***A. Bodnarashyk**, BA student*
***S. Davydovych**, assistant lecturer*
Zhytomyr Polytechnic State University

TOPOLOGICAL ANALYSIS OF TRANSIT WALLETS AND CONSOLIDATION PATTERNS IN CRYPTOCURRENCY

With the rapid integration of blockchain technology into the global financial ecosystem, tracing atypical digital asset movements has become a critical cybersecurity challenge. Although blockchain networks are inherently transparent, malicious actors and entities requiring extreme privacy employ complex structural obfuscation techniques to sever the link between the origin and destination of funds. To counter this, cybersecurity analytics must transition from relying solely on identified "blacklists" to proactively monitoring the topological structures of transaction graphs.

A highly effective methodology for identifying such anomalies is the "relationship investigation approach," which focuses on evaluating the behavioral lifecycle and transaction patterns of a specific address rather than its owner's identity. Within this framework, analysts scrutinize the velocity of funds and the chronological sequence of inflows and outflows to determine the true operational purpose of a node. A primary structural indicator of atypical activity is the presence of a "pass-through" or transit wallet. Such wallets are not designed for long-term asset retention; instead, funds are received and almost immediately transferred out, typically resulting in a final terminal balance of zero [1].

To validate this algorithmic profiling approach, an Open-Source Intelligence (OSINT) analysis was conducted on a suspicious Bitcoin address (bc1qcf6sh7yl4gs2kn3ysfs4ffdnqam75vyzrc7kg3) utilizing the Arkham Intelligence platform. The topological data of this address correlates directly with the mathematical signature of a transit node – a temporary checkpoint used to obscure the trail of digital assets. Unlike a standard user's wallet, which typically holds a fluctuating balance over time, this address exhibits a strictly mechanical behavior. Over its operational lifespan, the address processed exactly 19 transactions, receiving a total volume of 51.35363654 BTC (approximately $3.4 million) and executing outbound transfers for the exact same amount. This precise matching of incoming and outgoing funds, resulting in a deliberate terminal balance of exactly 0.00 BTC, strongly indicates that the wallet was never intended to store wealth. Instead, it functioned solely as a routing step designed to complicate financial tracking efforts [2].

Further structural analysis of the transaction logs revealed a distinct consolidation pattern, where multiple smaller deposits are swept together into one large transfer. Between April 22 and April 23, 2025, the wallet experienced rapid accumulation through 18 separate incoming transactions. Following a month of inactivity, a massive outbound sweep occurred on May 31, 2025. This single transaction combined 141 different sources of funds and was executed with an unusually high network fee of 26 million Satoshis (over $17,000) [2]. To understand the significance of this anomaly, it is important to clarify how cryptocurrency fees work. Unlike traditional banking, where transfer costs are generally fixed, the Bitcoin network operates like a priority auction. Because the system can only process a limited

number of transactions at a time, users attach a voluntary fee to their transfers to encourage the network to process them faster. An ordinary user typically pays a standard, minimal fee and waits for routine processing. Paying a fee as extreme as $17,000 is a deliberate tactic to skip all waiting lines and guarantee that the transfer is confirmed instantly. This massive overpayment signifies an urgent, high-priority movement of funds. It serves as a classic indicator of an orchestrated effort to rapidly merge and relocate layered assets before they can be traced or intercepted, completely disregarding the financial cost of the transaction.

Beyond the immediate anomaly of the network fee, mapping the broader transaction graph reveals a distinct “fan-in” topological structure during the wallet’s accumulation phase. The 141 individual inputs aggregated in the final sweep indicate that this transit node served as a centralized collection point for numerous dispersed micro-transactions. According to established blockchain intelligence frameworks, such aggregation nodes are typically strategically positioned just before an “off-ramp” – a juncture where digital assets are forwarded to centralized exchanges for liquidation. By funneling hundreds of smaller, fragmented deposits into a single massive transfer, the operators effectively consolidate liquidity while simultaneously obfuscating the transaction history. This structural bottleneck makes it significantly more difficult for investigators to perform backward-tracing to identify the original sources of the funds once they exit the transit node.

The analysis demonstrates that applying topological and structural profiling to cryptocurrency transactions is a vital tool for detecting atypical network behavior. By mathematically defining the parameters of transit nodes and consolidation sweeps – such as matching high-volume input/output ratios, short lifespans, and zero terminal balances – cybersecurity systems can algorithmically flag suspicious activity. This approach eliminates the reliance on subjective heuristics and allows for the automated, mathematically sound identification of complex asset layering in distributed ledgers.

REFERENCES

1. How to squeeze investigative evidence from any cryptocurrency address [Електронний ресурс] / Elliptic, 2025. URL: https://www.elliptic.co/blog/how-to-squeeze-investigative-evidence-from-any-cryptocurrency-address.
2. On-chain analysis of Ross Ulbricht’s cryptocurrency holdings [Електронний ресурс] / Arkham, 2026. URL: https://intel.arkm.com/explorer/entity/ross-ulbricht.