Crypto Focus

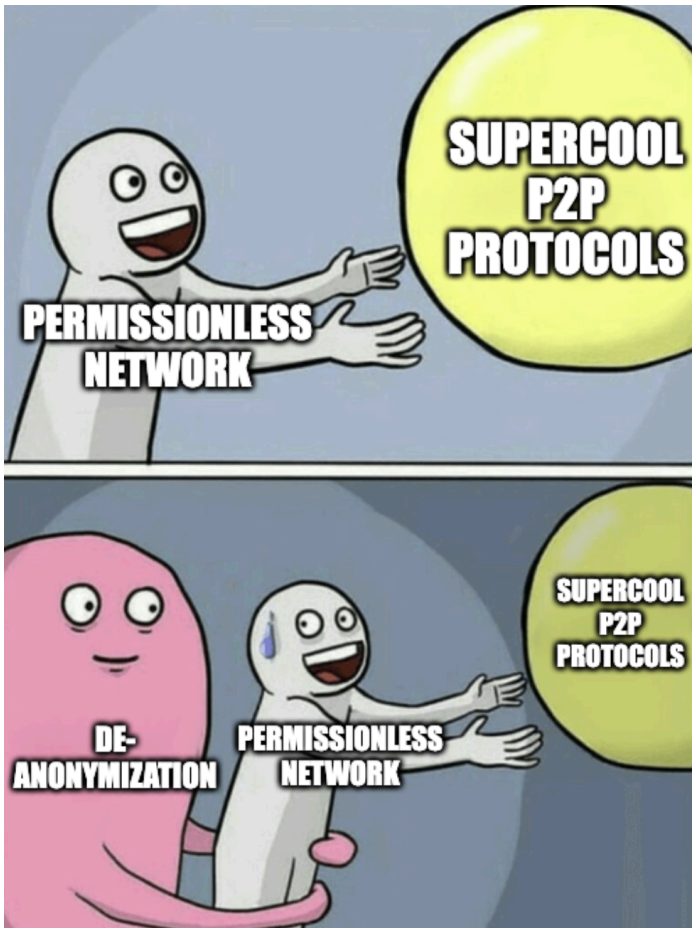
Deanonymization in Blockchain Networks

Feb 27, 2025

Jaehyun Ha I Research Analyst

jaehyunha@prestolabs.io

Contents



Source: imgflip

Summary

- Despite the common belief that permissionless blockchains ensure anonymity, their P2P architecture sometimes can expose participants' IP addresses to attackers through side channels, timing attacks, and gossip protocols. Research on Bitcoin and Ethereum has shown that this poses risks to privacy and network stability.

- Exposed IPs enable targeted DDoS attacks, consensus disruption, and real-world identity linkage, risking individual security and network decentralization, with potential exploits like MEV manipulation amplifying the stakes.

- Emerging solutions—such as secret leader election, distributed validator technology, and private peering agreements—aim to protect identities and resilience, but require collaborative innovation to balance privacy, scalability, and decentralization as blockchain adoption grows.

---

1. Introduction

Blockchain technology is often heralded as a bastion of anonymity, with wallet addresses—complex hashes detached from names, phone numbers, or emails—seemingly offering a shield of privacy. In theory, this design obscures real-world identities, promising users a degree of secrecy. Yet, reality tells a different story. Large institutions routinely publicize their hefty cryptocurrency holdings, turning their wallets into transparent ledgers for all to see. Meanwhile, individual users, compelled by Know Your Customer (KYC) requirements on exchanges, unwittingly tie their identities to specific addresses. Even beyond these systemic leaks, doxxing via social engineering or other tactics has unmasked supposedly private wallets, exposing "anonymity" as more myth than fact.

The fallout from such breaches extends well beyond privacy erosion. Once a wallet's owner is revealed, they become a beacon for hackers and scammers. Targeted phishing or sophisticated cyberattacks can follow, as seen last September when a single whale lost $243 million to a privacy lapse—a stark reminder that anonymity is often the first bulwark against catastrophic theft. These incidents underscore a critical truth: in the blockchain ecosystem, exposure can carry a steep price.

Less visible, but no less alarming, is the risk of deanonymization at the network level. A 2025 USENIX paper, "Deanonymizing Ethereum Validators: The P2P Network Has a Privacy Issue" by L.

Heimbach et al., revealed that an attacker with modest resources could unmask the IP addresses of 15% of Ethereum validators in just three days. This vulnerability not only opens the door to exploits like Maximal Extractable Value (MEV) manipulation but also threatens the network's core stability, its safety and liveness (***Note: This is not a FUD, the issue has already been disclosed to Ethereum Foundation.***)

Thus, this report investigates the critical issue of deanonymization within blockchain P2P networks. Section 2 defines "deanonymization," highlighting its risks—like MEV exploitation and network instability—and how it stems from exposed IP addresses. Section 3 traces the evolution of this threat through landmark studies, from Bitcoin's early vulnerabilities to Ethereum's recent attestation leaks. Finally, Section 4 evaluates the severity of these challenges and explores mitigation strategies, from past efforts like Dandelion to cutting-edge solutions like Single Secret Leader Election.

2. What is "Deanonymization" in Blockchain Networks?

Deanonymization in blockchain networks refers to the process of uncovering the real-world identity or location of participants—such as nodes, validators, miners, or transaction originators—by exposing their IP addresses. While blockchain addresses (public keys) appear pseudonymous on-chain, the peer-to-peer (P2P) infrastructure powering these systems operates over the public internet, where nodes exchange transaction & block messages with peers. Each interaction reveals IP addresses, which can be traced by attackers monitoring network traffic, analyzing timing patterns (e.g., how fast blocks propagate), or probing nodes to link specific actions to a device. In permissionless blockchains, where anyone can join, this vulnerability is especially pronounced, turning a supposedly private system into one where participants' network identities can be unmasked.

The exposure of an IP address creates serious risks, including the exploitation of MEV. For instance, if an attacker identifies the IP of a validator set to propose a block at 'slot n', they could launch a Distributed Denial-of-Service (DDoS) attack to knock them offline, especially if the attacker is slated for 'slot n+1.' This lets the attacker claim the MEV from both slots, scooping up fees and rewards—like those from arbitrage trades—that would've been split across two blocks. Home validators, lacking the advanced defenses of institutional players (e.g., proxy networks), are hit hardest. This can unintentionally encourage network centralization as only well-resourced entities can afford to participate safely.

Beyond MEV, deanonymization threatens the blockchain's safety (correct transaction finalization) and liveness (continuous block production). Once attackers map the network's topology—knowing which IPs belong to key nodes—they can target critical participants with DDoS attacks or isolate

parts of the system, halting block production or enabling exploits like double-spending. This not only disrupts individual nodes but also undermines the network's resilience, as revealing connections and key players hands adversaries a blueprint for strategic sabotage. In short, deanonymization transforms a technical vulnerability into a systemic risk, eroding trust in the blockchain's security and reliability.

3. Related Studies

One of the pioneering works on deanonymizing blockchain participants is the seminal paper ***"Deanonymisation of Clients in Bitcoin P2P Network (2014)"*** by Alex Biryukov et al. In the early Bitcoin network, each node was connected to eight designated "entry nodes" that served as intermediaries, relaying their transactions to the rest of the network. Upon joining, a client would share its IP address with these entry nodes, akin to providing a return address for communication, with the assumption that this would not compromise the privacy of their pseudonym.

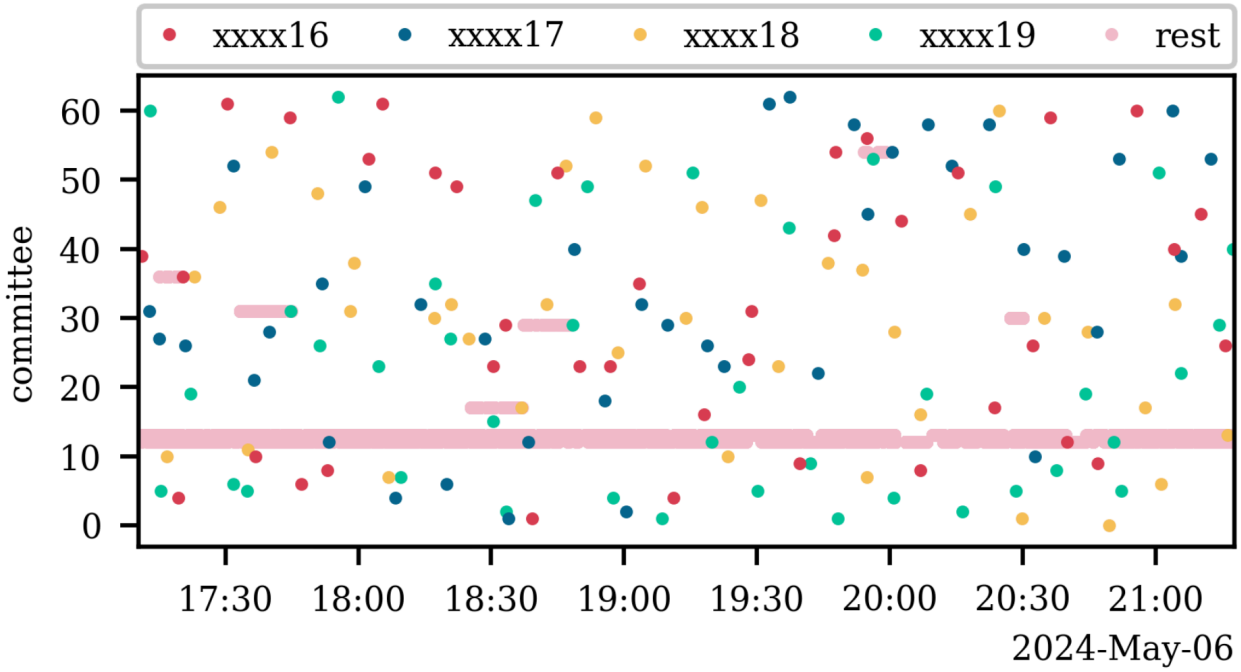
However, the authors devised an effective method to undermine this anonymity by deploying approximately 50 nodes to establish extensive connections—up to 50 per each—with around 8,000 Bitcoin servers, the publicly accessible nodes in the network back in May 2014. By monitoring the propagation of a client's IP address announcement, they identified the likely entry nodes relaying this information. Subsequently, when a client initiated a transaction, the earliest notifications (i.e., INVENTORY messages) typically came through these same entry nodes, allowing the attackers to correlate the transaction's pseudonym with the client's IP address. Though this kind of supernode-based deanonymization techniques are considered infeasible these days (due to expensive attack cost + mitigation through exponential random delays in transaction propagation), this pioneering strategy opened the community's eyes to the reality that the P2P networking layer is a significant privacy vulnerability, rather than a neutral medium for passing around blocks and transactions.

The most recent work in this area is ***"Deanonymizing Ethereum Validators: The P2P Network Has a Privacy Issue (2025)"*** presented at USENIX by L. Heimbach et al. In this study, the authors focused on Ethereum's proof-of-stake validators, showing that an attacker with limited computational and network resources could unmask the IP addresses of approximately 15% of all active validators within just three days. The key vulnerability that made deanonymizing Ethereum validators possible lies in how the Ethereum peer-to-peer (P2P) network shares messages, specifically the "attestations." Attestations are like votes that validators send to the network to confirm the blockchain's progress. To keep the network efficient, Ethereum splits these attestations into 64 smaller groups, or "subnets," and each node only handles a couple of these subnets at a time. The idea is that a node only passes along attestations for its assigned subnets, and this setup is meant to reduce the workload. However, here's the catch: when a node sends an

attestation for a subnet it's not supposed to handle, it's a big clue that the validator who made that attestation is actually running on that very node. This happens because nodes naturally send out their own validators' attestations, even if those attestations don't match their assigned subnets. By spotting this pattern, anyone watching the network can figure out which validators are tied to which nodes, breaking the privacy Ethereum tries to protect.

The attack method to uncover this is pretty straightforward and doesn't need fancy tools—just patience and observation. The authors set up four special nodes, called RAINBOW nodes, to listen to the Ethereum network over three days. These nodes watched all the attestations coming from other nodes they connected to. The trick was to look for attestations that didn't fit a node's usual job. For example, if a node is only supposed to handle subnets 12 and 13 but sends an attestation for subnet 25, it's a giveaway that the validator behind that attestation is hosted on that node (Figure 1). The researchers used some simple rules, or "heuristics," to confirm this pattern—like checking if most of a validator's attestations came from unexpected subnets and making sure they got enough messages to be confident. With just these four nodes, they managed to locate over 15% of Ethereum's validators, linking them to specific IP addresses (like a computer's online address). This shows how a basic setup can expose a lot about who's running the network, all because of one side channel in how messages are shared.

Figure 1: Attestation Received from Peers + Corresponding Subnets



Source: "Deanonymizing Ethereum Validators: The P2P Network Has a Privacy Issue", L.Heimbach et al.

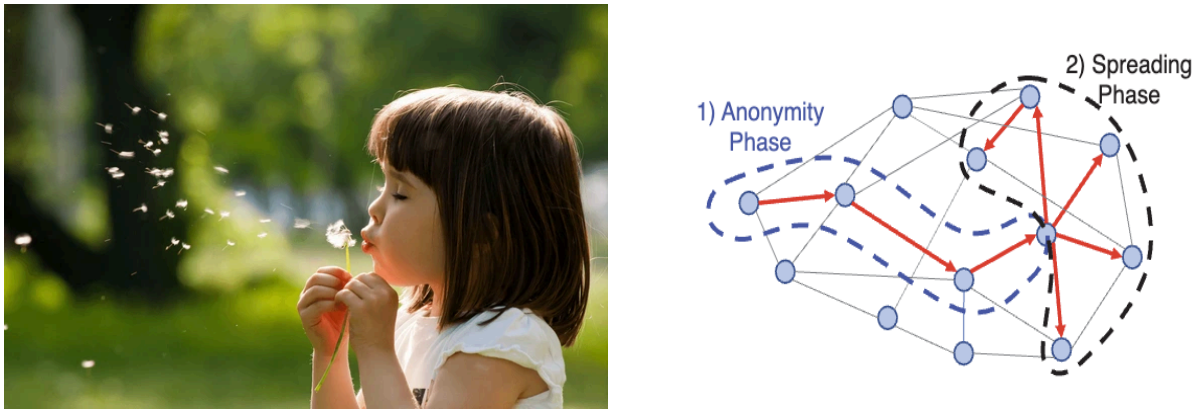
4. Mitigations

As demonstrated, the threats posed by deanonymization in blockchain networks are severe for both individual participants and the integrity of the blockchain. Any node—whether it serves as a regular full node, validator, or miner—may become a target of attacks (as discussed in Section 2), if its IP address is exposed. To address these issues, several countermeasures have been considered from researchers; these mitigation strategies focus on either hiding the validators' identities or making it tougher for attackers to disrupt the network.

4.1. Previous Approaches

The initial approach was to integrate **anonymous gossiping protocols**, such as Dandelion or Tor, into the blockchain network. Dandelion (Figure 2), proposed by Venkatakrishnan et al., aimed to anonymize the origin of a transaction by splitting message propagation into two phases–a stem phase (i.e., where a message is relayed along a predefined path of nodes) and a fluff phase (i.e., where the message is finally broadcast more widely). However, the additional complexity and latency introduced by Dandelion can run counter to miners' or validators' economic incentives, as they rely on timely block and transaction propagation to maximize rewards. Similarly, Tor also has been studied in Ethereum, but routing all node traffic through Tor introduces significant latency overheads and practical integration challenges that have prevented large-scale adoption in production networks.

Figure 2: Fluff Like Dandelion



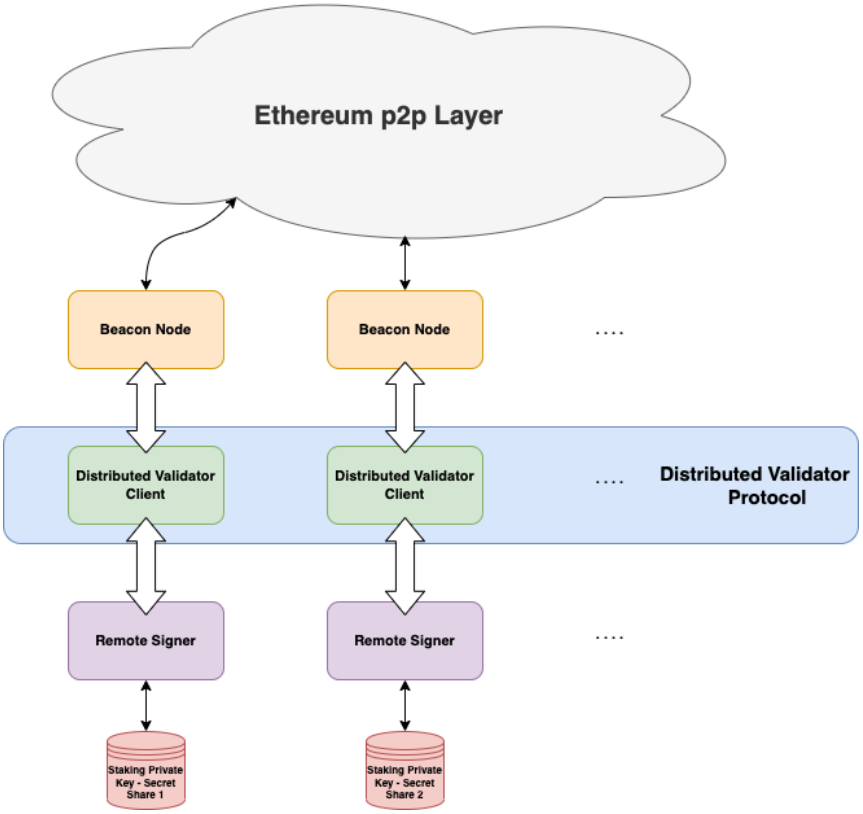
Source: Shutterstock, "Dandelion: Redesigning the Bitcoin Network for Anonymity", S.Venkatakrishnan et al.

4.2. Newly Proposed Approaches

Given the shortcomings from previous approaches, more robust approaches have been recently proposed. **Distributed validator technology (DVT)** is one of the contenders; DVT works by splitting a validator's key into pieces and distributing them across multiple computers (Figure 3),

like breaking a secret code into parts shared among friends. If an attacker tries to overwhelm one computer with a denial-of-service (DoS) attack, the others can still team up to complete the validator's tasks—think of it as a group project that keeps going even if one member drops out. This makes validators tougher and less prone to disruption, ensuring Ethereum stays reliable.

Figure 3: Distributed Validator Technology



Source: https://github.com/ethereum/distributed-validator-specs

While DVT offers a solid solution, **Single Secret Leader Election (SSLE)** stands out as the most promising approach right now, according to the Ethereum Foundation. In SSLE, clever cryptography ensures that only the chosen validator knows they've been picked to propose the next block, keeping everyone else in the dark until the moment arrives. Here's how it works with the leading implementation, called **Whisk**: Validators start by committing to a shared secret, designed so it ties to their identity but gets scrambled—making it impossible for outsiders to link it back to them. At the beginning of an epoch, a random group of validators samples commitments from 16,384 peers using RANDAO, a random number generator. Over the next 8,182 slots (about a day), block proposers shuffle these commitments with their own private twists. Then, RANDAO sorts them into a list tied to upcoming slots. When a validator sees their commitment pop up for a slot, they step up to propose a block. This process repeats, always staying ahead of the current slot. By hiding who's next until the last second, SSLE stops attackers from targeting validators with DoS attacks. SSLE is currently in the research phase, and hasn't shipped in testnet yet.

Lastly, **Private Peering Agreements** provide another layer of protection by letting validators share messages through a trusted inner circle. Normally, validators broadcast updates—like attestations—across the open P2P network, where anyone can spot them and figure out their location. With private peering, they quietly pass messages to a select group of reliable nodes, similar to whispering to trusted buddies instead of shouting in a busy room. This obscures their exact position, making it harder for attackers to track them down. The catch is finding enough dependable peers, which can be tricky, especially for smaller players. Still, it's a practical way to boost privacy, particularly for larger groups who can organize it.

5. Conclusion

Despite the common perception that blockchains guarantee anonymity, reality paints a more nuanced picture. The very architecture that fosters open participation and trustless consensus also exposes participants to potential privacy threats. As research has repeatedly demonstrated—both for Bitcoin and Ethereum (possibly other blockchains as well)—attackers can leverage side channels, timing attacks, and the gossip-based P2P protocol itself to pinpoint the IP addresses of miners, validators, or general network users.

Once an IP is revealed, the stakes rise sharply—ranging from targeted DDoS attacks to disrupted consensus or even real-world identity linkage. These risks threaten not just individual privacy but the resilience and decentralization of the network itself. Emerging solutions like secret leader election, distributed validator technology, and private peering agreements offer hope, aiming to shield identities and enhance robustness, though trade-offs like centralization remain a concern.

Going forward, it is imperative that developers, researchers, and node operators work in tandem to close these privacy gaps. As blockchain technologies continue to grow in complexity and adoption, understanding and mitigating deanonymization risks will be crucial for maintaining the core values of security, censorship-resistance, and decentralized governance. By recognizing the network layer as a critical frontier for privacy threats, we can focus our efforts on robust, scalable innovations that bolster both individual and systemic defenses.

About Presto

Presto is an algorithmic trading firm where researchers and engineers solve challenging problems in global financial markets. Our core strength lies in combining engineering, mathematics, and science to navigate both digital asset and traditional finance markets with precision. Presto Research, our research unit, provides expert-driven insights to help navigate these markets effectively.

Find out more at https://www.prestolabs.io.
Follow Presto for more content: X, LinkedIn
Follow Presto Research for latest research : X, Telegram

Authors

Jaehyun Ha, Research Analyst X, Telegram, LinkedIn

Required Disclosures