Zano Team Response to Recent Network Analysis Report

Ravaga
Jun 20, 2025 • 4 min read

Understanding the Core Issue

The report claims to have tracked node IPs using a "spying node" and estimated balances based on staking blocks produced. Let's address both the technical reality and the research methodology.

Key Points:

1. **This is standard P2P functionality, not an exploit** - The ability to see peer connections is inherent to how P2P networks operate
2. **The report conflates network-level data with privacy breach** - Seeing IP addresses of nodes doesn't break Zano's cryptographic privacy guarantees

Feedback on the Research Itself

Research Quality and Approach

While the research demonstrates technical competence, it suffers from several issues:

- **Somewhat legitimate research undermined by sensationalist framing** - While the technical approach has merit, the methodology has significant flaws and the presentation is misleading
- **Could have been much better if focused solely on network privacy** - Instead of conflating network topology with transaction privacy
- **Network privacy as a topic isn't Zano-specific** - The exact same approach can be applied to any privacy cryptocurrency, including Monero or Zcash
- **No definitive one-size-fits-all solution exists** - Different users have different threat models and requirements

Methodological Concerns

The research methodology relies on numerous assumptions that can neither be proven nor disproven, yet the results are presented as established facts. Furthermore, the authors claim to have completely deanonymized user IP addresses, while their own data table shows only half experiencing "IP address leakage" - a significant contradiction in their claims.

What the Research Actually Found vs. What It Claims

What Was Actually Discovered:

- Correlation between IP addresses and staking activity
- **Public network data** that any P2P participant can observe

What Remains Completely Private:

- **Unlinkability**: Transactions cannot be linked to specific addresses
- **Untraceability**: The flow of funds between addresses remains hidden
- **Transaction amounts**: Completely hidden through cryptographic commitments
- **Wallet addresses**: No connection between IP addresses and actual wallet addresses

The report never mentions these core privacy features, which are the actual foundation of Zano's anonymity.

Defensive Configuration Options

For users concerned about IP exposure, Zano provides comprehensive configuration options documented at https://docs.zano.org/docs/stake/security/proof-of-stake-recommendations:

1. Restricted Peer Connections

Configure your node to connect only to trusted peers, such as:

- Your own personal subset of exit nodes
- Nodes operated by trusted parties

- Zano team maintained infrastructure nodes

This approach:

- Prevents random nodes from connecting directly to yours
- Ensures a spying node never establishes a direct connection
- Distributes your blocks evenly among trusted infrastructure

2. Network Privacy Solutions

- **VPN Services**: Hide your real IP address (though VPN exit IP still shows staking activity)
- **Remote Node Setup**: Separate your staking operations from your primary IP
- **Personal Exit Nodes**: Run your own infrastructure for maximum control

3. Understanding P2P Network Reality

It's important to understand that what the research describes is **normal P2P network activity**. Every peer-to-peer network, from Bitcoin to BitTorrent, operates on the principle of nodes discovering and connecting to each other. This isn't a vulnerability - it's literally how distributed networks function.

The ability to observe peer connections and correlate activity is inherent to any P2P system. If someone claims this is a "breach" or "exploit," they're either misunderstanding fundamental networking concepts or deliberately misrepresenting them for effect.

We're always open to adopting better solutions if they emerge. If there were a magical way to have a P2P network where nodes can communicate without knowing each other exist, while maintaining reliability and performance, we'd implement it immediately. But the reality is that every proposed solution involves trade-offs:

- **Tor/I2P integration**: Massive latency increases, reliability issues
- **In-house developed mixnets**: Connection drops, synchronization problems and high vulnerability to spy node attacks in smaller networks

This remains an area of active research for us. We're constantly exploring both in-house developments and external innovations in network privacy. If a solution emerges - whether developed by our team or from the broader cryptography and networking community - that can provide stronger network-level privacy without significant drawbacks, we'll definitely implement it. The key is finding approaches that enhance privacy while maintaining the reliability, performance, and accessibility that our users depend on. Until then, we provide users with the tools to configure their setup according to their needs.

Why Certain Solutions Weren't Implemented

Dandelion and Similar Protocols

We chose not to implement Dandelion+ because it doesn't provide effective protection against spy nodes. Any large P2P network is flooded with monitoring nodes, and there's a very high probability that the entry point into a Dandelion stem would be exactly such a spy node. This would give users a false sense of security while providing no

definitive protection. The protocol essentially becomes security theater when the adversary controls a significant portion of the network nodes.

Tor/I2P Integration

These protocols exacerbate what's known as the Two Generals' Problem, which becomes a serious issue when broadcasting transactions. We actually implemented a Tor client that worked on both mobile and desktop several years ago - we were among the first to include Tor in our wallet by default, striving to provide users with IP-level privacy.

However, we immediately encountered severe issues with transaction delivery to the network. For many services, these delivery problems were critically sensitive - transactions would fail to propagate reliably, confirmations would be delayed or lost entirely, and users experienced significant frustration. We had to disable this feature because the cure was worse than the disease.

Flexible Security Configuration Approach

This approach recognizes that:

- Different users have different threat models
- A home user staking small amounts has vastly different needs than an exchange
- Enterprise operations require and can implement additional security measures
- Users should have the flexibility to choose their security posture

Practical Examples:

- **Casual User**: Desktop wallet with default settings provides strong transaction privacy - your funds and transaction history remain completely private
- **Privacy-Conscious Staker**: Add network-level privacy with VPN or restricted peer connections
- **Enterprise/Exchange**: Dedicated infrastructure with custom exit nodes for maximum operational security

Bottom Line

The research discovered basic P2P networking behavior and presented it with sensationalist framing. In reality:

- **No cryptographic privacy was compromised**
- **Transaction anonymity remains fully intact**
- **Network-level privacy can be achieved through proper configuration**
- **The flexibility exists for users to choose their desired security level**

If this were genuine research aimed at improving privacy, we'd welcome the discussion. We could even propose better methodologies for investigating network privacy - ideally conducted by researchers without obvious agendas. Instead, we got a report that conflates network topology with transaction privacy, making bold claims while ignoring the actual privacy guarantees that matter.

The comprehensive guide provides all the tools needed for users to configure their setup according to their specific security requirements.

Sign up for more like this.

Enter your email

Subscribe

Zano Monthly Project Update #8 - May 2025

Welcome zAnons to the 8th Zano Project Update! May was a huge month for the Zano ecosystem, marked by major...

Gonbatfire
Jun 3, 2025 • 6 min read

Zano Has Been Integrated Into Edge Wallet!

We're excited to announce that Zano has been integrated with Edge Wallet, one of the most trusted and user-friendly multi-...

Mr_Kwibs
May 27, 2025 • 2 min read