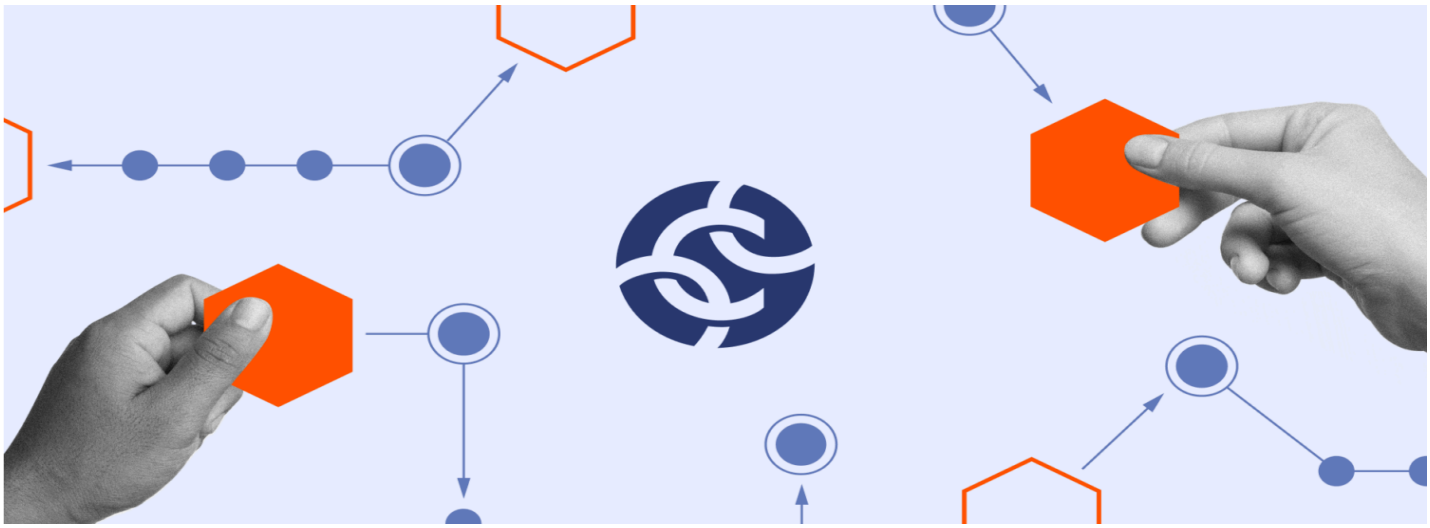
Chainalysis 暗号捜査ソリューションがリード発見から不正押収までのケースをどのようにサポートするか

AUGUST 13, 2024 | BY CHAINALYSIS TEAM



シェア

ちょうど10年以上前、暗号通貨とブロックチェーンを取り巻く新たな技術を理解している人はほとんどおらず、ブロックチェーンのデータを評価し、暗号犯罪に関連する資金を追跡する方法を知っている捜査官はさらに少なかった。 それ以来、犯罪者がブロックチェーン技術を悪意のある目的に活用する新しい方法を発見し、暗号の状況は広範囲に進化している。 2023年だけで、不正な暗号アドレスは少なくとも242億ドルを受け取っています。

ブロックチェーンの透明性により、政府機関や法執行機関は不換紙幣よりも簡単に犯罪行為を追跡・追跡することができる。 世界中で暗号の導入が進む中、アナリストや捜査官が包括的なブロックチェーンデータをリード生成に活用し、暗号捜査を実施し、その洞察を運用化して違法なオンチェーン活動を破壊することが非常に重要です。

犯罪の手口が複雑化するにつれて、Chainalysisはエンドツーエンドの調査用ブロックチェーン分析サービスに磨きをかけ続けています。 当社のChainalysis Crypto Investigations Solution は、不正な暗号活動の初期報告のトリアージから調査、資産の押収まで、すべてをサポートしています。 この投稿では、ロマンス詐欺のケースを通して、当社の最新のイノベーションを紹介します。

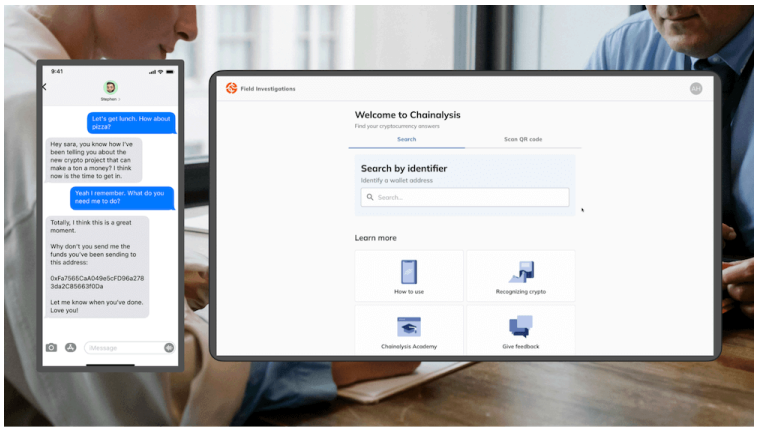
貴重なリードを発見し、説得力のあるケースを構築する

2023年、ロマンス詐欺の収益は2倍以上に増加し、被害者に経済的にも精神的にも壊滅的な影響を与えることが浮き彫りになりました。 被害者を「太らせて」可能な限りの価値を引き出すという悪質業者のやり方から、「豚の屠殺詐欺」としても知られており、詐欺師は最終的に被害者を説得して偽の投資機会にお金を投資させるまで、被害者との関係を深めていきます。

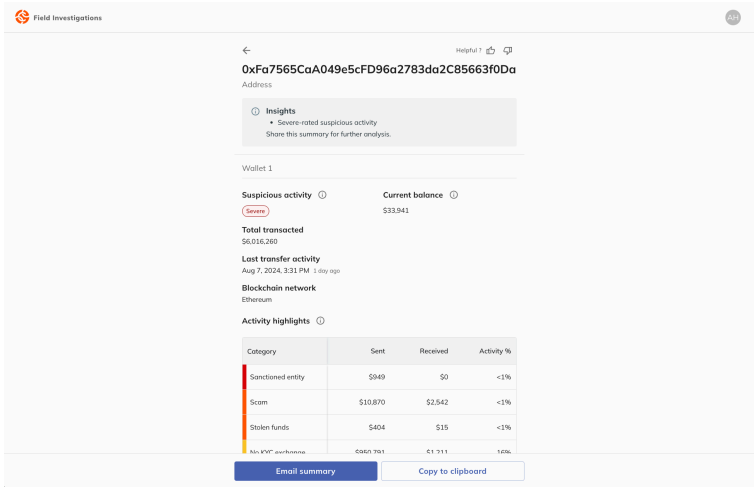
発見段階から、法執行機関がChainalysisを活用して暗号関連のロマンス詐欺を徹底的に調査する方法について、仮定のケーススタディを紹介します。

迅速な検索： 暗号に関する重要な洞察を評価し、エスカレーションする

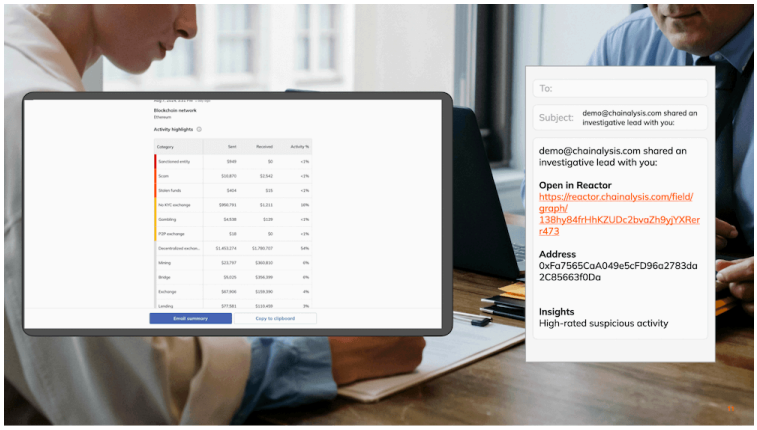
ある警官が、ロマンス詐欺師に数千ドルの暗号を奪われたと語る被害者にインタビューします。 被害者のアカウントを収集した後、警官は被害者が資金を送金したクリプトアドレスを収集し、Rapid Lookup、モバイルフレンドリーなウェブアプリを使用して、迅速な評価を行い、この情報を検証します。



暗号アドレスを入力すると、Rapid Lookupは関連するオンチェーン活動に関する洞察を明らかにします。 ここでは、アドレスは「詐欺」に分類され、被害者の話を裏付けています。



検索結果はまた、ダークネット市場や盗難資金などとのやり取りによって、このアドレスで取引された総額とその疑わしい活動レベルを明らかにします。 Rapid Lookupは、業界をリードするブロックチェーンインテリジェンス 実世界のエンティティをオンチェーンアクティビティに接続し、ウォレットの背後にあるエンティティやサービスについてより明確な理解を提供します。



ウォレットのアクティビティをさらに詳しく調べると、役員は制裁を受けたエンティティから資金を受け取り、暗号取引所で残高のほとんどをオフランピングした可能性が高いことがわかりました。 この担当者は、これらの発見を電子メールのサマリーで内部調査官にエスカレーションし、さらに調査を行います。

暗号活動を分析し、全体像を把握する

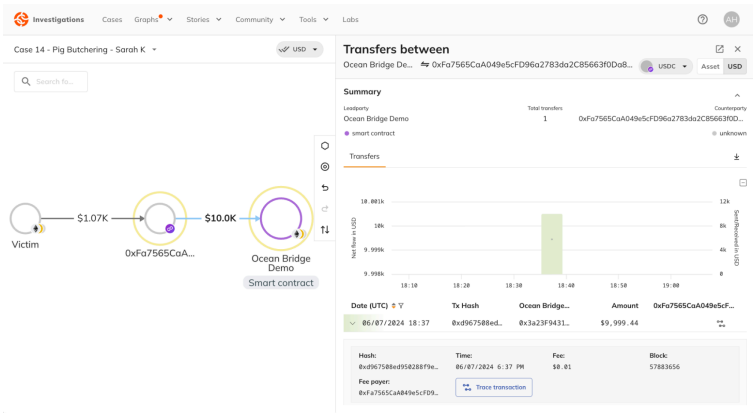
最初の情報をトリアージした後、調査員はトランザクションを分析します; 犯罪者が活動を不明瞭にするために使用する洗練された方法を考えると、これは複雑なプロセスになる可能性があります。

このケースでは、捜査官は容疑者がSocket.techと呼ばれるブリッジングインフラストラクチャの一部に暗号を送信したことを発見した。 ブリッジはスマートコントラクトを介して実行されるプロトコルであり、暗号をあるブロックチェーンから別のブロックチェーンに移動させるのに役立ち、今回のケースでは資金の難読化に使用された。

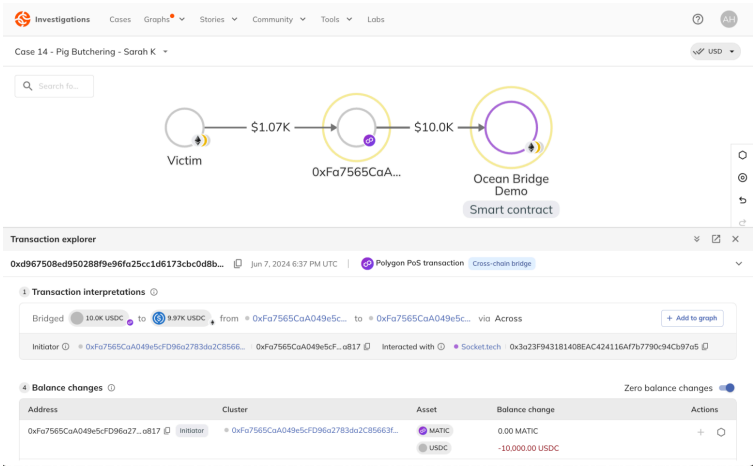
ブリッジを含む調査は、1つのステップに複数の転送が含まれるため、複雑になる可能性があります。

トランザクション・エクスプローラー： あらゆる取引を瞬時に把握

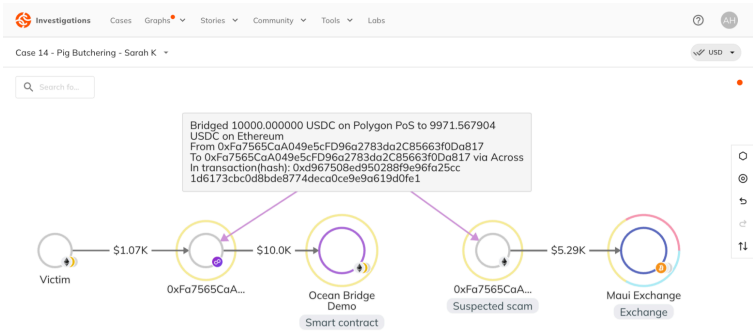
新しく発表されたトランザクション・エクスプローラーは、複雑なトランザクションを簡素化し、直感的な解釈とクロスチェーン・ブリッジ・アクティビティを自動的にトレースする機能を提供します。 Transposeのインデックス付きブロックチェーンデータを活用して、Transaction Explorerは、分散型取引所だけでなく、何百ものユニークなブリッジプロトコルにまたがる1億8000万以上のブリッジトランザクションのオンチェーンデータを解釈します。



捜査官は、容疑者からPolygonネットワーク上のSocket.techに1万ドルの送金が行われたことを確認します。 Transaction Explorer は、ブリッジを経由した資金を自動的に追跡し、関連するすべての情報を 1 か所で表示します。



トランザクションエクスプローラーは、詐欺師と思われる人物がAcrossプロトコルを使用してPolygonからイーサリアムに10KドルのUSDコイン（USDC）をブリッジした方法の概要を表示します。



調査担当者は送信先ウォレットをグラフに追加し、ブリッジされたトランザクションの詳細とトランザクションIDを含む注釈を自動的に生成します。 資金の追跡を続けると、調査員はウォレットがUSDCで5.29Kドルを Maui Exchangeに送ったことを発見します。

トランザクション・エクスプローラーがどのようにトランザクションを明確化するか、さらに深く掘り下げてみましょう、 今度のウェビナーに参加してください。

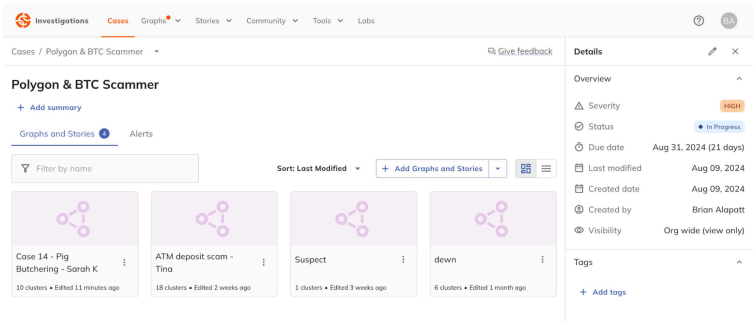
シグナル 捜査を支援する疑わしい分類的洞察

調査員が資金を追跡していると、未知のオンチェーン エンティティに遭遇することがよくあります。 シグナルは疑わしいカテゴリーラベルとして表示されます。

Signalsは、アクティビティに基づいてこれらのエンティティに関する予備的な洞察を表示し、リードの生成、問い合わせのサポート、および仮説の検証に役立つエンティティ インテリジェンスの新しいレイヤーを提供します。 現在、Signals には 110 万以上のクラスターに関する洞察が含まれており、定期的に追加されます。

ケース・ワークスペース チームコラボレーションを強化

複数の事件のデジタル証拠を整理することは、特に部署を越えて共同作業する場合、困難な場合があります。 ケース ワークスペースにより、捜査チームはケースを整理、共有、および共同作業することができます。 チームは、グラフ、ストーリー、アラートなどのデータや成果物を共有し、ケース名、重大度レベル、ステータス、期日、タグを割り当てて、取り組みを文書化し、優先順位を付けることができます。



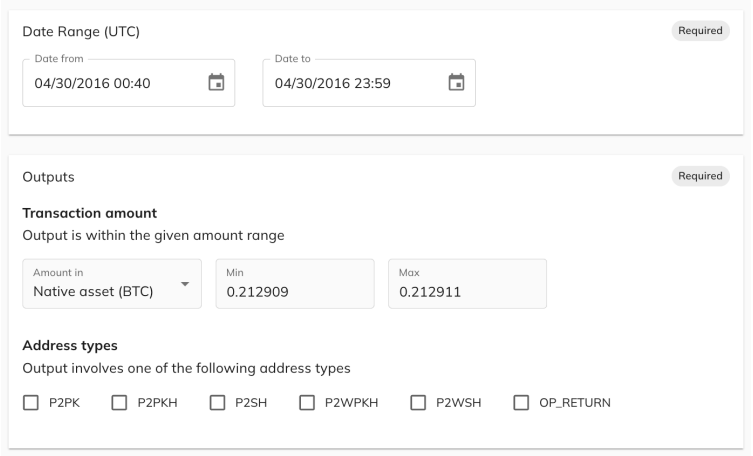
Chainalysis Labsで最も複雑な課題を解決

犯罪者がその手法を適応させ続ける中、一歩先を行くには絶え間ないイノベーションが必要です。 Chainalysis Labsは、ブロックチェーンインテリジェンスにおける最新のイノベーションのR&Dハブとして機能します。 実験的な環境から、Labsは対象となる顧客に、市場に出る前に最先端の機能のいくつかをプレビューし、テストする機会を提供します。

最新のラボの機能が、より複雑な調査上の課題を解決し、事件を解決に導く方法を探ってみましょう。

ビットコイン取引検索： 時間、日付、金額に基づいて特定の取引を検索する

ミキサーやタンブラーは資金の流れを難読化し、捜査の行き詰まりにつながります。 ビットコイン取引検索は、時間、日付、金額、および取引フィンガープリントを含む、45 以上の関連する検索パラメータを使用して特定の取引をフィルタリングおよび検索することにより、捜査官がこれらの課題を克服するのを支援します。



この機能は、利用可能な情報に基づいて特定の取引出力を特定する必要がある手動による混合除去ワークフローで特に役立ちます。 たとえば、調査員は不正な送金の詳細と一致するトランザクションを正確に特定できるため、複雑なマネーロンダリング手法による資金の流れを追跡しやすくなります。

高度なデミキシング： 不明瞭なトランザクションのトレース

Chainalysisはまた、一部のユースケース向けに自動デミキシング機能の改良を続けており、これまで捜査の障害となっていた不明瞭な暗号トランザクションの複雑な追跡を法執行機関がより簡単に行えるようにしています。

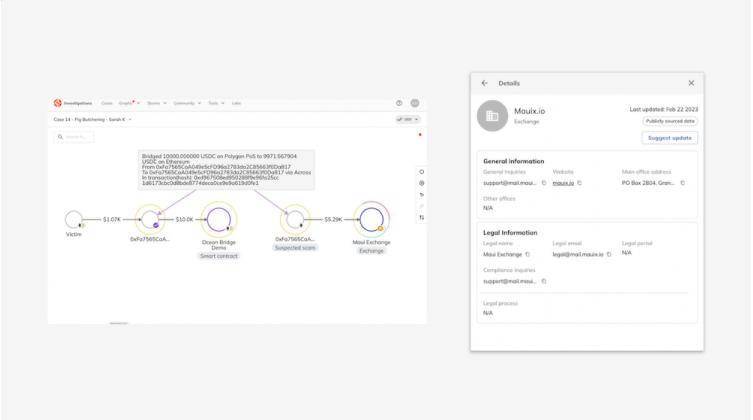
難読化技術を含む特殊なケースのサポートについては、当社の専門家チームにお問い合わせください。

犯罪者を追跡し、地域社会を守る

このケースでは、捜査官はマウイ・エクスチェンジが容疑者の資金の最終目的地であることを発見し、さらなる移動を防ぐために迅速に行動を起こしました。 捜査のこの段階で犯罪者を追跡するためにChainalysisが提供する機能を見てみましょう。

サービスプロバイダー照会： 仮想資産サービス プロバイダーとの通信を合理化

Service Provider Inquiry (以前は Directory として知られていました) を使用して、捜査官は容疑者の KYC 情報を取引所に要求し、犯罪者が資金を移動する前に資金を凍結するよう要求します。

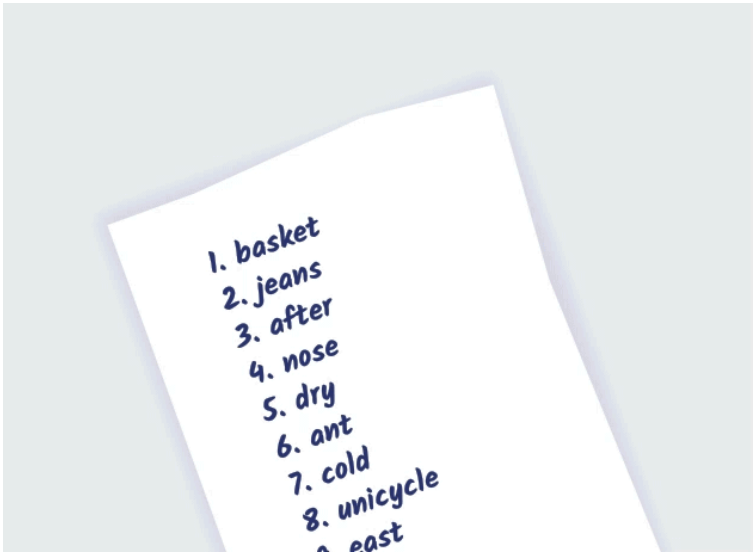


捜査官はこのKYCデータを使って法執行機関のデータベースの記録チェックを行い、不正資金を押収するための令状を取得するのに十分な証拠を確保する可能性がある。

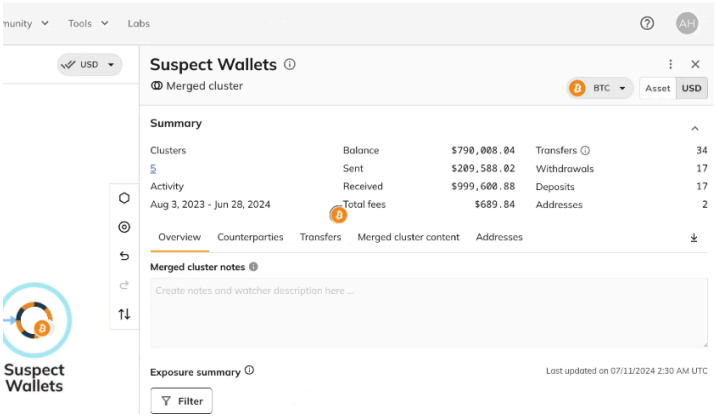
ウォレット スキャン： 関連するすべてのウォレットのアクティビティについて、シードフレーズをすばやくチェックします。

捜査令状の執行中に、捜査官はシードフレーズやその他の実行可能な証拠を見つけることがあります。 多くの一般的な暗号通貨ウォレットでは、1つのシードフレーズが何百万ものアドレスにリンクする可能性があり、針の穴を通すような難題です。

Chainalysis Labs によって開発された Wallet Scanは、このプロセスを合理化します。 捜査官は 残高や過去のアクティビティなど、関連するすべてのウォレットを評価することで、資産押収の機会をすばやく特定します。



ウォレットスキャンはオフラインで安全に動作し、チェーンオブカストディを維持します。 この情報はChainalysisによって保存されることはありません。 Chainalysisは、35の一般的なウォレットと15のブロックチェーンで資金をスキャンし、何百万ものアドレスをスケールで可視化します。



ロマンス詐欺の例に戻ると、Wallet Scanがどのようにさらなる洞察をもたらすかがわかります。 ここでは、シードフレーズに結びついたアドレスに79万ドル相当の不正資金があることがわかります。 捜査当局はこの資金を押収し、容疑者を逮捕し、被害者に返還しました。

> **Through the use of Wallet Scan we were able to identify and recover $11.4M in funds that were originally missed in the initial reconstitution of the wallet back in 2019 due to several derivation paths that were unknown at the time.**
>
> US Government agency

チェーン分析で調査を進める

政府機関や捜査官は、包括的な暗号捜査ソリューションを使用して、暗号化犯罪の複雑さに取り組んでいます。 手掛かりの迅速な発見から、特定の不正活動の追跡、クロスチェーンブリッジのような難読化戦術のナビゲート、資産の押収まで、Chainalysisは捜査活動を前進させ、加速させます。