The Forensic Imperative: A Technical Justification for the AltFlex AI-Powered Framework for Exploit Detection in Cross-Chain Bridges and DeFi Protocols

Authors: Jay Arre Talosig, Rinoah Venedict Dela Rama, Mark Jhosua Taberna, Nicko Nehcterg Dalida, Alexander Castillo

I. Foundational Concepts: Differentiating Blockchain Integrity from Application Layer Vulnerability

The assertion that "Blockchain is immutable and cannot be hacked represents a fundamental misunderstanding of the locus of modern decentralized finance (DeFi) security failures. While the underlying cryptographic structure and consensus mechanisms of Layer 1 blockchains remain remarkably resilient, the critical vulnerabilities and subsequent mass financial losses occur predominantly at the application layer, within the logic of smart contracts (SCs) and interoperability protocols such as cross-chain bridges.[1]

1.1. The Blockchain Security Paradox: Layer 1 Immutability vs. Application-Layer Exploitation

The core technical nuance lies in distinguishing between the integrity of the distributed ledger (Layer 1) and the correctness of the code executed atop that ledger (Layer 2/3). The immutability principle ensures that once a transaction is recorded and validated by the network's consensus, the cryptographic link binding that block to its predecessors cannot be altered retrospectively.[3] This principle of cryptographic finality is robust and stands unchallenged.

However, a transaction is immutable only if it is structurally and cryptographically sound, regardless of whether the *intent* of that transaction was fraudulent. If an exploit successfully manipulates a smart contract's logic to authorize an unauthorized withdrawal, the blockchain

records the resulting fraudulent transaction as valid. The ledger does not prevent the fraud; it merely confirms and permanently logs it.[3] This permanence transforms the immutable ledger into a repository of evidence of the successful attack.

Crucially, formal methods, while valuable for guaranteeing functional correctness based on existing specifications, are incapable of anticipating and finding vulnerabilities or bugs that the original smart contract developers failed to specify or foresee.[3] This limitation highlights the need for dynamic, real-time intrusion and anomaly detection mechanisms that operate during the execution phase, rather than relying solely on pre-deployment static analysis or post-facto forensic tools.

1.2. Defining the Threat Taxonomy: Exploit vs. Consensus Compromise

Modern security threats have shifted away from direct attacks on Layer 1 consensus (e.g., 51% attacks, which are economically prohibitive on major chains) toward manipulating the application layer's execution environment or business logic. The vulnerabilities targeted are rooted in code flaws or architectural design decisions.[2]

The most severe application-layer flaws include Access Control and Authentication Vulnerabilities, which involve a failure in privilege enforcement when authorization checks are incorrectly implemented, inconsistent, or outright missing.[2] Research indicates that these failures are among the most common and devastating root causes of major DeFi incidents.[2] Other critical attack vectors include:

- **Cross-Chain Attacks:** These exploit weaknesses in the interaction layer between disparate blockchain networks, such as issues in message passing or asset validation, allowing funds to be stolen from one chain and transferred to another.[1]
- **Execution Flow Flaws:** Vulnerabilities such as Re-entrancy or Transaction Order Dependency (TOD)/Frontrunning arise when developers assume atomic transaction behavior in a non-atomic environment, enabling adversaries to interleave or reorder transactions maliciously.[2]

The migration of the attack surface toward the complex application layer where financial assets are managed justifies the precise scope of the AltFlex framework.[5] The application layer is the repository of capital and the location of the most complex, fragile code, making it the highest return-on-investment target for malicious actors. The sheer volume of financial loss attributed to these application-layer flaws demonstrates that existing security measures, whether formal verification or simple perimeter controls, are systematically failing.

II. The Current State of Systemic Risk in Decentralized Finance: Empirical Justification

The proposal to develop an AI-powered forensic framework is not a proactive measure addressing theoretical risks but a necessary, immediate response to catastrophic systemic failure in the Web3 ecosystem. Empirical data unequivocally validates the necessity of a sophisticated solution like AltFlex.

2.1. Quantification of Financial Catastrophe: Analysis of Recent Exploits

The De.Fi REKT Report for Q1 2025 provides quantitative evidence of the market's acute vulnerability. The period saw total recorded financial losses surpassing **$2.052 Billion** across 37 separate incidents.[6] This staggering figure marks one of the worst quarters in blockchain exploit history and is five times higher than the losses recorded in Q1 2024 ($414.8 million).[6]

The scale of financial hemorrhage demonstrates a critical security gap. Furthermore, recovery efforts remain negligible, with only $44.5 million reclaimed in Q1 2025, underscoring the permanence of asset drainage once an exploit is successful and the funds are moved.[6]

A detailed breakdown of the losses reveals the primary points of failure:

- **Dominant Attack Vector:** The most damaging category was Access Control Vulnerabilities, responsible for an overwhelming **$1.46 Billion** in losses across just eight incidents, accounting for over 70% of all funds lost during the quarter.[6] This statistical concentration underscores the critical importance of AltFlex's focus on detecting anomalies related to privilege and authorization.[5]
- **Protocol Category:** Although CeFi entities, notably the Bybit Exchange breach ($1.5 billion), absorbed the largest recorded losses, these events involved the theft of decentralized assets (Ethereum) due to failure in the entity's access controls.[6] This demonstrates the inter-protocol contagion risk: the vulnerability vector transcends the strict definition of 'DeFi' and applies to any entity managing large pools of decentralized crypto assets. The risk is universal across the capital base, necessitating a forensic framework capable of analyzing massive, high-speed outflows typical of key compromises.

- **Secondary Risks:** Other protocol types also suffered significant damage, including $487 million lost in Token-Based projects (primarily exit scams) and smaller but notable losses across Borrowing/Lending protocols due to logic bugs and oracle misconfigurations.[6]

The evidence confirms that the majority of lost funds result from failures in implementing secure administrative logic or access mechanisms, precisely the issues AltFlex is designed to detect proactively.

Table 1: Systemic Financial Risk: Major Exploit Categories in Q1 2025

Protocol Category	**Total Funds Lost (Approx.)**	**Dominant Exploit Type**	**Forensic Rationale for AltFlex Intervention**
Centralized/Hybrid Finance (CeFi)	$1.46 Billion	Access Control Vulnerabilities (Private Key/Wallet Breach) [6]	Detection of anomalous intra-exchange or custodial asset movements; large, rapid outflows analysis [5]
Token-Based Projects	$487 Million	Exit Scams (Liquidity Withdrawal) [6]	Identification of abrupt, unauthorized liquidity pool depletion based on source address behavioral analysis [7]
Cross-Chain Bridges (Historical/Recent)	Hundreds of Millions (per incident)	Validator Takeover, Message Verification Flaws [8]	Behavioral analytics on validator consensus and cross-chain message path validation [10]

Borrowing/Lending Protocols	~$9.8 Million	Logic Bugs, Oracle Misconfiguration [6]	Sequence model analysis of smart contract opcodes and function calls [11]

2.2. Focus on Cross-Chain Bridge Vulnerability Taxonomy

Cross-chain bridges, essential for interoperability and the multi-chain ecosystem, represent an exposed point of systemic failure. They are structurally complex, often comprising multiple components such as validators, oracle mechanisms, and intricate smart contract logic, which inherently increases the attack surface.[9]

Attacks targeting bridges demonstrate sophisticated application-layer manipulation:

1. **Validator Takeover:** Many bridges rely on external validator mechanisms (multi-signature or a small set of nodes) to approve cross-chain transfers. If an attacker compromises a required threshold of these validators, they can approve fake and malicious transfers.[4] The fragility of this external mechanism is a recurring pain point.[12]
2. **Smart Contract Logic Flaws:** Vulnerabilities within the bridge's contracts often allow attackers to execute ‘zero-collateral minting’ or exploit flaws that permit infinite withdrawals without a corresponding legitimate deposit on the source chain.[9]
3. **Message Verification Bugs:** Lack of proper validation of signatures or messages passed between chains can be exploited, as occurred in the BSC chain attack that resulted in a withdrawal of $576 million.[4]

The systemic risk embedded in bridge infrastructure necessitates a specialized forensic approach like AltFlex, which is designed to analyze these complex, multi-component interactions for early signs of compromise.[5]

III. Detailed Case Studies of Application-Layer Exploitation

A deeper examination of two major historical exploits confirms that the primary security risk lies in application-layer logic and privileged access, not in the foundational immutability of the

blockchain itself.

3.1. Case Study 1: The Ronin Network Bridge Exploitation

In March 2022, the Ronin sidechain, which services the Axie Infinity game, suffered a catastrophic loss of 173,600 Wrapped Ethereum (WETH) and 25.5 million USDC.[8] The total value of the stolen assets was approximately $625.5 million.[13]

The attack was a definitive example of an application-layer failure known as **Validator Takeover**.[8] The Ronin bridge utilized a system where nine validators were required to approve transactions, and the threshold for approval was five signatures. The attacker successfully compromised the private keys belonging to four Sky Mavis validator nodes and one Axie DAO validator node, thereby achieving the necessary quorum of five signatures.[8]

By possessing the private keys, the attacker was able to forge two transactions one for WETH and one for USDC that were cryptographically valid, fooling the Ronin bridge's pool of funds into authorizing the drainage.[8] The failure was rooted in a lack of decentralization and inadequate access controls governing the validator keys, leading to the compromise of the external validation mechanism.[12] The system's "minimal monitoring and alerting" further allowed the attacker solid ground to launch and complete the attack without immediate detection.[8]

Since the resulting transactions were cryptographically legitimate from the blockchain’s perspective, any effective forensic solution must focus on **behavioral anomaly detection**. The forging of multiple signatures and the immediate, massive outflow of assets should register as a statistical deviation from the historical behavior patterns of those validator addresses.[10]

3.2. Case Study 2: The Poly Network Exploitation

The Poly Network exploit in August 2021 resulted in the transfer of over $610 million across three different blockchains (Ethereum, Binance Smart Chain, and Polygon).[13]

The root cause was a sophisticated exploitation of logic within the cross-chain interoperability protocol. Specifically, the attacker targeted the EthCrossChainManager smart contract. The attacker executed a cross-chain transaction from the Ethereum network, passing a specific

string value (f1121318093) as the method parameter, along with their own Ethereum wallet's public key as a corresponding parameter.[15]

This malicious input successfully manipulated the contract's internal state, granting the attacker the status of a "Keeper" for the Ethereum blockchain within the Poly Network system.[15] This was, fundamentally, an unauthorized privilege escalation achieved by exploiting a logic flaw in the smart contract's processing of cross-chain messages. Once granted this status, the attacker used the corresponding secret key to funnel tokens out of Poly's wallets into their own addresses.[15]

The analysis of these major incidents leads to a unified conclusion: the critical security challenge in Web3 is not the vulnerability of the underlying ledger, but the fragility of the application-layer code and the access controls protecting immense pools of capital. The purpose of AltFlex is to provide the means to analyze and flag these application-layer manipulations.

IV. Limitations of Conventional Digital Forensics in Web3 Environments

The pervasive nature of cross-chain crime renders traditional digital forensic techniques obsolete for modern blockchain investigations, thereby establishing the crucial operational requirement for the AltFlex framework.

4.1. Inadequacy for Cross-Chain Tracing and Multi-Protocol Complexity

Conventional blockchain analytics tools were primarily architected for tracking assets within a single blockchain environment, such as native Bitcoin or Ethereum tracking.[16] This single-chain dependency results in a devastating loss of visibility when criminals utilize cross-chain tactics to obscure the flow of illicit funds.[16]

The complexity of tracing funds that move across multiple, disparate networks often involving multiple smart contracts and bridge components overwhelms legacy systems. The criminal use of cross-chain methods has already resulted in the laundering of over $7 billion worth of

illicit crypto, confirming the inadequacy of current investigative tools.[16]

Without an automated, integrated cross-chain tracing capability, investigators must resort to a time-intensive manual process, piecing together transaction trails across numerous block explorers, each with unique interfaces and varying degrees of information fidelity.[16] This high demand for specialized expertise across multiple ecosystems (e.g., Ethereum, BSC, Polygon) creates a significant manual bottleneck, which is fatal in the context of high-speed exploits where assets can be liquidated or further obfuscated within minutes. The inability to rapidly acquire timely and accurate cross-chain information means investigators frequently lose the trail of stolen assets.[16]

4.2. The Challenge of Pseudonymity, Data Complexity, and Imbalanced Datasets

Beyond cross-chain movement, conventional forensics face inherent difficulties in interpreting the data itself:

- **Pseudonymity Linkage:** While all transactions are transparently recorded, the use of cryptographic addresses ensures pseudonymity. Linking these blockchain addresses to real-world entities is a complex challenge, making standard digital probes insufficient.[17] Advanced tracking methods often require external coordination that is not always feasible.
- **Data Structure Complexity:** Blockchain data is structured in cryptographically tied blocks, a non-standard format compared to traditional file systems or databases.[17] Parsing and interpreting this information successfully requires specialized tools and software.[17]
- **The Rare Event Problem (Imbalance):** From a machine learning perspective, exploitative or fraudulent transactions are extremely rare events when measured against the total volume of daily activity. This results in a highly imbalanced dataset, where traditional detection models are prone to bias toward the dominant (legitimate) class, leading to a high rate of false negatives (missed exploits).[7]

The convergence of multi-chain complexity, high-speed asset movement, and inherent data obfuscation requires a paradigm shift from reactive, manual tracing to proactive, data-centric analysis. AltFlex's AI/ML approach provides a necessary capability for predictive indexing: instead of chasing funds post-facto, the system flags suspicious activity based on deviation from established behavioral norms, providing early warning and preserving the forensic trail before asset obfuscation can finalize.

V. Academic Precedent: Integrating Artificial Intelligence for DeFi Security

The AltFlex framework is founded upon established and emerging research in cybersecurity and decentralized ledger technology, specifically the integration of Artificial Intelligence (AI) for intrusion and anomaly detection. Academic literature strongly supports the use of AI/ML methodologies to address the security deficits outlined in Sections II and III.

5.1. Literature Review: AI-Powered Intrusion Detection Systems (IDS)

The necessity for AI-powered intrusion detection systems (IDS) in blockchain networks has been recognized due to the inability of conventional IDS to interpret blockchain-specific semantics, such as transaction graphs, validator behaviors, and cross-chain flows.[10] Research confirms that AI-powered approaches offer a systematic way to detect fraudulent activities that have led to billions in losses.[19]

State-of-the-art academic designs propose sophisticated, multilayered architectures that directly inform AltFlex's technical strategy. These validated components include:

1. **Graph Neural Networks (GNNs):** These are essential for modeling and analyzing complex, dynamic transaction graphs, enabling the effective scoring of address behavior and contract interactions.[10]
2. **Sequence Models:** These models process execution traces (e.g., EVM opcodes) to identify runtime anomalies and pinpoint contract-level exploits.[10]
3. **Temporal Models:** Used for detecting time-sensitive manipulation, such as patterns in mempool activity, which can signal Frontrunning (TOD) or Denial of Service (DoS) attacks.[10]

This academic consensus confirms that AI, particularly graph-centric and deep learning methods, is not merely an enhancement but a fundamental necessity for achieving early detection of fraud patterns and validator misbehavior in complex Web3 systems.[10]

5.2. Methodology Justification: Anomaly Detection and High Recall

Strategy

The primary objective of AltFlex is the development of robust AI/ML models for anomaly detection.[5] This approach is strategically validated by researchers who investigate illicit activity via cross-chain bridges.[7]

In security-critical environments, the cost of a false negative (missing an actual exploit) is catastrophic, whereas the cost of a false positive (flagging a legitimate transaction) is manageable, as it triggers a secondary verification process.[7] Therefore, the AltFlex modeling strategy must prioritize **high recall** the ability to identify the maximum possible number of true exploits even at the expense of a lower precision score (increased false positives).[7]

The framework operationalizes this strategy through a layered approach. The AI Detection Module, trained on highly imbalanced datasets, is responsible for comprehensive coverage and identifying potential signals.[5] Any transaction flagged by these high-recall models is then routed to the **Forensic Analysis Module**.[5] This secondary verification, which may involve manual or deeper automated checks, transforms the strategic output of the high-recall AI models into actionable intelligence, ensuring the coverage of suspicious activities while maintaining accuracy through verification.

Table 2: AltFlex Methodology Validation: Application of Advanced AI Techniques in DeFi Forensics

AI/ML Technique	Academic Application & Source	AltFlex Framework Component	Target Exploit Vector
Graph Neural Networks (GNNs)	Modeling dynamic transaction graphs for address behavior [10]	AI Detection Module, Forensic Analysis Module	Cross-chain fund tracing, validator collusion, large-scale financial fraud [16]
Supervised Learning (Signature Matching)	Binary classification for illicit activity; prioritizing high recall [1]	AI Detection Module (Signature Matching)	Known vulnerability patterns (Re-entrancy, Oracle attacks) [2]

Unsupervised Anomaly Detection	Discovering patterns in unlabeled data; critical for identifying novel behaviors [1]	AI Detection Module (Real-time Monitoring)	Zero-day exploits, novel transaction sequences, unusual privilege escalations [5]
Sequence/Code Analysis	Analyzing EVM opcode traces and connecting Control Flow Graphs (CFGs) [10]	Forensic Analysis Module	Contract logic bugs, access control misconfigurations, transaction order dependency (TOD)

5.3. Advanced Methods: Graph Neural Networks and Control Flow Analysis

To overcome the limitations of traditional tools in multi-chain environments, AltFlex necessitates methodologies optimized for relational data analysis. Graph Neural Networks are ideally suited for this task, enabling the analysis of the intrinsic relationships between addresses, contracts, and transactions across chains.[10] GNNs allow for a holistic view of asset flow that fragmented, single-chain tools cannot achieve.[16]

Furthermore, detection must penetrate the complexity of smart contract code. Advanced academic frameworks demonstrate that detection can be achieved by unifying external and internal paths and connecting Control Flow Graphs (CFGs) between bytecode contracts.[11] This specialized approach, such as formulating data path validation into a path reachability problem, is effective at detecting crucial flaws like access control and flash loan exploits.[11] AltFlex's plans for future enhancements, including smart contract decompilation and symbolic execution [5], directly align with this requirement for rigorous code-level forensic analysis.

VI. The AltFlex Framework: Technical Architecture and Methodology Documentation

The AltFlex project is engineered as an integrated AI and digital forensics framework designed to actively detect and analyze security exploits in cross-chain bridges and DeFi protocols.[5] Its comprehensive, modular architecture is specifically designed to address the challenges of multi-chain complexity and evolving attack vectors.

6.1. AltFlex Project Overview and Core Components

The framework adopts a modular architecture encompassing data ingestion, preprocessing, AI/ML model training, exploit detection, alert generation, and visualization components.[5]

AltFlex System Architecture Components:

- **Blockchain Data Sources:** Raw input of historical transaction data, smart contract code, and exploit reports.[5]
- **Data Processing Engine:** Responsible for cleaning, transforming, and normalizing collected data, specifically structuring transaction data into graph formats suitable for GNNs and extracting features for anomaly detection models.[5]
- **AI Detection Module:** The core intelligence layer, housing trained AI/ML models (including GNNs, supervised, and unsupervised methods) for real-time anomaly detection, pattern recognition, and signature matching.[5]
- **Forensic Analysis Module:** Provides deeper, specialized analysis for flagged incidents. This module utilizes the database of known exploit signatures [5] and supports complex analysis techniques, aligning with future plans for symbolic execution and smart contract decompilation.[5]
- **Risk Assessment Engine:** Aggregates findings from the detection and analysis modules to assign a risk score, prioritizing alerts and supporting automated incident response.[5]
- **Dashboard & Alerting:** Provides a user-friendly interface for visualizing forensic analysis results [5] and generating immediate alerts for high-risk activity.

6.2. Detailed Methodology (Phases 1-6)

The project execution is rigorously phased to ensure technical contributions are built upon a solid foundation of data and model development.[5]

1. **Data Collection & Preprocessing:** This phase establishes the foundation by gathering necessary historical data, smart contract code, and known exploit reports. The critical focus during preprocessing is the cleaning, transformation, and normalization of this complex, multi-source data to create high-quality, labeled datasets (labeled dataset v1) suitable for training sophisticated machine learning models, particularly addressing the class imbalance issue.[5]
2. **Model Development & Training:** Utilizing frameworks such as TensorFlow and PyTorch, this phase trains AI/ML models prioritizing high-recall performance.[5] The models developed will specifically target anomaly detection in transaction data and pattern recognition related to known exploit signatures.
3. **Framework Implementation & Integration:** The developed models and core forensic analysis scripts are integrated into a working prototype, establishing the necessary API communication pathways between modules and creating the initial user interface.[5]
4. **Testing and Validation:** The framework's performance is evaluated against rigorous simulated and real-world exploit scenarios. This validation is critical for confirming that AltFlex effectively overcomes the known limitations of legacy tools, particularly its ability to trace and correlate data flows across multiple blockchain platforms.
5. **Integration and Testing (Deployment):** The solution is deployed and tested in sandboxed blockchain environments to ensure stability and accuracy before potential real-world deployment.[5]

6.3. Resource and Risk Management Documentation

The technical resource requirements and development stack—relying on Python, Web3.py, and advanced machine learning frameworks—are essential for handling the high computational demands of training GNNs and processing large-scale blockchain data.[5]

A proactive approach to risk assessment is integrated into the framework design. The high probability and high impact risk of **Evolving Attack Vectors** [5] is the primary justification for using an adaptive AI framework over static security tools. The mitigation strategy for this risk is the continuous updating of models and the exploit database.[5] This ongoing refinement ensures that AltFlex remains dynamic and capable of adapting to novel exploitation techniques, preventing the degradation of detection efficacy over time.

VII. Conclusion and Significance

The technical justification for the AltFlex AI-Powered Forensic Framework is irrefutable, resting on empirical evidence of systemic financial risk and the academic validation of AI/ML as the necessary security intervention.

The fundamental premise that blockchain is immune to attack must be revised: Layer 1 is secure, but the Layer 2/3 application ecosystem is structurally vulnerable, evidenced by the $2.052 Billion lost in Q1 2025 alone, primarily through Access Control and Smart Contract Logic Exploits.[6] Traditional forensic methods, constrained by single-chain focus and manual effort, are inadequate to trace assets laundered across multiple chains.[16]

The AltFlex framework addresses this critical security gap by synthesizing advanced technologies specifically Graph Neural Networks for cross-chain tracking and sophisticated sequence models for application logic analysis [10] into a unified platform. By strategically prioritizing high recall in its AI Detection Module and layering this with rigorous Forensic Analysis [5], AltFlex provides a proactive, adaptive solution that shifts the security focus from reactive damage control to preemptive exploit detection.

This project represents a crucial advancement in Web3 security, providing a foundation for real-time monitoring and comprehensive incident analysis that is both methodologically sound and empirically necessary for securing decentralized financial ecosystems.

Works cited

1. Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence, accessed November 27, 2025, https://www.mdpi.com/2073-431X/12/5/107
2. Attack-Centric by Design: A Program-Structure Taxonomy of Smart Contract Vulnerabilities, accessed November 27, 2025, https://arxiv.org/html/2511.09051v1
3. Blockchain smart contracts: Applications, challenges, and future trends - PubMed Central, accessed November 27, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC8053233/
4. How Cross-Chain Bridges are Hacked? | by Officer's Notes | Coinmonks | Medium, accessed November 27, 2025, https://medium.com/coinmonks/how-cross-chain-bridges-are-hacked-d6ddb448401e
5. AltFlex AI-Powered Forensic Framework.pdf
6. De.Fi REKT Report: Q1 2025 — Over $2 Billion Lost in DeFi and ..., accessed November 27, 2025, https://de.fi/blog/de-fi-rekt-report-q1-2025-over-2-billion-lost-in-defi-and-cefi-exploits
7. Anomaly Detection in Cross-Chain Bridges: A Data Analytics Study - ResearchGate, accessed November 27, 2025,

https://www.researchgate.net/publication/396245889_Anomaly_Detection_in_Cross-Chain_Bridges_A_Data_Analytics_Study
8. Hack Track: Analysis of Ronin Network Exploit - Merkle Science, accessed November 27, 2025, https://www.merklescience.com/blog/hack-track-analysis-of-ronin-network-exploit
9. Cross-chain Bridge Exploits: There Are More Risks Than You Know | Presto Research, accessed November 27, 2025, https://www.prestolabs.io/research/cross-chain-bridge-exploits-there-are-more-risks-than-you-know
10. (PDF) AI-Powered Intrusion Detection Systems in Blockchain Networks - ResearchGate, accessed November 27, 2025, https://www.researchgate.net/publication/396888653_AI-Powered_Intrusion_Detection_Systems_in_Blockchain_Networks
11. Penetrating the Hostile: Detecting DeFi Protocol Exploits through Cross-Contract Analysis, accessed November 27, 2025, https://arxiv.org/html/2511.00408v1
12. Cross-Chain Bridge Security Incident Review - Why Mitosis's Model is Safer? | azu_crypto1 on Binance Square, accessed November 27, 2025, https://www.binance.com/en/square/post/29838817876081
13. Blockchain Technology and Vulnerability Exploits on Smart Contracts - UWL Repository - University of West London, accessed November 27, 2025, https://repository.uwl.ac.uk/id/eprint/12337/1/Blockchain%20Technology%20and%20Vulnerability%20Exploits%20on%20Smart%20Contracts%20-%20UWL%20Repo.pdf
14. Poly Network exploit - Wikipedia, accessed November 27, 2025, https://en.wikipedia.org/wiki/Poly_Network_exploit
15. The Poly Network Hack Explained - Kudelski Security Research Center, accessed November 27, 2025, https://kudelskisecurity.com/research/the-poly-network-hack-explained
16. Cross-Chain Analytics: A Game-Changer for Law Enforcement in 2025 - Merkle Science, accessed November 27, 2025, https://www.merklescience.com/blog/cross-chain-analytics-law-enforcement-2025
17. Blockchain and Digital Investigation: Insights and Impacts - SalvationDATA, accessed November 27, 2025, https://www.salvationdata.com/knowledge/digital-investigation/
18. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions - MDPI, accessed November 27, 2025, https://www.mdpi.com/2079-9292/13/17/3568
19. [2308.15992] AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective - arXiv, accessed November 27, 2025, https://arxiv.org/abs/2308.15992