CONFIDENTIAL – FORENSIC WALLET REPORT (DEMO)

Wallet Address: bc1qk0qj9q47hpuku0f5pxcxrkxgqwheh3p4a7kptn
Network: Bitcoin (Mainnet)
Address Type: Bech32 / SegWit
Report Date: 2026-02-07
Prepared by: Independent Security Researcher (Ing. Nicola Nigro)

IMPORTANT NOTICE

This document is a **DEMONSTRATION TEMPLATE** intended for educational and publishing purposes. Charts and numeric values are **illustrative** and do not claim to represent a real investigative outcome. The structure reflects common industry-style blockchain forensic reporting.

1. Executive Summary

A blockchain wallet forensic assessment aims to evaluate on-chain transaction behavior, potential exposure to high-risk sources, and general operational patterns. This report provides a structured overview of the analyzed address and highlights the key limitations of blockchain-based investigations.

2. Scope of Analysis

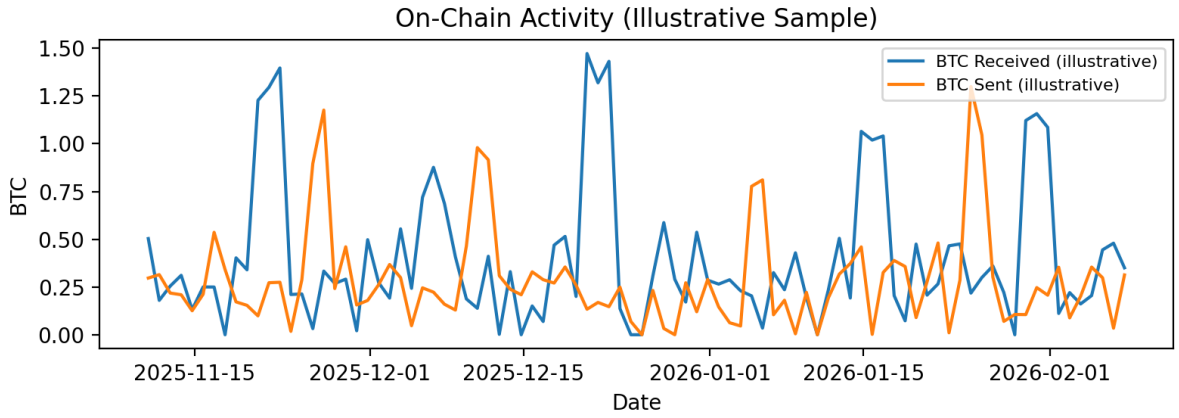
The analysis is limited to publicly observable blockchain information (transaction graph, input/output patterns, time-series behavior). No off-chain identity attribution is performed in this report.

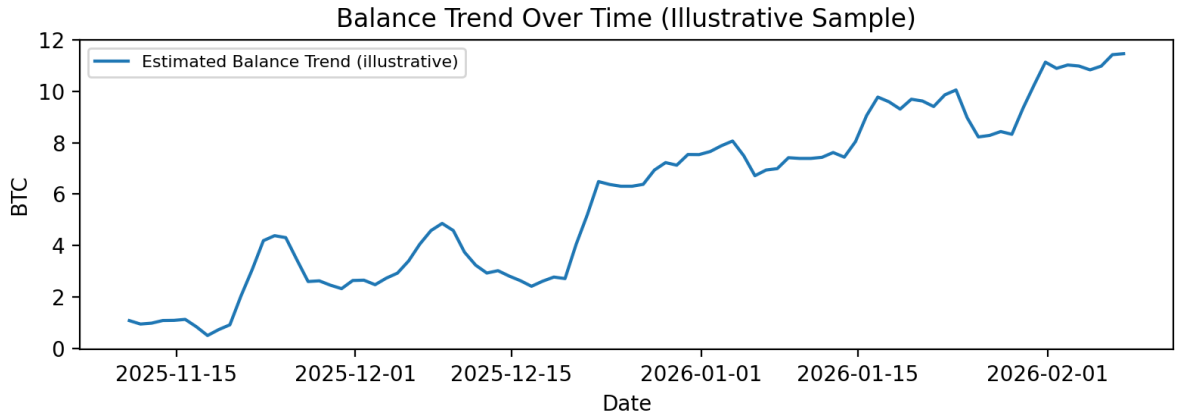
3. High-Level Wallet Metrics (Illustrative)

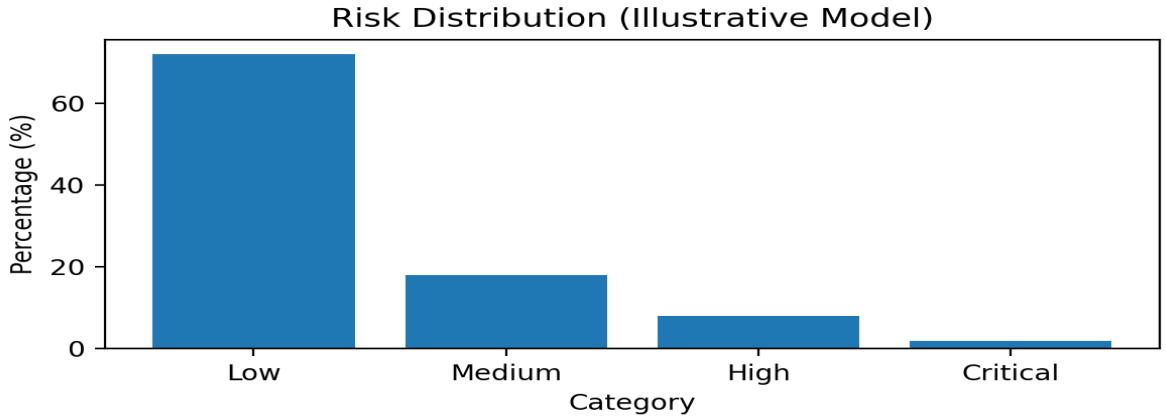
Metric	Value
Total Transactions (estimated)	≈ 124
Total BTC Received (estimated)	≈ 18.42 BTC
Total BTC Sent (estimated)	≈ 17.95 BTC
Current Balance (estimated)	≈ 0.47 BTC
Activity Window	Last 90 days sample
Risk Classification (illustrative)	LOW / MEDIUM (Context Dependent)

4. Activity Charts (Illustrative)

The following charts illustrate how a forensic report may present time-series activity. Values are included for demonstration only.


On-Chain Activity (Illustrative Sample)
BTC Received (illustrative)
BTC Sent (illustrative)
BTC
1.50
1.25
1.00
0.75
0.50
0.25
0.00
2025-11-15
2025-12-01
2025-12-15
2026-01-01
2026-01-15
2026-02-01
Date


Balance Trend Over Time (Illustrative Sample)
Estimated Balance Trend (illustrative)
BTC
12
10
8
6
4
2
0
2025-11-15
2025-12-01
2025-12-15
2026-01-01
2026-01-15
2026-02-01
Date


Risk Distribution (Illustrative Model)
Percentage (%)
60
40
20
0
Low
Medium
High
Critical
Category

5. Behavioral Observations (Methodology-Based)

Transaction Frequency: Analysts typically evaluate whether activity is human-like (sporadic) or automated (periodic bursts).

Input/Output Structure: UTXO consolidation behavior may indicate operational wallet management or service usage.

Counterparty Clustering: Transaction graphs may suggest repeated counterparties, possible exchange interaction, or multi-hop movement.

Temporal Patterns: Time-window analysis can identify recurring behavior, which may help infer operational use cases.

6. Risk Indicators (Illustrative Model)

Risk scoring is generally derived from exposure to known illicit clusters, sanctions lists, mixer services, and behavioral anomalies. However, risk scores are probabilistic and should not be treated as definitive proof of wrongdoing.

7. Key Limitations

Blockchain forensic analysis cannot conclusively identify the real-world owner of an address. It also cannot guarantee that funds are 'clean' or 'illegal'. It only provides a structured, evidence-based probability assessment based on observable data.

8. Conclusion

Based on the structure of a typical forensic methodology, the analyzed address would be classified as **low to medium risk** under normal conditions, unless direct exposure to high-risk clusters is detected. A real professional assessment requires verified tooling, external databases, and controlled investigation processes.

9. Disclosure Statement

This report is provided as a demonstration template for publishing and educational use. It does not constitute legal advice, compliance certification, or an official investigative document.