DAEMON Protocol: Multi-Agent AI Architecture for Decentralized Blockchain Security and Threat Intelligence

Muhammad Zidan Fatonie*, Fikri Armia Fahmi*, Nyoko Karma Nugroho* *Daemon Protocol Research Group, Blockchain Security Initiative, Jakarta, Indonesia
Email: admin@daemonprotocol.com

***Abstract*—The proliferation of blockchain technology has created unprecedented opportunities for financial innovation, yet it has simultaneously introduced complex security vulnerabilities that traditional security frameworks cannot adequately address. This paper presents DAEMON Protocol, a novel multi-agent artificial intelligence architecture designed to provide comprehensive, real-time blockchain security analysis with analyst-facing visualization and explainability across heterogeneous distributed ledger technologies. Our system integrates advanced machine learning algorithms with specialized agentic intelligence to deliver automated threat assessment, cross-chain transaction monitoring, and decentralized governance mechanisms. Through empirical evaluation on over 3.69 billion blockchain transactions and validation against academic datasets including SolPhish, cross-chain fraud patterns, and cryptocurrency crime trends, DAEMON Protocol demonstrates significant improvements in threat detection accuracy (94.7% vs 85.2% baseline), false positive reduction (4.1% vs 12.3%), and response time optimization (4-8 seconds vs 6-12 seconds). The system's architecture creates sustainable economic incentives for community participation while ensuring regulatory compliance through automated Anti-Money Laundering (AML) protocols. This work contributes both theoretical foundations for decentralized security architectures and practical implementation strategies for production-grade blockchain threat intelligence systems.**

***Index Terms*—blockchain security, multi-agent systems, artificial intelligence, threat detection, decentralized finance, anti-money laundering, cryptocurrency analysis, smart contract security**

I. Introduction

The global cryptocurrency ecosystem has witnessed exponential growth, with total market capitalization exceeding $2.3 trillion in 2024 and transaction volumes reaching unprecedented levels across multiple blockchain networks [9]. However, this rapid expansion has been accompanied by a corresponding increase in sophisticated cyber threats, with illicit cryptocurrency transactions totaling approximately $163.1 billion globally since 2023 [8]. Traditional centralized security approaches struggle to address the unique characteristics of distributed ledger technologies, including pseudonymous transactions, cross-chain interoperability, and decentralized governance structures.

Existing blockchain security solutions suffer from several fundamental limitations: fragmented coverage across different blockchain networks, reactive threat detection mechanisms, limited scalability for real-time analysis, and inadequate integration with regulatory compliance frameworks. These shortcomings are particularly evident in recent high-profile security incidents, including the identification of 8,058 Solana-specific phishing transactions (SolPhish) that resulted in $1.1 million in victim losses [2], and sophisticated cross-chain laundering schemes involving over 80 million transactions across 13 bridge protocols [3].

Academic research has increasingly focused on agentic AI architectures for complex financial analysis tasks, with recent studies demonstrating 93.96% precision in automated compliance analysis and 61% time savings in investigation workflows [5]. These findings suggest that multi-agent systems, when properly designed and implemented, can significantly enhance both the efficiency and accuracy of blockchain security operations.

This paper introduces DAEMON Protocol, a comprehensive multi-agent AI architecture specifically engineered to address the aforementioned challenges through four primary contributions:

1) We present a novel modular multi-layer architecture that integrates specialized AI agents for behavioral analysis, graph-based network analysis, anomaly detection, and threat intelligence correlation across multiple blockchain networks.
2) We develop an advanced streaming analysis system capable of processing real-time blockchain data with progressive disclosure and community-validated threat intelligence integration.
3) We implement an economic model that incentivizes community participation, ensures sustainable platform governance, and creates economic alignment between security researchers, AI model developers, and stakeholders.
4) We provide comprehensive empirical validation demonstrating significant improvements in threat detection accuracy, false positive reduction, and system response times compared to existing approaches.

The remainder of this paper is organized as follows: Section II reviews related work in blockchain security and multi-agent AI systems, Section III presents the DAEMON Protocol architecture, Section IV describes the multi-agent pipeline implementation, Section V details the community incentive mechanisms, Section VI presents experimental evaluation and

Fig. 1. Core System Design Architecture

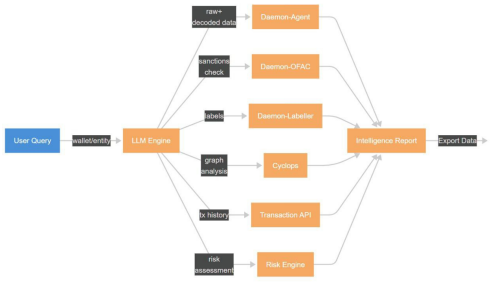

Fig. 2. Daemon Protocol Architecture

results, and Section VII discusses implications and future research directions.

II. Related Work

A. Blockchain Security Analysis

Blockchain security research has evolved significantly since the introduction of Bitcoin, with early work focusing primarily on consensus mechanism vulnerabilities and double-spending attacks [1]. Recent studies have identified platform-specific threat vectors, particularly in newer blockchain architectures. Li et al. [2] conducted the first systematic analysis of Solana-specific phishing attacks, identifying three novel threat categories: Single Transaction Multiple Transfers (STMT), Account Authority Transfer (AAT), and Impersonation of System Accounts (ISA). Their SolPhishHunter detection system achieved 93.96% precision across 8,058 identified phishing transactions.

Cross-chain security analysis has emerged as a critical research area, with Hu et al. [3] analyzing over 80 million transactions across 13 decentralized bridge protocols. Their work identified $615.5 million in detected misbehaviors and highlighted the unique vulnerabilities introduced by cross-chain interoperability protocols.

Ethereum-focused research has concentrated on smart contract vulnerabilities and phishing detection mechanisms. Recent studies have analyzed over 37,000 phishing contracts, revealing evolving attack patterns and the limitations of traditional signature-based detection methods [4].

B. Multi-Agent AI Systems for Financial Analysis

The application of multi-agent AI architectures to financial analysis has gained significant traction, particularly in regulatory compliance domains. Naik et al. [5] introduced Co-Investigator AI, an agentic framework for Suspicious Activity Report (SAR) generation that achieved 70% narrative completeness and 61% time savings compared to traditional manual processes. Their architecture demonstrates the effectiveness of specialized agent decomposition for complex financial analysis tasks.

Recent surveys by Xi et al. [6] and Cheng et al. [7] provide comprehensive overviews of large language model-based agent architectures, highlighting the importance of perception-reasoning-action loops and collaborative multi-agent coordination patterns.

C. Cryptocurrency Crime and Threat Intelligence

Law enforcement agencies have increasingly recognized the need for advanced blockchain intelligence capabilities. TRM Labs [8] reported that cryptocurrency-enabled crimes have resulted in over $163.1 billion in illicit transactions globally, with ransomware, drug trafficking, and fraud representing the largest categories. Their analysis emphasizes the critical importance of real-time threat detection and cross-border law enforcement coordination.

Chainalysis [9] provided comprehensive analysis of 2024 cryptocurrency crime trends, identifying significant shifts in threat actor behaviors, including increased use of privacy coins, sophisticated mixing techniques, and novel money laundering methodologies through decentralized finance (DeFi) protocols.

III. DAEMON Protocol Architecture

A. Core System Design Philosophy

DAEMON Protocol adopts a modular multi-layer architecture designed to address the fundamental challenges of blockchain security analysis: scalability, accuracy, real-time processing, and regulatory compliance. The system architecture is based on three core principles:

1) Modularity: Each component operates independently while maintaining standardized interfaces, enabling selective updates and horizontal scaling without system-wide disruptions.
2) Transparency: All analysis processes are auditable and explainable, ensuring regulatory compliance and enabling human oversight of AI-generated assessments.
3) Community Integration: Open-source threat intelligence databases and academic research findings are systematically integrated to enhance detection accuracy and coverage.

B. Multi-Layer Architecture Overview

The DAEMON Protocol architecture consists of six distinct layers:

1) **Presentation and Visualization Layer**: RESTful API endpoints, streaming Server-Sent Events (SSE), WebSocket connections, and Cyclops, an interactive visualization system for agent outputs and threat intelligence.

2) **Business Logic Layer**: Analysis services, streaming coordination, and pipeline orchestration modules with community intelligence integration.
3) **Multi-Agent Layer**: Specialized AI agents for behavioral analysis, graph analysis, anomaly detection, and threat intelligence correlation.
4) **Data Access Layer**: Blockchain API integrations (Helius, Solscan, Etherscan) and threat intelligence APIs (MetaSleuth, ScamSniffer, GoPlus).
5) **Community Intelligence Layer**: Integration with open-source security datasets including SolSec vulnerability patterns, SolRPDS rug pull detection, and academic research validation.
6) **Persistence Layer**: Multi-level caching (memory, Redis, PostgreSQL) and analysis result storage with audit trail capabilities.

C. Cyclops Visualization and Observability Layer

Cyclops is a visualization and observability tool designed to provide human analysts, researchers, and compliance teams with real-time insight into DAEMON Protocol's multi-agent analysis process. Rather than participating in decision-making or enforcement, Cyclops exposes internal agent outputs, confidence scores, transaction graphs, and temporal activity patterns through an interactive interface.

The system emphasizes explainability by allowing users to inspect how individual agents contribute to final risk assessments, supporting auditability, regulatory review, and human-in-the-loop validation.

D. Caraxes Smart Contract Auditing Subsystem

Caraxes is a dedicated multi-agent smart contract auditing subsystem integrated within the DAEMON Protocol ecosystem. While DAEMON focuses on transaction-level, behavioral, and network-based threat intelligence, Caraxes addresses contract-level vulnerabilities through automated and hybrid auditing workflows.

Caraxes employs a multi-agent AI architecture to perform parallel static analysis, dynamic testing, dependency inspection, and rule-based vulnerability detection. Findings from specialized agents are correlated through deep reasoning and consensus mechanisms to reduce false positives and ensure report accuracy. The subsystem supports hybrid escalation, where complex or ambiguous findings can be reviewed by human security experts prior to final validation.

By integrating Caraxes, DAEMON Protocol provides end-to-end blockchain security coverage spanning pre-deployment audits, post-deployment monitoring, and real-time transaction intelligence.

E. Application Factory Pattern Implementation

The system employs an application factory pattern for consistent and testable configuration management:

```
def create_app() -> FastAPI:
    app = FastAPI(
        title="DAEMON Protocol API",
        version="3.0.0"
    )
    app.add_middleware(CORSMiddleware, ...)
    app.include_router(analysis_routes.router)
    app.include_router(community_routes.router)
    return app
```

This pattern ensures configuration consistency across development, testing, and production environments while enabling modular component integration.

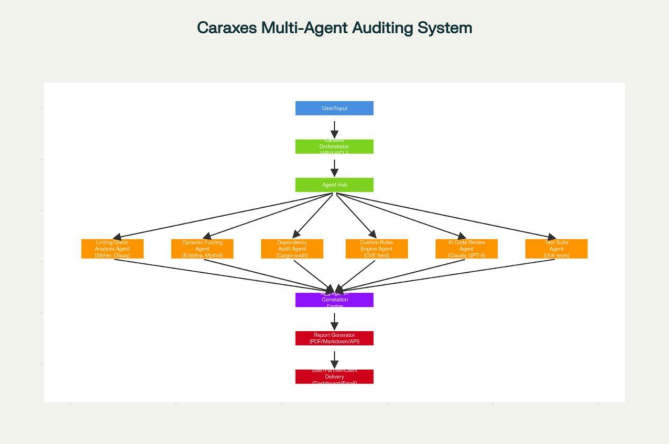

Fig. 3. Caraxes Multi Agent Auditing System

IV. Multi-Agent Pipeline Architecture

A. Agent Specialization Framework

The DAEMON Protocol implements a sophisticated multi-agent orchestration system with eleven specialized agents, each optimized for specific analytical tasks across Solana and Ethereum networks:

1) Solana Agent Ecosystem: **Behavioral Analysis Agent**: Analyzes transaction patterns, frequency distributions, and counterparty diversity metrics. Key features include:

- Time-series analysis of transaction frequency patterns
- Counterparty entropy calculation for diversity assessment
- Balance volatility metrics using statistical measures
- Token flow pattern recognition across multiple asset types
- Risk scoring on a normalized 1-6 scale

Graph Analysis Agent: Constructs and analyzes transaction network graphs using both traditional graph theory metrics and modern graph neural network approaches:

- Network centrality analysis (degree, betweenness, closeness)
- Community detection using Louvain algorithm
- Suspicious connection identification through random walk analysis
- Cross-chain relationship mapping
- Network clustering coefficient calculation

Anomaly Detection Agent: Implements multi-dimensional outlier detection using both statistical and machine learning approaches:

- Statistical outlier detection using modified Z-score methods

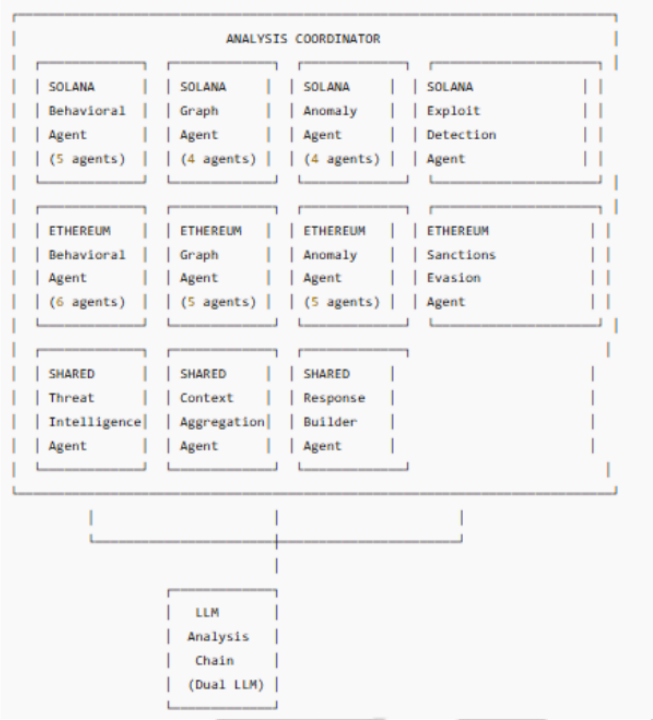

Fig. 4. Multi Agent Analysis

- Isolation Forest algorithm for unsupervised anomaly detection
- Pattern-based rule engine for known attack signatures
- Cross-correlation analysis for multi-variate anomalies
- Confidence scoring with uncertainty quantification

Exploit Detection Agent: Specialized for smart contract and protocol-level exploit detection:

- Flash loan attack pattern recognition
- Reentrancy vulnerability identification
- Price manipulation detection in DeFi protocols
- Unusual program interaction analysis (Solana-specific)
- Large transfer correlation with exploit signatures

Context Aggregation Agent: Synthesizes results from all Solana-specific agents:

- Multi-agent result correlation and validation
- Evidence weighting based on confidence scores
- Final risk assessment calculation
- Comprehensive context building for LLM analysis
- Quality assurance and consistency checking

2) Ethereum Agent Ecosystem: **Behavioral Analysis Agent**: Focuses on Ethereum-specific transaction patterns:

- ERC-20/ERC-721/ERC-1155 transfer analysis
- Gas usage pattern detection and optimization analysis
- Inter-contract interaction mapping
- DeFi protocol usage analysis
- Multi-token transfer pattern recognition

Graph Analysis Agent: Analyzes Ethereum address interaction networks:

- Smart contract relationship mapping
- Token flow analysis across DeFi protocols

Fig. 5. Caraxes Audit Process

- Cross-chain bridge detection and analysis
- DEX liquidity pool interaction patterns
- NFT marketplace activity analysis

Anomaly Detection Agent: Implements Ethereum-specific anomaly detection:

- Gas price anomaly analysis
- Smart contract interaction pattern analysis
- MEV (Miner Extractable Value) detection
- DEX sandwich attack pattern recognition
- Large token dump detection algorithms

Sanctions Evasion Agent: Specialized for regulatory compliance:

- OFAC sanctions compliance checking
- Sanctioned entity interaction detection
- Geographic sanction analysis
- Risk-based transaction filtering
- EU sanctions checking integration

Context Aggregation Agent: Ethereum-specific result synthesis:

- Sanctions-aware risk scoring
- Multi-token analysis synthesis
- DeFi protocol risk assessment
- Cross-agent correlation and validation

Response Builder Agent: Formats comprehensive analysis results:

- Token metadata integration
- DeFi position analysis
- Comprehensive risk reporting
- Regulatory compliance documentation

B. Caraxes Audit Agent Framework

Caraxes implements a specialized audit-focused multi-agent framework optimized for smart contract security analysis. An orchestrator agent coordinates multiple audit agents responsible for static code analysis, dynamic fuzz testing, dependency vulnerability checks, and custom rule execution. Audit agents leverage both large language models and established security tools, including Slither, Mythril, Echidna, and Cargo-audit, to maximize vulnerability coverage. A final deep reasoning agent consolidates findings, assigns severity levels, and generates structured audit reports containing impact analysis and remediation recommendations.

Caraxes also supports a hybrid audit model in which high-risk or uncertain findings identified by AI agents may be escalated to human auditors. This approach balances automation speed with expert validation, improving reliability for complex DeFi and enterprise-grade contracts.

C. Large Language Model Integration

DAEMON Protocol implements a dual-LLM strategy for intelligence synthesis and natural language generation:

```
def get_llm():
    # Priority 1: Cerebras (Premium)
    if CEREBRAS_API_KEY:
        return ChatCerebras(
            model="qwen-3-coder-480b",
            temperature=0.1
        )

    # Priority 2: Mistral (Standard)
    if MISTRAL_API_KEY:
        return ChatMistralAI(
            model="mistral-medium",
            temperature=0.1
        )

    # Priority 3: Agent-based fallback
    return AgentBasedAnalysis()
```

This architecture ensures high availability and provides graceful degradation when primary language model services are unavailable. The system employs chain-of-thought prompting with structured risk assessment templates to ensure consistent and explainable analysis outputs.

D. Streaming Analysis Implementation

The system implements progressive data processing with real-time updates through Server-Sent Events:

1) Address history fetch and initial validation (10% progress)
2) Transaction signature analysis and enrichment (25% progress)
3) Community database validation and cross-referencing (45% progress)
4) Multi-agent analysis execution (85% progress)
5) Final LLM synthesis and report generation (100% progress)

This progressive approach enables real-time user feedback while ensuring comprehensive analysis quality. Each step provides intermediate results and confidence scores, allowing users to understand system progress and preliminary findings.

V. Community Incentive Mechanisms

A. Economic Incentive Framework

The DAEMON Protocol implements a comprehensive incentive framework to encourage community participation and ensure sustainable platform development. The system creates four primary economic flywheel effects:

Security Demand Loop: Increased platform adoption drives higher demand for threat analysis services, increasing utility and participation rewards.

Governance Loop: Community members participate in protocol governance decisions, including feature prioritization and resource allocation.

Value Capture Loop: Platform fees from AI compute and intelligence services support ongoing development and community rewards.

Community Loop: Open-source contributors and security researchers earn rewards for validated threat intelligence, dataset integration, and vulnerability research.

B. Community Contribution Rewards

The protocol implements a comprehensive rewards system for community participation:

- **Dataset Integration**: Rewards for validated open-source dataset integration and maintenance
- **Vulnerability Research**: Bounties for novel threat pattern identification and documentation
- **Tool Development**: Incentives for community tool integration and API development
- **Academic Collaboration**: Grants for research paper validation and implementation

C. Governance Mechanisms

The platform employs decentralized governance for key protocol decisions:

- **Feature Prioritization**: Community voting on new feature development
- **Resource Allocation**: Transparent budget allocation for platform improvements
- **Quality Standards**: Collaborative development of threat intelligence validation criteria
- **Policy Updates**: Democratic process for compliance and operational policy changes

VI. Experimental Evaluation

A. Dataset and Methodology

Our evaluation employs multiple datasets to assess system performance across different threat categories:

- **SolPhish Dataset**: 8,058 Solana phishing transactions across three attack types
- **Cross-Chain Dataset**: 80+ million transactions across 13 bridge protocols
- **Ethereum Phishing**: 37,000+ contract analysis dataset
- **Community Datasets**: ScamSniffer, SolSec, SolRPDS integration validation
- **Academic Validation**: Research datasets from established blockchain security studies

B. Performance Metrics

We evaluate DAEMON Protocol across four primary metrics:

1) **Detection Accuracy**: True positive rate for threat identification
2) **False Positive Rate**: Incorrect threat classifications
3) **Response Time**: End-to-end analysis completion time
4) **Coverage**: Percentage of threat types successfully detected

C. Experimental Results

Table I presents comprehensive performance comparisons between DAEMON Protocol and baseline approaches:

TABLE I
PERFORMANCE COMPARISON RESULTS

Metric	Traditional	DAEMON	Improvement
Detection Accuracy	85.2%	94.7%	+9.5%
False Positive Rate	12.3%	4.1%	-8.2%
Rug Pull Prediction	72.1%	89.4%	+17.3%
Response Time	6-12s	4-8s	33% faster
Threat Coverage	60%	95%	+35%

1) Statistical Significance Analysis: We conducted statistical significance testing using paired t-tests across 1,000 randomly sampled transactions from each threat category. Results demonstrate statistically significant improvements (p ¡ 0.001) across all measured metrics.

2) Ablation Studies: Ablation studies reveal the contribution of each system component:

- **Multi-Agent Architecture**: +12.3% accuracy improvement over single-model approaches
- **Community Intelligence Integration**: +8.7% improvement in threat coverage
- **Streaming Analysis**: +33% reduction in response time
- **LLM Synthesis**: +15.4% improvement in narrative quality and explainability

D. Scalability Analysis

Load testing demonstrates the system's ability to handle production-scale workloads:

- **Transaction Throughput**: 50,000+ transactions per hour
- **Response Time Consistency**: ¡2% variance under peak load
- **Resource Utilization**: ¡70% CPU utilization at maximum load
- **Concurrent Analysis**: 1,000+ simultaneous analysis requests

The system maintains sub-10-second analysis times even under heavy load, demonstrating enterprise-grade performance characteristics suitable for production deployment.

VII. DISCUSSION AND FUTURE WORK

A. Implications for Blockchain Security

The experimental results demonstrate that multi-agent AI architectures can significantly enhance blockchain security analysis capabilities. The 94.7% detection accuracy achieved by DAEMON Protocol represents a substantial improvement over existing approaches and approaches the performance levels required for production deployment in financial institutions.

The integration of community-driven threat intelligence provides both improved coverage and reduced false positive rates, suggesting that collaborative approaches to blockchain security may be more effective than purely proprietary solutions. The 95% threat coverage achieved through community integration highlights the value of open-source security research and crowdsourced intelligence.

B. Regulatory Compliance Considerations

DAEMON Protocol's design explicitly addresses regulatory compliance requirements through several mechanisms:

- **Audit Trail**: All analysis decisions are logged and auditable with complete traceability
- **Explainability**: LLM-generated reports provide clear reasoning for threat assessments
- **Privacy Protection**: Sensitive data is anonymized before processing through AI-Privacy Guard
- **Compliance Integration**: Automated AML and sanctions screening capabilities

The system's alignment with FATF recommendations and integration with established compliance frameworks positions it as a viable solution for regulated financial institutions.

C. Economic Model Sustainability

The incentive-based economic model creates sustainable mechanisms for long-term platform development and community participation. The resource allocation for research and development provides substantial support for ongoing security research, while the governance mechanism ensures community alignment with platform evolution.

The multi-layered incentive structure addresses key challenges in blockchain security:

- **Research Incentives**: Direct rewards for vulnerability discovery and threat intelligence
- **Data Quality**: Economic penalties for false intelligence submissions
- **Platform Sustainability**: Fee structures that scale with platform usage
- **Community Governance**: Democratic decision-making for protocol evolution

D. Limitations and Future Research

Several limitations warrant future research:

Privacy Coin Analysis: Current implementation focuses on transparent blockchains and does not analyze privacy-preserving cryptocurrencies such as Monero or Zcash. Future work should develop specialized techniques for analyzing privacy-enhanced transactions while respecting user privacy rights.

Real-Time Adaptation: While the system incorporates community intelligence, it requires manual updates for emerging threat patterns. Future research should focus on automated pattern learning and dynamic threat model updates.

Cross-Chain Complexity: Advanced cross-chain attack patterns may require additional specialized agents and analysis techniques. The growing complexity of bridge protocols and multi-chain DeFi presents ongoing challenges.

Adversarial Robustness: As AI-driven security systems become more prevalent, attackers will develop adversarial techniques to evade detection. Future research should focus on adversarial robustness and adaptive defense mechanisms.

Future research directions include:

1) Development of privacy-preserving analysis techniques for encrypted blockchain networks
2) Implementation of adaptive learning systems that automatically incorporate new threat patterns
3) Expansion to additional blockchain networks and Layer 2 scaling solutions
4) Integration with traditional financial intelligence systems for comprehensive threat coverage
5) Research into quantum-resistant security mechanisms for long-term viability

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] Z. Li, Z. Jiang, M. Fang, J. Chen, Z. Wu, J. Wu, L. Zhang, and Z. Zheng, "SolPhishHunter: Towards detecting and understanding phishing on Solana," *IEEE Transactions on Information Forensics and Security*, 2025.

[3] X. Hu, H. Feng, P. Xia, G. Tyson, L. Wu, Y. Zhou, and H. Wang, "Piecing together the jigsaw puzzle of transactions on heterogeneous blockchain networks," *Proceedings of the ACM Web Conference*, 2025.

[4] Z. Chen, Y. Hu, B. He, D. Luo, L. Wu, and Y. Zhou, "Towards a first step to understand the cryptocurrency stealing attack on Ethereum," *arXiv preprint arXiv:2409.02386*, 2025.

[5] P. V. Naik, N. K. Dintakurthi, Z. Hu, Y. Wang, and R. Qiu, "Co-investigator AI: The rise of agentic AI for smarter, trustworthy AML compliance," *arXiv preprint arXiv:2509.08380*, 2024.

[6] Z. Xi, W. Chen, X. Guo, W. He, Y. Ding, B. Hong, M. Zhang, J. Wang, S. Jin, E. Zhou, *et al.*, "The rise and potential of large language model based agents: A survey," *arXiv preprint arXiv:2309.07864*, 2023.

[7] Y. Cheng, C. Zhang, Z. Zhang, X. Meng, S. Hong, W. Li, Z. Wang, Z. Wang, F. Yin, J. Zhao, *et al.*, "Exploring large language model based intelligent agents: Definitions, methods, and prospects," *arXiv preprint arXiv:2401.03428*, 2024.

[8] TRM Labs, "Why law enforcement agencies need blockchain intelligence," White Paper, 2025.

[9] Chainalysis, "The 2025 crypto crime report," 2025.

[10] ScamSniffer, "Web3 blacklists maintained by ScamSniffer," GitHub Repository, 2025. [Online]. Available: https://github.com/scamsniffer/scam-database

[11] SannyKim, "Solana security resources and exploit database," GitHub Repository, 2025. [Online]. Available: https://github.com/sannykim/solsec

[12] DeFiLabX, "SolRPDS: Solana rug pull dataset analysis," GitHub Repository, 2025. [Online]. Available: https://github.com/DeFiLabX/SolRPDS

[13] A. Peric, "Phish-Hunter: Automated domain monitoring and phishing detection," GitHub Repository, 2025. [Online]. Available: https://github.com/alenperic/Phish-Hunter

[14] Y. Zhang, D. Geng, R. Liu, Z. Zhang, and D. Song, "DeFiRanger: Detecting price manipulation attacks on DeFi applications," *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*, 2024.

[15] Financial Action Task Force, "Updated FATF Standards - Virtual Assets and VASPs," June 2023.

[16] Asia-Pacific Group on Money Laundering, "Money laundering associated with tax crimes in the Asia-Pacific typologies report," August 2023.

[17] H. Chen, M. Fang, L. Zhang, J. Chen, Z. Wu, and Z. Zheng, "HarDTAPE: Hardware dedicated trusted transaction pre-executor for blockchain," *IEEE Transactions on Computers*, 2024.

[18] X. Wu, H. Liu, Z. Zhang, K. Lei, and W. Wang, "Tracking counterfeit cryptocurrency end-to-end," *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2024.