Vision Paper: CERTHTRACE - Transforming Cryptocurrency-Facilitated Crime Investigation through Explainable, Hybrid Intelligence

Eleftheria Katsoura, Georgios Stavropoulos, Konstantinos Votis

Information Technologies Institute (ITI), Centre for Research and Technology Hellas (CERTH), Thessaloniki, Greece
{el_katsoura, stavrop, kvotis}@iti.gr

***Abstract*—The increasing sophistication of cryptocurrency-facilitated crime has created an urgent demand for analytical systems that combine technological depth with human interpretability. Existing blockchain forensic tools, while effective in data aggregation and visualisation, often function as opaque systems with limited explainability, narrow currency coverage, and weak integration with other investigative domains. This vision paper presents CERTHTRACE, a forward-looking framework designed to evolve current cryptocurrency analysis capabilities into an explainable, multimodal, and hybrid-intelligence environment for law-enforcement agencies. CERTHTRACE envisions the fusion of blockchain analytics, graph neural networks, and natural-language-enabled AI co-pilots into a transparent investigation ecosystem that connects cyber and physical evidence within the emerging European Anti-CFCT ecosystem envisioned by the CRYPTOACTION project. The paper outlines the conceptual architecture, guiding research directions, and anticipated impact of CERTHTRACE as a next-generation, trustworthy AI environment for cryptocurrency forensics.**

***Index Terms*—Cryptocurrency forensics, Blockchain analytics, Hybrid intelligence, Anti-money laundering, CFCT (Cryptocurrency-Facilitated Crime and Terrorism)**

I. Introduction

The rapid expansion of cryptocurrencies has transformed global finance, enabling borderless transactions and new decentralised economic models. Yet, the same characteristics that drive innovation—pseudonymity, decentralisation, and global reach—have also turned cryptocurrencies into potent enablers of illicit activity. Criminal networks now exploit these systems for money laundering, ransomware operations, terrorism financing, and trafficking, often combining blockchain-based transactions with off-chain infrastructures such as darknet markets, social platforms, and decentralised finance (DeFi) protocols.

For law-enforcement agencies (LEAs), investigating these cryptocurrency-facilitated crimes and terrorism (CFCT) presents growing operational and analytical complexity. Offenders continuously adapt, employing privacy-enhancing coins, mixing services, and cross-chain bridges to obscure transactional trails. While investigators rely on blockchain analysis tools to follow these digital traces, current forensic systems remain constrained by three critical limitations: lack of algorithmic transparency, incomplete coverage of privacy-enhanced protocols, and insufficient integration with off-chain intelligence sources.

CERTHTRACE aims to bridge this divide by advancing toward a transparent, multimodal, and explainable investigation framework. We envision a next-generation environment where human expertise and artificial intelligence converge in a hybrid-intelligence setting. By integrating blockchain analytics with graph-based reasoning, natural-language-enabled co-pilots, and diverse intelligence sources, the framework aspires to transform cryptocurrency forensics into a truly interpretable process—one that seamlessly connects on-chain transactions with physical-world evidence.

This vision raises two fundamental research questions: First, can multimodal data fusion—combining blockchain, open-source, and cyber-threat intelligence—reveal hidden patterns across complex transactional ecosystems that single-source analysis cannot detect? Second, can explainable, human-in-the-loop AI enhance investigator trust, reproducibility, and evidential credibility in LEA operations while maintaining the analytical depth required for complex investigations?

This paper outlines the conceptual trajectory of CERTHTRACE. Section II reviews current cryptocurrency forensic systems and their limitations. Section III presents the CERTHTRACE vision and proposed technical approach. Section IV highlights representative application scenarios, and Section V concludes with expected research challenges and anticipated impact within the European Anti-CFCT ecosystem.

II. Current Cryptocurrency Forensic Systems and Limitations

Over the past decade, cryptocurrency forensics has matured into a commercial ecosystem of investigation platforms (e.g., Chainalysis, Elliptic, TRM Labs) that provide clustering, attribution, and risk scoring for major blockchains. While these tools have improved situational awareness for investigators, the rapidly expanding volume and structural complexity of blockchain ecosystems—spanning multiple chains, privacy layers, and DeFi protocols—have outpaced the evolution of forensic methodologies. Moreover, their proprietary architectures and undisclosed heuristics limit methodological trans-

parency and reproducibility—constraints that become pressing in evidentiary contexts.

In parallel, academic work has rigorously characterised on-chain behaviour and illicit use, establishing baselines for transparent analysis. For Bitcoin, early transaction-network studies mapped address typologies and flows at scale [1], and macro-economic analyses quantified the prevalence of illegal activity within cryptocurrency transactions [2]. Subsequent methods advanced anomaly and fraud detection [3], functional/behavioural address classification [4], and supervised or graph-based illicit account detection on Ethereum [5]–[7], supported by labelled datasets and benchmarks like in [8].

Alongside commercial platforms, open-source frameworks such as BlockSci [9] and GraphSense [10] have provided transparent, research-oriented alternatives for blockchain analysis. However, the maintenance challenges facing these community-driven projects—both are now effectively archived rather than actively developed—illustrate a broader sustainability gap in cryptocurrency forensics. As blockchain ecosystems evolve rapidly in scale and complexity, the absence of continuously maintained, transparent analytical infrastructure leaves investigators dependent on proprietary systems or aging research prototypes.

Despite this progress, critical practical gaps persist for operational investigations:

(i) Limited coverage of obfuscation and privacy technologies. Techniques such as mixers, peeling chains, and privacy-preserving ledgers reduce traceability, and their sophistication grows as blockchain ecosystems scale. Empirically, large-scale dark-web measurements illustrate both the prominence of Bitcoin in underground markets and the analytic difficulty posed by privacy coins. In a 15-month crawl (27.7M pages), Lee et al. extracted 10M unique crypto addresses and found that over 80% of Bitcoin addresses appearing on the dark web were used with malicious intent, with flows largely cashing out to popular exchanges [11]. By contrast, most candidate Monero strings were invalid or unverifiable due to privacy properties, leaving only 61 addresses after filtering—underscoring the challenge of analysing privacy-enhanced assets at scale. Related research on transaction-graph learning and multi-graph methods suggests directions to reason over obfuscation and complex transaction patterns, but these remain primarily research-prototype capabilities rather than routinely available features of operational platforms [7], [12], [13].

(ii) Fragmented coverage of DeFi, DEXs, and cross-chain activity. Illicit behaviour increasingly spans smart contracts, token transfers, and bridge/DEX pathways that are not uniformly parsed by today's tools. Studies have shown the feasibility of classifying smart-contract behaviours and Ethereum account risk from transactional properties [5], [6], [14], but comprehensive, explainable, and cross-chain DeFi analytics are still emergent in practice.

(iii) Explainability and investigator-centred transparency. Many ML-driven approaches in the literature optimise predictive performance while offering limited insight into why a wallet, cluster, or flow is flagged. For investigators and courts, interpretable rationales (e.g., salient features, temporal motifs, counterfactual traces) are essential for trust and admissibility—yet most operational systems expose risk labels without sufficient explanatory context.

Together, these observations motivate next-generation, transparent and modular analysis environments that (a) extend native support to privacy-enhanced and multi-chain ecosystems, (b) incorporate DeFi/DEX/bridge semantics, and (c) embed explainability for human-in-the-loop use—bridging the demonstrated strengths of the research literature with the demands of real-world investigations.

CERTHTRACE is proposed precisely to address this convergent set of challenges. Unlike commercial platforms that prioritize breadth of coverage within closed architectures, or open-source tools that offer transparency but lack sustained maintenance and multimodal integration, CERTHTRACE envisions a continuously maintained, explainable, and interoperable framework. It distinguishes itself through three core commitments: (1) native explainability as a design principle rather than a post-hoc addition, ensuring every analytical output includes interpretable rationales suitable for judicial contexts; (2) hybrid intelligence architecture that positions AI as an investigator co-pilot rather than a replacement, preserving human agency while augmenting analytical capacity; and (3) multimodal evidence fusion that transcends blockchain-only analysis to correlate on-chain transactions with cyber and physical intelligence

III. The CERTHTRACE Vision and Proposed Approach

A. Conceptual Overview

CERTHTRACE envisions a new generation of explainable, multimodal, and hybrid-intelligence solutions for investigating cryptocurrency-facilitated crime. The tool represents an evolution of CERTH's blockchain forensic systems, re-engineered to ensure transparency, interoperability, and alignment with European principles of trustworthy AI.

At its core, CERTHTRACE integrates three complementary dimensions:

1) Multimodal blockchain forensics, capable of analysing heterogeneous evidence spanning multiple blockchains, decentralised finance (DeFi) ecosystems, and off-chain intelligence sources;
2) Explainable and human-centric artificial intelligence, designed to support, not replace, the investigator, offering interpretable insights into model reasoning;
3) Hybrid and collaborative intelligence, where human expertise, machine learning, and natural-language-enabled co-pilots interact seamlessly in a transparent environment.

Through this integration, CERTHTRACE aims to move beyond isolated analytics toward a unified evidence-correlation framework—linking blockchain, cyber, and physical data into coherent narratives of criminal activity. This vision positions the framework not merely as an analytical tool, but as an

investigative ecosystem where technological capability and human expertise converge.

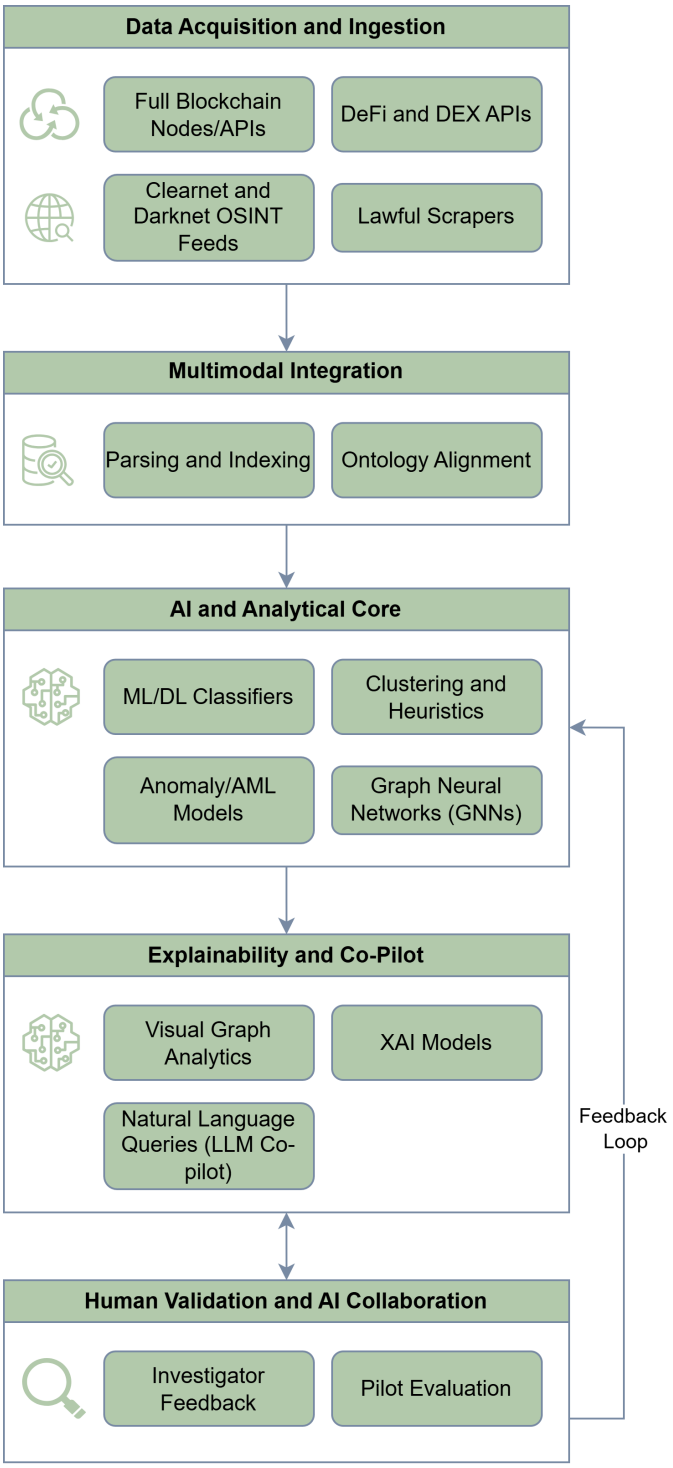


Fig. 1. Conceptual architecture and data flow of CERTHTRACE, illustrating the progression from multimodal data acquisition through AI reasoning to human-interpretable insights and validation.

B. From Requirements to Architecture

The conceptual foundation of CERTHTRACE rests on a rigorous analysis of operational requirements provided by law-enforcement agencies (LEAs) and domain experts. This requirement-gathering process begins with a systematic review of cryptocurrency-facilitated crime modus operandi, examining how offenders exploit darknet marketplaces, social-media-enabled schemes, and DeFi environments. By characterising these criminal patterns—including their data-gathering sources, typologies, and evasion techniques—the initial research phase establishes an empirical baseline that grounds subsequent technical development in observed criminal behaviour rather than abstract capability.

This criminological foundation, conducted in collaboration with investigative practitioners, enables the identification of recurring investigative gaps: limited visibility across privacy-enhanced assets, fragmented monitoring of DeFi environments, insufficient transparency in AI reasoning, and weak integration between blockchain analytics and broader investigative intelligence. The translation from observed crime patterns to technical requirements follows a structured methodology: each identified modus operandi is mapped to analytical capabilities (e.g., mixer detection, cross-chain tracing, smart-contract assessment), which in turn define data-source needs, algorithm priorities, and explainability requirements.

These requirements guide the envisioned system architecture, defining data sources, interoperability needs, and design priorities for explainability and usability. CERTHTRACE follows a modular architecture (Figure 1), structured around five conceptual layers that together form a continuous analytical workflow—from raw data acquisition through multimodal integration and AI-driven reasoning to human-interpretable insights and investigator-in-the-loop validation.

The architectural approach emphasises modularity and openness: analytical components will expose standardised APIs and share data models to enable future interoperability with other investigative systems, compliance with emerging European Anti-CFCT infrastructure standards, and integration within federated data spaces. This commitment to interoperability reflects a broader vision in which CERTHTRACE operates not as a standalone platform, but as a contributing service within a collaborative ecosystem of law-enforcement tools.

C. Multimodal AI Core: Blockchain Analytics and Cross-Domain Intelligence Fusion

The envisioned AI backbone of CERTHTRACE integrates cryptocurrency-specific analytics with broader multimodal intelligence capabilities, forming a unified analytical core that can process heterogeneous evidence streams. Blockchain and DeFi Analytics. CERTHTRACE will combine native blockchain parsing, DeFi data ingestion, and cross-chain intelligence synthesis. The framework is designed to process transactional data from major cryptocurrencies (Bitcoin, Ethereum), with research directions exploring expanded coverage of privacy-oriented networks (Monero, Zcash, Dash),

smart-contract activity, token transfers, and decentralised-exchange (DEX) operations. Implementation will leverage full blockchain nodes, indexers, and APIs—selected during development to balance coverage, performance, and LEA-specific requirements.

The analytical approach will explore multiple methodologies to identify optimal techniques for different investigative contexts. Machine- and deep-learning models—including classification algorithms, clustering methods, and graph neural networks (GNNs)—will be investigated for their capacity to characterise addresses and entities into behavioural categories (exchange, mixer, ransomware operator, illicit marketplace) and generate behavioural profiles supporting risk scoring and flow tracing. Entity recognition and clustering techniques will be examined for their ability to group related addresses and reconstruct organisational structures within transactional networks.

Experimental work will assess anomaly-detection and anti-money-laundering (AML) algorithms for identifying suspicious transaction typologies, while dedicated research modules will explore methods for analysing privacy-enhancing techniques—including mixing, tumbling, and peeling—to quantify their impact on traceability and develop model-based linking heuristics that correlate obscured transactions.

A complementary research direction will examine DeFi-forensics methodologies, exploring techniques to assess smart-contract logic, tokenised transactions, and DeFi service interactions (escrow mechanisms, DEXs, cross-chain bridges) for detecting manipulation, vulnerability exploitation, or laundering routes. Token market manipulation detection will be investigated, building on established academic approaches. The selection and refinement of these methods will be guided by empirical evaluation and LEA feedback, ensuring that adopted techniques align with operational requirements. All experimental components will incorporate explainability considerations from the outset, with the goal of ensuring that classification decisions and risk assessments can be accompanied by interpretable rationales.

To ensure interoperability across the broader Anti-CFCT ecosystem, analytical services will be designed to comply with emerging technical standards, enabling seamless integration with complementary investigative tools and shared data infrastructure.

Multimodal Intelligence Integration. Beyond blockchain data, CERTHTRACE will integrate open-source AI algorithms for processing unstructured text, speech, and visual content—critical for investigations that span multimedia evidence.

The text-processing pipeline will combine traditional Natural-Language Understanding (NLU) techniques with large language model (LLM) technologies. NLU methods will transform unstructured sources such as darknet advertisements, chat transcripts, or forum discussions into structured ontologies, identifying semantic entities (actors, locations, cryptocurrency addresses) and events related to illicit activities. This process includes detecting suspicious dialogues, extracting embedded cryptocurrency identifiers, and analysing linguistic patterns indicative of criminal coordination or market activity. Building upon this foundation, LLM-based services—hosted as GPU/NPU-accelerable modules accessible via standardised APIs—will support higher-order tasks such as automatic curation of scraped content, enhanced precision in marking texts as CFCT-related, translation to investigators' working languages, and summarisation of analytical findings. This layered approach aims to reduce cognitive load and accelerate investigative workflows while maintaining interpretability.

Visual-analysis modules will employ deep neural networks for object recognition and concept detection, enabling automated categorisation of digital media relevant to criminal investigations. These capabilities are intended to enrich blockchain evidence with contextual information drawn from visual content associated with criminal activity. These multimodal capabilities are not envisioned as standalone features but as integrated analytical layers that can correlate findings across data types—linking, for example, cryptocurrency addresses mentioned in textual sources with transactional patterns observed on-chain.

CERTHTRACE will adopt a modular fusion approach in which each evidence type is processed by specialised models optimised for its modality—for example, blockchain graph classifiers and clustering methods for transactional data, LLM-based NLU components for text intelligence, and deep-vision models for visual media. Rather than forcing all inputs into a single model, their outputs will be normalised into a shared representation layer containing entities, relationships, risk indicators, and behavioural features. Fusion will initially take place at this structured-knowledge level, enabling cross-domain reasoning without sacrificing explainability. This design allows investigators to trace how each modality contributes to an analytical result, while leaving open the possibility of exploring deeper joint-embedding or early-fusion techniques as part of future research. The resulting unified representation naturally feeds into the graph-based evidence correlation layer described in the next subsection.

All AI services will be designed with transparent parameterisation, respecting data management principles and enabling investigators to understand and control model behaviour.

D. Graph-Based Evidence Correlation and Explainable AI

Cyber-Physical and Inter-Incident Correlation: Building upon the blockchain analytics and multimodal AI capabilities described above, a central research component of CERTHTRACE is the construction of composite evidence graphs that link on-chain cryptocurrency transactions with off-chain intelligence—including open-source information, cyber-threat intelligence, and contextual data from investigative workflows. This capability aims to reveal connections that remain hidden when evidence sources are analysed in isolation, supporting criminal network reconstruction and the identification of patterns spanning multiple incidents or jurisdictions.

Evidence graphs in CERTHTRACE are constructed by combining on-chain and off-chain intelligence into a unified heterogeneous graph schema. Nodes represent semanti-

cally distinct entities—including individual addresses, clustered wallet entities, smart contracts, infrastructure services (e.g., exchanges, mixers), darknet actors, and contextual entities extracted from OSINT or CTI sources. Edges encode relationships such as direct transactions, shared ownership inferred through clustering, temporal co-occurrence, reuse of infrastructure, or semantic links extracted from text (e.g., "forum post mentions address X"). Graph construction does not require a fixed modality: blockchain-only investigations produce address–transaction graphs, while multimodal cases incorporate additional node and edge types without altering the overall structure. Different application scenarios therefore populate the same schema with different evidence sources rather than requiring separate graph designs, enabling GNNs to perform node-level, edge-level, and subgraph reasoning across cases with varying degrees of multimodality.

In CERTHTRACE, cyber-physical correlation refers to linking blockchain and digital intelligence with real-world investigative artefacts. "Physical" assets include individuals, organisations, seized devices (e.g., phones, USB wallets), postal shipments, weapon or drug parcels, IP/hosting infrastructure tied to physical operators, and geolocated events such as arrests or controlled deliveries. These entities appear in the evidence graph as nodes enriched with attributes collected from law-enforcement reports, darknet marketplace listings, OSINT sources, or investigative case files. Correlating cyber traces (wallet flows, smart-contract interactions, threat-actor aliases) with physical-world entities enables investigators to move beyond purely on-chain attribution and reconstruct end-to-end criminal activity that connects digital transactions with real-world actors, assets, and events.

The approach builds upon Graph Neural Network (GNN) architectures capable of integrating heterogeneous datasets, detecting critical nodes, and predicting hidden relationships between wallets, actors, and events. These GNN-based methods will operate over the behavioural profiles, entity classifications, and anomaly signals generated by the analytical modules, contextualising blockchain findings within broader investigative intelligence. Planned analytics include node-level classification and regression to characterise entities, edge-level link prediction and correlation to describe connections, and hierarchical scoring algorithms to map multi-level interrelations—essential for understanding network structures and their evolution over time.

Machine-learning clustering methods will identify complex correlations and latent structures within these evidence graphs. The correlation component will be developed as an interoperable external service with a web API, designed to integrate seamlessly across multiple investigative tools and connect with complementary data sources—with architectural provision for future integration with systems such as Know Your Customer (KYC) repositories and other lawfully accessible intelligence sources—without duplicating existing functionality. Rather than replacing LEA systems, the service will enable diverse intelligence outputs to inform and enrich blockchain investigations, creating a unified analytical narrative.

This cross-domain correlation represents a shift from single-source analytics toward a federated intelligence model, where digital traces converge with broader investigative evidence within a shared framework.

Explainability and Generative Co-Piloting: The analytical capabilities described above—from blockchain classification to multimodal intelligence to graph-based correlation—generate complex outputs that require transparent interpretation. Explainability is therefore treated not as an auxiliary feature but as a first-class design principle throughout CERTHTRACE. Model outputs—whether classification decisions, anomaly detections, or graph-based correlations—will include interpretable rationales that identify the features, entities, temporal relations, or transactional patterns driving each prediction. For graph analytics specifically, explanations will highlight which nodes, edges, or subgraph structures contributed to correlation findings, enabling investigators to trace the reasoning behind network reconstructions. This transparency is intended to enable investigators to understand, verify, and communicate AI-assisted findings, strengthening both trust and judicial reliability.

Beyond static explanations, CERTHTRACE will explore AI-driven co-piloting as an emerging form of human–machine collaboration. By employing large language models and generative AI, investigators will interact with blockchain data, analytical results, and evidence graphs through natural-language interfaces. Queries such as "explain why this cluster is flagged as suspicious," "summarise transactions linking these two wallets," or "what connections exist between these entities across multiple incidents" will receive contextualised, interpretable responses drawing on both structured blockchain data and unstructured intelligence. This conversational interface aims to make complex analytical outputs—including multi-hop graph correlations and cross-domain evidence links—more accessible to investigators without requiring deep technical expertise.

The co-pilot functionality is envisioned primarily in reactive mode: responding to investigator requests for summaries, explanations, or analytical guidance. Research will explore whether proactive features—such as suggesting potential next analytical steps based on current findings—can enhance investigative workflows without compromising user control or introducing unwanted automation. This capability aims to reduce manual effort, accelerate hypothesis generation, and support iterative investigative reasoning while ensuring that investigators retain full agency over analytical direction.

Later research will assess collaborative and multi-user scenarios in which multiple analysts work concurrently on shared cases, coordinated by AI that tracks investigative state, suggests task allocation, and highlights emerging cross-analyst insights—a step toward distributed, swarm-intelligence-inspired workflows. All co-piloting developments will prioritise transparency, user control, and ethical safeguards, ensuring that automation enhances rather than substitutes human judgement and that investigators retain agency over investigative decisions. The combination of explainable outputs and conversa-

tional AI interfaces seeks to transform cryptocurrency forensics from an opaque, tool-driven process into a transparent, investigator-centred collaboration between human expertise and artificial intelligence.

E. Validation and Iterative Refinement

The validation of CERTHTRACE will follow a living-lab methodology, ensuring that the system evolves through continuous practitioner feedback rather than one-off evaluation. This iterative co-design process will involve law-enforcement officers, analysts, judicial representatives, and technical partners throughout development. The methodology combines stakeholder co-design from early requirement-definition through prototype assessment, progressive pilot evaluations moving from simulated datasets to near-operational case studies, and regular practitioner workshops that serve both as training and structured feedback mechanisms. Validation will draw on curated datasets—including labelled transaction graphs and synthetic criminal scenarios—assessing not only predictive accuracy but also interpretability, reduction of investigative effort, and alignment with legal and ethical requirements. Results from each validation phase will inform iterative refinement, closing the feedback loop between design, testing, and deployment. This approach seeks to build trust and accountability, demonstrating that explainable, hybrid-intelligence frameworks can be effectively adopted in real-world cryptocurrency-forensics workflows. The living-lab methodology reflects a commitment to co-creation, recognising that success depends as much on human confidence and institutional acceptance as on technical capability.

IV. Application Scenarios

To illustrate the directions in which CERTHTRACE could evolve, several representative scenarios are considered. They do not describe implemented capabilities but rather outline potential research paths where explainable, multimodal, and hybrid-intelligence methods may enhance cryptocurrency-forensic practice.

A. Multi-Chain Money Laundering and Obfuscation

Money laundering constitutes a critical process across most cryptocurrency-enabled crimes, as offenders seek to conceal illicit proceeds and reintegrate them into the legitimate economy. Modern laundering schemes exploit the cryptocurrency ecosystem's complexity, employing multi-chain hopping, exchange services, mixers and tumblers, the CoinJoin protocol, and peeling patterns to obscure fund origins and complicate transactional trails.

CERTHTRACE research will examine how graph-based analytics, behavioural clustering, and privacy-technique analysis can assist investigators in mapping these multi-stage laundering routes. The framework's cross-chain intelligence capabilities and model-based linking heuristics will be tested against obfuscated transaction patterns, exploring whether behavioural profiling can highlight unusual structural signatures indicative of laundering typologies. Graph neural networks will be assessed for their capacity to detect critical nodes and predict hidden relationships within complex laundering networks, while explainable outputs will enable analysts to understand why certain flows trigger suspicion and support informed investigative decisions. Rather than guaranteeing full asset recovery, this research aims to provide stronger analytical transparency and earlier detection of laundering patterns.

B. Ransomware Payments and Cybercrime-as-a-Service Ecosystems

Ransomware operations—ranging from high-value extortion campaigns against critical infrastructure operators to distributed attack models leveraging service-based ransomware platforms—have emerged as a significant threat to societal and economic stability. Perpetrators employ increasingly sophisticated obfuscation techniques to impede payment tracing and channel proceeds through privacy-preserving mechanisms.

CERTHTRACE will be used experimentally to study how transaction-graph learning and inter-incident correlation can connect ransom payments with clusters of related wallets, infrastructure services, or operational patterns. Research will explore whether combining blockchain traces with cyber-threat intelligence feeds and dark-web monitoring can reveal cybercrime-as-a-service ecosystems where malicious tools are rented or sold. The cyber-physical correlation component will be assessed for its ability to link cryptocurrency flows with broader cybercrime infrastructure, while the co-pilot interface will be tested for supporting hypothesis generation about operational relationships. The emphasis will remain on generating investigative leads and correlation cues rather than definitive attribution.

C. Fraud, DeFi Manipulation, and Illicit Marketplace Activity

A third research direction addresses deceptive financial schemes, decentralized finance exploitation, and clandestine marketplace operations. These activities leverage blockchain pseudonymity and distributed infrastructure to perpetrate victim deception, enable prohibited commerce (including narcotics, weaponry, and counterfeit goods), and evade regulatory oversight.

Work in this area will test anomaly-detection methods and smart-contract assessment techniques to reveal irregularities in DeFi projects or token markets. The framework's multimodal capabilities—including NLU for analysing darknet marketplace listings and forum discussions, and visual analysis for processing associated media—will be explored for their capacity to surface early fraud indicators. Research will assess whether combining on-chain transaction analysis with dark-web crawling and marketplace metadata can highlight trafficking networks or identify coordinated fraud operations. Pilot studies will also examine terrorism-financing detection, evaluating whether correlating blockchain patterns with open-source signals and social-media monitoring provides actionable investigative leads.

All experimental efforts will be accompanied by critical assessment of detection reliability, false-positive rates, pro-

portionality of methods, and ethical implications, ensuring that research advances are grounded in realistic operational constraints.

V. Conclusion

The vision outlined in this paper positions CERTHTRACE as a step toward more transparent, explainable, and human-centred cryptocurrency-forensic capabilities. Development is envisioned to progress incrementally—from focused blockchain analytics toward broader cross-chain intelligence—while investigating whether explainability and hybrid human–AI collaboration can enhance investigator understanding and confidence in analytical outcomes. Realizing this vision presents substantial research challenges. Privacy-enhanced cryptocurrencies and obfuscation techniques pose analytical difficulties requiring methodological innovation. Integrating heterogeneous data sources while maintaining evidential integrity and respecting legal constraints presents technical and procedural complexity. Ensuring explainable AI outputs meet judicial standards will demand interdisciplinary work bridging machine learning, legal considerations, and operational practice. Establishing trust within law-enforcement communities will depend on demonstrating reliability and alignment with institutional values through iterative validation and co-design. This vision is deliberately ambitious, reflecting a conviction that addressing the complexity of cryptocurrency-enabled crime requires equally sophisticated responses—responses that do not sacrifice transparency for capability, nor substitute algorithmic outputs for human judgement. By contributing to an interoperable European Anti-CFCT ecosystem and setting high standards for explainability and ethical alignment, CERTHTRACE seeks to demonstrate that effective cryptocurrency investigation and trustworthy, human-centred AI are not opposing goals but complementary imperatives—advancing both the capability and the accountability of law enforcement in confronting cryptocurrency-facilitated crime.

Acknowledgment

This work was framed in the context of the project CRYPTOACTION, under grant agreement 101226139, which receives funding from the European Union's Horizon Europe research and innovation programme.

References

[1] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Communications of the ACM*, vol. 59, no. 4, pp. 86–93, Apr. 2016. [Online]. Available: https://doi.org/10.1145/2896384

[2] S. Foley, J. R. Karlsen, and T. J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?," *The Review of Financial Studies*, vol. 32, no. 5, pp. 1798–1853, Apr. 2019. [Online]. Available: https://doi.org/10.1093/rfs/hhz015

[3] M. J. Shayegan, H. R. Sabor, M. Uddin, and C.-L. Chen, "A Collective Anomaly Detection Technique to Detect Crypto Wallet Frauds on Bitcoin Network," *Symmetry*, vol. 14, no. 2, p. 328, 2022. [Online]. Available: https://doi.org/10.3390/sym14020328

[4] M. Febrero-Bande, W. González-Manteiga, B. Prallon, and Y. F. Saporito, "Functional Classification of Bitcoin Addresses," *Computational Statistics & Data Analysis*, vol. 181, p. 107687, 2023. [Online]. Available: https://doi.org/10.1016/j.csda.2022.107687

[5] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," *Expert Systems with Applications*, vol. 150, Article no. 113318, 2020. [Online]. Available: https://doi.org/10.1016/j.eswa.2020.113318.

[6] A. Bella Baci, K. Brousmiche, I. Amal, F. Abdelhédi, and L. Rigaud, "Detecting illicit Ethereum accounts based on their transaction history and properties and using machine learning," in *Proc. Int. Conf. on Deep Learning, Big Data and Blockchain (DBB 2022)*, I. Awan, M. Younas, J. Bentahar, and S. Benbernou, Eds., vol. 541, Lecture Notes in Networks and Systems. Cham: Springer, 2023, pp. 97–108. [Online]. Available: https://doi.org/10.1007/978-3-031-16035-6_8.

[7] V. Patel, L. Pan, and S. Rajasegarar, "Graph deep learning based anomaly detection in Ethereum blockchain network," in *Proc. Network and System Security (NSS 2020)*, vol. 12570, Lecture Notes in Computer Science, M. Kutyłowski, J. Zhang, and C. Chen, Eds., Cham, Switzerland: Springer, 2020, pp. 132-148. [Online]. Available: https://doi.org/10.1007/978-3-030-65745-1_8.

[8] S. Al-E'mari, M. Anbar, Y. Sanjalawe, and S. Manickam, "A labeled transactions-based dataset on the Ethereum network," in *Advances in Cyber Security (ACeS 2020)*, M. Anbar, N. Abdullah, and S. Manickam, Eds., Singapore: Springer, 2021, vol. 1347, Communications in Computer and Information Science, pp. 57-67. [Online]. Available: https://doi.org/10.1007/978-981-33-6835-4_5.

[9] H. Kalodner, S. Goldfeder, A. Chator, M. Möser, and A. Narayanan, "BlockSci: Design and Applications of a Blockchain Analysis Platform," *arXiv preprint*, 2017. doi: 10.48550/arXiv.1709.02489. [Online]. Available: https://doi.org/10.48550/arXiv.1709.02489.

[10] B. Haslhofer, R. Stütz, M. Romiti, and R. King, "GraphSense: A General-Purpose Cryptoasset Analytics Platform," *arXiv preprint*, 2021. doi: 10.48550/arXiv.2102.13613. [Online]. Available: https://doi.org/10.48550/arXiv.2102.13613.

[11] S. Lee, C. Yoon, H. Kang, Y. Kim, Y. Kim, D. Han, S. Son, and S. Shin, "Cybercriminal Minds: An Investigative Study of Cryptocurrency Abuses in the Dark Web," in *2019 Network and Distributed System Security Symposium (NDSS)*, 2019. [Online]. Available: https://doi.org/10.14722/ndss.2019.23055

[12] Z. Ding, J. Shi, Q. Li, and J. Cao, "Effective Multi-Graph Neural Networks for Illicit Account Detection on Cryptocurrency Transaction Networks," 2023. [Online]. Available: https://doi.org/10.48550/arXiv.2309.02460

[13] D. Chaudhari, R. Agarwal, and S. Shukla, "Towards Malicious Address Identification in Bitcoin," 2021. [Online]. Available: https://doi.org/10.48550/arXiv.2112.11721

[14] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, and Y. Liu, "Transaction-based classification and detection approach for Ethereum smart contract," *Information Processing & Management*, vol. 58, no. 2, p. 102462, 2021. [Online]. Available: https://doi.org/10.1016/j.ipm.2020.102462.