On-Chain Intelligence

Scoring the Invisible Economy - Crypto Risk Management

● AI/ML Technical Documentation ● Production Systems ● Fintech Innovation ●

Technical Documentation Series

December 2024

Executive Summary

Cryptocurrency is paradoxically transparent (all transactions public) yet opaque (no names, only addresses). Coinbase and Revolut use On-Chain Intelligence - Graph AI and sequence modeling to 'dox' the blockchain, identifying risk without knowing identity.

100% Transaction Transparency	**0%** Identity Visibility	**Millions** Addresses Scored
Seq2Win Coinbase Model	**Graph AI** Entity Clustering	**Chainalysis** Attribution Data

The Paradox of Transparency

Crypto is the most transparent financial system (every transaction public on blockchain) and most opaque (no names, only alphanumeric addresses). AML controls require identifying risk without identity - a new class of AI called On-Chain Intelligence.

Coinbase: Blockchain Address Risk Scoring

• The Seq2Win Architecture

- **NLP for Transactions:** Treat transaction history like sentences
- **Addresses as Words:** Predict behavior based on sequence patterns

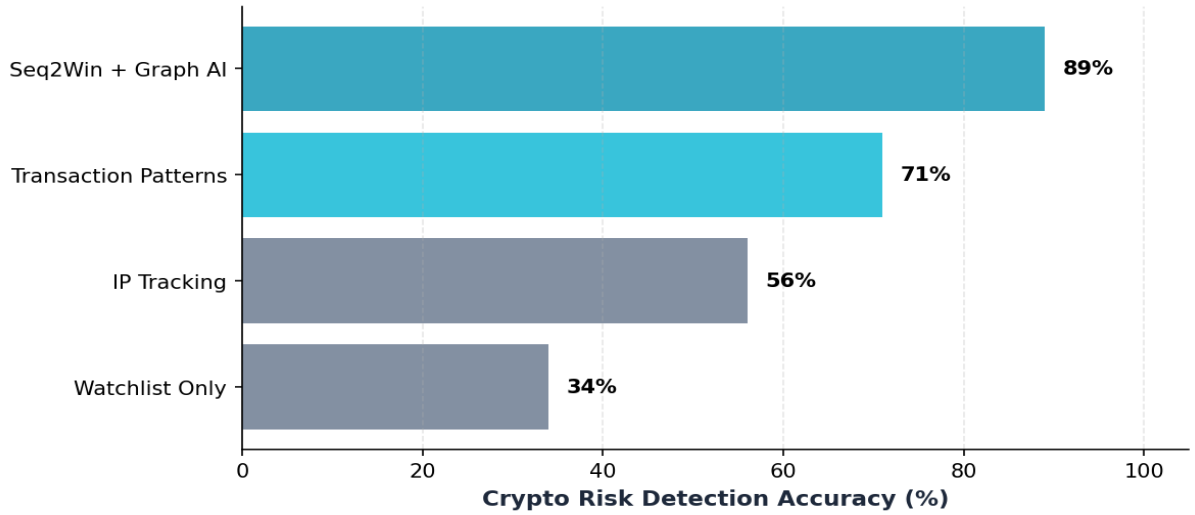
- **Sequence Modeling:** Human (occasional, random) vs Bot (high frequency, fixed)
- **Behavioral Embeddings:** Vector representations cluster similar addresses

• Mathematical Clustering

Even if addresses never interacted, close embeddings in vector space = likely same entity type (darknet market, exchange). Flag new address as high-risk because it 'acts' like sanctioned entity, not because it's on a list.

• Heuristic Clustering

- **Co-Spend Heuristic:** Multiple inputs in one transaction = same owner
- **Entity Clusters:** Collapse millions of addresses into single entities
- **Peeling Chains:** Detect laundering pattern (100s of wallets, small amounts)
- **Graph Shape Recognition:** AI trained on transaction graph patterns



Coinbase Innovation: Seq2Win treats blockchain transactions like NLP sentences, generating behavioral embeddings for addresses. Clustering in vector space identifies risky entities even without prior interaction - 'acts like' sanctioned address.

Revolut: Sherlock for Crypto

• Wealth Protection Interventions

- **Scam Detection:** AI flags 'likely scam' based on address age, graph, volume
- **'Break the Spell' Flow:** Forces pause, selfie, quiz before sending
- **Friction as Feature:** Breaks psychological control of pig butchering scams
- **Context Analysis:** High urgency + new beneficiary + high value = intervention

• AI-Driven User Protection

Revolut doesn't just block - it intervenes. If user attempts to send crypto to flagged address, app forces pause: 'Did someone on WhatsApp ask you to send this?' AI detects payment context, not just address itself.

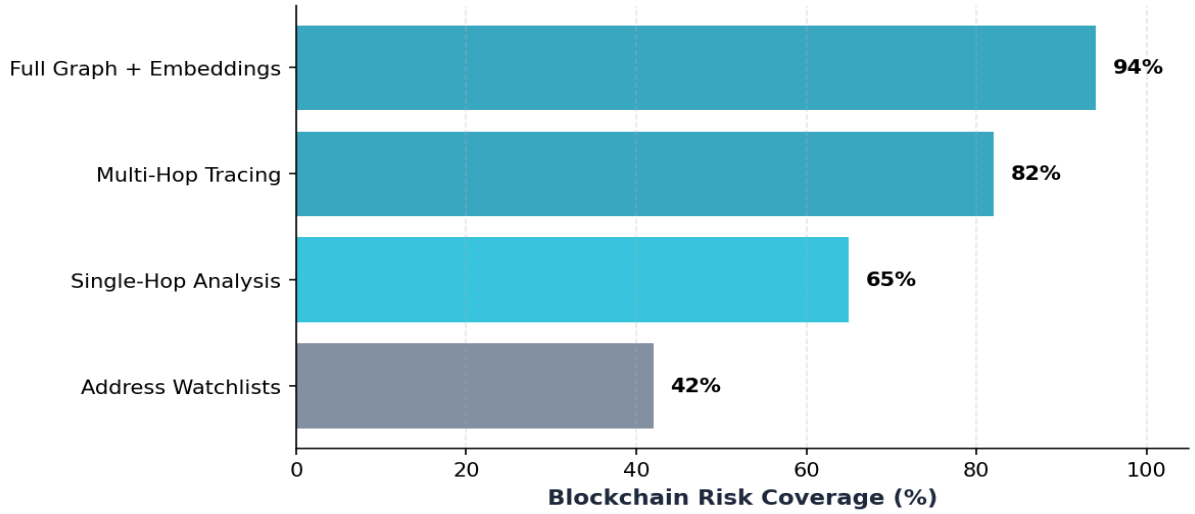
The Graph as Source of Truth

• Chainalysis Attribution Layer

- **Labeled Database:** Millions of addresses categorized (Exchange, Dark Market)
- **Transitive Risk:** Calculate exposure based on hop distance
- **Risk Exposure Score:** 3 hops from sanctioned entity = moderate risk
- **Granular Policies:** 'Block if <2 hops from ransomware, allow if >5 hops'

• Oracle Layer for Fintech

- Maps entire blockchain with attribution data
- Provides risk intelligence to exchanges, banks, fintechs
- Enables compliant crypto services for regulated institutions



Reputation Layer for Decentralized Web: On-Chain Intelligence proves you don't need identity to assess trustworthiness. Graph clustering + sequence modeling builds reputation system for pseudonymous blockchain addresses.

Strategic Implications

- **Perfect Data, Hidden Meaning:** Immutable blockchain, pseudonymous actors
- **Sequence Modeling:** NLP techniques applied to transaction patterns

- **Graph Clustering:** Entity resolution without names
- **Transitive Risk:** Calculate exposure through multi-hop connections
- **Regulatory Compliance:** AML controls for decentralized systems