Date: 15 May 2023

In this article, the writers examine the use of artificial intelligence ("AI") to improve anti-financial crime efforts, and such AI systems supporting usage must comply with the upcoming European Union Artificial Intelligence Act (the "EU AI Act").

Authors: Sean Musch, AI & Partners, Michael Borrelli, AI & Partners, and Marco Morazzoni, Elliptic

**AI is a game changer in the fight against financial crime**

To deter financial crime in the cryptoasset markets, cryptoasset firms can utilise the full benefits of artificial intelligence ("AI"), machine learning ("ML") and advanced analytics in enforcement efforts. To do this, firms need anti-money laundering ("AML") experts, strong data science talent, and reliable data sources in the fight against multiple types of financial crime, such as money laundering and countering terrorist financing ("TF").

The volume of TF and other financial crimes is increasing globally—and the tools and techniques used to evade their detection are becoming ever more developed. This has elicited a rigorous response from cryptoasset firms, which, in aggregate, are investing hundreds of millions each year to improve their safeguards against financial crime.
Moreover, the resultant regulatory fines linked to compliance are growing annually as regulator’s impose tougher penalties. Notwithstanding, cryptoasset firms’ traditional rule- and scenario-based approaches to fighting financial crimes has may seem a step behind the malicious actors, making the fight against financial crime an ongoing hurdle for compliance, monitoring, and risk-focused cryptoasset firms.

**Applying AI to blockchain analytics**

At least in theory, cryptoasset firms can apply ML across the entire AML value chain (Exhibit 1). But we are of the view that blockchain analytics—specifically, combining ML with other advanced algorithms (for example, random forest, gradient boosting, deep learning)—is where cryptoasset firms can reap one of the most immediate and significant benefits in their AML efforts.

**A range of sophisticated tools exist throughout the AML value chain**

**Exhibit 1: AML Value Chain**

<table>
<thead>
<tr>
<th>Component</th>
<th>Current</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client risk rating and onboarding</td>
<td>✓ Expert weighted-factor approach</td>
<td>✓ Use of advanced algorithms (statistical or ML approach)</td>
</tr>
<tr>
<td></td>
<td>✓ Traditional statistical-regression approach</td>
<td></td>
</tr>
<tr>
<td>Client screening</td>
<td>✓ Sanctions screening</td>
<td>✓ Advanced algorithms with feedback mechanisms</td>
</tr>
<tr>
<td></td>
<td>✓ Negative media screening</td>
<td></td>
</tr>
<tr>
<td>Transaction monitoring</td>
<td>✓ Rules-based approaches</td>
<td>✓ Use of ML to bolster effectiveness and efficiency</td>
</tr>
<tr>
<td></td>
<td>✓ ML as point-of-contact or on top of existing rules-based engine</td>
<td></td>
</tr>
<tr>
<td>Event-driven review</td>
<td>✓ Additional rules implemented through time on top of system scheduled</td>
<td>✓ Dynamically introduce highly precise rules for newly identified rules</td>
</tr>
<tr>
<td></td>
<td>know-your-customer (“KYC”) refreshes</td>
<td></td>
</tr>
<tr>
<td>Transaction filtering and screening</td>
<td>✓ Sanctions screening using basic matching algorithms</td>
<td>✓ Advanced algorithms with feedback mechanism</td>
</tr>
<tr>
<td></td>
<td>✓ Negative media screening</td>
<td></td>
</tr>
<tr>
<td>Refresh (CRR + expected vs. actual)</td>
<td>✓ KYC calendar-focused approach</td>
<td>✓ Perpetual KYC through behaviour scores</td>
</tr>
</tbody>
</table>
As of current, many cryptoasset firms use rule- and scenario-based tools or basic statistical approaches for blockchain analytics. These rules and thresholds are driven predominantly by industry red flags, basic statistical indicators, and expert judgment. However, the rules often fail to capture the latest trends in financial crime behaviour. ML models, on the other hand, leverage more granular, behaviour-indicative data to construct sophisticated algorithms. They are also more adaptive in quickly adjusting to new trends and continually improving over time. By substituting rule- and scenario-based tools with ML models, cryptoasset firms can improve both suspicious activity identification and efficiency.

When transitioning to an ML model for blockchain analytics, cryptoasset firms should address three key questions:

**Where should cryptoasset firms use ML?**

To begin with, it is important for cryptoasset firms to understand the instances where they can use ML effectively and where they can’t. ML is certainly advantageous when there is a high degree of freedom in selecting data attributes, as well as sufficient availability of quality data (as an example, in scenarios where there is a rapid movement of funds and a large number of attributes can be considered). ML is also appropriate when it becomes difficult to identify the dynamics and relationships between risk factors.

In contrast, ML is not useful when there is not enough current data to build forward-looking intelligence. In these circumstances, a traditional approach (rule- and scenario-based tools, for instance) may be more effective.

**What additional data sources are needed?**

When working with suspicious-activity reports, bad quality data inevitably results in poor model performance. It is vital, for example, not to be overly dependent on suspicious-activity-report categories (as an example, structuring, TF, ML, fraud), which are limited in today’s world. With this under consideration, cryptoasset firms can explore a range of initiatives to improve data gathering for their ML models to provide enriched context for transaction monitoring.
This straddles modeling against individual transactions or cases, components of suspicious-activity-report filings or client relationships terminated for AML reasons, and data from historical subpoenas and other law enforcement requests for information. These more complex ML models can incorporate a wide range of new elements and variables, such as the following:

- **enhanced** client data (for example, nature of business, type of clients).
- more comprehensive product data (for instance, granular product type and usage).
- more granular channel data (for example, channels for different products).
- **risk** indicators across risk type (for instance, business geography).
- **external data** sources (for example, bureau data, financial-crime registries).

**How should cryptoasset firms service the model?**

ML models are not as transparent than rule-based ones, and model risk management (“MRM”) teams and regulators are more frequently requiring better model “explainability”—insofar as, better methods of interpreting “black box” machine learning models, which develop and learn directly from the data with typically no or limited human supervision or guidance—so they can evaluate the models.

At leading cryptoasset firms, model development teams are working with AML investigators to help ensure that the teams understand the modelling data, create interpretable modelling features rather than a data dump, and integrate ML modules with existing rule- and scenario-based models and tools (that is, the transition process should leverage the existing platform, thus improving the status quo and not dismantling it entirely). Leading cryptoasset firms are also beginning to create AML-specific model guidelines. Some of the specific ways that cryptoasset firms are improving explainability and generating more high-quality alerts for downstream investigators include the following methods:

- **Out-of-time sample**: Cryptoasset firms must reserve sufficient testing samples to conduct model testing.
- **Model validation**: Cryptoasset firms consider ML-specific risks, including feature engineering, hyperparameter calibration, model bias against protected classes, model drift and interpretability, transparency, and explainability.
- **Ongoing monitoring**: Cryptoasset firms conduct frequent, ongoing, below-the-line (BTL) testing to help monitor model performance.
Best practices for bringing AI to blockchain analytics

We have identified three best practices that leading cryptoasset firms can use to adopt ML for AML transaction monitoring:

1. Sync stakeholders on design and vision

One of the main reasons that ML projects fail is because of an absence of buy-in from various stakeholders, including the data, technology, line-of-business, MRM, and compliance teams. It is imperative to engage these stakeholders from the start of the project to align on vision, to make architectural design choices, and to consider trade-offs for all processes from end to end (Exhibit 2). This helps to ensure that all business-as-usual activities and ongoing regulatory actions are considered. For example, leading institutions will often start meeting with regulators up to a year before development even begins—and then through the development process—to avoid surprises.

Exhibit 2: Dimensions for consideration for anti-financial crime approaches

<table>
<thead>
<tr>
<th>Data</th>
<th>Methodology</th>
<th>Monitoring and Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intended Application</strong></td>
<td><strong>Interval of analysis</strong></td>
<td><strong>Monitoring</strong></td>
</tr>
<tr>
<td>✓ Suppress and/or prioritise scenario outputs</td>
<td>✓ Daily</td>
<td>✓ Metrics and thresholds</td>
</tr>
<tr>
<td>✓ Input to individual and/or multiple scenarios</td>
<td>✓ Weekly</td>
<td>✓ Governance and decision support</td>
</tr>
<tr>
<td><strong>Targeted Variable</strong></td>
<td><strong>Sampling</strong></td>
<td><strong>Implementation</strong></td>
</tr>
<tr>
<td>✓ Scenario vs. client level</td>
<td>✓ Definition of known population</td>
<td>✓ Data storage</td>
</tr>
<tr>
<td>✓ PVA, SAR</td>
<td>✓ Development</td>
<td>✓ Model calculation</td>
</tr>
</tbody>
</table>
In essence, gathering a range of perspectives and aligning on the vision, design, and trade-offs for using ML improves transparency across the business while uncovering and reducing risks.

The value proposition is linked to improving effectiveness by better capturing the risk and generating high-quality alerts for downstream investigation—efficiency, accordingly, follows effectiveness.

2. Construct a safe technology transition plan

Transformations are about more than just introducing new technologies. For successful transformation, we are of the view that three key elements matter most:

- Be **intentional** when using the approach (for example, focus on the transition plan, not just the end state).
- Implement a **collaborative** mindset that fuses technology and business goals (for instance, for the user, by the user—involves the business at all times and in all phases of the process).
- Move forward with **rigorous** and transparent execution tailored to the realities of modern technology systems (for example, apply a modular approach to plug and play).

Nonetheless, all technology transformations experience failures. Employees often resist adopting new approaches to work, and new technologies can inject unforeseen risks.

To secure early support during the pilot phase and to help minimise risks, a cryptoasset firm could run existing rule- and scenario-based risk scenarios in parallel with ML-based scenarios to build confidence among stakeholders.

To further build adoption and reduce risk, the cryptoasset firm might choose projects that can leverage existing platforms (those that employees are already comfortable using) and integrate the new components in consecutive fashion.

Ideally, cryptoasset firms will start with the low-hanging fruit—projects that offer significant potential rewards with manageable risk.
3. Optimise the model risk management framework

To embed ML solutions into the blockchain analytics framework, MRM teams need to conduct the following:

- *Enlarge capabilities* to work closely with the data science team in the model development and validation process. MRM teams should educate data scientists about possible risks during the development process.
- *Influence validation standards, policies, and frameworks* to take on the specific risks linked to ML models, including bias detection and explainability.
- *Define specific performance and monitoring requirements*, including out-of-time testing, and when to recalibrate ML models.

### Best practices for bringing AI to blockchain analytics

In the fight against financial crime, cryptoasset firms have traditionally been one step behind malicious actors. Now, they have a chance to change the game. Advanced-analytics techniques, specifically ML with network analytics, promise to improve blockchain analytics dramatically by reducing false-negative and false-positive rates—and by sending higher-quality alerts to downstream AML investigators. For most cryptoasset firms, the development requires investing significant time and resources. To realize the full benefit, cryptoasset firms will need to build a talent pool, create reliable data sources, and leverage the knowledge of subject matter experts. A tall order, but well worth the effort given the high stakes.

### How AI & Partners can help

We can help you start assessing your AI systems using recognised metrics ahead of the expected changes brought about by the EU AI Act. Our leading practice is geared towards helping you identify, design, and implement appropriate metrics for your assessments.

**Website:** [https://www.ai-and-partners.com/](https://www.ai-and-partners.com/)