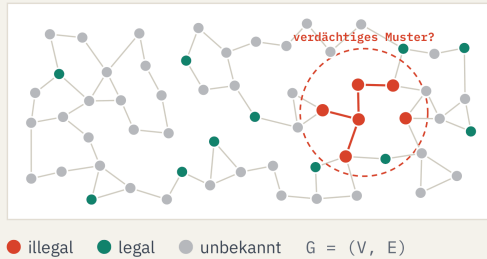


Identifizierung krimineller Akteure in Blockchain-Transaktionsnetzwerken mit Graph Neural Networks

Sven König Erstprüfer: Prof. Dr. Buschermöhle Zweitprüfer: Simon Schwientek (M. Sc.) Betreuer: Erik Weber, LKA Niedersachsen

01 Problem

Pseudonyme Bitcoin-Adressen verschleiern Geldwäsche, Ransomware und Terrorfinanzierung. **Heuristische Verfahren** stoßen bei großen, dynamischen Transaktionsgraphen an ihre Grenzen.



02 Forschungsfrage

Wie effektiv sind Graph Neural Networks bei der Klassifikation krimineller Aktivitäten im Bitcoin-Netzwerk?

- Welche Graph-Eigenschaften sind relevant?
- Welche GNN-Architektur eignet sich?
- GNN vs. klassisches ML?
- Hürden in der Ermittlungspraxis?

03 Daten & Methodik

DATENSATZ

Elliptic++

Gelabelte Bitcoin-Transaktionen als gerichteter Graph mit Features & Zeit

LABELS · STARKES UNGLEICHGEWICHT

Illegal	Legal	Unbekannt
Geldwäsche, Ransomware	regulierte Börsen	größter Anteil

TEMPORAL SPLIT

Training	Val.	Test
----------	------	------

Zeitlich: frühe Daten trainieren, späte prüfen – kein Data Leakage.

300 Epochen · Precision · Recall · F1 · PR-AUC

04 Acht Modelle im Vergleich

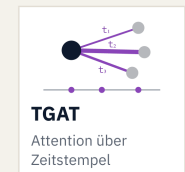
KLASSISCHES ML · BASELINE



STATISCHE GNNs

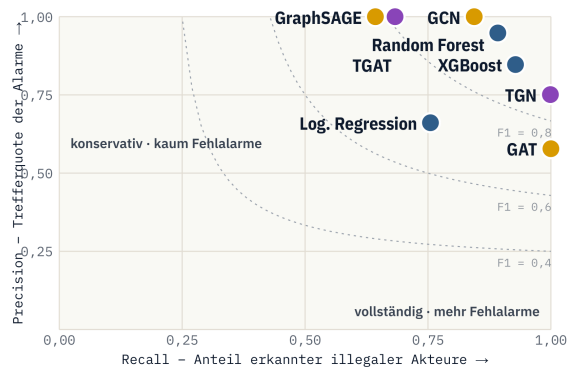


ZEITDYNAMISCHE GNNs

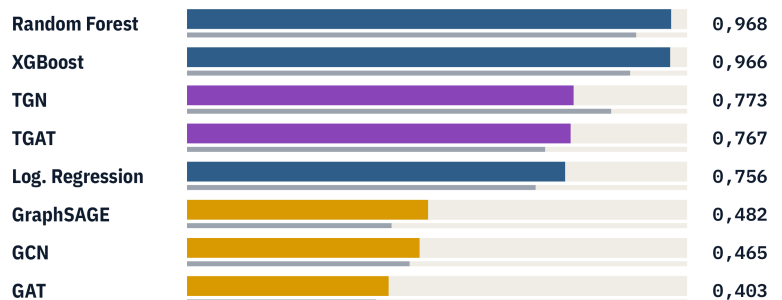


05 Ergebnisse: Zielkonflikt Precision ↔ Recall

Bestwerte je Metrik über 300 Epochen (Tab. 6.2) · gestrichelt: gleicher F1-Score



Trennschärfe je Modell



06 Welches Modell wofür?

Compliance & digitaler Euro

Ziel: hohe Precision

Automatische Sperren dürfen legitime Nutzer nicht treffen.

TGAT GCN GraphSAGE
RF / XGBoost

Forensik & Ermittlungen

Ziel: hoher Recall

Keine Spur übersehen – Treffer werden ohnehin manuell geprüft.

TGN · Recall 0,999

07 Fazit & Ausblick

- Kein Modell für alle Fälle – die Wahl folgt dem Einsatzzweck.
- Zeit zählt: TGN/TGAT schlagen statische GNNs deutlich (PR-AUC ≈ 0,77 vs. < 0,5).
- Baumverfahren bleiben die robuste Benchmark.

→ 1
Hyperparameter-Optimierung

→ 2
Hybrid: GNN-Embeddings + XGBoost

→ 3
Cross-Chain-Graphen