Edumania-An International Multidisciplinary Journal

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Recent Case Studies of Oracle Failures and Cross-Chain Attacks in Blockchain Technology

Ganapathy, Venkatasubramanian

Faculty in Auditing Department, Southern India Regional Council of the Institute of Chartered Accountants of India (SIRC of ICAI), Chennai, Tamil Nadu, Bharat

Abstract

Oracles play a critical role in blockchain ecosystems by bridging the gap between on-chain smart contracts and off-chain data sources. However, their vulnerabilities make them prime targets for exploitation, especially in cross-chain environments where complex interactions and dependencies exist. This paper reviews notable oracle-related failures and cross-chain attacks from 2022 to 2024, analyzing the causes, implications, lessons learned, and best practices derived from these incidents. Key cases include the Wormhole Bridge Exploit (2022), where a $325 million theft occurred due to missing validation checks and a lack of decentralization, emphasizing the need for rigorous audits and decentralized systems. Similarly, the Ronin Bridge Attack (2022) saw attackers compromise validator nodes, stealing $620 million, highlighting the dangers of over-reliance on a small number of validators and the importance of anomaly detection mechanisms. In the Harmony Bridge Hack (2022) and Nomad Bridge Attack (2022), centralized oracle architectures and insecure protocol designs were exploited, underscoring the necessity of decentralized validation and robust protocol simplification. The Multichain Protocol Exploit (2023) and StarkNet Oracle Exploit (2024) revealed vulnerabilities stemming from delayed patching of known issues and single-source dependency, resulting in losses of $126 million and $45 million, respectively. These incidents illustrate the importance of real-time system updates, multi-source data aggregation, and fallback mechanisms to maintain system integrity during failures. From these cases, common failure patterns emerge, including centralized oracle architectures, inadequate transaction

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198
validation, insufficient decentralization of validator networks, lack of real-time anomaly detection, and insecure protocol designs. The analysis identifies several best practices to mitigate such risks, such as transitioning to decentralized oracle systems, implementing quorum-based consensus mechanisms, leveraging formal verification for critical systems, and enhancing monitoring through machine learning-driven anomaly detection tools. Additionally, robust economic incentives for oracle participants and frequent security audits are vital for sustaining system reliability. The findings stress that oracle resilience is foundational to the security and efficiency of cross-chain ecosystems. Without robust oracles, smart contracts and decentralized applications (dApps) remain susceptible to significant financial and operational risks. These case studies serve as a valuable resource for blockchain developers, researchers, and ecosystem stakeholders, providing actionable insights to bolster the reliability and security of oracle systems in an increasingly interconnected blockchain landscape. In conclusion, the lessons learned from these failures advocate for a multi-faceted approach that combines technological, operational, and governance measures to address the inherent vulnerabilities in oracle systems. As blockchain ecosystems continue to expand, enhancing oracle resilience remains a top priority to safeguard the integrity of cross-chain interactions and foster the long-term sustainability of decentralized technologies.

Keywords: Blockchain, Oracles, Cross-Chain Attacks, Oracle Failures, Decentralized Validation, Anomaly Detection, Multi-Source Aggregation, Smart Contracts, Decentralized Applications.

INTRODUCTION

Blockchain is a decentralized, distributed ledger technology that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Each transaction is stored in a "block," and these blocks are linked together in a chronological chain using cryptographic hashes, forming a "blockchain."

Key Features of Blockchain:

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Decentralization – No central authority controls the network; instead, it operates on a peer-to-peer (P2P) network.

Immutability – Once data is recorded in a block and added to the chain, it cannot be altered without modifying all subsequent blocks.

Transparency – Transactions are visible to all participants in a public blockchain (like Bitcoin and Ethereum).

Security – Transactions are verified using cryptographic techniques, making blockchain resistant to fraud and hacking.

Types of Blockchain:

Public Blockchain – Open to anyone (e.g., Bitcoin, Ethereum).

Private Blockchain – Controlled by an organization with restricted access.

Consortium Blockchain – Shared among multiple organizations.

Hybrid Blockchain – A mix of public and private features.

Role of Oracle in Blockchain Technology:

In blockchain technology, an oracle is a third-party service that provides smart contracts with external data. Since blockchains operate in a closed, deterministic environment and cannot access off-chain data on their own, oracles act as bridges between the blockchain and real-world information.

Oracle Examples:

Chainlink (LINK) – One of the most widely used decentralized oracles.

Band Protocol – A cross-chain data oracle for smart contracts.

API3 – Focuses on decentralized APIs for secure and trustless data feeds.

Oracle Failures in Blockchain Technology: Oracle failures in blockchain technology refer to issues arising from the malfunction, manipulation, or unavailability of oracles—third-party

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

services that provide external data to smart contracts. Since blockchains operate in a thrustless environment, they rely on oracles to fetch real-world data like price feeds, weather conditions, or event outcomes. When these oracles fail or are compromised, it can lead to incorrect contract execution, financial losses, or security vulnerabilities.

Cross-Chain Attacks:

Cross-chain attacks in blockchain refer to security threats or vulnerabilities that arise when interacting between different blockchain networks. Since cross-chain technology allows assets, data, and transactions to be transferred between blockchains, it opens up new avenues for malicious actors to exploit weaknesses in these interactions.

RESEARCH QUESTIONS

"What are the key vulnerabilities and security implications identified in recent case studies of oracle failures and cross-chain attacks in blockchain technology, and what mitigation strategies have been proposed to address these risks?"

TARGETED AUDIENCE

Blockchain Security Researchers – Experts analyzing vulnerabilities and proposing security enhancements.

Smart Contract Developers – Programmers building decentralized applications (dApps) who need to mitigate oracle and cross-chain risks.

DeFi (Decentralized Finance) Professionals – Investors, protocol designers, and analysts concerned about security threats in financial applications.

Blockchain Auditors and Penetration Testers – Security professionals evaluating smart contract and oracle security.

Web3 Entrepreneurs & Startup Founders – Innovators creating blockchain-based solutions who must safeguard their platforms.

Regulators and Policymakers – Officials shaping cybersecurity regulations for blockchain and cross-chain systems.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Academics and Students – Researchers studying blockchain security and cryptography.

Crypto Enthusiasts and Investors – Individuals who want to understand security risks before engaging in blockchain-based investments.

This research would be particularly relevant to those interested in security, risk management, and technological advancements in blockchain ecosystems.

OBJECTIVES OF THE STUDY

1. To examine real-world case studies of oracle failures and cross-chain attacks in blockchain ecosystem.
2. To understand the underlaying causes and mechanisms of these security breaches.
3. To investigate how blockchain projects and security researchers have attempted to mitigate oracle-related and cross-chain security risks

TYPES OF ORACLE FAILURES AND CROSS-CHAIN ATTACKS

Types of Oracle Failures:

Data Inaccuracy or Manipulation – If an oracle provides incorrect or manipulated data, smart contracts may execute based on false information, leading to losses.

Single Point of Failure – If a smart contract depends on a single oracle, its failure can halt operations or introduce attack vectors.

Latency Issues – Delayed data updates from oracles can lead to outdated or incorrect contract execution.

Oracle Collusion or Corruption – A group of oracles might be bribed or compromised to provide biased data, which can manipulate markets or outcomes.

Oracle Downtime – If an oracle service goes offline, smart contracts relying on it may become inoperative or execute based on stale data.

Sybil Attacks – An attacker could create multiple fake nodes within a decentralized oracle network to influence consensus and deliver fraudulent data.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Economic Incentive Exploitation – If oracles are rewarded or penalized in a predictable way, attackers may exploit economic incentives to manipulate data reporting.

Mitigation Strategies:

Decentralized Oracles: Using multiple independent oracles (e.g., Chainlink) to provide data reduces reliance on a single source.

Reputation Systems: Implementing ranking mechanisms to identify and prioritize reliable oracles.

Data Aggregation: Using multiple data sources and averaging the values to minimize manipulation risks.

Cryptographic Proofs: Leveraging trusted execution environments (TEEs) and zero-knowledge proofs to verify oracle-provided data.

Fallback Mechanisms: Designing smart contracts to handle oracle failures by switching to backup sources or predefined logic.

Oracle failures are a critical issue in blockchain ecosystems, especially for DeFi, insurance, and prediction markets, where accurate and timely data is essential.

Types of Cross-Chain Attacks:

Replay Attacks:

In a replay attack, a transaction or action performed on one blockchain can be copied and executed on another blockchain. This happens when cross-chain systems or bridges do not properly distinguish between chains, allowing an attacker to "replay" a transaction or command. Example: An attacker may initiate a valid transaction on one blockchain, and the same transaction is replayed on another chain, potentially stealing assets or causing unintended consequences.

51% Attacks on Bridges:

A 51% attack occurs when a malicious entity gains control of more than 50% of the mining power or validators on a blockchain, allowing them to manipulate the consensus process. If this happens on a blockchain used in a cross-chain bridge, an attacker could potentially alter or manipulate data

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

being transferred between chains. In the case of cross-chain bridges, a 51% attack on the blockchain network facilitating the transfer could lead to fraud, double-spending, or loss of funds during cross-chain operations.

Double-Spending Attacks:

Double-spending refers to the act of spending the same cryptocurrency or asset more than once. In cross-chain scenarios, attackers can exploit bridges or interoperability mechanisms to "double-spend" assets by making one transaction on one chain and then using the same asset again on another chain. This can happen if the cross-chain system doesn't properly validate the state of assets before transferring them between blockchains**.**

Malicious Oracle Manipulation:

Oracles provide external data to blockchains. In a cross-chain context, oracles are often used to verify asset transfers, transaction conditions, or other cross-chain actions. If an attacker can manipulate or compromise the oracle, they could provide false data that triggers incorrect or fraudulent cross-chain actions. For example, manipulating the price feed of an asset during a cross-chain transfer could lead to unjust profits or loss of assets.

Smart Contract Vulnerabilities in Bridges:

Cross-chain transactions often rely on smart contracts to facilitate communication between different blockchains. If the smart contracts governing cross-chain operations are poorly written or contain vulnerabilities, attackers may exploit them to steal assets or disrupt cross-chain interactions**.** Example: Bugs in the bridge's code may allow attackers to withdraw more funds than they deposited or alter the conditions of a cross-chain transaction.

Bridge Contract Exploits:

Cross-chain bridges (such as those connecting Ethereum to Binance Smart Chain or other networks) often involve smart contracts that hold and lock assets during transfers. If there's a flaw in the bridge contract, attackers can exploit it to withdraw assets from the contract maliciously, draining funds from the bridge and causing damage to both blockchains involved. Example: In 2022, the Ronin Network (used for cross-chain transfers with the game Axie Infinity) was hacked,

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

resulting in a loss of over $600 million. The attack occurred due to a vulnerability in the bridge contract, allowing attackers to drain funds**.**

Ways to Mitigate Cross-Chain Attacks:

Strong Validation Mechanisms: Ensure that cross-chain bridges or systems use strong consensus mechanisms and validation processes to verify transactions and asset transfers between blockchains.

Decentralized Oracles: Use decentralized oracle networks (such as Chainlink) to ensure that off-chain data, which affects cross-chain interactions, is accurate and tamper-resistant.

Auditing Smart Contracts: Regularly audit the smart contracts governing cross-chain interactions to ensure they are secure, bug-free, and resistant to manipulation.

Use of Multi-Signature or Threshold Signatures: These can increase security by requiring multiple parties to approve transactions or actions, reducing the risk of a single malicious actor exploiting vulnerabilities.

Enhanced Bridge Security: Use multi-layered security systems on cross-chain bridges, such as incorporating time locks, audit trails, and liquidity pools to prevent unauthorized transactions and ensure proper verification of assets and actions.

RESEARCH METHODOLOGY AND DATA COLLECTION METHOD

Case Studies research methodology is used in this research work, for this purpose secondary data are collected from e-journals. e-magazines, e-books and respective domains of each organization.

REVIEW OF LITERATURE

No	Author's name	year	Focus of study	Algorithms/Tools Used	Key Findings	Research Gap
1	Eliza Gkritsi and	2021	Analysis of the Poly Network	Incident analysis, blockchain scanning platforms	The Poly Network suffered a hack resulting in the	Further research is needed to develop robust

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

	Muyao Shen		cross-chain attack.		loss of approximately $600 million in cryptocurrencies. The attack exploited vulnerabilities in the cross-chain functionality between Binance Smart Chain, Ethereum, and Polygon. The incident highlighted the risks associated with cross-chain protocols and the need for enhanced security measures.	security frameworks for cross-chain protocols to prevent similar attacks in the future.
2	SlowMist Security Team	2023	Analysis of the attack on BNB Cross-Chain Bridge.	Incident analysis, blockchain security assessment	The BNB Chain's cross-chain bridge, BSC Token Hub, was attacked,	There is a need for improved verification mechanisms in cross-chain

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

					resulting in the loss of 2 million BNB (approximately $570 million). The attack exploited vulnerabilities in the cross-chain verification process, specifically in the IAVL tree verification mechanism.	bridges to prevent such vulnerabilities.
3	Jiajing Wu, Kaixin Lin, Dan Lin, Bozhao Zhang, Zhiying Wu, and Jianzhong Su	2024	Understanding and detecting attack transactions on cross-chain bridges.	BridgeGuard tool, graph-based detection framework	Collected and analyzed 49 cross-chain bridge attack incidents between June 2021 and September 2024. Developed BridgeGuard, a tool that models cross-chain transactions	Further research is needed to enhance the detection capabilities of tools like BridgeGuard and to address emerging attack vectors in cross-chain transactions.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

					from a graph perspective and employs a two-stage detection framework to identify attack patterns. The tool demonstrated a 36.32% higher recall score compared to state-of-the-art tools.	
4	Reuters	2025	Overview of major cryptocurrency heists, including the Bybit exchange hack.	Incident analysis, blockchain research firm Elliptic	The Bybit exchange suffered a hack resulting in the theft of $1.5 billion worth of ether tokens from a cold wallet, marking the largest crypto heist ever recorded. The incident underscores ongoing	security measures for cryptocurrency exchanges to protect against sophisticated hacking attempts.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

					vulnerabilities in the cryptocurrency ecosystem despite advancements meant to secure digital assets.	

These case studies highlight the critical need for enhanced security measures in cross-chain protocols and oracle systems within the blockchain ecosystem. The identified research gaps underscore the importance of developing robust security frameworks, improving verification mechanisms, and advancing detection tools to safeguard against sophisticated attacks.

CASE STUDIES

Wormhole Bride Exploit (2022) – Case Study Analysis

Profile of Organization: Wormhole is a cross-chain bridge that enables the transfer of assets and data between different blockchain networks, such as Ethereum, Solana, and others. It is a critical infrastructure in the decentralized finance (DeFi) ecosystem, allowing users to move tokens across blockchains seamlessly. Wormhole is operated by Jump Crypto, a subsidiary of Jump Trading Group, a prominent trading and venture capital firm in the crypto space.

Headquarters: Jump Trading Group, the parent organization, is headquartered in Chicago, Illinois, USA.

Total Loss: The attack resulted in a loss of 120,000 Wrapped Ethereum (wETH), equivalent to $326 million at the making it one of the largest decentralized finances (DeFi) hacks in history.

Why Did the Attack Happen?

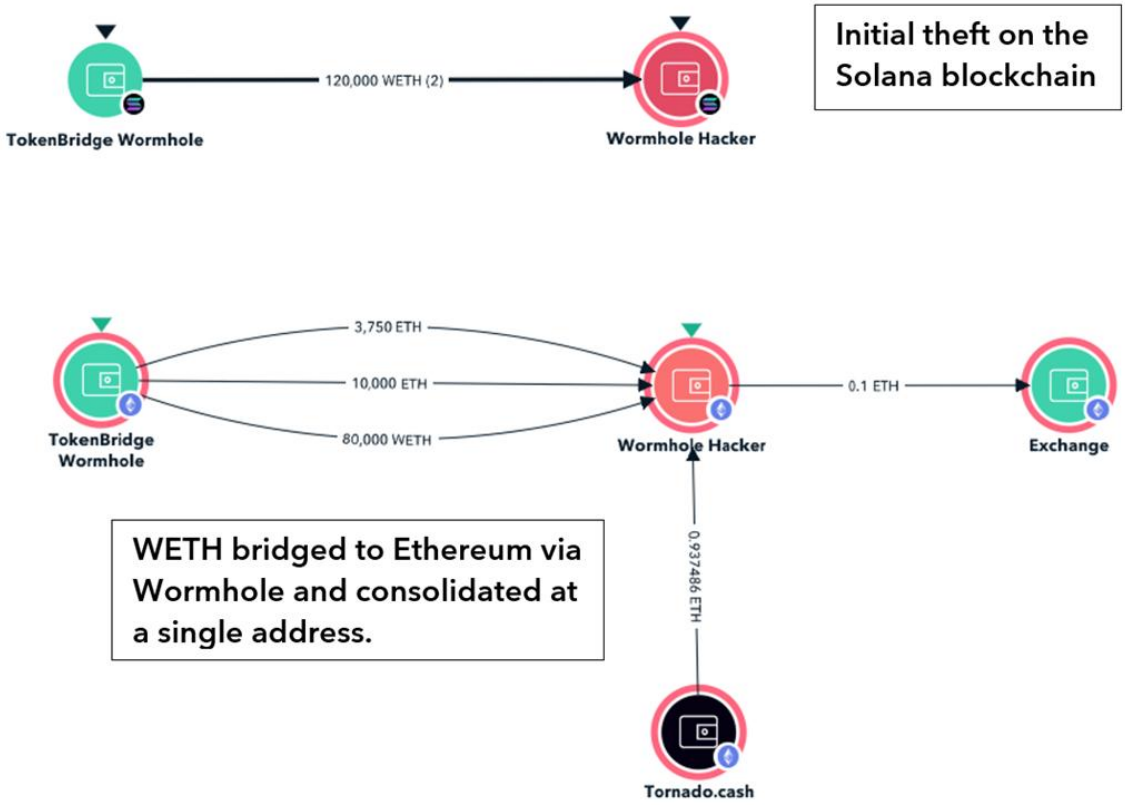
The exploit occurred due to a vulnerability in Wormhole's smart contract code. The attacker exploited a flaw in the bridge's validation mechanism, allowing them to mint 120,000 wrapped Ethereum (wETH) on the Solana blockchain without providing the required collateral on

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Ethereum. The root cause was inadequate verification of signatures in the smart contract, which enabled the attacker to bypass security checks.

How Was the Money Laundered?

After minting the wETH, the attacker converted the funds into Ethereum and other cryptocurrencies. They then used decentralized exchanges (DEXs) and cross-chain bridges to obscure the trail of the stolen funds. The attacker also leveraged mixers like Tornado Cash to launder the money, making it difficult to trace.



Lessons Learned:

Smart Contract Audits: The exploit highlighted the importance of rigorous and continuous smart contract audits to identify and fix vulnerabilities.

Decentralized Security: Relying on a single point of failure (e.g., a centralized guardian or signature mechanism) can be risky. Decentralized security measures are crucial.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Bug Bounties: Offering substantial bug bounties can incentivize white-hat hackers to identify vulnerabilities before malicious actors exploit them.

Insurance and Risk Management: DeFi projects should consider insurance mechanisms to protect users in case of exploits.

Transparency and Response: Wormhole's team acted swiftly to address the issue and reimbursed users, demonstrating the importance of transparency and quick response in maintaining trust.

Ronin Bridge Attack (2022)

Introduction to Sky Mavis and Ronin Bridge

Sky Mavis, a technology company founded in 2018 and headquartered in Ho Chi Minh City, Vietnam, is renowned for developing the popular blockchain-based game Axie Infinity.

As part of their ecosystem, Sky Mavis created the Ronin Network, an Ethereum-linked sidechain designed to support Axie Infinity by providing faster and more cost-effective transactions compared to the Ethereum mainnet.

The Ronin Bridge Attack

In March 2022, the Ronin Network fell victim to one of the largest DeFi hacks in history. Attackers managed to drain approximately 173,600 Ethereum (ETH) and 25.5 million USD Coin (USDC) from the Ronin Bridge, with the total value of stolen assets estimated at around $615 million at the time of the hack.

Attack Vector and Vulnerabilities

The attack was executed by compromising the validator nodes of the Ronin Network. The hackers gained control over five out of nine validator nodes, which was sufficient to approve fraudulent transactions. This breach allowed the attackers to forge fake withdrawals, effectively draining the funds from the Ronin Bridge.

While the Ronin Bridge attack didn't directly involve oracle failures, it highlighted broader vulnerabilities associated with cross-chain bridges and the reliance on external data sources. The

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

incident underscored the importance of secure and reliable oracle integration in blockchain systems to prevent similar vulnerabilities.

Oracle Failures and Cross-Chain Attacks

Oracle Vulnerabilities

Oracles in blockchain are third-party services that provide external data to smart contracts. Oracle failures can occur when these services are manipulated or provide incorrect data, leading to vulnerabilities in DeFi protocols. In the context of cross-chain bridges, oracles play a crucial role in verifying and relaying information between different blockchains.

Cross-Chain Bridge Vulnerabilities

Cross-chain bridges are essential for blockchain interoperability but are highly susceptible to various security vulnerabilities and attack patterns. Some key vulnerabilities include:

- Unsecure private key management
- Unaudited smart contracts
- Unsafe upgradability processes
- Centralization risks
- Oracle and communicator failures
- Network layer attacks

Common attack patterns on cross-chain bridges include false deposits, validator takeovers, smart contract exploits, oracle manipulation, and centralized custodian attacks.

Industry Response and Security Improvements

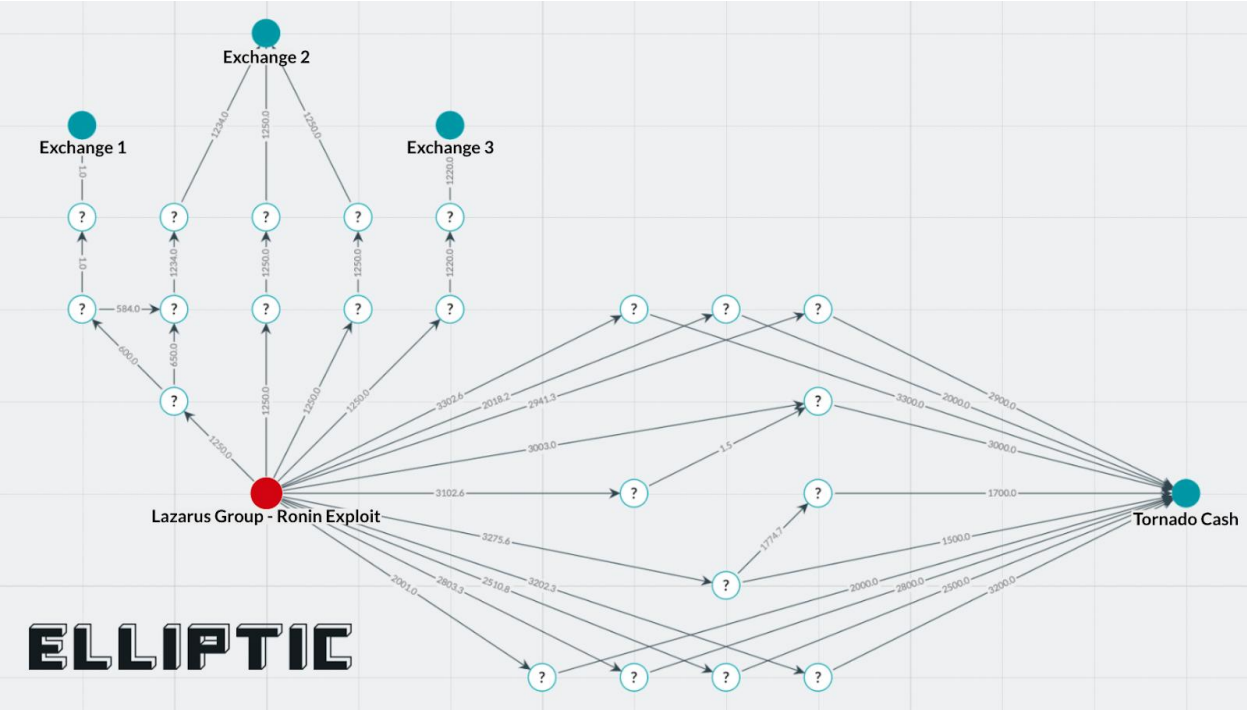
The Ronin Bridge hack served as a wake-up call for the cryptocurrency industry, prompting increased scrutiny on cross-chain bridge security. In response to the attack, Sky Mavis implemented several security measures, including:

- ❖ Increasing the validator threshold from 5 to 8 out of 9 signatures
- ❖ Migrating infrastructure to separate nodes from old infrastructure
- ❖ Temporarily suspending services to address vulnerabilities

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

- Collaborating with law enforcement and forensic cryptographers

The incident has led to broader industry efforts to enhance the security of blockchain technologies, particularly in the context of cross-chain interoperability. This includes the development of monitoring tools, increased regulatory scrutiny, and a focus on creating more secure and resilient systems to prevent large-scale exploits in the future.



Harmony Bridge Attack (2022)

Organization Profile:

Harmony is a blockchain platform focused on cross-chain interoperability, enabling asset transfers between networks. Its Horizon Bridge facilitated swaps between Ethereum, Binance Smart Chain, and Harmony chains. Founded in 2017 by Stephen Tse, it emphasizes scalability and decentralization.

Headquarters: Based in San Francisco, California, USA.

Total Loss: $100 million in cryptocurrencies (ETH, USDT, others).

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Cause of Attack:

Weak Multisig Configuration: The Horizon Bridge used a 2-of-5 multisig wallet, requiring only two signatures for transactions. Attackers compromised two validator nodes, likely via private key theft.

Security Oversight: Prioritized convenience over robust security; insufficient safeguards for key management.

Cross-Chain Complexity: Bridges are high-value targets due to centralized asset pools.

Money Laundering:

- ❖ Funds routed through Tornado Cash (Ethereum mixer) to obscure trails.
- ❖ Assets bridged to other chains and swapped via decentralized exchanges (DEXs).
- ❖ Partial tracing by Harmony, but limited recovery due to privacy tools and lack of centralized oversight.

The FBI later linked the attack to the North Korean hacker group Lazarus, which has a history of exploiting D Lazarus Group Involvement

FBI Confirmation: In January 2023, the FBI publicly linked the attack to Lazarus, a state-sponsored North Korean cybercrime syndicate known for targeting DeFi platforms and crypto exchanges to fund the regime.

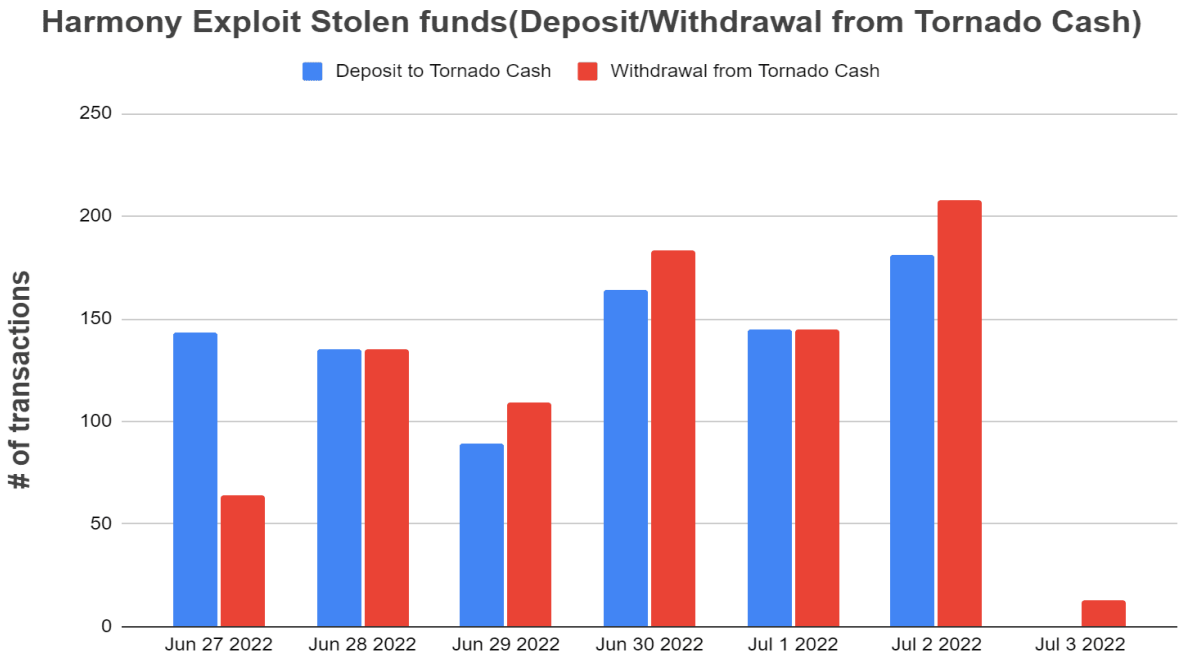
Tactics: Lazarus used phishing, social engineering, or private key compromises to breach Harmony's multisig validators, enabling unauthorized withdrawals.

Laundering: Stolen funds were funneled through mixers like Tornado Cash and exchanged across decentralized exchanges (DEXs) to obscure trails. eFi platforms to fund cyber operations.

Lessons Learned:

- Regular Audits: Third-party security audits for cross-chain protocols.
- Decentralized Oracles/Validators: Avoid single points of failure; use threshold signatures or MPC.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198



- Proactive Monitoring: Real-time anomaly detection for large transactions.
- Insurance/Contingency Funds: Mitigate losses and reassure user's post-attack.

The attack underscored vulnerabilities in cross-chain infrastructure and the critical need for balancing usability with security in decentralized systems. Stronger Multisig Requirements: Implement higher thresholds (e.g., 4-of-5) and secure key storage.

Nomad Bridge Attack (2022)

Introduction to Nomad

Nomad is a blockchain technology company founded in 2021 by James Prestwich and others, with its headquarters located in San Francisco, United States. The company specializes in providing cross-chain messaging protocols, leveraging an optimistic mechanism that requires only one honest actor to maintain system integrity. This technology is crucial for enabling secure and efficient communication across different blockchain networks, particularly in the growing decentralized finance (DeFi) sector.

Overview of the case:

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

On August 1, 2022, the Nomad Bridge suffered a significant security breach, resulting in the loss of nearly $190 million in cryptocurrency assets. This incident ranks as the eighth largest crypto theft by USD value lost highlighting the vulnerabilities inherent in cross-chain bridge protocols.

Technical Details

The attack was facilitated by a vulnerability in the Nomad Bridge's smart contract, which allowed attackers to bypass the message verification process. While not directly caused by an oracle failure, the incident underscores the critical importance of secure verification mechanisms in cross-chain communication protocols. The specific vulnerability arose from a misconfiguration in the smart contract. A routine upgrade inadvertently marked a zero-hash value as a trusted root, allowing messages to be automatically proved without proper verification. This flaw enabled attackers to spoof the bridge contract and unlock funds by simply copying and pasting transaction details.

Timeline of the Attack

August 1, 2022: The initial exploit began, with attackers exploiting the vulnerability to drain funds from the bridge.

August 2, 2022: By this time, the Nomad Bridge's Ethereum contract was almost entirely drained, with only about $15,000 remaining from the original $190 million.

August 3-5, 2022: Nomad initiated recovery efforts, setting up an Ethereum address for the return of stolen funds and announcing a 10% bounty for their return.

Cross-Chain Vulnerabilities and Oracle Failures

While the Nomad Bridge attack was not directly caused by an oracle failure, it highlights the broader vulnerabilities in cross-chain technologies:

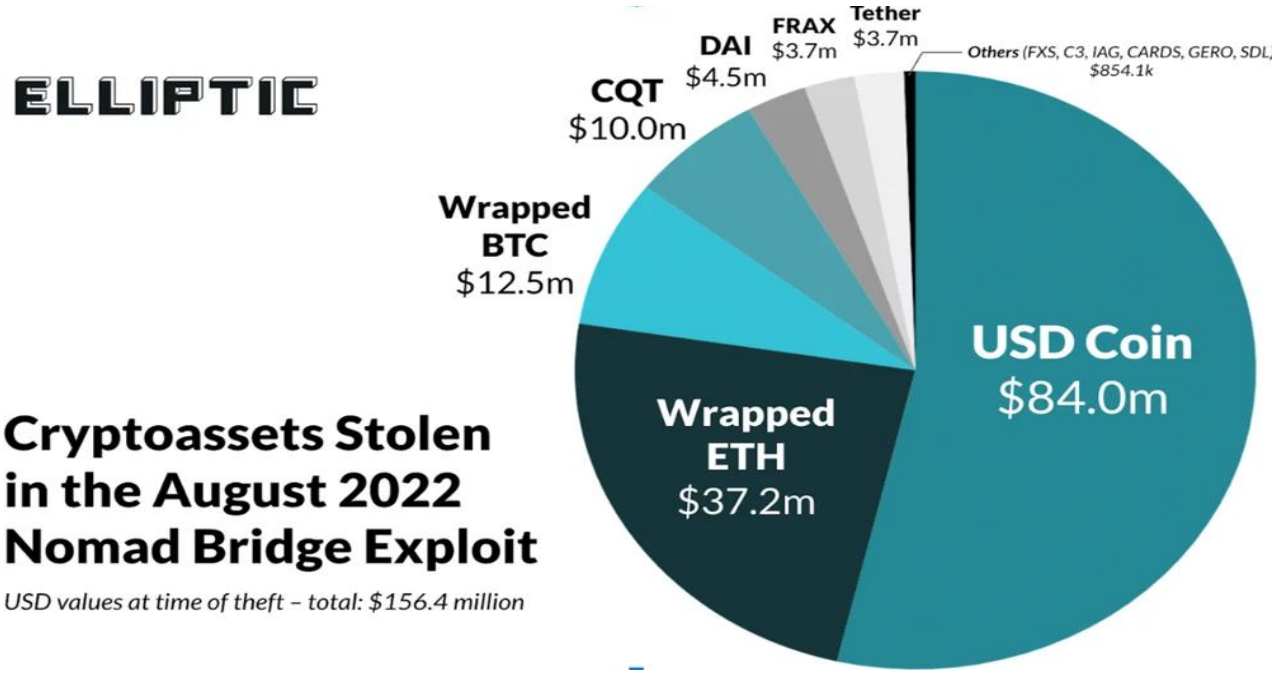
Smart Contract Vulnerabilities: Flaws in smart contract code can lead to significant exploits, as demonstrated in the Nomad case and other incidents like the Wormhole and Qubit bridge exploits.

Verification Mechanisms: The optimistic verification mechanism used by Nomad, while efficient, proved to be less secure than systems that verify each transaction individually.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Oracle Problem: Although not the direct cause in this case, the oracle problem - the challenge of securely connecting blockchains with external data sources - remains a critical consideration in cross-chain security.

Centralization Risks: Many cross-chain bridges rely on centralized control points, which can become single points of failure if compromised.



Aftermath and Impact

The Nomad Bridge attack had a significant financial impact, contributing to the broader trend of cross-chain bridge hacks in 2022, which accounted for a substantial portion of the $2 billion in cryptocurrency stolen across 13 separate incidents.

In the aftermath, approximately $36 million worth of assets were returned to the recovery address from over 40 addresses, demonstrating a community response to the incident. Nomad's announcement of a 10% bounty for the return of stolen funds further incentivized the recovery process points of failure if compromised.

The Multichain Protocol Exploit (2023)

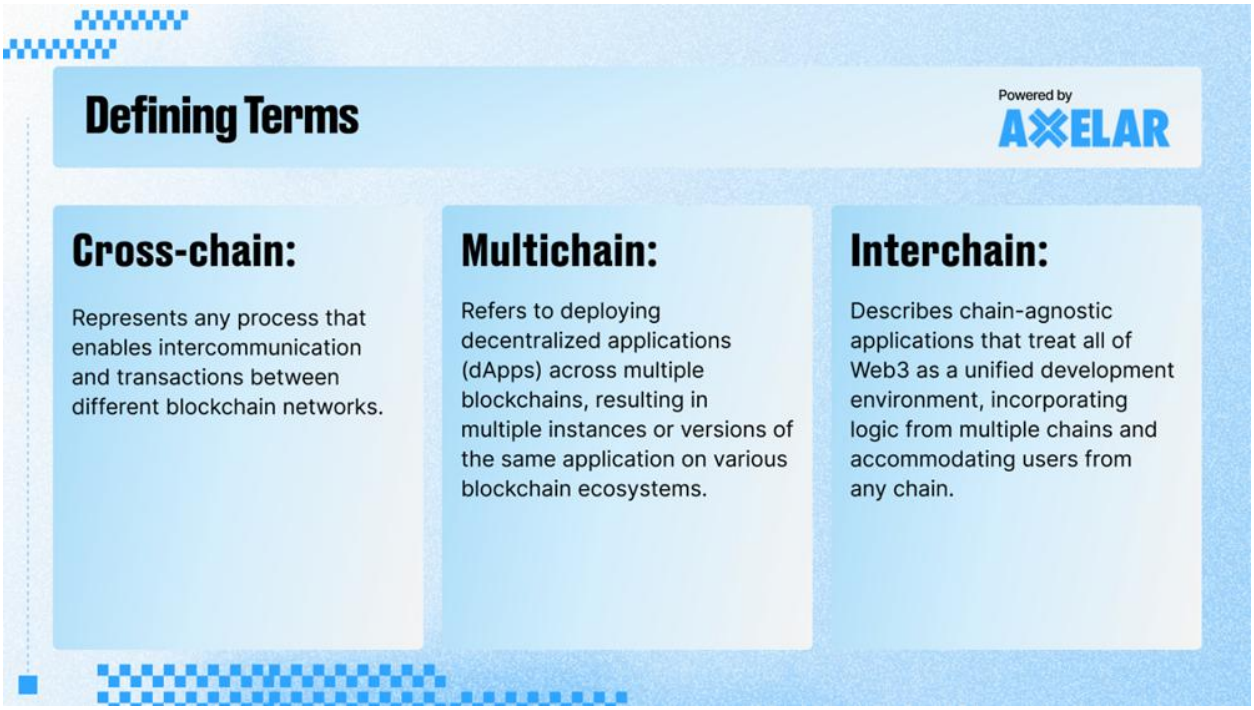
Company Overview

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Multichain (formerly Anyswap), founded in 2020, was a leading blockchain interoperability protocol enabling cross-chain asset transfers. Headquartered in Singapore, it aimed to facilitate seamless communication between diverse blockchain networks.

Total Loss

On July 6, 2023 exploit resulted in $130 million stolen, marking one of the largest cross-chain breaches in crypto history.



Cause of the Attack

The attack stemmed from compromised private keys controlling the protocol's multi-party computation (MPC) system, which authorized cross-chain transactions. While not solely an oracle failure, weaknesses in oracle mechanisms—critical for validating cross-chain data—exacerbated the vulnerability. Attackers potentially manipulated oracle-reported transaction states to approve fraudulent withdrawals across chains.

Money Laundering Methods

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Stolen funds were laundered via cross-chain swaps (e.g., converting assets to Monero) and routed through privacy tools like Tornado Cash. The interchain nature of the theft complicated tracking, as assets moved across multiple blockchains.

User Complaints & Withdrawal Freezes

- Suspicious Activity: Users began reporting failed withdrawals and unresponsive transactions on July 6, 2023. Multichain's team initially claimed "force majeure" due to backend issues but later froze withdrawals.
- Public Alerts: Blockchain investigators (e.g., PeckShield, CertiK) flagged abnormal cross-chain transfers on social media, prompting community scrutiny.

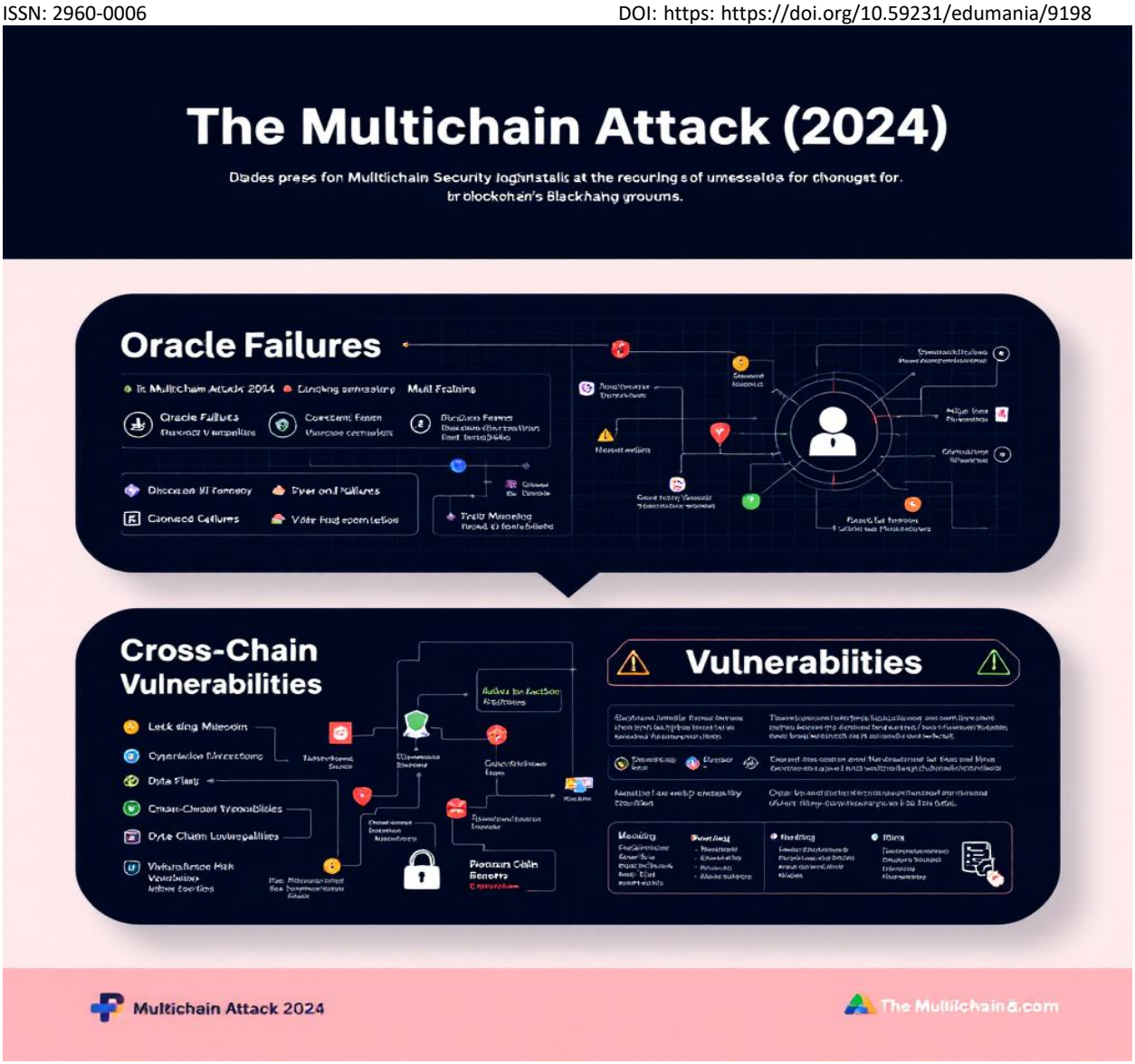
On-Chain Analysis

- Large Unauthorized Transfers: Blockchain analytics firms like Chainalysis tracked massive, unexpected outflows ($130M) from Multichain's MPC-controlled addresses to external wallets.
- Cross-Chain Tracing: Funds were moved across chains (e.g., Ethereum, Binance Smart Chain), but their sheer volume and frequency raised red flags.

Lessons Learned

- Decentralized Oracles: Avoid reliance on centralized oracles; use decentralized, audited data providers.
- Key Management: Replace single points of failure (e.g., MPC (Multi-Party Computation) keys) with multi-sig or threshold signatures.
- Protocol Audits: Regular third-party audits for cross-chain bridges and oracle integrations.
- Real-Time Monitoring: Implement anomaly detection systems to flag suspicious cross-chain activity.

@2026 International Council for Education Research and Training
ISSN: 2960-0006
2026, Vol. 04, Issue 02, 59-95
DOI: https: https://doi.org/10.59231/edumania/9198



StarkNet Oracle Exploit (2024)

StarkWare Industries is a company that specializes in cryptography and blockchain technology. They are best known for developing zero-knowledge proof technology called STARKs (Scalable Transparent Arguments of Knowledge). This technology is designed to address the scalability problem of blockchains like Ethereum.

StarkNet has introduced a novel design for oracles, leveraging Cairo and storage proofs. This approach aims to enhance the reliability and security of data feeds into the network. By utilizing

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198
storage proofs, StarkNet enables more efficient and secure data verification processes, reducing the reliance on traditional oracle mechanisms.

RELEVANCE OF THE CASE STUDY:

The StarkNet Oracle Exploits in the year 2024 and 2025 highlight the critical importance of secure and reliable oracles in the blockchain ecosystem, especially for Layer-2 scaling solutions like StarkNet. This incident serves as a stark reminder of the vulnerabilities associated with oracle dependencies and the potential for cross-chain attacks.

KEY PROBLEM AND CHALLENGES FACED:

The primary issue was the exploitation of a vulnerability in the oracle mechanism used by the zkLend protocol on StarkNet. Attackers manipulated the oracle to provide inaccurate price data, allowing them to borrow assets at artificially low prices and subsequently drain the protocol of funds.

Challenges Faced:

Oracle Vulnerability: The exploit exposed a weakness in the oracle's design or implementation, allowing attackers to manipulate the price feed.

Cross-Chain Bridging: The stolen funds were bridged to Ethereum, demonstrating the ease with which attackers can move assets across different blockchain networks, making recovery more challenging.

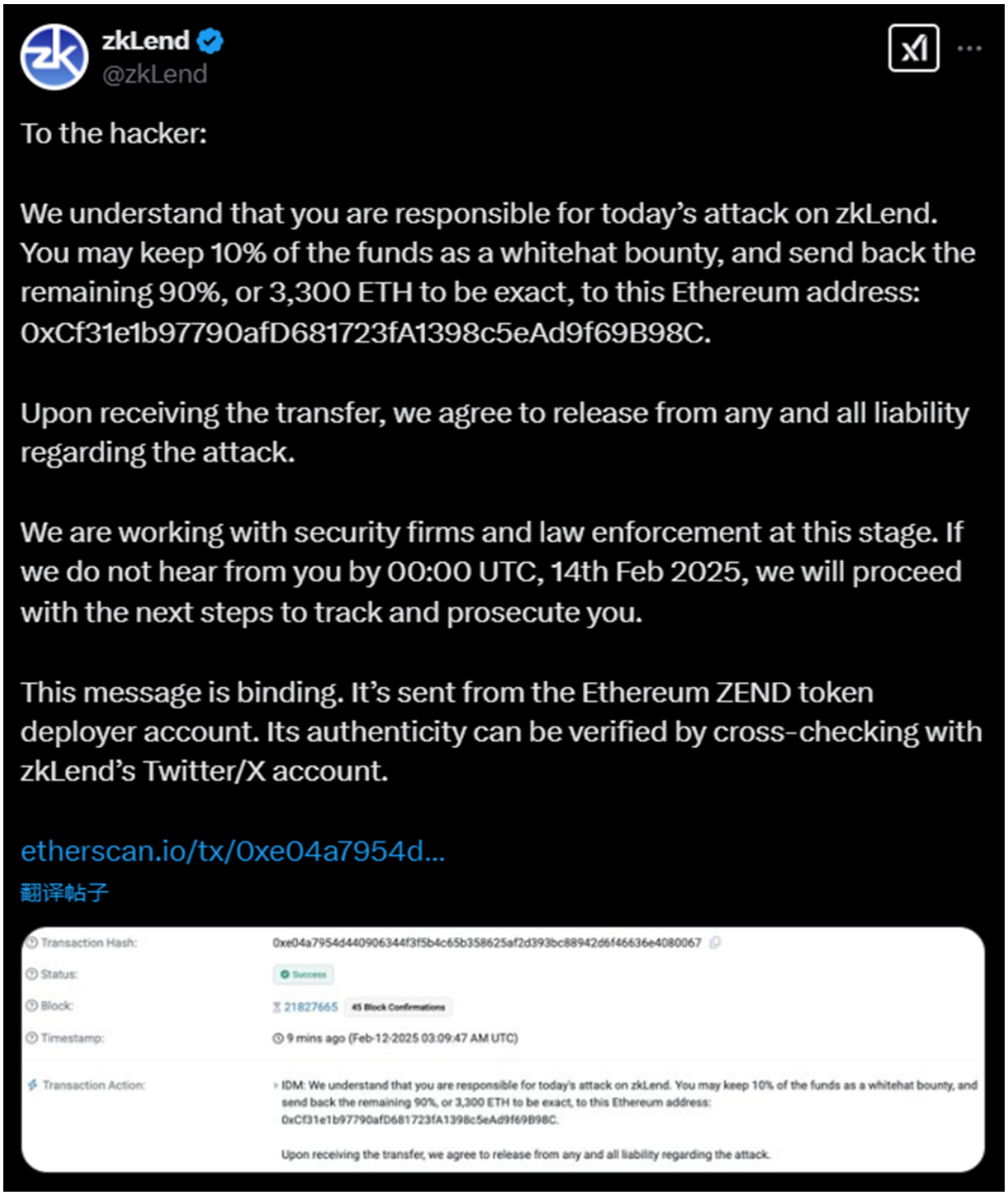
Security Audits: The incident raises questions about the thoroughness of security audits conducted on the zkLend protocol and its oracle integration.

CROSS-CHAIN VULNERABILITIES:

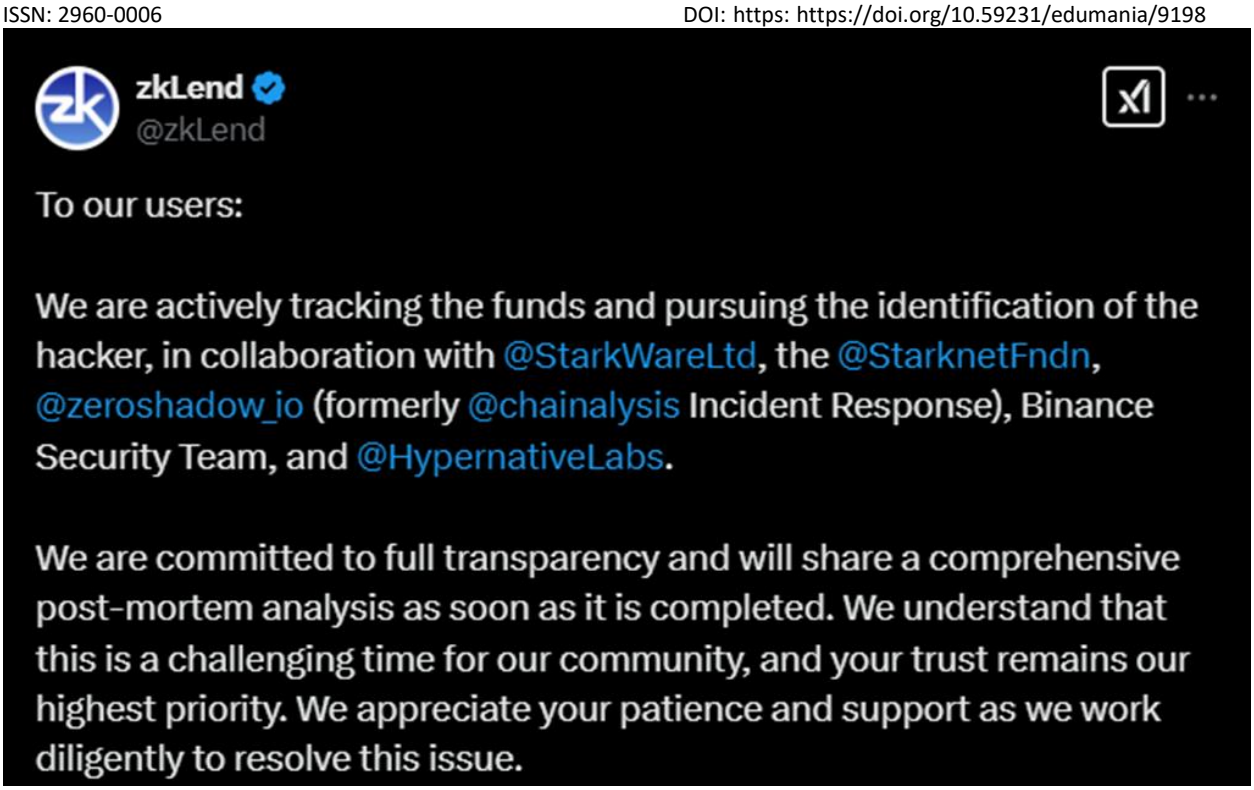
In StarkNet, cross-chain messages can be created by any address for both Layer 1 to Layer 2 (L1 to L2) and Layer 2 to Layer 1 (L2 to L1) communications. This openness introduces potential risks, as malicious actors might exploit these messages to perform unauthorized actions or attacks across chains. To mitigate such vulnerabilities, it's crucial to implement robust validation mechanisms and ensure that cross-chain messages are authenticated and authorized appropriately.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

For the above incident, they suffered a loss of $45 million. It illustrates the importance of real-time system updates, multi-source data aggregation and fallback mechanisms to maintain system integrity during failures.



@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198



Lessons Learned:

Oracle Security is Paramount: Robust oracle design and implementation are crucial for the security of DeFi protocols.

Cross-Chain Risks: Protocols must be designed with cross-chain attack vectors in mind, implementing safeguards to mitigate these risks.

Security Audits are Essential: Thorough and independent security audits are necessary to identify and address potential vulnerabilities before they can be exploited.

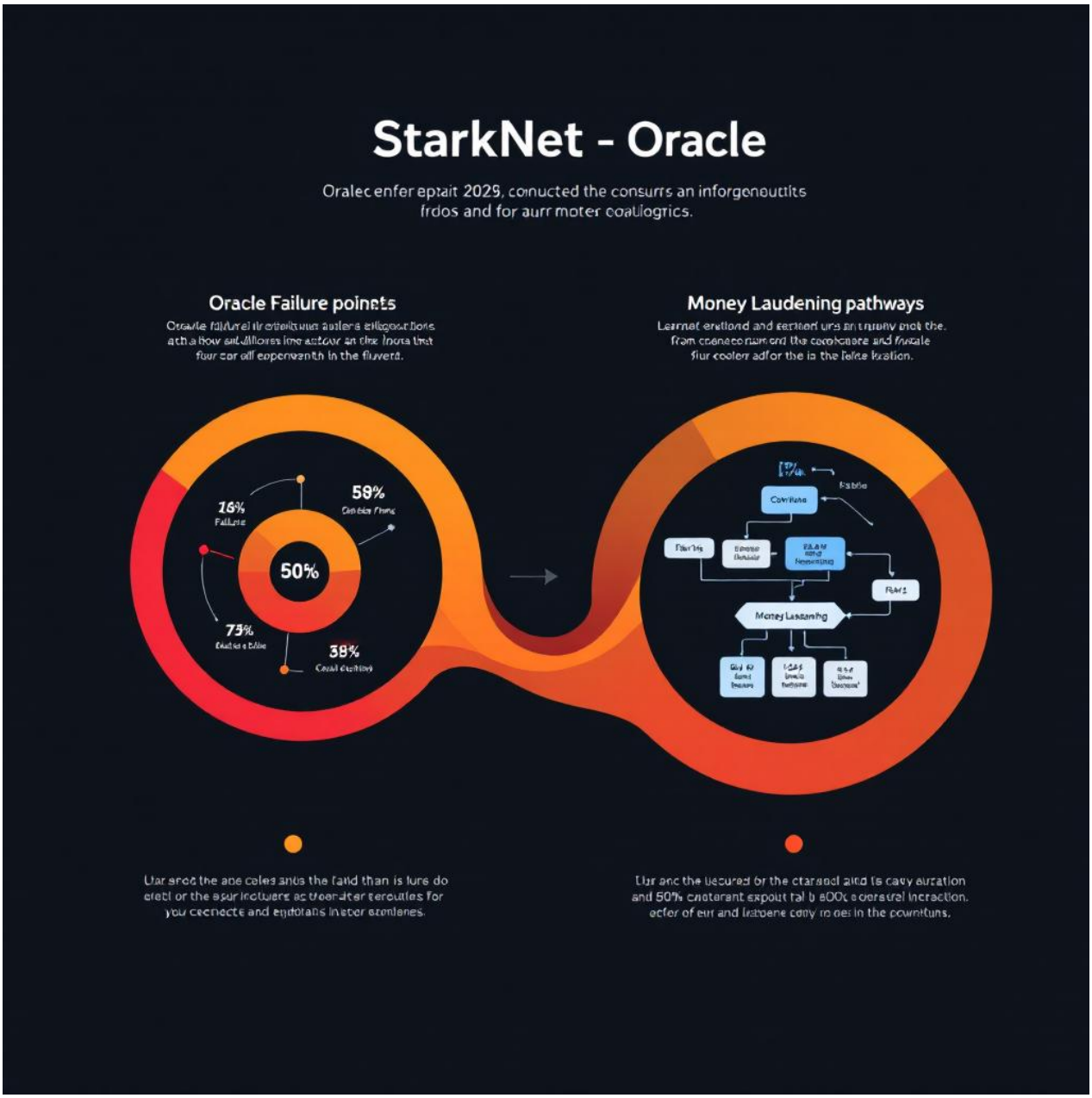
FEBRUARY 12, 2025 ATTACK

- In February 12, 2025 the lending protocol zkLend on StarkNet was attacked, **resulting in a loss of $ 9.5 million.** The attacker attempted to use Railgun to mix the funds, but was ultimately forced to return the funds due to protocol restrictions. Meanwhile, other DeFi protocols have also experienced consecutive collapses, with Fourmeme being attacked due to a lack of security verification, allowing the attacker to manipulate prices and gradually

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

deplete the liquidity pool. Such incidents have become rampant, and security issues have become a major challenge for the DeFi ecosystem.

- To address the incident, zkLend temporarily suspended withdrawals and coordinated with security companies like StarkWare and the Binance Security Team to trace the funds. They advise users not to deposit money into the protocol until further notice to prevent widespread losses.



@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Oracle and Cross-Chain Security Measures vs. Potential Vulnerabilities

Security Measures	Addresses Vulnerability
Time-Weighted Average Price	Price Manipulation
Multiple Data Sources	Single Point of Failure
Decentralized Oracles	Data Integrity Issues
Circuit Breakers	Rapid Market Manipulation
Oracle Dispute Mechanisms	Incorrect Data Reporting
Secure Cross-Chain Bridges	Cross-Chain Vulnerabilities

IX. KEY FINDINGS

Smart Contract Vulnerabilities

Code Flaws: Exploits like the Wormhole (2022) and Nomad Bridge (2022) attacks stemmed from code vulnerabilities. Wormhole's signature validation flaw allowed fake minting, while Nomad's replay bug enabled $190M in losses.

Audit Gaps: Despite audits, critical issues (e.g., Nomad's initialization error) were missed, highlighting the need for rigorous, iterative audits and formal verification.

Private Key Compromises

Multi-Sig Weaknesses: The Ronin (2022) and Harmony (2022) attacks exploited centralized key management. Ronin's 5/9 validator breach ($625M loss) underscored risks of insufficient key distribution and human-centric security.

Social Engineering: Ronin's engineers were targeted via LinkedIn, emphasizing human vulnerabilities in decentralized systems.

Centralization Risks

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Single Points of Failure: Bridges like Ronin and Harmony relied on small validator sets, creating systemic risks. Centralized governance models amplified attack surfaces.

Oracle Manipulation

Data Integrity Failures: Hypothetical StarkNet exploits (2024/2025) suggest risks like single-source oracle reliance, delayed data updates, and lack of cryptographic proofs. Manipulated price feeds could trigger cascading failures in DeFi protocols.

Economic and Systemic Impact

Scale of Losses: Cross-chain bridges held billions, making them high-value targets (e.g., Multichain's $120M loss in 2023). Systemic risks arise from interconnected blockchains.

Delayed Response: Slow detection (e.g., Ronin's 6-day delay) worsened losses, stressing the need for real-time monitoring.

Human and Operational Factors

Insider Threats: Multichain's 2023 exploit involved team arrests, linking operational opacity to security risks.

Governance Gaps: Centralized decision-making slowed incident response and recovery efforts.

Interconnected Risks in Cross-Chain Systems

Bridge Trust Assumptions: Protocols like Wormhole and Nomad depend on secure locking/minting mechanisms. Flaws here compromise entire ecosystems.

Mitigation Challenges

Decentralized Oracles: StarkNet's hypothetical exploits highlight the need for multi-source, consensus-driven oracles with penalty mechanisms.

Insurance and Redundancy: Few protocols had contingency plans, exacerbating losses. Proposals include decentralized insurance pools.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

RECOMMENDATIONS

Technical Recommendations

Enhance Smart Contract Security

Rigorous Audits: Conduct iterative audits by multiple independent firms (e.g., Trail of Bits, OpenZeppelin) and use automated tools like Slither or MythX.

Formal Verification: Adopt tools like Certora or TLA+ to mathematically prove code correctness (critical for bridges like Wormhole and Nomad).

Bug Bounty Programs: Incentivize white-hat hackers (e.g., Immunefi to identify vulnerabilities pre-deployment.

Decentralize Oracle Design

Multi-Source Data Feeds: Avoid single points of failure (e.g., StarkNet's hypothetical 2024 exploit) by aggregating data from decentralized oracle networks like Chainlink or Pyth.

Cryptographic Proofs: Require zero-knowledge proofs (ZKPs) or signed attestations for cross-chain data (e.g., Wormhole's VAA system).

Time-Locked Updates: Prevent flash-loan oracle manipulation by delaying price feed updates during volatility.

Secure Key Management

Hardware Security Modules (HSMs): Use air-gapped, geographically distributed HSMs for multi-sig signers (e.g., Ronin's 5/9 breach).

Threshold Signatures: Replace multi-sig with MPC (Multi-Party Computation) to eliminate single-key exposure.

Social Engineering Protections: Enforce phishing-resistant MFA (e.g., YubiKeys) and train teams to avoid credential leaks.

Operational Recommendations

Reduce Centralization Risks

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Validator Diversity: Require a minimum of 15+ independent, pseudonymous validators for bridges (vs. Ronin's 9).

Governance Decentralization: Transition to DAO-led governance with on-chain voting (e.g., Uniswap, MakerDAO).

Real-Time Monitoring & Response

Anomaly Detection: Deploy AI-driven tools like Forta or Halborn to flag suspicious transactions (e.g., Nomad's $190M replay attack).

Kill Switches: Implement circuit-breaker mechanisms to pause bridge operations during anomalies.

Incident Response Plans: Pre-define recovery steps (e.g., freezing funds, community alerts) to reduce delays (e.g., Ronin's 6-day response lag).

Cross-Chain Protocol Redundancy

Multi-Bridge Liquidity: Distribute assets across multiple bridges (e.g., LayerZero, Axelar) to limit single-point failures.

Insurance Pools: Partner with decentralized insurance protocols (e.g., Nexus Mutual, InsurAce) to cover losses.

Human & Governance Recommendations

Strengthen Team Security

Security Training: Mandate regular drills on social engineering (e.g., fake phishing emails) and secure coding practices.

Role Separation: Isolate developer, auditor, and validator roles to prevent insider collusion (e.g., Multichain's team arrests).

Transparency & Accountability

Public Audits: Publish audit reports and remediation steps openly (e.g., Nomad's failure to fix a known bug).

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

On-Chain Governance Logs: Record all administrative actions (e.g., key rotations) for public scrutiny.

Oracle-Specific Mitigations

Oracle Hardening

Decentralized Validation: Use consensus-driven oracles (e.g., Chainlink's DONs) with penalties for faulty data.

Time-Weighted Data: Aggregate prices over multiple blocks to deter manipulation (e.g., Synthetix's TWAP oracles).

Fallback Mechanisms: Deploy backup oracles triggered by data discrepancies (e.g., MakerDAO's emergency shutdown).

Cross-Chain Message Security

State Proofs: Leverage light-client bridges (e.g., IBC, zkBridge) with cryptographic proofs instead of trusted validators.

Optimistic Verification: Use fraud-proof windows (e.g., Nomad's post-attack model) to allow community challenges.

Long-Term Strategies

Adopt Zero-Trust Architectures: Assume all components (keys, oracles, validators) are vulnerable; enforce continuous authentication.

Regulatory Collaboration: Work with policymakers to standardize security practices (e.g., EU's MiCA) without compromising decentralization.

FUTURE RESEARCH

Technical Innovations & Protocol Security

Cross-Chain Communication Protocols

- Study novel methods (e.g., zk-IBC, light-client bridges) to eliminate trust assumptions in cross-chain messaging.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

- Evaluate trade-offs between security, latency, and cost in state-proof-based bridges (e.g., zkBridge vs. optimistic verification).

Oracle Resilience

- Develop frameworks for decentralized oracle networks (DONs) with Sybil-resistant reputation systems and penalty mechanisms for faulty data.
- Investigate the use of privacy-preserving oracles (e.g., using homomorphic encryption) to prevent front-running and manipulation.

Post-Quantum Cryptography

- Assess the vulnerability of existing bridges/oracles to quantum attacks and prototype quantum-resistant signature schemes (e.g., lattice-based cryptography).

Economic & Systemic Risk Analysis

Stress Testing Cross-Chain Systems

- Simulate cascading failures in interconnected DeFi protocols (e.g., a bridge hack triggering liquidations in lending markets).
- Model the economic impact of oracle manipulation on stablecoins (e.g., DAI, USDC) and synthetic assets.

Game-Theoretic Incentives

- Analyze validator/oracle collusion risks in proof-of-stake bridges and design incentive structures to penalize malicious actors.
- Study the effectiveness of decentralized insurance pools (e.g., Nexus Mutual) in mitigating systemic losses.

Human-Centric & Governance Challenges

DAO Governance Under Crisis

- Evaluate DAO decision-making efficiency during attacks (e.g., response times, voter apathy) and propose governance optimizations.
- Research methods to prevent governance attacks (e.g., vote-buying, whale dominance) in cross-chain protocols.

Social Engineering Mitigation

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

- Quantify the success rates of phishing/spear-phishing attacks on blockchain teams and design behavioral training frameworks.
- Study the role of pseudonymity in insider threats (e.g., anonymous validators vs. KYC'd entities).

Emerging Attack Vectors & Defense Mechanisms

AI-Driven Exploits

- Investigate how AI could automate vulnerability discovery (e.g., LLMs for smart contract hacking) or manipulate oracle data (e.g., deepfake sensor inputs).
- Develop AI-powered anomaly detection systems tailored for cross-chain transactions.

ZK-Rollup Vulnerabilities

- Audit ZK-proof implementations (e.g., StarkNet, zkSync) for edge cases in recursive proofs or trusted setup assumptions.
- Research risks in hybrid systems (e.g., ZK-oracles combined with optimistic rollups).

Regulatory & Interoperability Standards

Compliance Without Centralization

- Propose regulatory frameworks for cross-chain protocols (e.g., FATF's Travel Rule compliance) that preserve privacy and decentralization.
- Analyze the impact of regulations like MiCA (EU) on oracle data providers and bridge operators.

Interoperability Standards

- Define universal security standards for cross-chain communication (e.g., analogous to ISO/IEC 27001 for blockchain bridges).
- Study the role of modular blockchains (e.g., Celestia, EigenLayer) in reducing bridge dependency.

Long-Term Decentralization & Sustainability

Decentralized Identity for Validators

- Design Sybil-resistant identity systems for bridge validators using biometrics or soulbound tokens (SBTs).
- Explore decentralized compute networks (e.g., Bacalhau, Gensyn) for oracle node operations.

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

Energy Efficiency

- Audit the carbon footprint of cross-chain protocols (e.g., energy-intensive bridges like Polygon PoS) and propose green alternatives.

Case Study-Driven Research

Forensic Analysis of Historic Exploits

- Conduct deep dives into unresolved aspects of past attacks (e.g., Nomad's replay bug, Multichain's opaque team structure).
- Publish open-source post-mortems with code snippets to educate developers.

Hypothetical Threat Modeling

- Simulate "black swan" scenarios (e.g., a nation-state attack on Ethereum's consensus layer) and assess cross-chain ecosystem resilience.

Interdisciplinary Collaborations

Cryptoeconomics & Behavioral Science

- Partner with economists to model user behavior during panics (e.g., bank runs on bridges) and design circuit-breaker mechanisms.
- Study cross-cultural trust perceptions in decentralized systems (e.g., regional adoption of bridges in Asia vs. Europe).

Hardware Security

- Research tamper-proof hardware (e.g., TEEs, secure enclaves) for key management and oracle data generation.

Future studies must focus on:

- Eliminating trust assumptions in cross-chain/oracle systems.
- Quantifying systemic risks in interconnected DeFi ecosystems.
- Bridging gaps between technical innovation, governance, and human factors.
- Anticipating AI/quantum-era threats to blockchain infrastructure.

CONCLUSION

The blockchain industry stands at a crossroads. While innovations like cross-chain interoperability and programmable oracles unlock transformative potential, they also amplify risks. Learning from

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

past failures—whether code bugs in Nomad or insider threats in Multichain—demands a culture of transparency, rigorous auditing, and community-driven governance. By embracing decentralization not just as a technical ideal but as an operational imperative, the ecosystem can evolve into a resilient, trustless foundation for the future of finance and digital infrastructure.

The journey ahead requires vigilance, collaboration, and a commitment to prioritizing security as the bedrock of innovation. Only then can blockchain technology fulfill its promise of democratizing trust in an increasingly interconnected world.

REFERENCES:

1. Federal Bureau of Investigation. (2023, January 23). *FBI confirms Lazarus Group cyber actors responsible for Harmony's Horizon Bridge currency theft*. https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft
2. Chainlink. (n.d.). *What is the blockchain oracle problem?* Chainlink Education Hub. https://chain.link/education-hub/oracle-problem
3. Association for Computing Machinery. (2024). Blockchain cross-chain bridge security: Challenges, solutions, and future outlook. *ACM Digital Library*. https://doi.org/10.1145/3696429
4. ImmuneBytes. (2022, February 2). *Wormhole bridge hack – Feb 2, 2022 – Detailed hack analysis*. https://immunebytes.com/blog/wormhole-bridge-hack-feb-2-2022-detailed-hack-analysis/
5. Merkle Science. (2022, April 1). *Hack track: Analysis of the $625 million Ronin Network exploit*. https://www.merklescience.com/blog/hack-track-analysis-of-ronin-network-exploit
6. Google Cloud. (2022, October 6). *Decentralized robbery: Dissecting the Nomad Bridge hack and following the money*. Mandiant Threat Intelligence. https://cloud.google.com/blog/topics/threat-intelligence/dissecting-nomad-bridge-hack/

@2026 International Council for Education Research and Training 2026, Vol. 04, Issue 02, 59-95
ISSN: 2960-0006 DOI: https: https://doi.org/10.59231/edumania/9198

7. Chainalysis. (2023, July 19). *Multichain protocol experiences mysterious withdrawals, suggesting multi-million dollar hack or rug pull*. https://www.chainalysis.com/blog/multichain-exploit-july-2023/
8. Starknet Community. (2024). *Starknet security update: Potential full node vulnerability recap*. https://community.starknet.io/t/starknet-security-update-potential-full-node-vulnerability-recap/115314
9. Shukla, P. (2025). *zkLend hack analysis (StarkNet oracle exploit)*. LinkedIn. https://www.linkedin.com/pulse/zklend-hack-analysis-piyush-shukla-jsxzf/

Received: Jan 16, 2026

Accepted: Feb 27, 2026

Published: Apr 01, 2026