**Technical report on Atala PRISM Modular KYC Solution by IAMX with ID 1100031**
**Milestone: 3**

| | |
|---|---|
| Project ID | 1100031 |
| Link full project | https://projectcatalyst.io/funds/11/cardano-use-cases-solution/atala-prism-modular-kyc-solution-by-iamx |
| Challenge | F11: Cardano Use Cases: Solution |
| Milestone 3 | https://milestones.projectcatalyst.io/projects/1100031/milestones/3 |
| Live-URL | https://kyc.iamx.id/onboarding/atalaprism |
| GitHub | https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution |
| Acceptance criteria | Acceptance criteria<br>An individual has the ability to complete the text- and rules-based chatbot, including ID Verification, AML check and wallet and transaction monitoring based on the following acceptance criteria:<br><br>1. Video Walkthrough<br>Capture a video walkthrough of the entire process of interacting with the chatbot, ID verification, AML check and wallet and Transaction Monitoring. This should include the start page, each step of interaction, and the completion or confirmation page that indicates the process has been successfully finished.<br>a. Wallet and transaction monitoring is connected via REST API and not visible for the user in the frontend. The results and reports are shown on pages 14 ff as screenshots and attachments.<br>b. A demonstration of the software used in a frontend version is shown here: https://www.youtube.com/watch?v=Ew-xdSFeEuI.<br>c. The video walkthrough of the entire process of interacting with the chatbot, ID verification, AML check has been uploaded within milestone 2.<br><br>2. Technical Reports<br>Provide technical reports that show the interaction data with the chatbot, AML check and wallet and Transaction Monitoring. This data is anonymized to protect personal information but will include timestamps, types of questions answered, and the completion status.<br>a. This document is the technical report for milestone 3.<br><br>3. The chatbot, ID-Verification, AML and wallet and transaction monitoring are not open-source. |
| Evidence of milestone completion | 1. Documentation of Video Walkthrough in GitHub (https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution) for Chatbot, ID-Verification, AML and wallet and transaction monitoring.<br>2. Documentation of technical reports in GitHub (https://github.com/IAMXID/Atala-PRISM-Modular-KYC-Solution) for Chatbot, ID-Verification, AML and wallet and transaction tonitoring. |

The color green is used to point out evidence.

**Table of Contents**

1. About ........ 3

Table 1: Overview Elements and Functions included in Milestones 1-5 and Partners ........ 3

2. Milestone 2 KYT , wallet and transaction monitoring ........ 4

2.1 What KYT Includes ........ 4

2.1.1 Components of KYT ........ 4

2.1.2 How KYT is Performed ........ 4

2.1.3 Results of KYT ........ 5

2.1.4 Actions Based on KYT Results ........ 5

2.1.5 Legal Obligations ........ 5

2.2 Features of KYT, wallet and transaction monitoring ........ 6

Table 2: Features of KYT in basic and advanced KYT ........ 6

2.3 KYT Partner ........ 7

2.4 Goals and Intentions of KYT ........ 7

2.4 Main Legal Sources ........ 8

Table 3: Legal Sources for KYT per jurisdiction ........ 8

3. Cryptocurrency transaction monitoring, wallet monitoring ........ 10

Table 4: Key functions of the REST API ........ 10

3.1 How it works ........ 12

3.1.1 Match with aggregated wallet addresses and transactions, that have been associated with certain services ........ 12

3.1.2 Flagged services / categories ........ 12

Table 5: Risk policy to identify risk level ........ 12

3.1.3 Rules ........ 13

Table 6: Rules and description example ........ 13

3.1.4 Counterparty Analysis ........ 13

3.1.5 Full Coverage vs Sanctions Screening ........ 14

3.2 Result example address report with risk level no risk ........ 14

3.3 Result example KYT no match ........ 14

3.4 Result example risk level high ........ 15

3.5 Risk Classifiers: List of risks which have been checked for ........ 16

## 1. About

- This technical report details the development and implementation of the Atala PRISM Modular KYC Solution by IAMX, with ID 1100031.

- The solution introduces a chatbot-based prototype designed to facilitate identity verification and management, leveraging Atala PRISM's infrastructure.

- This initiative aims to enable developers to craft and deploy compliant, reusable digital identities for a variety of real-world applications.

- The Atala PRISM Modular KYC Solution is divided into several modules, each designed to enhance different aspects of identity verification and compliance. The milestones 1-5 build sequentially on each other. Milestone 3 includes everything from previous milestones.

**Table 1: Overview Elements and Functions included in Milestones 1-5 and Partners**

| Overview Elements and Functions included in Milestones 1-5 and Partners | | |
|---|---|---|
| **Milestone** | **Element / Functions** | **Partner** |
| 1 | • Chatbot | IAMX |
| 2 | • ID-Verification Level 3<br>• Liveness & face match<br>• Security features document<br>• Address verification<br>• AML (pep, sanction, crime)<br>• Enhanced due diligence | IDnow<br>Intrum |
| 3 | • KYT, transaction and wallet monitoring | Merkle Science |
| 4 | • creation of did:prism, creation of verifiable credential | IAMX |
| 5 | • Demo with 3 different individuals / nationalities | IAMX |

## 2. Milestone 2 KYT , wallet and transaction monitoring

KYT (Know Your Transaction) is a compliance practice focused on monitoring and analyzing financial transactions to detect and prevent illegal activities like money laundering and fraud. It involves real-time transaction monitoring, risk assessment, and generating alerts for suspicious activities. Advanced KYT systems use technologies such as machine learning and blockchain analytics to identify unusual transaction patterns that traditional methods might miss. This practice helps financial institutions comply with regulatory standards, manage risks, and enhance customer trust by ensuring transaction security and legality. KYT complements Know Your Customer (KYC) procedures, providing a comprehensive approach to financial compliance.

Wallet and transaction monitoring in cryptocurrency involve continuously tracking wallet activities and scrutinizing individual transactions to detect suspicious behaviors, prevent illicit activities, and ensure regulatory compliance based on the wallet address. Wallet monitoring focuses on the frequency, volume, and patterns of transactions associated with a wallet address to identify anomalies. Transaction monitoring scrutinizes each transaction for compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations, assigning risk scores and generating alerts for high-risk activities.

### 2.1 What KYT Includes

#### 2.1.1 Components of KYT

1. Transaction Monitoring: KYT involves real-time monitoring of transactions to detect suspicious activities. This process uses predefined rules and advanced behavioral analytics to identify potential money laundering, fraud, and other illicit activities.
2. Wallet Address Analysis: Each transaction linked to a wallet address is scrutinized. The analysis includes the entire transactional history, identifying patterns, and assessing risk levels based on various factors such as transaction amount, frequency, and counterparties involved.

#### 2.1.2 How KYT is Performed

1. Data Collection: Transaction data is collected from blockchain networks and other relevant sources. This includes details like transaction amounts, timestamps, wallet addresses, and associated metadata.
2. Risk Scoring: Transactions are assigned risk scores based on predefined criteria and behavioral analysis. High-risk transactions are flagged for further investigation.
3. Behavioral Analysis: Advanced algorithms analyze transaction patterns to detect anomalies. This includes examining the flow of funds, identifying links to known illicit activities, and assessing the behavior of wallet addresses over time.
4. Alert Generation: Real-time alerts are generated for transactions that exceed predefined risk thresholds. These alerts are sent to compliance officers for immediate action.

### 2.1.3 Results of KYT

1. Risk Scores: Each transaction and wallet address is assigned a risk score. High-risk scores indicate potential involvement in illicit activities, while low-risk scores suggest normal transactional behavior.
2. Detailed Reports: Comprehensive reports are generated, providing insights into transaction patterns, risk levels, and potential links to illicit activities. These reports include data visualizations such as fund flow charts and behavior analysis summaries.
3. Alerts and Notifications: Compliance officers receive alerts and notifications for high-risk transactions. These alerts help prioritize investigations and prompt immediate responses to potential threats.

### 2.1.4 Actions Based on KYT Results

1. Investigate High-Risk Transactions: Compliance officers investigate high-risk transactions by examining the detailed reports and conducting further analysis. This may involve tracing the flow of funds, identifying counterparties, and verifying transaction legitimacy.
2. Report Suspicious Activities: If a transaction is confirmed to be suspicious, it must be reported to the relevant authorities. This includes filing Suspicious Activity Reports (SARs) with regulatory bodies such as the Financial Crimes Enforcement Network (FinCEN) in the U.S.
3. Adjust Risk Policies: Based on the findings, organizations may adjust their risk policies and monitoring rules to improve the detection of suspicious activities and reduce false positives.

### 2.1.5 Legal Obligations

1. Reporting Requirements: Financial institutions and cryptocurrency businesses are legally obligated to report certain suspicious activities and transactions that exceed specific thresholds. These requirements vary by jurisdiction but generally include filing SARs and other regulatory reports.
2. Compliance with AML and CFT Regulations: Organizations must comply with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations. This includes implementing robust KYT processes and ensuring timely reporting of suspicious transactions to prevent financial crimes.
3. Record-Keeping: Detailed records of transactions, risk assessments, and investigations must be maintained. These records are essential for regulatory audits and demonstrating compliance with legal obligations.

## 2.2 Features of KYT, wallet and transaction monitoring

KYT identifies transactions linked to the wallet address and analyzes the entire transactional history of the address, detecting links to illicit activities and changes in risk level.

**Table 2: Features of KYT in basic and advanced KYT**
Information: The partner Merkle Science uses all advanced features.

| Feature | Basic | Advanced |
|---|---|---|
| Scope and Approach | Monitors transactions using predefined rules | Behavior-based analysis with advanced machine learning for proactive detection of illicit activities |
| Customization and Flexibility | Basic customization based on standard compliance | Extensive customization of risk policies and alerts, tailored to specific needs |
| Real-Time Monitoring and Alerts | Provides real-time monitoring and alerts | Continuous monitoring and re-screening of addresses for real-time detection and response |
| Reporting and Case Management | Basic reporting features | Robust case management, automated report generation, and detailed audit trails |
| Multi-Chain Support | Generally limited to specific blockchains | Supports multiple blockchains, enhancing versatility across different crypto ecosystems |
| Advanced Alerts and Notifications | Standard alerts based on risk thresholds | Real-time alerts using comprehensive analysis with source of funds and behavior-based rules |
| Integration and Compatibility | Limited integration capabilities | Seamless integration into various crypto ecosystems, supporting multiple blockchains |
| Regulatory Compliance | Ensures compliance with basic regulations | Provides tools for compliance with AML, KYC, and CFT regulations using behavior-based monitoring and risk reporting |

### 2.3 KYT Partner

IAMX uses the services of Merkle Science for this proposal for wallet and transaction monitoring.

Merkle Science is a leading provider of predictive blockchain monitoring and investigative solutions, enhancing compliance, risk management, and operational security in the cryptocurrency space. Their platform employs advanced machine learning and behavior-based rule engines for real-time monitoring and alerts. Customizable risk policies and alerts ensure the platform meets specific regulatory requirements and operational needs.

Supporting multiple blockchains, including Cardano, the platform offers comprehensive monitoring across various crypto ecosystems. Robust case management tools and automated report generation streamline compliance processes and provide detailed documentation for regulatory reporting. Seamless integration with existing systems enhances operational efficiency.

Merkle Science's proven track record includes partnerships with major industry players and regulatory bodies, showcasing their reliability and effectiveness. Customers benefit from continuous innovation, regular updates, and educational resources, helping build internal expertise in detecting and preventing crypto crimes. Trusted globally, Merkle Science equips clients with the latest tools and techniques to combat illicit activities, ensuring secure and compliant operations in the cryptocurrency ecosystem.

### 2.4 Goals and Intentions of KYT

1. Enhancing Security and Fraud Prevention
Detection of Suspicious Activities: KYT aims to identify and prevent fraudulent activities, such as money laundering and terrorist financing, by monitoring transaction patterns and behaviors. This helps in detecting unusual activities that deviate from normal transaction patterns.
Proactive Risk Management: By continuously monitoring transactions, KYT systems can proactively identify potential threats and take necessary actions to mitigate risks before they escalate.

2. Ensuring Regulatory Compliance
Adherence to Legal Standards: KYT helps organizations comply with local and international regulatory requirements, such as Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) regulations. This is crucial for avoiding legal penalties and maintaining the integrity of financial operations.
Timely Reporting: KYT facilitates the timely reporting of suspicious activities to regulatory authorities, ensuring that organizations fulfill their legal obligations to report certain transactions that exceed specified thresholds or appear suspicious.

3. Improving Transparency and Accountability
Detailed Transaction Analysis: KYT provides a comprehensive analysis of transactions, offering detailed insights into the flow of funds and the relationships between different entities involved in transactions.
Audit Trails: By maintaining detailed records of all transactions and associated risk assessments, KYT ensures that there is a clear audit trail. This is essential for internal reviews and external audits to verify compliance and investigate any anomalies.

4. Enhancing Customer Trust
Secure Transactions: By ensuring that all transactions are monitored and compliant with regulatory standards, KYT helps build trust with customers. They can be assured that their financial activities are secure and protected from fraudulent practices.
Customer Protection: KYT systems help in identifying and preventing activities that could harm customers, such as fraud and scams, thereby protecting customer assets and maintaining their trust in the financial institution.

5. Facilitating Business Growth and Expansion:
Reputation Management: By maintaining robust KYT processes, businesses can enhance their reputation for security and compliance. This is particularly important for attracting and retaining customers and partners who prioritize security and compliance.
Market Expansion: Effective KYT practices enable businesses to operate confidently in different markets, knowing they can comply with varying regulatory requirements across jurisdictions.

### 2.4 Main Legal Sources

The legal framework for KYT is defined by various international and national regulations:

**Table 3: Legal Sources for KYT per jurisdiction**

| Jurisdiction | Legal Sources for KYT | What Needs to be Checked | Incidents/Thresholds Causing KYT in Crypto |
|---|---|---|---|
| World | • Financial Action Task Force (FATF) Recommendations: FATF | • Transaction patterns<br>• Source of funds<br>• High-risk countries | • Transactions over $10,000<br>• Unusual transaction patterns |
| USA | • Bank Secrecy Act (BSA)<br>• USA PATRIOT Act<br>• Financial Crimes Enforcement Network (FinCEN) regulations: FinCEN | • - Large cash transactions<br>• Wire transfers<br>• Customer profiles | • Transactions over $10,000<br>• Suspicious activity reports (SARs) |
| EU | • -5th Anti-Money Laundering Directive (5AMLD)<br>• 6th Anti-Money Laundering Directive (6AMLD): European Commission | • Customer due diligence<br>• Beneficial ownership<br>• Transaction monitoring | • Transactions over €1,000<br>• High-risk customer activities |

| | | | |
|---|---|---|---|
| Japan | • Act on Prevention of Transfer of Criminal Proceeds<br>• Financial Services Agency (FSA) regulations: FSA | • - Customer identification - Transaction history - Suspicious transactions | • - Transactions over ¥1,000,000 - Unusual transaction patterns |
| Asia | • Monetary Authority of Singapore (MAS) regulations<br>• Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regulations: MAS | • - Customer profiles - Source of funds - Transaction patterns | • - Transactions over SGD 20,000 - Suspicious transaction reports |
| Switzerland | • - Anti-Money Laundering Act (AMLA)<br>• Swiss Financial Market Supervisory Authority (FINMA) regulations: FINMA | • - Customer identification - Transaction history - Beneficial ownership | • - Transactions over CHF 10,000 - Suspicious transaction patterns |
| Germany | • German Money Laundering Act (Geldwäschegesetz, GwG)<br>• Federal Financial Supervisory Authority (BaFin) regulations: BaFin | • - Customer due diligence - Source of funds - Transaction monitoring | • - Transactions over €1,000<br>• Unusual transaction patterns |

## 3. Cryptocurrency transaction monitoring, wallet monitoring

Transaction and wallet monitoring are performed via REST API of Merkle Science.

**Table 4: Key functions of the REST API**

<table>
<tr><td>REST API</td><td>Merkle Science's Compass is an enterprise-grade, real-time cryptocurrency transaction monitoring, wallet monitoring, and customer-level monitoring tool.</td></tr>
<tr><td>API Overview</td><td>The REST APIs enable real-time queries to a risk decision engine, providing risk scores for various resources.
<table>
<tr><th>Resource</th><th>Identifier</th></tr>
<tr><td>Transaction</td><td>Transaction Hash</td></tr>
<tr><td>Address</td><td>Address</td></tr>
<tr><td>Deposits & Withdrawals</td><td>Customer Id, Address, Transaction Hash</td></tr>
</table></td></tr>
<tr><td>Authentication</td><td>The Compass API uses API keys for authentication, included in all requests via the X-API-KEY header.</td></tr>
<tr><td>HTTPS Requirement</td><td>All API requests must be made over HTTPS. HTTP requests will fail, as will unauthenticated requests.</td></tr>
<tr><td>Rate Limits</td><td>100 calls per minute, 1000 calls per hour, 10,000 calls per day.</td></tr>
<tr><td>Full coverage blockchains</td><td>
<table>
<tr><th>Blockchain</th><th>Code</th></tr>
<tr><td>Bitcoin</td><td>0</td></tr>
<tr><td>Ethereum</td><td>1</td></tr>
<tr><td>Litecoin</td><td>2</td></tr>
<tr><td>Bitcoin Cash</td><td>3</td></tr>
<tr><td>Ripple</td><td>4</td></tr>
<tr><td>Dogecoin</td><td>6</td></tr>
<tr><td>Zilliqa</td><td>7</td></tr>
<tr><td>Binance Smart Chain</td><td>8</td></tr>
<tr><td>Polygon</td><td>9</td></tr>
<tr><td>Tron</td><td>10</td></tr>
<tr><td>Cardano</td><td>11</td></tr>
<tr><td>Polkadot</td><td>12</td></tr>
<tr><td>Stellar</td><td>13</td></tr>
<tr><td>Hedera</td><td>14</td></tr>
<tr><td>Cronos</td><td>15</td></tr>
<tr><td>Optimism</td><td>16</td></tr>
<tr><td>Arbitrum</td><td>17</td></tr>
<tr><td>Solana</td><td>24</td></tr>
<tr><td>Avalanche C-Chain</td><td>25</td></tr>
</table></td></tr>
</table>

Risk Levels

| Risk Level | Description |
|---|---|
| 0 | No Risk Detected |
| 1 | Info |
| 2 | Caution |
| 3 | Medium |
| 4 | High |
| 5 | Critical |

Integration Overview

Monitor the following events / make API calls:
a. Deposit Confirmation: Cryptocurrency received and confirmed.
b. Withdrawal Request: User-initiated withdrawal, pending blockchain submission.
c. Withdrawal Confirmation: Approved withdrawal confirmed on blockchain.
d. Customer Signup: New user registration and deposit address creation.

Data Model

| Event | API | Basic Model Params | Advanced Model Params |
|---|---|---|---|
| Deposit Confirmation | Transaction Screening | a.Transaction Hash<br>b. Blockchain Code | a. Transaction Hash<br>b. Blockchain Code<br>c. Beneficiary address<br>d. Customer ID |
| Withdrawal Request | Address Screening | a. Beneficiary address<br>b. Blockchain Code | a. Beneficiary address<br>b. Blockchain Code<br>- Customer ID |
| Withdrawal Confirmation | Transaction Screening | - Transaction Hash - Blockchain Code | - Transaction Hash<br>- Blockchain Code - Beneficiary address - Customer ID |
| Customer Signup | Customer Screening | Not Applicable | - Customer ID |

### 3.1 How it works

#### 3.1.1 Match with aggregated wallet addresses and transactions, that have been associated with certain services

Most digital assets pass through various services, including both legal businesses like retail exchanges and illegal ones like darknet marketplaces. Merkle Science aggregates wallet addresses and transactions to detect and analyze the risk associated with a service. These addresses and transactions are assigned to specific entities and organizations, such as a particular exchange, mixing service, or darknet market. Once the entity is identified, it is grouped into Entity Categories based on the type of real-world service it represents. The different Entity Categories are each assigned a rating of Critical, HIGH, MEDIUM, or Caution. A service's rating is determined by its potential for criminal activity. Hosted wallets and merchant services are less commonly used for illegal activities, so they receive a Caution risk rating. Terrorist financing and sanctions, however, are illegal under all circumstances and therefore receive a Critical risk rating. Services with MEDIUM or HIGH ratings fall somewhere in between.

#### 3.1.2 Flagged services / categories

Abuse, certain marketplaces, compromised credit cards, darknet with human trafficking, Coin Mixer, narcotics, sanctions, scam, stolen accounts, weapons, ...

**Table 5: Risk policy to identify risk level**

| Category | Description |
|---|---|
| Risk Policy | A collection of rules developed to identify the Risk Level of the Transaction/Address/Customer. Each rule has an associated risk level, following in the decreasing order of severity: CRITICAL, HIGH, MEDIUM, CAUTION, or INFO. The overall risk level of an entity is determined by the most severe rule flagged. |
| Risk Levels | CRITICAL, HIGH, MEDIUM, CAUTION, INFO |
| Types of Risk Policies | 1. Address - Source of Funds<br>2. Transactions - Source of Funds<br>3. Address - Behaviour |
| Source of Funds Risk Policy | Refers to the source of the specific cash or assets involved in the contract between the business and the client, as well as the transactions the firm is expected to carry out on the client's behalf. It involves tracking and monitoring addresses and transactions to identify the origin and conditions of the funds. Analytics should cover more than just the bank or financial institution involved. Learn more about source of funds rule condition here. |
| Behavioural Risk Policy | Merkle Science's Behavioural Rule Engine allows users to create bespoke warnings for various suspicious transaction behaviours. Users can combine several suspicious behaviours to detect complex money laundering schemes, starting with basic rule templates. The engine tracks various behaviours, such as concentration of payments into a single user's accounts, use of transit addresses to conceal provenance, and splitting transactions to avoid reporting thresholds. |

### 3.1.3 Rules

A predefined set of rules that covers a range from Risk Level: CRITICAL to Risk Level: INFO has been applied to this solution. Please note: These preloaded rules are based on Merkle Science's expertise. Rules can be reviewed and edited to reflect specific risk considerations. Based on those rules you can configure auto-assignment to stages based on object's (address, transaction or customer) risk level to enable a rules-based assignment workflow.

**Table 6: Rules and description example**

| rule_name | rule_type | description |
|---|---|---|
| Sanctions | Address | If this address has directly received payments from any of the actors with type in Sanctions for at least US$0 and at most any USD amount and has at least 0% taint |
| Sanctions | Address | If this address has directly sent payments to any of the actors with type in Sanctions for at least US$0 and at most any USD amount and has at least 0% taint |
| Sanctions | Sanctions | If this address is owned by any actor of type in Sanctions |
| Coin Mixer | Address | If this address has directly received payments from any of the actors with type in Coin Mixer for at least US$0 and at most any USD amount and has at least 0% taint |
| Darknet | Address | If this address has directly received payments from any of the actors with type in Darknet for at least US$0 and at most any USD amount and has at least 0% taint |

### 3.1.4 Counterparty Analysis

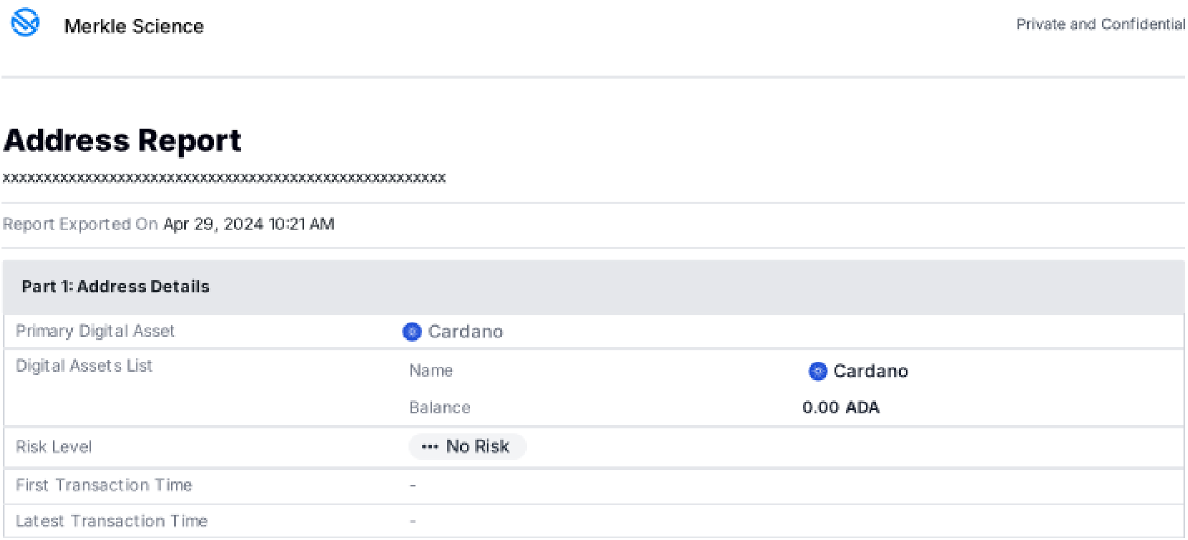
Understanding normal and illicit activities hinges significantly on exposure. In Compass, exposure refers to the relationships formed between entities and wallets through transactions. How Compass Determines Exposure: An entity is a business that manages funds for multiple individuals, such as an exchange, a merchant services provider, or a darknet market. These entities are often linked to numerous addresses within their services. Within this framework, an identified cluster consists of addresses that Compass has recognized as being controlled by a single entity. Unidentified clusters, or unidentified entities, are groups of addresses that Compass has not yet linked to a specific entity.

Merkle Science monitors the movement of funds between clusters and other entities or identified clusters to assess exposure. Compass tracks funds until one of the following events occurs:
1. Funds are transferred to a group of addresses identified by Compass as belonging to a specific entity or organization (a specified cluster).
2. Payments are sent to an unidentified cluster, which Compass assumes to be an entity. Due to the high likelihood of entities mixing consumer funds, tracking stops in this scenario.

### 3.1.5 Full Coverage vs Sanctions Screening

Full Coverage: Entities (addresses or transactions) monitored on full coverage blockchains, or tokens on those chains, are screened for all entity types and subtypes. This includes sanctions, high-risk entities, exchanges, and more. Full coverage also involves a counterparty analysis of the entity being screened. Sanctions Screening Only: Entities monitored on blockchains designated for sanctions screening only (also known as 'lite coverage') are screened exclusively for sanctions-related activities. There is no counterparty analysis, transaction investigation graph, or other types of attribution available. Sanctions Screening provides essential sanctions-related information about addresses, allowing compliance teams to expand their screening scope beyond full coverage chains.

## 3.2 Result example address report with risk level no risk



Merkle Science

Private and Confidential

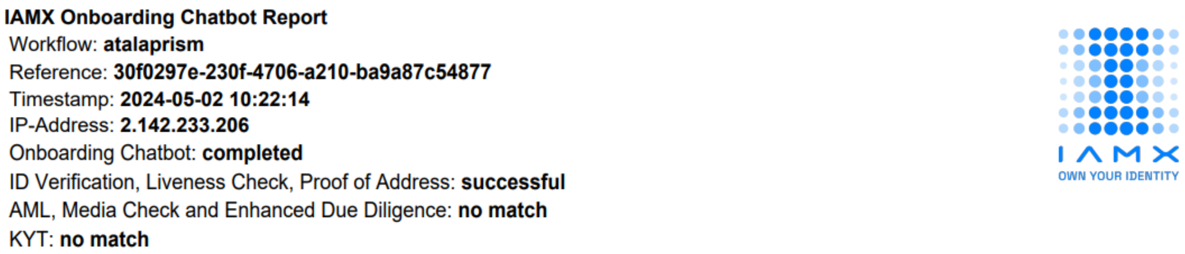
**Address Report**

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Report Exported On Apr 29, 2024 10:21 AM

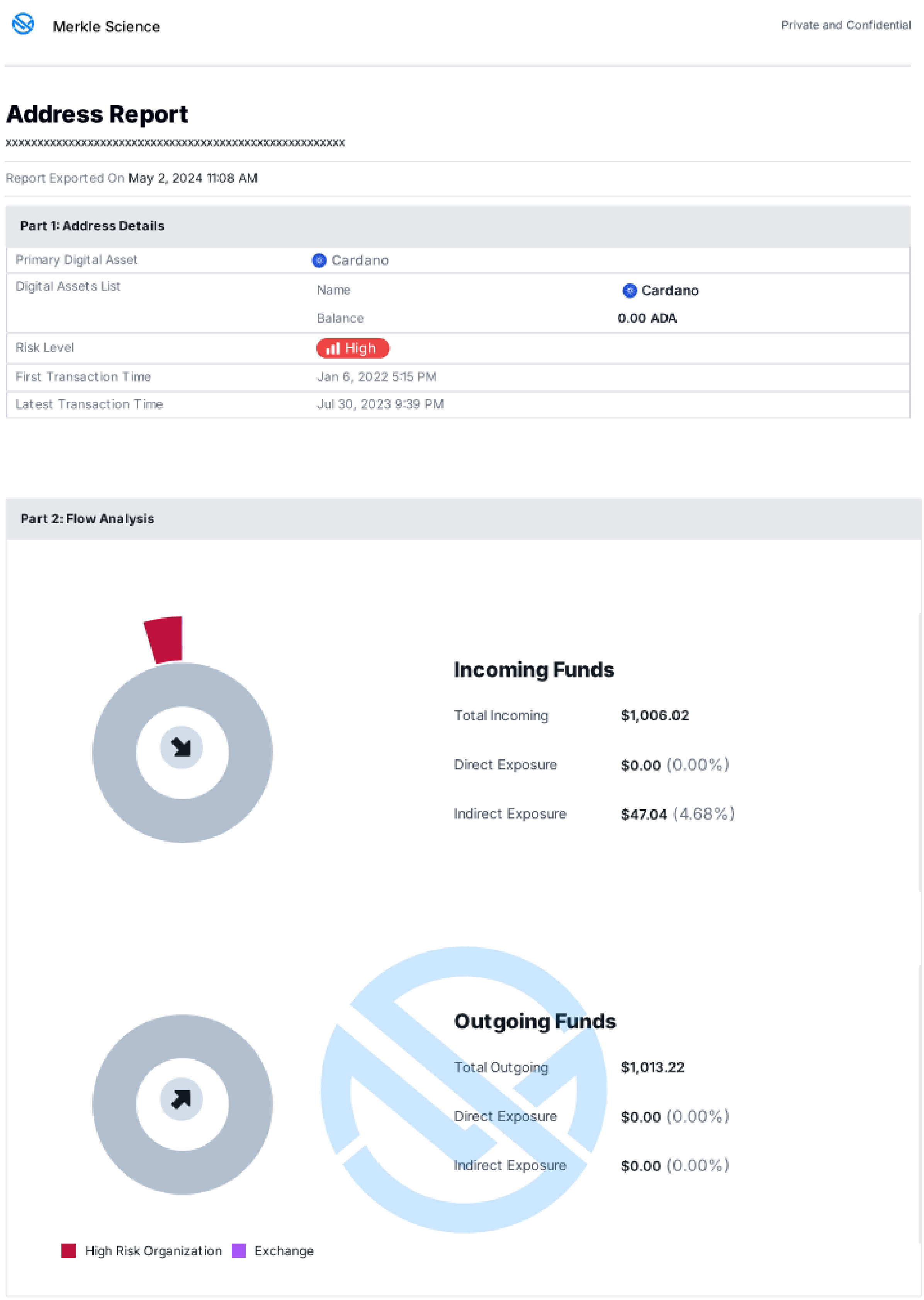
| Part 1: Address Details | | |
|---|---|---|
| Primary Digital Asset | Cardano | |
| Digital Assets List | Name | Cardano |
| | Balance | 0.00 ADA |
| Risk Level | ••• No Risk | |
| First Transaction Time | - | |
| Latest Transaction Time | - | |

## 3.3 Result example KYT no match



**IAMX Onboarding Chatbot Report**
Workflow: **atalaprism**
Reference: **30f0297e-230f-4706-a210-ba9a87c54877**
Timestamp: **2024-05-02 10:22:14**
IP-Address: **2.142.233.206**
Onboarding Chatbot: **completed**
ID Verification, Liveness Check, Proof of Address: **successful**
AML, Media Check and Enhanced Due Diligence: **no match**
KYT: **no match**

## 3.4 Result example risk level high



Merkle Science

Private and Confidential

# Address Report

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Report Exported On May 2, 2024 11:08 AM

| Part 1: Address Details | | |
|---|---|---|
| Primary Digital Asset | Cardano | |
| Digital Assets List | Name | Cardano |
| | Balance | 0.00 ADA |
| Risk Level | High | |
| First Transaction Time | Jan 6, 2022 5:15 PM | |
| Latest Transaction Time | Jul 30, 2023 9:39 PM | |

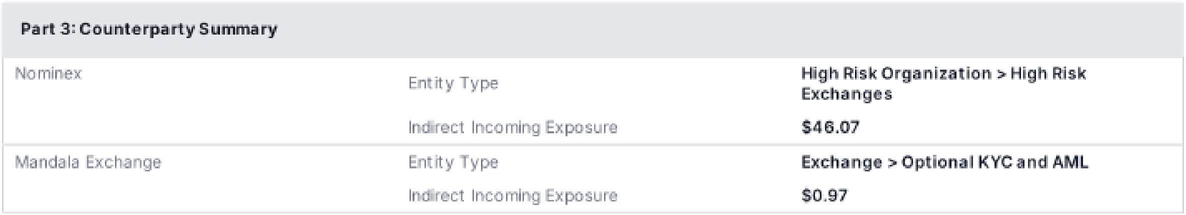
**Part 2: Flow Analysis**

### Incoming Funds

| | |
|---|---|
| Total Incoming | $1,006.02 |
| Direct Exposure | $0.00 (0.00%) |
| Indirect Exposure | $47.04 (4.68%) |

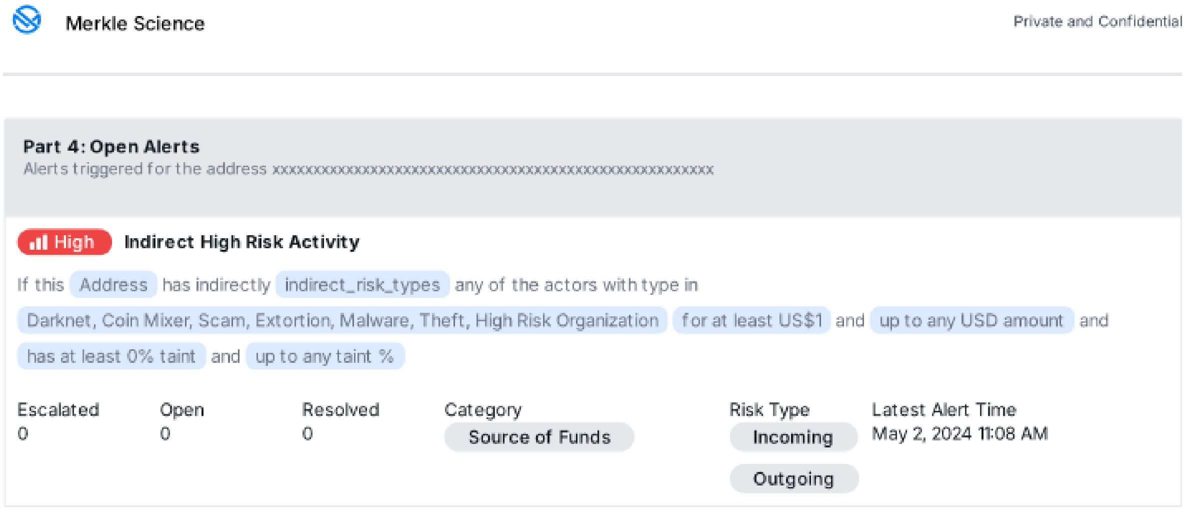
### Outgoing Funds

| | |
|---|---|
| Total Outgoing | $1,013.22 |
| Direct Exposure | $0.00 (0.00%) |
| Indirect Exposure | $0.00 (0.00%) |



**Part 3: Counterparty Summary**

| | | |
|---|---|---|
| Nominex | Entity Type | High Risk Organization > High Risk Exchanges |
| | Indirect Incoming Exposure | $46.07 |
| Mandala Exchange | Entity Type | Exchange > Optional KYC and AML |
| | Indirect Incoming Exposure | $0.97 |



Merkle Science

Private and Confidential

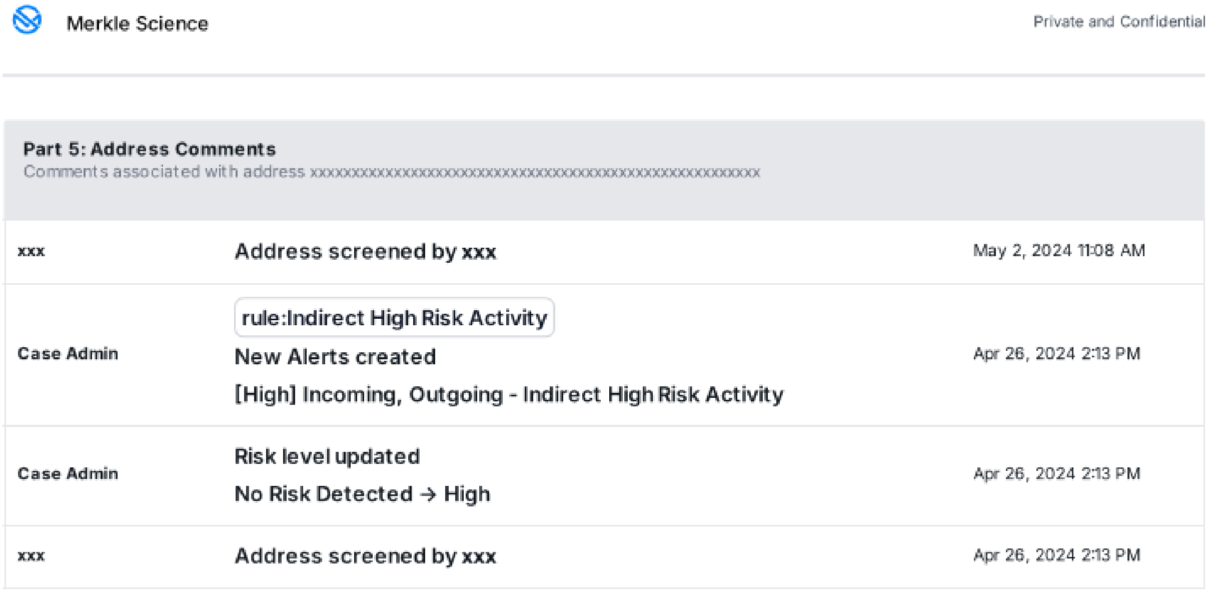
**Part 4: Open Alerts**

Alerts triggered for the address xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

High **Indirect High Risk Activity**

If this Address has indirectly indirect_risk_types any of the actors with type in Darknet, Coin Mixer, Scam, Extortion, Malware, Theft, High Risk Organization for at least US$1 and up to any USD amount and has at least 0% taint and up to any taint %

| Escalated | Open | Resolved | Category | Risk Type | Latest Alert Time |
|---|---|---|---|---|---|
| 0 | 0 | 0 | Source of Funds | Incoming<br>Outgoing | May 2, 2024 11:08 AM |



Merkle Science

Private and Confidential

**Part 5: Address Comments**

Comments associated with address xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

| | | |
|---|---|---|
| xxx | Address screened by xxx | May 2, 2024 11:08 AM |
| Case Admin | rule:Indirect High Risk Activity<br>New Alerts created<br>[High] Incoming, Outgoing - Indirect High Risk Activity | Apr 26, 2024 2:13 PM |
| Case Admin | Risk level updated<br>No Risk Detected → High | Apr 26, 2024 2:13 PM |
| xxx | Address screened by xxx | Apr 26, 2024 2:13 PM |

### 3.5 Risk Classifiers: List of risks which have been checked for

Please see annex on next pages.

# Appendix A

Risk Classifiers: An list of risks which have been checked for.

## List of Rules

The list of rules which have been run against this address

Info **Exchange**

If this Address has directly received payments from any of the actors with type in Exchange for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Exchange**

If this Address has directly sent payments to any of the actors with type in Exchange for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Exchange**

If this Address is owned by any actor of type in Exchange

Info **Mining Pool**

If this Address has directly received payments from any of the actors with type in Mining Pool for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Mining Pool**

If this Address has directly sent payments to any of the actors with type in Mining Pool for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Mining Pool**

If this Address is owned by any actor of type in Mining Pool

Info **Service**

If this Address has directly received payments from any of the actors with type in Service for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Service**

If this Address has directly sent payments to any of the actors with type in Service for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Service**

If this Address is owned by any actor of type in Service

High **Darknet**

If this Address has directly received payments from any of the actors with type in Darknet for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Darknet**

If this Address has directly sent payments to any of the actors with type in Darknet for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Darknet**

If this Address is owned by any actor of type in Darknet

Medium **Gambling**

If this Address has directly received payments from any of the actors with type in Gambling for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Medium **Gambling**

If this Address has directly sent payments to any of the actors with type in Gambling for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Medium **Gambling**

If this Address is owned by any actor of type in Gambling

High **Coin Mixer**

If this Address has directly received payments from any of the actors with type in Coin Mixer for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Coin Mixer**

If this Address has directly sent payments to any of the actors with type in Coin Mixer for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Coin Mixer**

If this Address is owned by any actor of type in Coin Mixer

High **Scam**

If this Address has directly received payments from any of the actors with type in Scam for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Scam**

If this Address has directly sent payments to any of the actors with type in Scam for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Scam**

If this Address is owned by any actor of type in Scam

High **Extortion**

If this Address has directly received payments from any of the actors with type in Extortion for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Extortion**

If this Address has directly sent payments to any of the actors with type in Extortion for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Extortion**

If this Address is owned by any actor of type in Extortion

High **Malware**

If this Address has directly received payments from any of the actors with type in Malware for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Malware**

If this Address has directly sent payments to any of the actors with type in Malware for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Malware**

If this Address is owned by any actor of type in Malware

High **Theft**

If this Address has directly received payments from any of the actors with type in Theft for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Theft**

If this Address has directly sent payments to any of the actors with type in Theft for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

High **Theft**

If this Address is owned by any actor of type in Theft

Info **Donation**

If this Address has directly received payments from any of the actors with type in Donation for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Donation**

If this Address has directly sent payments to any of the actors with type in Donation for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

Info **Donation**

If this Address is owned by any actor of type in Donation

Info **Smart Contract Platform**

If this Address has directly received payments from any of the actors with type in Smart Contract Platform for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### ⓘ Info **Smart Contract Platform**

If this Address has directly sent payments to any of the actors with type in Smart Contract Platform for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### ⓘ Info **Smart Contract Platform**

If this Address is owned by any actor of type in Smart Contract Platform

### ⚠ Critical **Sanctions**

If this Address has directly received payments from any of the actors with type in Sanctions for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### ⚠ Critical **Sanctions**

If this Address has directly sent payments to any of the actors with type in Sanctions for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### ⚠ Critical **Sanctions**

If this Address is owned by any actor of type in Sanctions

### High **High Risk Organization**

If this Address has directly received payments from any of the actors with type in High Risk Organization for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### High **High Risk Organization**

If this Address has directly sent payments to any of the actors with type in High Risk Organization for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### High **High Risk Organization**

If this Address is owned by any actor of type in High Risk Organization

### ⓘ Info **Law Enforcement**

If this Address has directly received payments from any of the actors with type in Law Enforcement for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### ⓘ Info **Law Enforcement**

If this Address has directly sent payments to any of the actors with type in Law Enforcement for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### ⓘ Info **Law Enforcement**

If this Address is owned by any actor of type in Law Enforcement

### ⓘ Info **DeFi**

If this Address has directly received payments from any of the actors with type in DeFi for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### Info DeFi

If this Address has directly sent payments to any of the actors with type in DeFi for at least any USD amount and up to any USD amount and has at least 0% taint and up to any taint %

### Info DeFi

If this Address is owned by any actor of type in DeFi

### Medium Indirect Medium Risk Activity

If this Address has indirectly indirect_risk_types any of the actors with type in Gambling for at least US$1 and up to any USD amount and has at least 0% taint and up to any taint %

### High Indirect High Risk Activity

If this Address has indirectly indirect_risk_types any of the actors with type in Darknet, Coin Mixer, Scam, Extortion, Malware, Theft, High Risk Organization for at least US$1 and up to any USD amount and has at least 0% taint and up to any taint %

### Critical Indirect Sanctions

If this Address has indirectly indirect_risk_types any of the actors with type in Sanctions for at least US$1 and up to any USD amount and has at least 0% taint and up to any taint %

### Info Indirect from Businesses

If this Address has indirectly indirect_risk_types any of the actors with type in Exchange, Service, Mining Pool for at least US$1 and up to any USD amount and has at least 0% taint and up to any taint %

### Caution Anomaly Detection

If this Address has risk_types_1 in previous 30 days for at least 5 times the usual US$ amount it normally does over a 30 days period

### Caution Transit Address Detection

If this Address has received a payment in the previous 300 minutes but has withdrawn at least 50% since then

### Caution Dormant Address Reactivation

If this Address has risk_types_1 after not having sent payments to or received payments from for previous 90 days

### Caution Large Transaction

If this Address has risk_types_1 of at least US$ 10000.0000% in a single transaction

### Caution Young Address as Counterparties

If this Address has sent payments to or received payments from an address created in the 7 days

### Caution High Transaction Fee

If this Address has risk_types_1 in a transaction which paid an abnormally large transaction fee

### Caution Range-bound Transaction amount

If this Address has risk_types_1 with transaction amounts between US$ 700 and US$ 900

Caution **High Transaction Count**

If this Address has risk_types_1 more than 10 times in the previous analysis_window_2