Proactive Defense: Real-Time Detection of Malicious Ethereum Transactions

Tamer Abdelaziz and Karim Ali

New York University Abu Dhabi

RESEARCH INSTITUTE NYU ABU DHABI
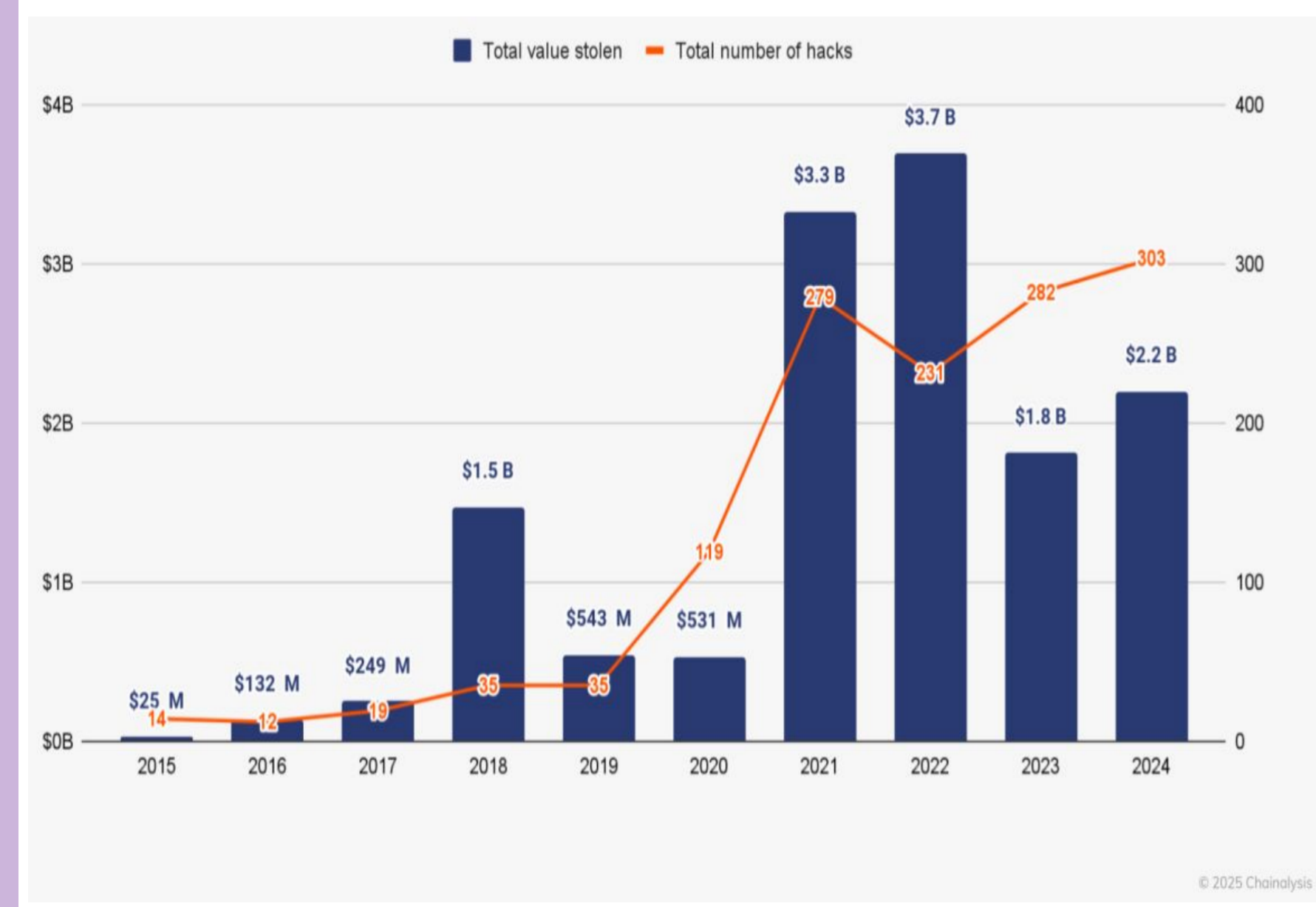
SANAD SOFTWARE ANALYSIS AND DEVELOPER SUPPORT
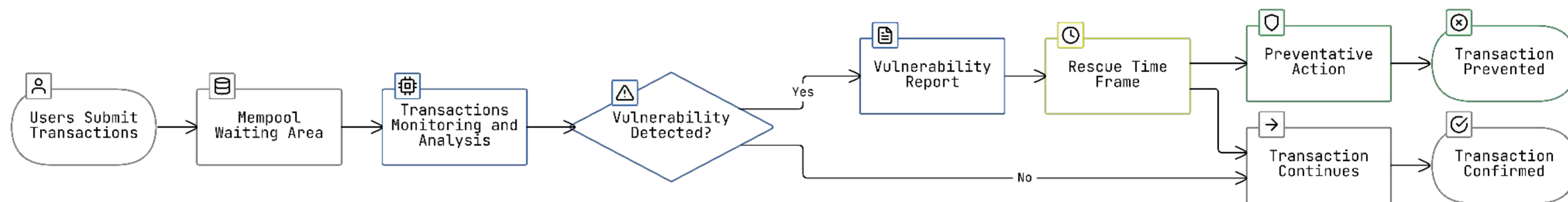
Why It Matters?

- A **transaction** records cryptocurrency transfers or smart contract execution.
- Ethereum processes ~**1.25M transactions daily**.
- Transactions are confirmed in **15 seconds to 5 minutes** (rescue time frame).
- **Cryptocurrency attacks** cost **$2.2B in 2024**, up 21% year-over-year.
- **Challenges**:
  - Detect malicious transactions *before* confirmation.
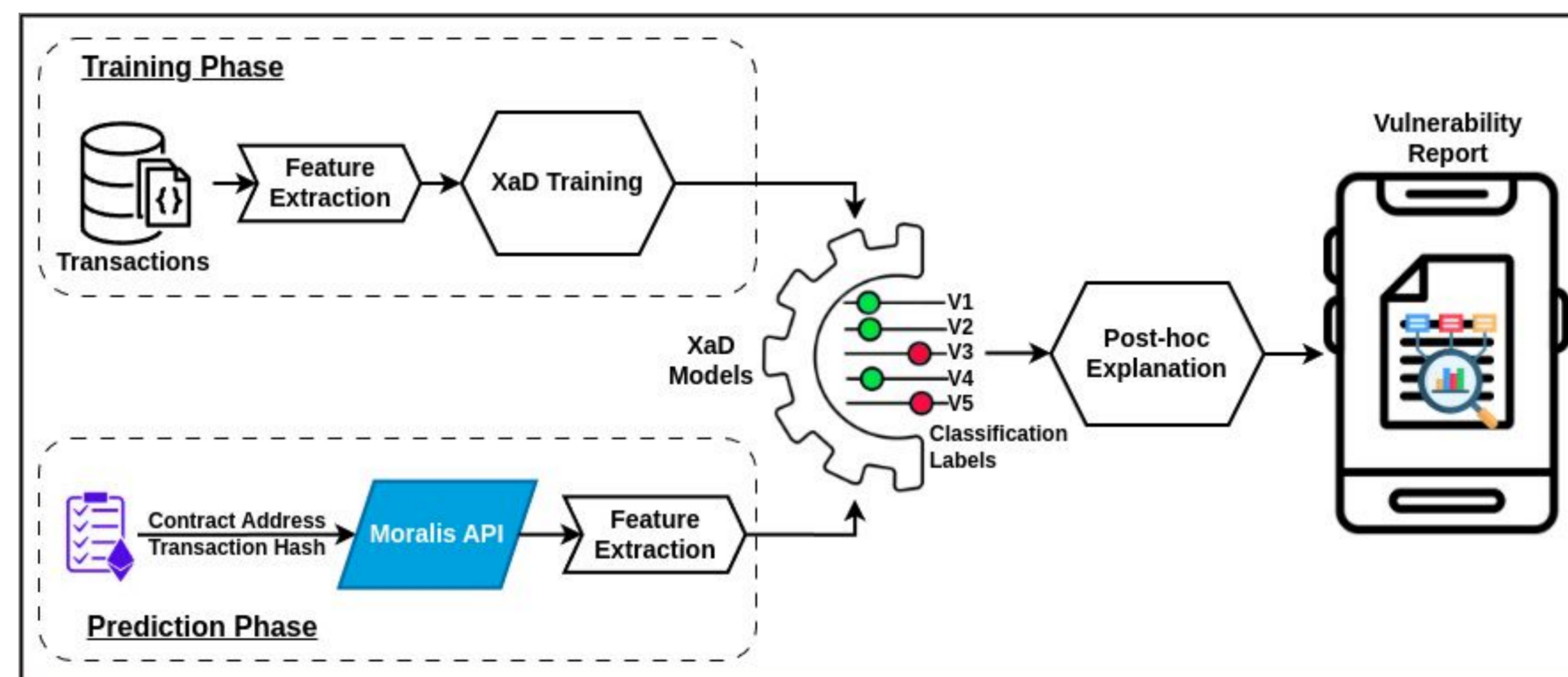 - Enable *real-time* detection with interpretable explanations.

Total value stolen / Total number of hacks chart (2015–2024). © 2025 Chainalysis

Malicious Transaction Example

Proactive Defense Workflow

Users Submit Transactions → Mempool Waiting Area → Transactions Monitoring and Analysis → Vulnerability Detected? → Yes → Vulnerability Report → Rescue Time Frame → Preventative Action → Transaction Prevented / Transaction Continues → Transaction Confirmed. No → Transaction Continues.

How Transactions Monitoring and Analysis Work

Training Phase: Transactions → Feature Extraction → XaD Training → XaD Models → Classification Labels (V1–V5) → Post-hoc Explanation → Vulnerability Report. Prediction Phase: Contract Address, Transaction Hash → Moralis API → Feature Extraction.

Vulnerability Report

ⓘ Transaction Hash:

0x516e11f52cadd4820a782a548952836bd993f34d0171ec8ffdd3b51903eb6062

To understand why this transaction has been flagged as vulnerable to a Reentrancy Attack, we rely on the machine learning output from XaD and the associated SHAP analysis. The prediction probability of 0.921 indicates a high confidence level from the model that this transaction exhibits characteristics typical of a Reentrancy Attack ...

What We Found

- **ML Power**: Well-trained machine learning detects security vulnerabilities effectively.
- **LLM Insights**: Large language models enhance vulnerability explanations and mitigation guidance.
- **High Accuracy**: Achieves **98.9%** minimum F1-score across all vulnerability types.
- **Rapid Detection**: Identifies vulnerabilities in **0.0014 seconds**.
- **Rescue Window**: Provides **14 seconds to minutes** for mitigation before transaction confirmation.
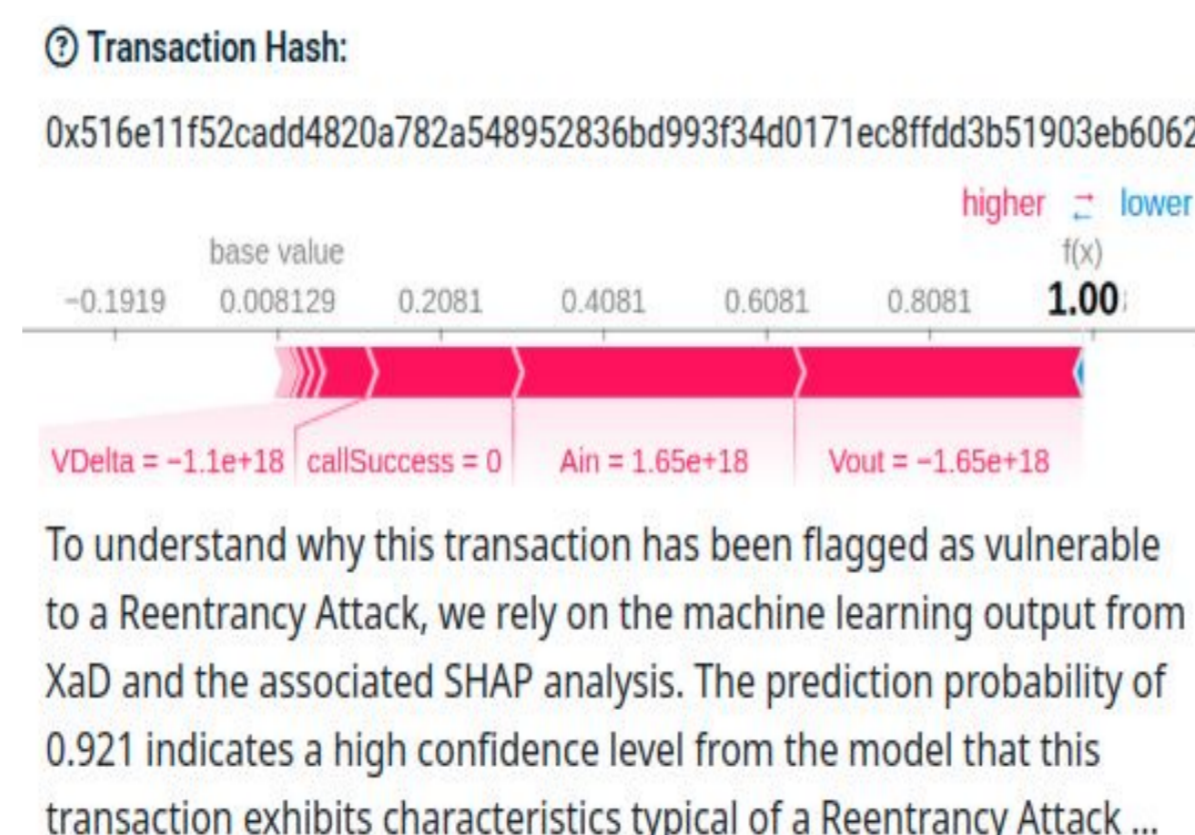
Key Takeaways

- **XAD**: First open-source, ML-based tool for real-time detection of malicious blockchain transactions.
- **Mechanism**: Monitors mempool, simulates pending transactions, and detects vulnerabilities pre-confirmation.
- **Explainability**: Offers detailed reasoning, explanations, and mitigation.
- **Rapid Detection**: Identifies vulnerabilities in **0.0014 seconds**.
- **Performance**: Outperforms **14** leading tools by **29.4%** on average.
- **Accessibility**: Web-based, no installation required.
- **Impact**: Integrates into workflows, delivering actionable security insights for developers and professionals.

✅ Scan the QR code to access our tool! 🚀

About SANAD Lab

Mission:
At NYU Abu Dhabi, SANAD Lab equips software engineers with tools and insights for secure, efficient systems.

Scan QR code for author profiles and lab details.

Collaborate: Want to advance software security?
Email tamer.m@nyu.edu or karim.ali@nyu.edu !

Acknowledgement