus identifiés, en mettant particulièrement l'accent sur l'appareil ID3.

A. Requête d'un co-voyageur

L'application d'une requête de co-voyageur pour l'appareil ID3, depuis l'aéroport de Lagos jusqu'au « B&C Diamond Hotel & Suites », a permis de détecter la présence d'un nouvel appareil, l'appareil ID4, qui s'est déplacé en parallèle avec l'appareil ID3 tout au long du trajet. La capture d'écran associée à cette analyse fournit des éléments de preuve essentiels confirmant leur lien.

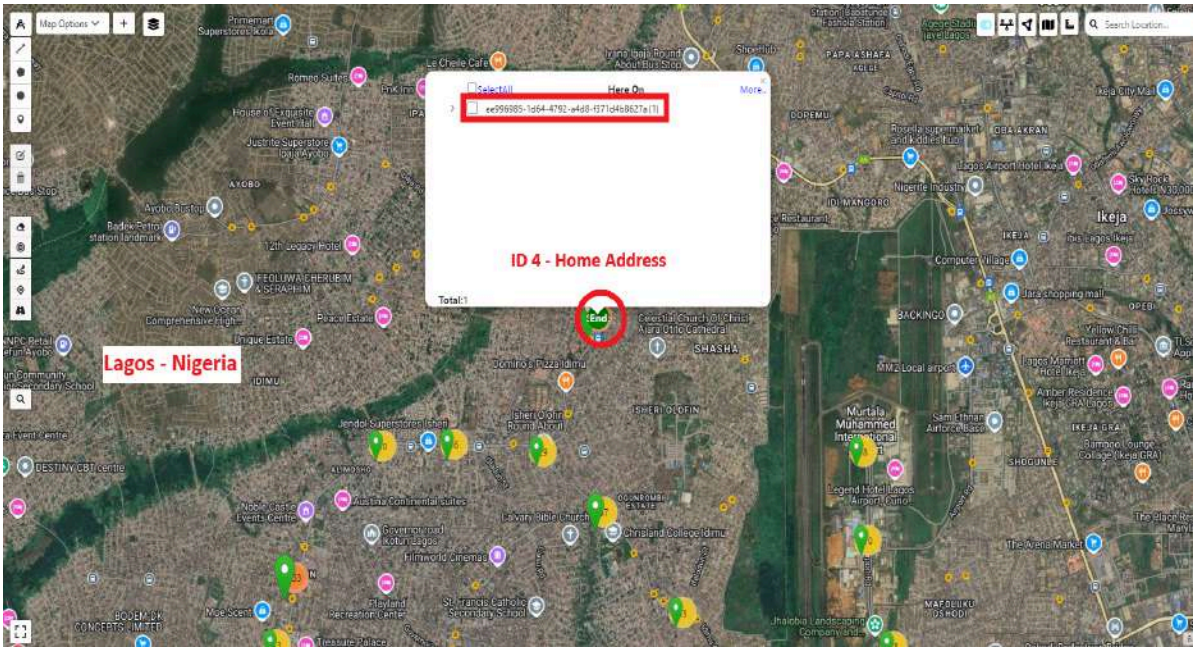


B. Device ID4 Home Address

Subsequent analysis through a device history query for Device ID4 allowed us to identify their residential address and identity. The screenshot capturing Device ID4's home address strengthens our understanding of their background and potential involvement in the suspicious activities. (*DH - ID4)*

B. Adresse personnelle de l'ID4 de l'appareil

Une analyse approfondie, réalisée à partir d'une requête sur l'historique de l'appareil ID4, a permis d'identifier son adresse résidentielle ainsi que l'individu associé. La capture d'écran correspondant à l'adresse du domicile de l'appareil ID4 apporte des éclairages supplémentaires sur son profil et son implication potentielle dans les activités suspectes. (DH-ID4)



C. Activities of Devices ID3 and ID4

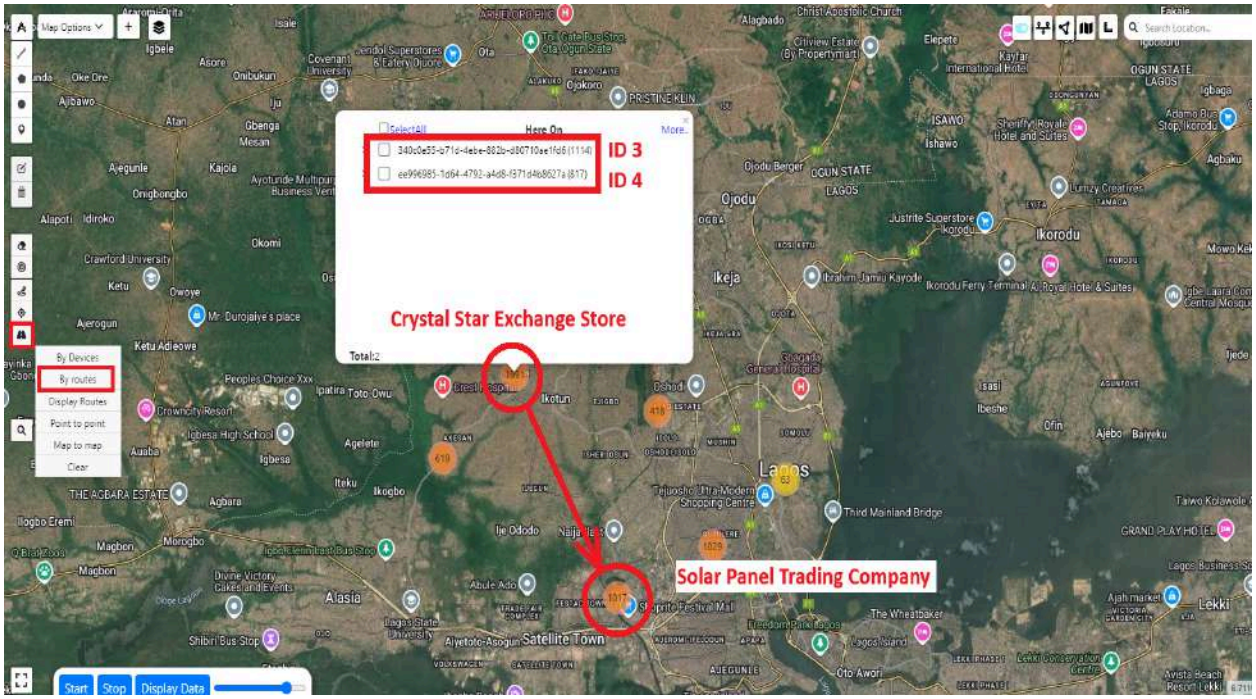
Further examination of the device histories of ID3 and ID4 revealed compelling patterns. They were observed moving together to the Crystal Star exchange location to facilitate the cash-out of cryptocurrency transactions. Following this, they proceeded to a solar panel trading company working between

C. Activités des appareils ID3 et ID4

Une analyse approfondie de l'historique des appareils ID3 et ID4 a révélé des comportements significatifs. Les deux appareils ont été observés se déplaçant ensemble vers l'emplacement du Crystal Star Exchange pour effectuer des encaissements de transactions en crypto-monnaies. Par la suite, ils se sont rendus dans une société de

Lagos and Turkey. This company's operations suggest potential involvement in trade-based money laundering schemes. *(DH - ID3 and ID4)*

négoce de panneaux solaires opérant entre Lagos et la Turquie. Les activités de cette société suggèrent une possible implication dans des schémas de blanchiment d'argent basés sur le commerce. (DH-ID3 et ID4)



D. Identification of Employees

An activity scan conducted around the trade company (6.470216, 3.300636) during working hours for one week led to the identification of 13 device IDs belonging to employees of this company. The screenshot around the company's area sheds light on the network of individuals associated with this enterprise. *(AS - Trade Company)*

D. Identification des employés

Une analyse des activités autour de l'entreprise de négoce (6.470216, 3.300636) pendant les heures de travail sur une période d'une semaine a permis d'identifier 13 appareils appartenant à des employés de la société. Les captures d'écran détaillant la zone autour de l'entreprise mettent en évidence le réseau d'individus associés à ces opérations. (AS - Société Commerciale)

E. Encounters and Points of Interest (POI)

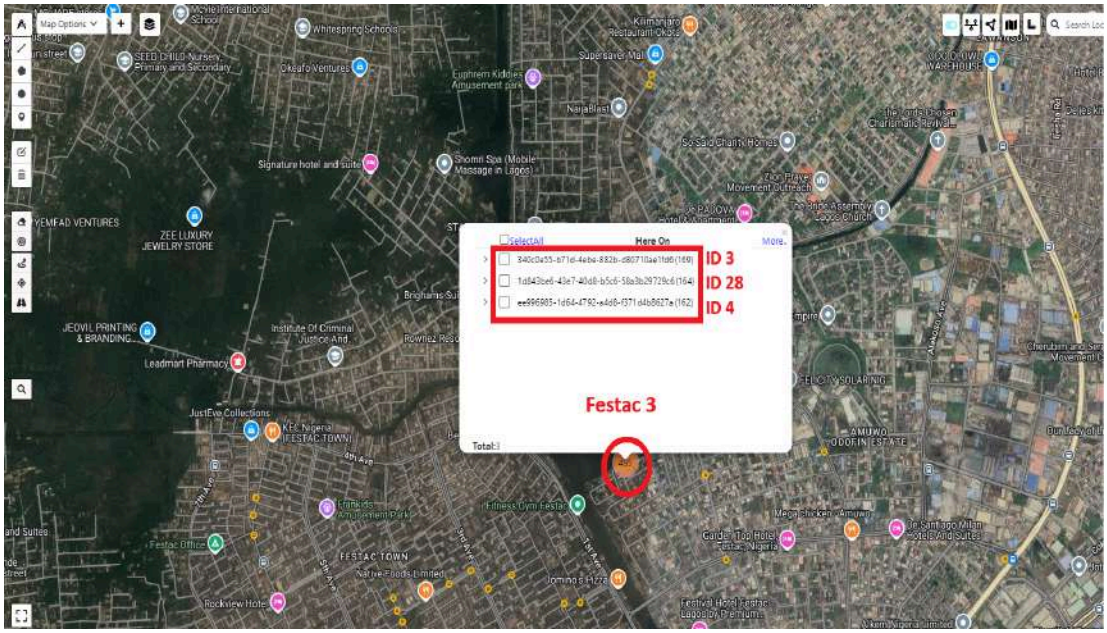
By executing POI query between Devices ID3, ID4, and the identified employees, several encounters were identified, particularly with Device ID28, at various locations in Lagos, notably two different Locations. *(DH - ID3 ID4 ID28)*

1. "Festac 3"

E. Rencontres et points d'intérêt (POI)

EL'exécution d'une requête POI entre les appareils ID3, ID4 et les employés identifiés a révélé plusieurs rencontres, notamment avec l'appareil ID28, à divers endroits à Lagos, y compris deux emplacements distincts. (DH-ID3, ID4, ID28)

1. "Festac 3"



2. "Adetayo" Cafe

These encounters suggest potential meetings or transactions occurring between the suspects and key individuals within the network.

F. Background of Device ID28 - CEO of Solar Panel Trading Company

Executing a device history query of Device ID28, we discovered that they reside in DXB3173 building, AL Karama Street (6.4958823815,3.31767120329), serving as the CEO of the solar panel trading company associated with the suspicious activities. The screenshot capturing Device ID28's home address further solidifies their pivotal role in this investigation.
(DH - CEO Chinese Company)

2. Café « Adetayo »

Ces rencontres indiquent des interactions ou des transactions potentielles entre les suspects et des acteurs clés du réseau.

F. Contexte de l'appareil ID28 - PDG de Solar Panel Trading Company

En exécutant une requête d'historique de l'appareil pour l'ID28, nous avons découvert que la personne réside au Bâtiment DXB3173, rue Al Karama (6.4958823815, 3.31767120329), et occupe le poste de PDG de la société de négoce de panneaux solaires impliquée dans les activités suspectes. La capture d'écran associée à cette adresse renforce son rôle clé dans cette enquête.
(DH - *CEO Chinese Company*)

G. Previous Activities of Device ID3 in Istanbul

Tracing back through the device history query of Device ID3, we uncovered their visits to a Turkish solar Panel company located in Istanbul before their arrival to Lagos. This historical connection raises concerns regarding potential links between the suspects and the trade-based money laundering scheme through two different solar panel trading companies. *(DH - ID3)*

G. Activités précédentes du périphérique ID3 à Istanbul

En analysant l'historique de l'appareil ID3, nous avons identifié plusieurs visites dans une entreprise turque de panneaux solaires située à Istanbul avant leur arrivée à Lagos. Cette connexion historique soulève des préoccupations concernant d'éventuels liens entre les suspects et un système de blanchiment d'argent basé sur le commerce, impliquant deux sociétés commerciales de panneaux solaires distinctes. *(DH - ID3)*

In summary, leveraging the capabilities of the VCIS tool, we have unveiled a suspicious nexus between the suspects and a Chinese company engaged in exporting solar panels to Europe through a Turkish intermediary company. This operation appears to disguise illicit funds through cryptocurrency transfers in Lagos, subsequently converting them into fiat currency for purchasing solar panels destined for the European market. These panels are then sold, integrating the laundered money into legitimate bank accounts under the guise of trading revenues. This sophisticated scheme underscores the significance of our ongoing investigation and the imperative need for further scrutiny by all involved parties.

En résumé, grâce aux capacités avancées de l'outil VCIS, nous avons identifié un lien suspect entre les individus impliqués et une entreprise chinoise exportant des panneaux solaires vers l'Europe via une société intermédiaire turque. Cette opération semble dissimuler des fonds illicites en utilisant des transferts de crypto-monnaies à Lagos, convertis en monnaie fiduciaire pour l'achat de panneaux solaires destinés au marché européen. Ces panneaux sont ensuite revendus, permettant l'intégration des fonds blanchis dans des comptes bancaires légitimes sous forme de revenus commerciaux. Ce schéma complexe met en lumière l'importance cruciale de notre enquête continue et souligne la nécessité d'une analyse approfondie de la part de toutes les parties concernées.

Chapter 3: New wallets' addresses involved in the money laundering

A. Illicit Money New Destinations

In this phase of our investigation, we leveraged the VCIS knowledge graph to analyze all transactions linked to the wallet address. **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2**, source of illicit money, and its final destinations. Two new transactions were sent from this wallet to a new suspected address. **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbG**.

The transactions flow is the following:

1. From **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2** towards the wallet address **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR**
   - On 17/2/2024, a transfer of $4.5 million
   - On 18/2/2024, a transfer of $5.5 million
2. From **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR** towards two new wallets
   - **TSn6Ka98AMQczmKxBbyj7xrGXscvKrkLsu** at 13:05 on 17/2/2024
   - **TUJjqPZM4i9Nthf2NX3e1ueLzpecdPraLG** at 18:35 on 18/2/2024

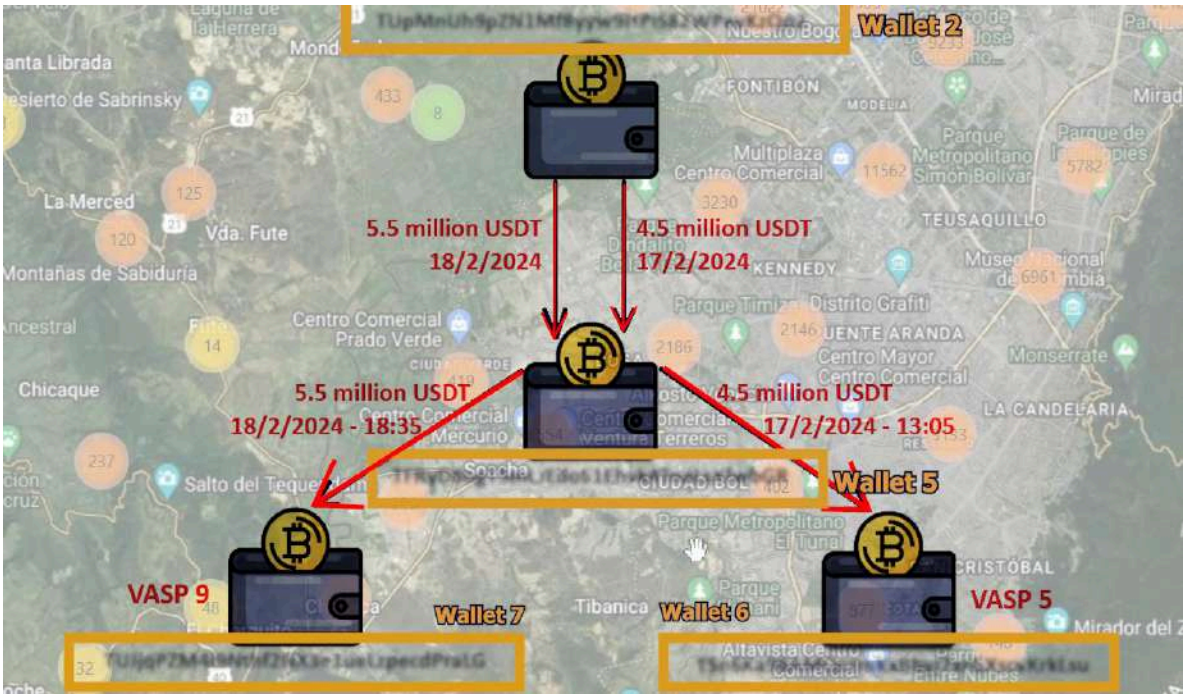
Chapitre 3: Adresses des Nouveaux Portefeuilles Impliqués dans le Blanchiment d'Argent

A. L'argent illicite, nouvelles destinations

Au cours de cette phase de l'enquête, nous avons utilisé le graphe de connaissances VCIS pour analyser en détail toutes les transactions associées à l'adresse du portefeuille. **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2**, source d'argent illicite, et ses destinations finales. Deux nouvelles transactions ont été effectuées depuis ce portefeuille vers une adresse suspecte récemment identifiée. **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR**.

Le flux des transactions est le suivant:

1. Depuis **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2** vers l'adresse du portefeuille **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR**
   - Le 17/2/2024, un transfert de 4,5 millions de dollars
   - Le 18/2/2024, un transfert de 5,5 millions de dollars
2. Depuis **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR** vers deux nouveaux portefeuilles
   - **TSn6Ka98AMQczmKxBbyj7xrGXscvKrkLsont** à 13h05 le 17/2/2024
   - **TUJjqPZM4i9Nthf2NX3e1ueLzpecdPraLG** à 18h35 le 18/2/2024

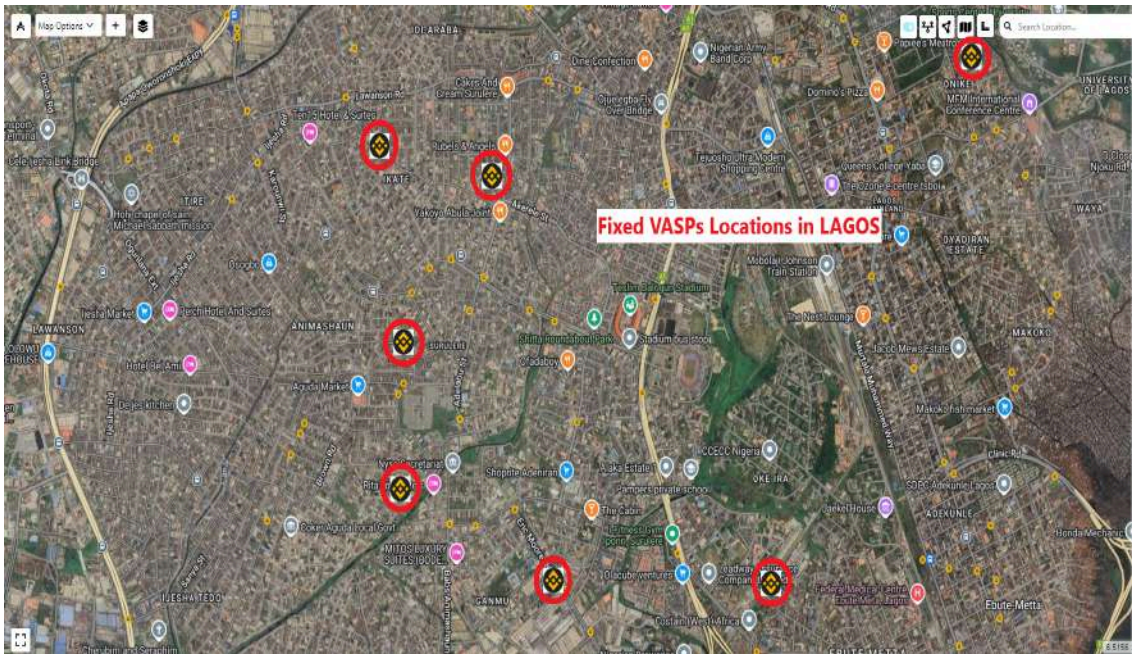


B. VASPs Locations as Fixed Elements

We integrated fixed elements into our analysis, specifically the geo locations of known VASPs (Virtual Asset Service Providers) operating as exchange stores within Nigeria.

B. Emplacements des VASP en tant qu'éléments fixes

Deux nouvelles transactions ont été effectuées depuis ce portefeuille vers une adresse suspecte récemment identifiée. Nous avons également intégré les données géospatiales des VASP opérant comme magasins d'échange au Nigeria.



C. New Suspicious Wallet Address

We conducted an activity scan in proximity to these VASP locations within a 30-minute timeframe surrounding the aforementioned two transactions to identify which device ID moved to any of their locations in the same dates and times to exchange the cryptocurrencies into Fiat.

By comparing the transactions recorded on the Tron blockchain database through an AI engine to our geospatial database resulting from these activity scans around the VASPs' exchange stores , we conclusively identified that the common device located at two different virtual asset service providers locations on the same date and time of each one of these two transactions is device ID 4.

This device ID4 was consistently present at:

1. VASP 5 (6.4906403656548495,3.3454441026910735) exchange store location while the first transaction was made at 13:05 on 17/2/2024 *(AS - VASP 5.)*

C. Nouvelle adresse de portefeuille suspecte

Nous avons mené une analyse d'activité autour des emplacements VASP dans un délai de 30 minutes suivant les deux transactions mentionnées, afin d'identifier les appareils ayant accédé à ces sites aux mêmes dates et heures pour effectuer des échanges de crypto-monnaies contre des devises fiat.

En comparant les transactions enregistrées sur la blockchain Tron via un moteur d'IA avec notre base de données géospatiale issue des analyses d'activité autour des magasins d'échange des VASP, nous avons conclu que l'appareil commun identifié comme l'ID de périphérique 4 était présent chez deux fournisseurs de services d'actifs virtuels différents, aux mêmes dates et heures de ces transactions.

Cet appareil ID4 était systématiquement présent à:

1. VASP 5 (6.4906403656548495,3.3454441026910735) emplacement du magasin d'échange alors que la première transaction a été effectuée à 13h05 le 17/2/2024 *(AS - VASP 5.)*

2. **VASP 9** (6.520315310442519,3.380041208002049 7) exchange store location while the second transaction was made at 18:35 on 18/2/2024. (*AS - VAPS 9)*

2. **VASP 9** (6.520315310442519,3.3800412080020497) emplacement du magasin d'échange tandis que la deuxième transaction a été effectuée à 18h35 le 18/2/2024. (*AS - VAPS 9)*

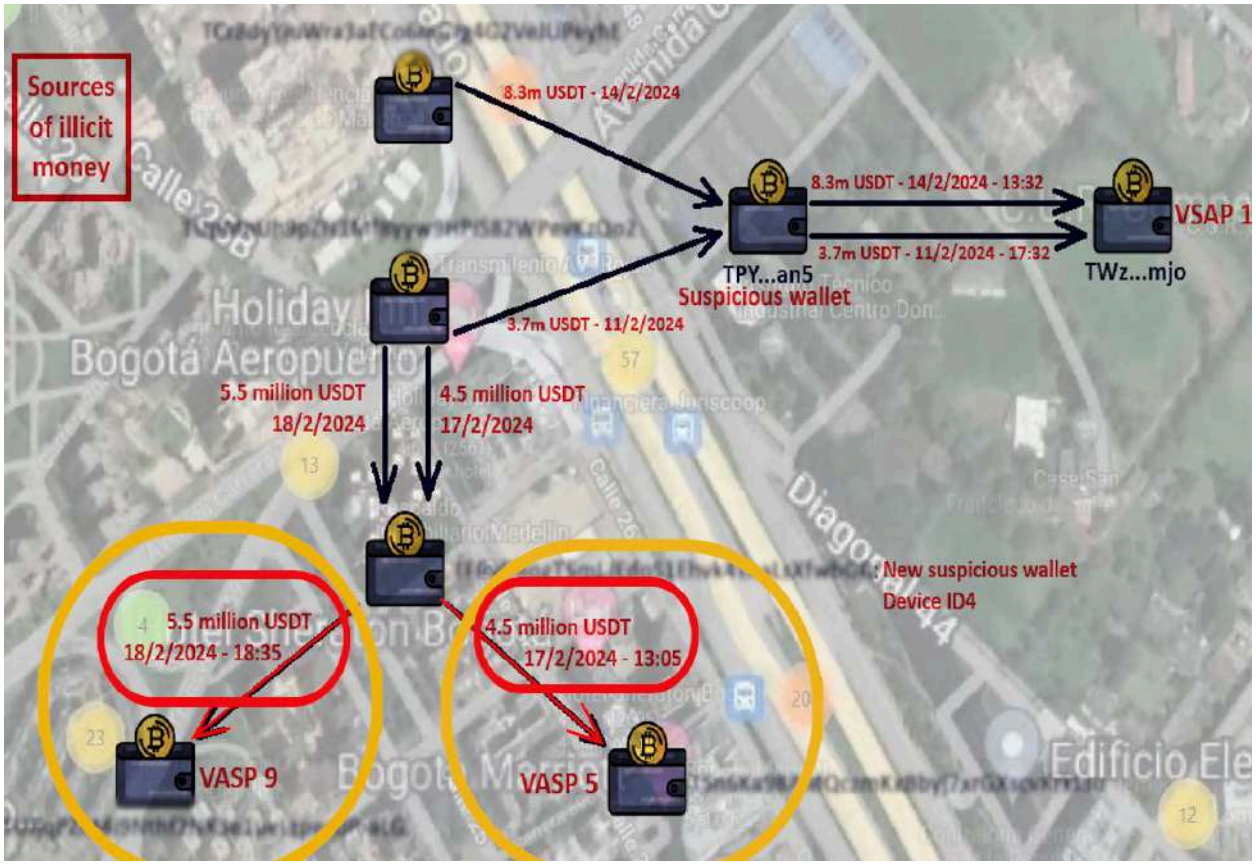
Based on the previous findings, device ID4 is the owner of the wallet address **TFRyD8ogT5mLJEdS1Ehvk4TnaLsXfwbGR** who received funds from **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2** and sent them to the VASP 5's wallet address **TSn6Ka98AMQczmKxBbyj7xrGXscvKrkLsu**, and the VASP 9's wallet address, **TUJjqPZM4i9Nthf2NX3e1ueLzpecdPraLG**, to cash them out.

In summary, our comprehensive analysis of the transactions involving these new wallet addresses unveils intricate connections within the money laundering network. By linking blockchain databases with geospatial insights and leveraging AI-powered analytics, we continue to unravel the complex web of illicit financial activities. The integrated use of VCIS tools and data visualization techniques provides compelling evidence to support ongoing investigative efforts and uncover additional layers of the laundering operation. Attached screenshots and detailed findings further document these critical advancements in our investigation and regulatory compliance measures.

D'après les résultats précédents, l'appareil ID4 est le propriétaire de l'adresse du portefeuille. **TFryD8ogT5mLJEdS1Ehvk4TnaLsXfwbGR** qui a reçu des fonds de **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2** et les a envoyés à l'adresse du portefeuille du VASP 5 **TSn6Ka98AMQczmKxBbyj7xrGXscvKrkLsu**, et l'adresse du portefeuille du VASP 9, **TUJjqPZM4i9Nthf2NX3e1ueLzpecdPraLG**, pour les encaisser.

En résumé, notre analyse approfondie des transactions impliquant ces nouvelles adresses de portefeuille met en lumière des liens complexes au sein d'un réseau de blanchiment d'argent. En combinant les bases de données blockchain avec les données géospatiales et en utilisant des analyses basées sur l'IA, nous continuons à démêler ce réseau d'activités financières illicites. L'intégration des outils VCIS et des techniques de visualisation des données fournit des preuves solides pour appuyer les efforts d'enquête en cours, permettant ainsi de dévoiler des couches supplémentaires de l'opération de blanchiment. Les captures d'écran et résultats détaillés ci-joints documentent ces avancées critiques dans le cadre de nos démarches d'enquête et de conformité réglementaire.

Money Laundering Schema
Schéma de Blanchiment d'Argent



Conclusion

This case study illustrates the multifaceted challenges posed by illicit financial activities within the realm of virtual assets.

The investigation outlined in this study exemplifies the pivotal role of advanced technological solutions like the VCIS in uncovering and dismantling sophisticated money laundering schemes. By leveraging geospatial data, telecommunication

Conclusion

Cette étude de cas illustre les défis multiformes posés par les activités financières illicites dans le domaine des actifs virtuels.

L'enquête présentée dans cette étude met en évidence l'importance des solutions technologiques avancées, telles que le VCIS, dans la détection et l'éradication de systèmes sophistiqués de blanchiment d'argent. En intégrant les données géospatiales, les

records, and transactional insights, law enforcement agencies can identify key actors, trace illicit funds, and disrupt criminal networks operating across borders.

The case also underscores the need for an advanced investigation tool to address the evolving tactics of financial criminals effectively.

Extrapolating to the UAE´s vision in the realm of virtual assets, and as the country continues to position itself as a leading hub for blockchain innovation, it is imperative to enhance investigation oversight and enforcement mechanisms to mitigate the risks associated with virtual asset activities. By harnessing the power of technology and collaboration, stakeholders can safeguard the integrity of the financial system and uphold the principles of transparency, security, and trust in the digital era.

enregistrements de télécommunications et les informations transactionnelles, les autorités répressives peuvent identifier les acteurs clés, suivre les flux financiers illicites et perturber les réseaux criminels opérant à l'échelle internationale.

Cette affaire met en évidence la nécessité d'utiliser des outils d'enquête avancés pour répondre de manière proactive et efficace aux tactiques évolutives des criminels financiers.

Les Émirats arabes unis, en tant que leader dans le domaine des actifs virtuels et de l'innovation blockchain, doivent renforcer les mécanismes de surveillance et d'application pour atténuer les risques associés. En exploitant les technologies avancées et la collaboration entre les parties prenantes, il est possible de garantir l'intégrité du système financier tout en préservant la transparence, la sécurité et la confiance à l'ère numérique.