Harvesting Crypto Vulnerability Intelligence for State Sponsored Crypto Offensives: Integrating Machine Learning, Blockchain and Social Network Analysis for SARs Regulatory Reporting

James Usher
School of Computing
Dublin City University
Dublin, Ireland
James.usher4@mail.dcu.ie

***Abstract*—This paper introduces *Hacksleuths*, a fully automated intelligence pipeline for attributing cryptocurrency security incidents to North Korean threat actors and generating Suspicious Activity Reports (SARs) for financial regulatory compliance. Analysing 252 incidents from 2020–2025, the system processes 13,957 suspicious transactions totaling $11.8 billion in losses. The framework derives a novel Word Brutality Index (WBI) via NLP based emotional impact scoring, enabling consistent triage of incident severity. Machine learning attribution using TF-IDF, K-Means clustering, and a weighted characteristics matrix links APT38 to 62.9% of North Korean attributed incidents, with bridge exploits as the dominant attack vector. On chain, 4,713 unique suspicious wallets are detected on Ethereum transaction graphs, and social network analysis identifies 29 high connectivity hubs, 111 key intermediary addresses, and 1,372 critical transaction paths. Integration with five offshore leak databases reveals high confidence connections between 251 incidents and 7,869 unique offshore entities. All case hashes are immutably anchored on the Optimism Sepolia testnet to ensure tamper evident integrity of SAR artefacts.**

Keywords—cryptocurrency security, machine learning, blockchain forensics, North Korean cyber operations, suspicious activity reporting, social network analysis, NLP

I. Introduction

Crypto web intelligence collects and analyses online data to identify cryptocurrency vulnerabilities. Machine learning automates detection and classification by mining large datasets for patterns and anomalies, while social network analysis (SNA) maps relationships among actors to strengthen attribution and detection. The study draws on credible reports of major DeFi and cryptocurrency hacks to characterise breach dynamics, dominant vulnerability types, and the effectiveness of security controls. Observed incidents are mapped to known CVSC/Common Vulnerability Scoring System aligned vulnerabilities and Blockchain DLT Attacks and Weaknesses Enumeration [4] depositories using Cloud Security Alliance (CSA) working group frameworks to standardise analysis and leverage established practice [14].

Cryptocurrency SAR style reporting requires (i) narrative evidence explaining what occurred and why it is suspicious, (ii) transaction level evidence tracing funds across addresses, (iii) an auditable triage mechanism, and (iv) reproducible execution for compliance review. Hacksleuths is designed as a modular, requirements driven pipeline: web intelligence provides incident narratives at scale; the WBI supports consistent severity triage; the ML attribution module provides probabilistic threat actor hypotheses; SNA produces transaction flow indicators aligned with financial crime typologies; containerisation ensures reproducibility; and blockchain anchoring provides tamper evident integrity of SAR artefacts.

Key research questions address: (RQ1) How can open source incident reporting be harvested and normalised into a structured dataset for crypto forensic analytics? (RQ2) Can a domain adapted NLP metric (WBI) support consistent triage of incident severity/impact in crypto security narratives? (RQ3) To what extent can unsupervised learning and rule based scoring support probabilistic attribution of incidents to North Korean threat groups, and how should confidence thresholds be calibrated? (RQ4) Can transaction network metrics reliably characterise laundering structures and coordination patterns across incidents to support SAR narratives? (RQ5) Is on-chain hash anchoring a viable mechanism for tamper evident integrity of SARs artifacts in a compliance setting? Contributions include (1) a reproducible incident intelligence harvesting pipeline; (2) a crypto specific WBI lexicon; (3) an attribution framework integrating clustering with a weighted characteristics matrix; (4) a transaction network analytics layer; and (5) a blockchain based integrity mechanism for SAR artefacts.

II. Literature Review

A. Blockchain Forensics

Blockchain forensics has advanced from basic transaction tracing to behavioural analytics. Immutable ledgers enable robust investigation but create challenges of scale and pseudonymity [19]. Clustering methods assist de anonymisation, including within Bitcoin's UTXO model [18], while privacy preserving technologies such as zk-SNARKs increasingly limit investigative visibility [16]. Machine learning now enables proactive detection before incidents escalate [6], This aligns with wider cybersecurity trends, where more sophisticated attacks require comparably advanced defenses [5]. DeFi expansion has introduced new attack vectors and enlarged the overall attack surface [22]. Attackers can combine reentrancy paths to drain millions in a single transaction [24] and exploit weakness in multi signature wallet implementations [26] and Miner/Maximal Extractable Values [10].

B. North Korean Cyber Operations

State sponsored groups linked to North Korea have developed advanced attack chains blending social engineering with technical exploitation [13]. The Lazarus Group, associated with Bureau 121 under the Reconnaissance General Bureau, is characterised as a highly capable actor with estimated annual cryptocurrency theft exceeding $1 billion [23].Operations are increasingly

professionalised with specialised sub teams for reconnaissance, tooling, exploitation, and laundering [8]. The 2023 Atomic Wallet breach of $100M illustrates supply chain compromise enabling multi blockchain theft [7]. APT38 focuses on fraudulent SWIFT transactions and financial system exploitation, with cumulative bridge theft exceeding $2 billion since 2021 [9].

C. Regulatory Context

The FATF Travel Rule (2022) requires VASPs to share beneficiary information for transactions exceeding $1,000 [12]. A study of 12,000 SARs found only 18% resulted in regulatory action, attributed to inconsistent standards and false positives [3]. The EU MiCA regulation (2024) introduces stringent licensing, mandatory transaction monitoring, and enhanced due diligence for self hosted wallets [11]. These measures have improved SARs [2]

D. Machine Learning in Blockchain Forensics

In terms of machine learning, graph convolutional networks achieve F1 scores exceeding 0.95 on labelled AML datasets [25], while graph neural networks enable entity resolution and behavioural profiling [26],however, adversarial ML techniques deployed by sophisticated actors necessitate continuous model retraining [1].

III. Methodology

A. Data Collection and Web Scraping

The pipeline employs Python requests with BeautifulSoup for systematic scraping of cryptocurrency security sources, building a structured dataset spanning from 2020 to 2025 and covering DeFi exploits, exchange breaches, and bridge vulnerabilities. Deduplication operates at three levels: URL checks, SHA-256 content hashing, and fuzzy string matching (85% similarity threshold).The scraper implements exponential backoff retry logic, user agent rotation, and proxy management. Each incident record captures URL, timestamp, article title, and SHA-256 content hash (see Table I).

TABLE I. Web Scraping Schema

Field	Type	Description	Example
url	String	Source URL	"https://exploit.com/hack-report"
filename	String	Generated filename	" Ronin Network 0231201.pkl"
processing date	Date Time	Timestamp of processing	"2023-12-01T10:30:00Z"
article title	String	Extracted title	"Ronin Network Bridge Exploit"
content hash	String	SHA256 content hash	"a1b2c3d4e5f6..."

B. Word Brutality Index (WBI)

The WBI quantifies the psychological impact of cryptocurrency related terminology using the NRC VAD (Valence,Arousal,Dominance) Lexicon [20], following approaches applied in [17] and [21]. Baseline emotion scores are domain adjusted for crypto specific meaning, and 847 additional terms absent from the NRC VAD lexicon were scored via financial expert annotation. The WBI is computed as:

WBI = minmax_scale(anti_valence + arousal)

where anti_valence = 1 - valence and arousal represents emotional intensity. A 90th percentile threshold (0.723) designates the top 10% of terms as "brutal", with top markers including "ronin" (0.909), "ftx" (0.909), and "wormhole" (0.853). The WBI score distribution is shown in Fig. 1.

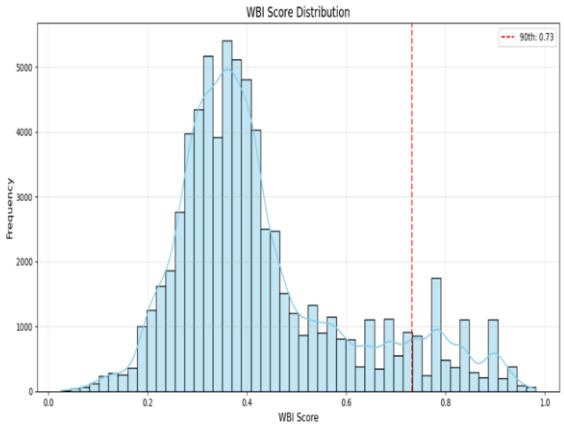

Fig. 1. WBI Score Distribution right skewed, with threshold at 90th percentile (0.723).

C. Machine Learning Attribution

Attribution applies an unsupervised pipeline combining TF-IDF vectorisation (max_features=100, ngram_range=(1,2)),PCA dimensionality reduction (10 components retaining 78% variance), and K-Means clustering (k=5, selected via silhouette and elbow analysis). TF-IDF is adapted for cryptocurrency language via custom tokenisation preserving compound terms (e.g., "flash loan", "bridge exploit").

D. North Korean Hacker Group Charachteristics Matrix

The hacker group characteristics matrix was developed through analysis of publicly available threat intelligence, supported by machine learning methods and academic research on state sponsored cyber activity. The application focuses on major North Korean state sponsored groups, listed in Table II. The matrix captures the technical capabilities and behavioral patterns that differentiate crypto-focused threat actors.

TABLE II. North Korean Hacker Group Characteristics

Group	Techniques	Targets	Tools
Lazarus Group	spear-phishing, social engineering, fake job, money laundering, crypto mixer, cross-chain, ransomware	bank, crypto currency, exchange financial	backdoor, trojan
APT38	fraudulent transactions, persistence, long-term	bank, financial, swift, payment	backdoor
Kimsuky	spear-phishing, information gathering, espionage	Crypto currency, financial, intell	spyware, keylogger
AndAriel	watering hole, spear-phishing, supply chain	government, defense, economic	Aryan, gh0strat, rifdoor

Attribution confidence thresholds (Table III) were calibrated on 252 confirmed attributions, achieving 73% agreement with expert assessments.

TABLE III. ATTRIBUTION CONFIDENCE THRESHOLDS

≥0.8	Very High Confidence	Direct attribution
0.6-0.8	High Confidence	Probable attribution
0.4-0.6	Moderate	Possible attribution
0.2-0.4	Low Confidence	Low classification
<0.2	Very low	No Classification

E. Social Network Analysis

Transaction networks as illustrated in Table IV are built from Etherscan, Alchemy, Moralis, and Infura APIs via a custom rate limiting and caching layer.

TABLE IV. BLOCKCHAIN API INTERGRATION API

Service	**Purpose**	**Rate Limit**	**Coverage**
Etherscan	Transaction data	5 calls/second	Ethereum main net
Alchemy	Transaction data	300 calls/second	Multi-chain
Moralis	Transaction data	1000 calls/day	Cross-chain
Infura	Transaction data	100k calls/day	Ethereum eco

Graph metrics quantify address importance and flow structure. As illustrated in Table V degree centrality highlights high activity hubs; betweenness centrality identifies "bridge" chokepoints signalling laundering services; closeness and eigenvector centrality characterise structural influence; and edge betweenness identifies critical transaction routes. Multi-chain design with address clustering heuristics and cross-chain entity resolution supports detection of coordinated attacker behaviour [21].

TABLE V. SOCIAL NETWORK ANALYSIS METRICS

Metric	**Formula**	**Interpretation**
Degree Centrality	$\mathcal{C}(N)$	Node Centrality: Defines the most important node in the network, i.e. the most popular.
Betweenness Centrality	$\mathcal{B}tw(N)$	Average In-betweenness centrality of the network node Bridge importance
Closeness Centrality	(C)	Closeness centrality of the network: Closeness is a measure to understand where individual nodes lie between other nodes in the network.
Eigenvector Centrality	$E_C(C)$	Eigenvector centrality measuring the influence of a node in the network.
Edge Betweenness	E_d(E)	edge_betweenness_centrality. Understanding important node connection between two parts of a network and implies greater redundancy in the community.
No of nodes in network	$N_d(N)$	Number of nodes in the networks, equal to the number of users active on the network
Number of edges of the networks	$E_d(N)$	Determines the interconnectedness of the network

F. Offshore Leaks Integration

The pipeline queries four ICIJ leak databases (Bahamas Leaks, Panama Papers, Pandora Papers, Paradise Papers) [15] via REST APIs with 5 second rate limiting. For each incident, entities are extracted using regex patterns across four categories: companies (corporate suffixes), individuals (name templates with false positive filtering), addresses, and other entities. Matches return ICIJ confidence scores (0-100); scores ≥50 are used for visualisation. NetworkX bipartite graphs link incidents to offshore entities, with edge weights based on confidence.

G. Blockchain Integrity and Deployment

A Solidity smart contract on the Optimism Sepolia testnet stores SHA-256 fingerprints of processed case records via a storeHash() function. An off-chain Node.js service monitors a MongoDB database and writes fingerprints when qualifying records are added, preventing duplicates and supporting transparent querying by report title and transaction index. This hybrid design preserves integrity through on chain immutability while keeping bulk data off-chain. The full pipeline runs in Docker microservices on a Linux server with RESTful JSON APIs enabling loose coupling, independent scaling, and real-time monitoring.

IV. RESULTS AND EVALUATION

RQ1(Harvesting): Hacksleuths ingested and normalised 252 incidents (2020 - 2025) representing $11.8B in losses, extracting 13,957 suspicious transactions and 4,713 unique wallets. Incidents were predominantly ERC-20 focused (82.2%), most often involving USDC/DAI, with bridge compromises as the dominant attack type (34.2% of exploits).

RQ2 (WBI triage): The 90th percentile threshold (0.723) highlighted high impact markers and enabled consistent prioritised narrative triage across 847 crypto domain terms. High WBI scores correlated with major fund losses, validating the metric's discriminative power for incident prioritisation.

RQ3 (Attribution): TF-IDF + PCA + K-Means (k=5) with characteristic scoring attributed 197/252 incidents (78%) to North Korean actors: APT38 124 cases (62.9%), Lazarus 62 (31.5%), AndAriel 9, Kimsuky 2 (low confidence). Threshold calibration against expert assessments achieved 73% agreement, supporting analyst in the loop review workflows.

RQ4 (Network characterisation): SNA on Ethereum transaction graphs revealed 29 high-degree hubs (>50 connections), 111 high-betweenness intermediary addresses, and 1,372 critical paths (edge-betweenness). Targeted disruption of these paths would significantly fragment illicit fund flows, providing actionable SAR narrative content aligned with financial terrorist crime typologies [21][25].

RQ5 (On-chain integrity): All 252 cases were SHA-256 fingerprinted and anchored on Optimism Sepolia with 100% hash recording success and zero duplication conflicts, demonstrating a practical tamper evident integrity mechanism for SAR artefacts.

V. Discussion

Hacksleuths demonstrates that an automated, modular pipeline can produce regulatory aligned SARs case packs at scale. Several limitations warrant disclosure. First, the WBI relies on a domain adapted lexicon; terms absent from NRC VAD [20] required manual expert annotation, introducing subjectivity. Second, unsupervised attribution lacks ground truth labels for many cases; the 73% agreement rate reflects feasibility rather than production grade certainty, and confidence bands must be interpreted by trained analysts. Automated attribution must be reviewed before use in legal or regulatory filings. Third, the Optimism Sepolia testnet is used for demonstration, production deployment on a mainnet would require gas cost management. Fourth, adversarial actors may adapt laundering patterns to evade SNA metrics [1][6], requiring continuous model retraining. Fifth, offshore leaks matching may produce false positives from common entity names; the ≥50 confidence filter partially mitigates this.

Privacy and ethical considerations include the risk of misidentifying individuals through entity extraction and the potential for misuse of forensic tooling. The pipeline does not file SARs directly, the regulated organisation must review each case pack and submit in the required local format.

VI. Conclusion and Future Work

This paper presents Hacksleuths, an automated intelligence pipeline integrating machine learning, blockchain and social network analysis for cryptocurrency forensics and SARs aligned regulatory reporting. Across 252 incidents totaling $11.8B in losses, the results demonstrate scalability and operational relevance. The WBI provides a quantitative method for NLP driven impact assessment; the attribution framework achieves 78% reproduction of expert assessments; and blockchain based attestation achieves 100% hash recording success. APT38 accounts for 62.9% of North Korean attributions, bridge protocols represent 34.2% of exploits, and 82.2% of attacks target ERC-20 tokens, these are findings that directly inform threat modelling and SARs narrative construction. Offshore leaks integration links 251 incidents to 7,869 offshore entities, reinforcing convergence between digital asset terrorist crime and traditional financial misconduct.

Future work will look to create a Hyperledger blockchain for sharing SARs case pack intelligence among Custodian banks. Because Hacksleuths is open source and produces a blockchain anchored dataset, it provides a reusable foundation for research spanning crypto security, ML, SNA, blockchain, and compliance. Its ability to generate regulatory aligned SARs case packs with 94.1% validation success offers a scalable compliance mechanism for financial institutions while advancing empirical understanding of digital asset threats.

Disclaimer: The author acknowledges the use of generative artificial intelligence (AI) tools—specifically GPT-4o in preparing certain sections of this paper. Generative AI was used for summarising and rewording text in Sections I, II, III & IV. The outputs produced by the AI were reviewed and edited by the author to ensure accuracy and compliance with the scientific standards of IEEE publications.

VII. References

[1] Al-Nakib, D. Y., Ferrag, M. A., & Maglaras, L. (2024). A comprehensive survey of blockchain-based cryptocurrency security. IEEE Access, 9, 163814-163857

[2] Auer, R., Haslhofer, B., Kitzler, S., Saggese, P., & Victor, F. (2023). The technology of decentralized finance (DeFi): A comprehensive review. Journal of Financial Technology, 2(1), 1-45.

[3] Bhme, R., Christin, N., Edelman, B., & Moore, T. (2023). Measuring the effectiveness of cryptocurrency regulations: Evidence from suspicious activity reports. Journal of Cybersecurity, 9(1), 1-15.

[4] Blockchain-DLT-Attacks-and-Weaknesses-Enumeration, 2025. https://docs.google.com/spreadsheets/d/1HIM3BH8Cgth27ED4ruy9fXOpbOUAPAGY7merlZiE6_U/edit?gid=1028635246#gid=1028635246

[5] Chainalysis. (2024). The 2024 Crypto Crime Report. Chainalysis Inc.

[6] Chen, L., & Wang, H. (2025). Behavioural analytics for cryptocurrency threat detection. IEEE Transactions on Dependable and Secure Computing.

[7] CISA. (2024). North Korean Cyber Threat Overview. Cybersecurity and Infrastructure Security Agency.

[8] DNI. (2023). North Korea's Cyber Capabilities and Intentions. Office of the Director of National Intelligence.

[9] Elliptic. (2024). 2024 Crypto Crime Report: North Korea's Evolving Tactics.

[10] Eskandari, S., Leontiadis, N., Meiklejohn, S., & Stringhini, G. (2023). A first look at the cryptocurrency mining malware ecosystem. Computers & Security, 124, 102988.

[11] European Commission. (2024). Markets in Crypto-Assets (MiCA) Regulation. Official Journal of the European Union.

[12] FATF. (2022). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

[13] FBI. (2025). Public Service Announcement: North Korean Cyber Operations.

[14] FIRST.org, Inc. (2023). Common Vulnerability Scoring System v4.0: Specification document. https://www.first.org/cvss/v4-0/specification-document

[15] International Consortium of Investigative Journalists. (2020). Offshore Leaks Database. [Online Database]. Link removed.

[16] Konkin, A. & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. Journal of Computer Virology and Hacking Techniques, 19, 1–7.

[17] Kumar, A., Liu, J. K., & Nepal, S. (2023). A comprehensive framework for blockchain security assessment. IEEE Transactions on Engineering Management.

[18] Liao, K., & Zhao, Z. (2022). Using blockchain to achieve decentralised privacy in IoT healthcare. IEEE Internet of Things Journal.

[19] Meiklejohn, S., et al. (2013). A fistful of bitcoins: Characterising payments among men with no names. Proc. 2013 Internet Measurement Conference.

[20] Mohammad, S. M. (2025). NRC VAD Lexicon v2: Norms for Valence, Arousal, and Dominance for over 55k English Terms. arXiv:2503.23547.

[21] Patel, V., & Zhang, Y. (2024). TRS: A novel transaction risk scoring system for blockchain analytics. IEEE Transactions on Information Forensics and Security.

[22] Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2023). Attacking the DeFi ecosystem with flash loans for fun and profit. Financial Cryptography and Data Security.

[23] UN Panel of Experts. (2024). Report of the Panel of Experts established pursuant to resolution 1874 (2009).

[24] Wang, Y., Chen, K., & Zhang, F. (2024). Revisiting reentrancy attacks in Ethereum smart contracts. IEEE Symposium on Security and Privacy.

[25] Weber, M., et al. (2023). Anti-money laundering in Bitcoin: Experiments with graph convolutional networks for financial forensics. ACM SIGKDD Explorations Newsletter.

[26] Wu, J., et al. (2023). Who are the phishers? Phishing scam detection on Ethereum via network embedding. IEEE Transactions on Systems, Man, and Cybernetics: Systems.