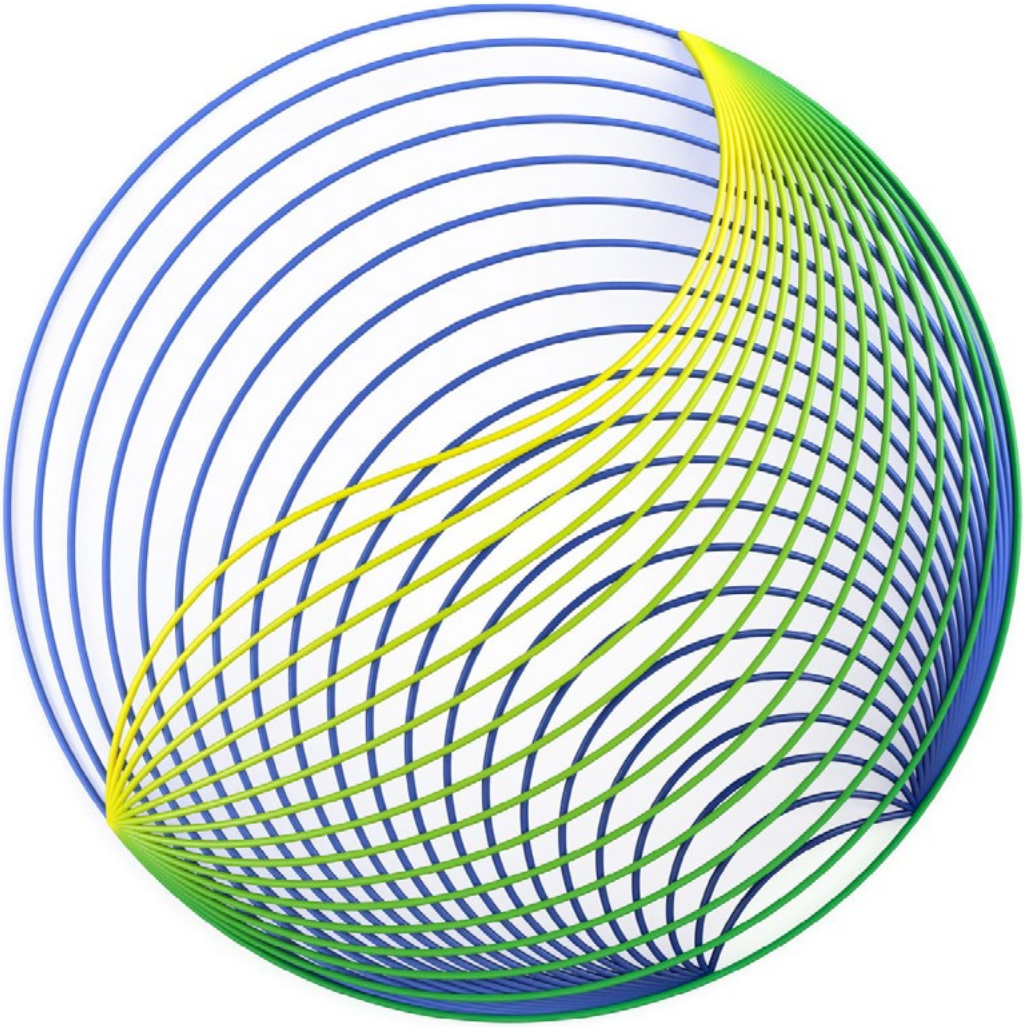
Deloitte.

HAWK



Conquering Crypto Crime

Combining Blockchain Analytics with Real-Time Transaction Monitoring

The current cryptocurrency anti-money laundering landscape is dominated by Blockchain Analytics Tools (BATs) like Chainalysis, Scorechain or Elliptic. Although their capabilities are undeniably impressive, they are not sufficient for comprehensive money laundering detection.

This paper proposes the combination of BATs with Anti-Money Laundering (AML) transaction monitoring solutions. We anticipate that this approach will lead to more effective AML compliance measures in the crypto space.

Introduction

Blockchain technology and cryptocurrency have gained considerable attention in recent years. However, pseudonymity – and in some cases anonymity – features make these technologies susceptible to misuse for money laundering activities. Blockchain Analytics Tools (BATs) are presently at the forefront of combating money laundering threats in the crypto sector. Firms like Chainalysis, Elliptic, and Scorechain collect risk data about pseudonymous and anonymous blockchain addresses and cluster them to consolidate insights.

For instance, if a BAT identifies a blockchain address connected to a ransomware attack, it absorbs and stores the associated risk information with the address. Still, despite their effectiveness, the current methods and tools have certain limitations:

1. **End-to-End Fiat & Crypto Monitoring**: BATS often lack the ability to track the exchange of fiat money into cryptocurrency and vice versa – a critical aspect of money laundering schemes.
2. **Pattern Analysis**: BATs usually cannot identify suspicious transactional or behavioral patterns beyond simplistic rule-based scenarios, which is a key regulatory requirement and a necessity for identifying money laundering.
3. **Indirect Risk Scoring**: BATs often assign indirect risk scores, as only a limited number of blockchain addresses are directly connected to identified crimes. Indirectly scored addresses often leave analysts with too much room to decide whether to file a Suspicious Activity Report (SAR) or not.

Apart from low detection rates (and thus an increased risk of being misused for money laundering), these limitations can also lead to technical shortcomings in complying with applicable money laundering laws and regulations. Regulators often prescribe (directly or indirectly) a recurrence to published typologies provided by Financial Intelligence Units (FIUs) and/or law enforcement agencies. Available typologies published by local FIUs and the Financial Action Task Force (FATF) comprise scenarios which include combined fiat and crypto transactions, as well as other more complex behavioral patterns. These scenarios cannot be covered by BATs alone.

Furthermore, these shortcomings lead to inefficiencies in alert clearing processes. Indirect linkages to tainted addresses in the mid risk range often cause a high number of alerts, leaving operators with only low additional risk information. These alerts usually get classified as false positives. This causes operators to spend a considerable amount of time on hard-to-decide alerts – which are ultimately unproductive.

"Apart from low detection rates (and thus an increased risk of being misused for money laundering), these limitations can also lead to technical shortcomings in complying with applicable money laundering laws and regulations."

Complementing Blockchain Analytics with Real-Time Transaction Monitoring

The identified constraints underscore the necessity to complement BATs with the Anti-Money Laundering (AML) transaction monitoring solutions already applied to fiat transactions. These solutions are designed to process fiat transactions and analyze them based on complex scenario models. Together, a combination of BAT and crypto-ready AML transaction monitoring solutions can overcome the shortcomings.

Combining Fiat and Crypto Transactions

For effective risk management, monitoring systems should link fiat and crypto transactions to display overall customer behavior, e.g., based on a customer or account ID. Particularly at crypto exchanges, which have data available about both types of transactions, this can uncover relevant insights which would not be available analyzing either only crypto or fiat transactions. Key typologies focus on the entire crypto customer journey, from depositing fiat currency, to trading different crypto assets, to finally withdrawing fiat currency to another bank account.

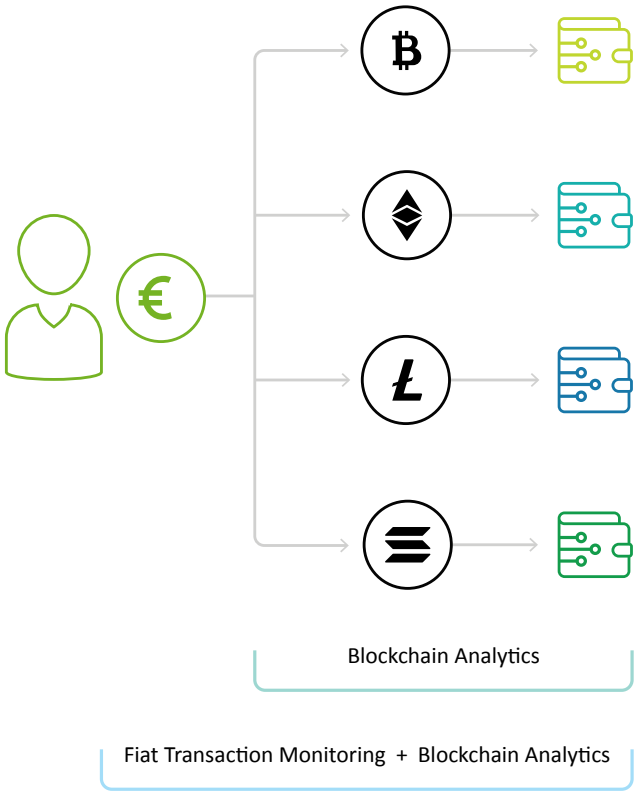
Analysis of Complex Transaction Patterns

To achieve effective and efficient money laundering detection, it is imperative to recognize known (yet unidentified) intricate money laundering behavioral patterns. Although modern BATs allow rule creation, they are mostly confined to simple and usually one-dimensional criteria, like amount thresholds. More complex rule sets, or even Artificial Intelligence (AI)-based models – as seen in many modern AML transaction monitoring solutions – allow operators to uncover complex suspicious behaviors such as money muling, account passthrough, and other common money laundering techniques.

Inclusion of Customer Risk Data

Even though the traditional fiat sector has yet to fully combine and integrate static Know-Your-Customer (KYC) data with dynamic transactional data, modern AML transaction monitoring solutions provide for this combined view. This allows operators to make use of all available customer data for optimal risk detection. The connection between customer and transaction data is even more critical in cryptocurrency, due to the pseudonymity of blockchain transactions. For adequate risk detection – and regulatory coverage of available typologies – the integration of static customer data, transactional data, and BAT-derived risk information is paramount.

Figure 1: Simultaneous ingestion and pattern analysis across fiat and crypto transactions



The Way Forward

While BATs are a fundamental necessity for mitigating crypto-related money laundering risk, they require supplemental features provided by modern transaction monitoring solutions. Integration of tools from the crypto market with modern monitoring systems is the future roadmap for efficient and effective AML compliance. The usage of AI-based models to identify existing and unknown patterns and to prioritize risks originally identified from BATs makes perfect sense; it may well be inevitable.

We advocate for the harmonized and comprehensive use of BATs along with modern traditional fiat money monitoring tools for efficient and effective anti-money laundering compliance. This will help achieve the ultimate goal of curbing the misuse of blockchain technology and cryptocurrency transactions.

In particular, we recommend integrating BATs with modern financial crime technology systems in the following way.

Integrated User Interfaces

Integrating user interfaces fills the need for a unified platform where operators can seamlessly access and present relevant information for analyzing and verifying transactions. Making relevant data available on a single, synchronized platform rather than multiple standalone applications provides a considerable advantage to operators. Linking and presenting customer data, fiat and crypto transactions, complex behavioral patterns, and risk prioritization models together leads to a smooth processing experience.

Combined Representation of Fiat and Crypto Payment Flows

This key recommendation stems from the value of representing fiat and crypto transactions in a unified format. As criminals aim to integrate illicit proceeds back into the legal financial system, effective monitoring processes should include the linking and analysis of fiat and crypto transactions. When operators have access to this linkage, they can better understand and mitigate complex money laundering patterns.

AI Models for Detection and Result Prioritization

AI models can increase efficiency and accuracy by detecting anomalous behavior and prioritizing alerts based on comparative risk analysis. In addition, these models can also dynamically prioritize initial BAT findings based on diverse risk dimensions, especially with crypto transactions, where multiple sequential transactions occur and risk scores often lie in the “grey area,” AI-based prioritization models help significantly. Notably, the models used in this context should be transparent and comprehensible. For regulatory purposes especially, AI-generated decisions should include explanations in human-understandable language.

Complex transaction patterns and customer risk data can inhibit effective crypto-related AML compliance. However, integrating user interfaces, combining fiat and crypto payment flows, and using AI models for result prioritization can significantly improve monitoring processes. Consequently, an integration of blockchain analytics systems with traditional AML systems is the best way to improve efficiency and effectiveness in crypto-related AML compliance.

Deloitte Case Study: From Independent Review to Integration Support

As a starting point for any changes on transaction monitoring systems, we support our crypto as well as non-crypto clients in an independent review of their transaction monitoring landscape. The scope of our review can be modularly adjusted covering different regulatory relevant packages, e.g., analyzing underlying policies and procedures towards data processing, coverage, and lineage topics.

In this example, we examined the coverage of relevant risks and typologies as well as how effective and efficient existing rules and parameters were configured to detect those risks. Apart from the analysis of internal documents such as the risk assessment, we specifically assessed how well publicly available crypto-related typologies from relevant FIUs and the FATF are applied through the transaction landscape. Based on a prioritized list of more than 50 applicable typology scenarios, we identified that some of the scenarios were not covered at all, whereas the majority of the scenarios were covered in a highly manual, non-integrated way.

Most of the relevant information, crypto and fiat transactions as well as other customer data, was available. However, it was spread across disparate systems, which made it almost impossible for an alert operator to connect the dots. The analysis of the alert clearing process and the review of alert statistics, indicated that alert operators spent most of their time cumbersomely investigating false alarms. On the other hand, almost no material suspicious behavior was identified proactively through the transaction monitoring process. Knowing from law enforcement and other agency driven requests that the customer set was by no means free of suspicious behavior, this further painted the picture that changes need to be made to both detection and alert prioritization.

Based on our independent review, we subsequently supported the client in assessing mitigation options, starting with drawing a target operating model from which available make and buy options could be assessed. For the assessment of available (make- or buy) options, we further support the client in defining and breaking down detailed requirements based upon the entire range of our assessment criteria used in the independent review.

After the final vendor selection was performed independently by the client, we supported the integration project with various roles on demand. First and foremost, we assisted the client in breaking down relevant fiat-crypto typologies into rule and model configurations and helped test them to achieve adequate results with regards to effectiveness and efficiency. Secondly, we supported the integration project from a business as well as a technical perspective. From a business perspective we helped – among other things - to map existing endpoints to the new vendor endpoints. From a technical standpoint we supported in configuring the API setup as well as building relevant connectors.

All in all, we helped to ensure that

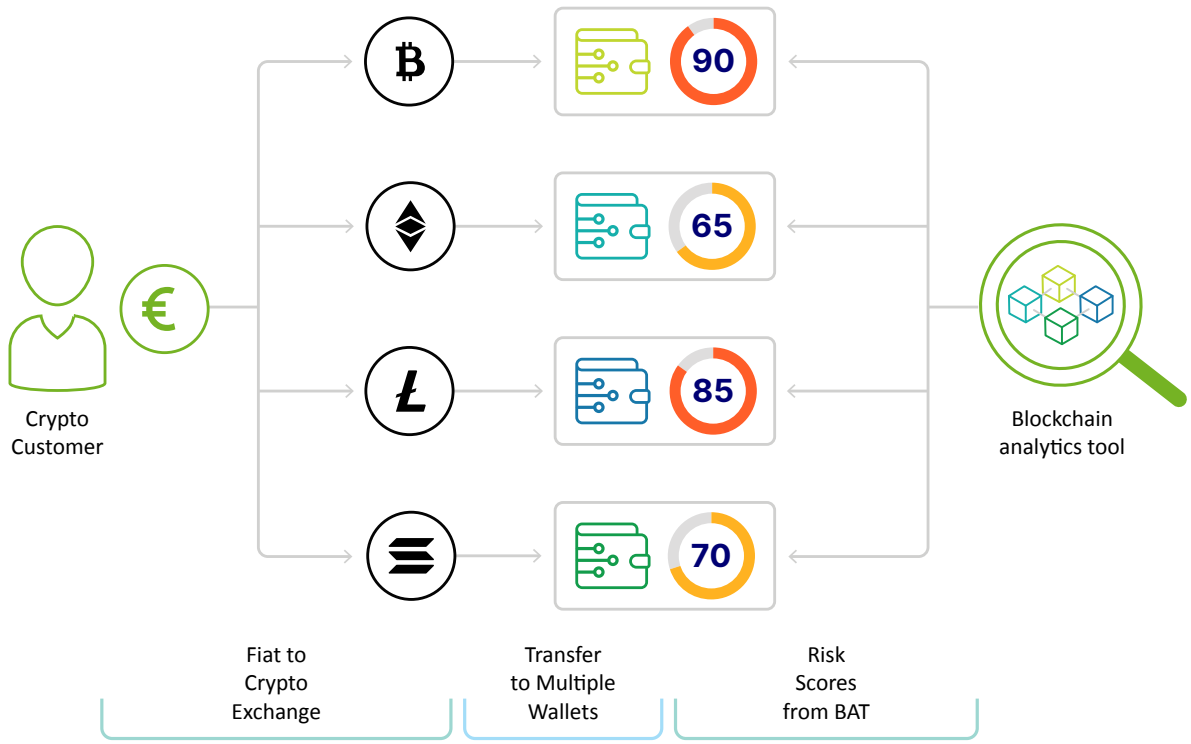
1. the (regulatory) problem was clearly defined and grounded on facts,
2. the best possible solution on the market was hired,
3. the integration was performed in minimum time without overburdening the client's already stretched resources.

Hawk Case Study: Integrated Crypto-Fiat Monitoring

Hawk has developed a crypto monitoring solution that integrates its own AML Transaction Monitoring technology with the capabilities of BATs. Hawk also provides modules such as Customer Risk Rating, Customer Screening, Payment Screening. The Hawk platform can read any kind of transactional data, from standard fiat transaction protocols like SWIFT and SEPA to crypto transaction data. Hawk's system can ingest crypto and fiat transactions at the same time, meaning it can identify patterns across all sources.

Consider an example. A newly onboarded client of a crypto exchange deposits a large amount of fiat money, then rapidly exchanges the fiat money into various crypto currencies. Within a short timeframe, the client moves the smaller crypto amounts to various external crypto addresses. Because BATs only track crypto movements, they cannot detect this classic layering scheme – which money launderers frequently employ on crypto exchanges. Hawk can identify the full scheme by monitoring both fiat and crypto transactions.

Figure 2: Adding BAT risk scores to the combined fiat and crypto pattern analysis



Combining Blockchain Analytics and Customer Risk Information

In addition to the ability to process both fiat and crypto transactions, Hawk has also developed a standard integration with BAT providers, incorporating BAT risk scores into their rules and models for additional money laundering risk insights. Applying BAT wallet risk scores to the scheme detected in the above example would give additional insights to the external wallets being used for the withdrawal. The wallets might be already directly or indirectly connected to other wallets known for illicit activity, e.g., as deposit addresses for proceeds from ransomware attacks. This would add another contextual layer to the alert, which will help operators decide whether the detected behavior is illicit.

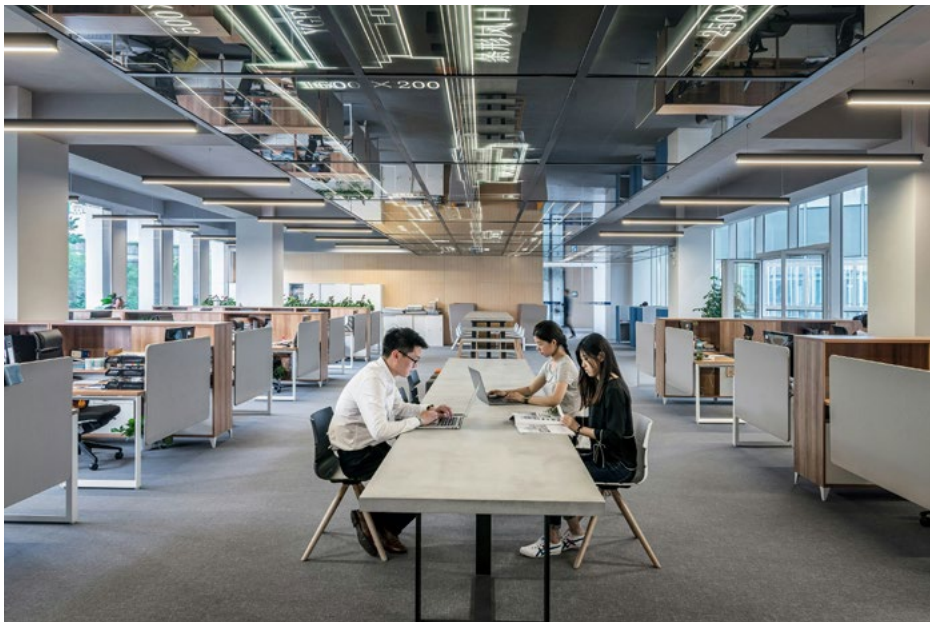
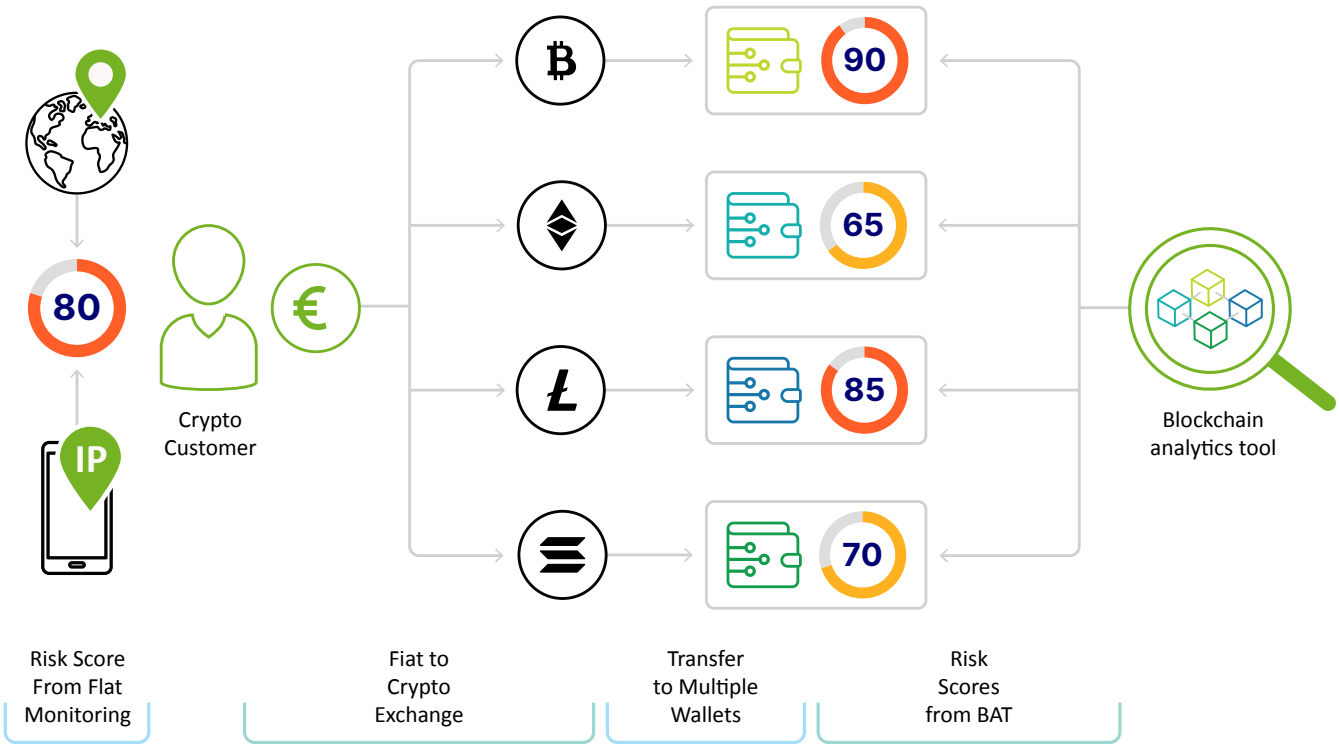


Figure 3: Adding other relevant customer risk data for a full 360 degree crypto customer risk view



Out of the box, the Hawk solution also integrates other relevant customer risk information into alerts. The system adds background information (e.g., geographic location, occupational information, watchlists, and adverse media results) to the detected suspicious activity. In the example above, the customer's German residency, as well as his or her use of a device connected to a Vietnam IP address, would add relevant context to the investigation.

Finally, all information is presented in a unified case management system, where all information related to the transaction(s) and the customer is presented together. The case manager also allows for the maximum possible automation for subsequent authority, such as SAR filing.

Putting AI on Top to Enter a New Era of Crypto Transaction Monitoring

One of Hawk's focuses is applying transparent and explainable AI on top of relevant data to further enhance transaction monitoring results. Hawk's AI models can specifically integrate crypto signals into their detection and false positive reduction models, harnessing the combination of available transactional and customer information as well as relevant data provided by a BAT.

Not only does this approach enable the extremely powerful models to detect illicit schemes, but it also helps overcome challenges in current crypto transaction monitoring procedures. As a lot of monitoring results provided by the BAT are somewhere in the "grey area," it is extremely difficult for analysts to decide on true suspicion. Hawk's crypto models, by integrating latest data analytics technology and using all available transactional and customer data, allow operators to precisely triage "grey" BAT alerts which would otherwise consume a tremendous amount of resources.

Summary

We have discussed the current limitations in relying solely on Blockchain Analytics Tools like Chainalysis, Scorechain, or Elliptic for AML measures. These tools, although impressive, require more comprehensive money laundering detection, i.e., the ability to process fiat transactions and identify suspicious transactional or behavioral patterns. Their methods for assigning risk are also indirect, thus resulting in inefficiencies in alert clearing processes.

To overcome the limitations of BATs, we suggest supplementing these tools with traditional AML transaction monitoring solutions, allowing for combination of fiat and crypto transactions and analysis of complex transaction patterns. We also propose the inclusion of customer risk data. More specifically, we advocate for the integration of BATs with modern financial crime technology systems. This includes integrated user interfaces that can seamlessly present and access transaction analysis data, represent fiat and crypto payment flows in one format, and use AI models to detect and prioritize results. We have also outlined case studies to illustrate the possibilities. These examples include Deloitte supporting clients in reviewing their transaction monitoring landscape and Hawk integrating their own AI-augmented solution with BAT capabilities to enhance transaction monitoring results.

In conclusion, we advocate for a comprehensive use of BATs with traditional fiat money monitoring detection tools to achieve effective and efficient crypto-related AML compliance.

"To overcome the limitations of BATs, we suggest supplementing these tools with traditional AML transaction monitoring solutions, allowing for combination of fiat and crypto transactions and analysis of complex transaction patterns."

If you want to learn more

Martin Hirtreiter

Partner | Deloitte
Anti-Financial Crime Advisory
mhirtreiter@deloitte.de

Dr. Robert Schmuck

Director | Deloitte
Anti-Financial Crime Advisory
rschmuck@deloitte.de

Wolfgang Berner

Co-Founder & CTO/CPO | Hawk
wolfgang.berner@hawk.ai

Deloitte.

Issue 01/2025