# Protecting Bitcoin against BGP Hijacking Attacks using the SCION Internet Architecture

Tony John
OVGU Magdeburg
tony.john@ovgu.de

Justus Krebs
TU Berlin
justus.krebs@campus.tu-berlin.de

David Hausheer
OVGU Magdeburg
hausheer@ovgu.de

***Abstract*—The Bitcoin network exhibits increasing centralization, with over 50% of nodes hosted in just 14 Autonomous Systems, amplifying the impact of Border Gateway Protocol (BGP) hijacking attacks that can partition the network. We propose a hybrid IP/SCION Bitcoin node, built on btcd, that uses the SCION Internet architecture's path-aware networking and cryptographic path verification to resist BGP hijacking. Because SCION today reaches only a small fraction of Bitcoin-hosting ASes, we treat deployment feasibility as a first-class question and quantify it on the AS-level topology of 8,861 Bitcoin nodes across 1,213 ASes (December 2025): 5 strategically placed SCION bridges already provide 81% routing-secure coverage (vulnerable only to sub-prefix hijacking of the client-to-bridge path), while full SCION deployment in 198 ASes achieves 80% direct coverage immune to all BGP attacks including sub-prefix (/25) hijacking. SEED-emulator experiments further demonstrate that SCION connections remain functional during active BGP hijacks, allowing nodes to bridge otherwise-partitioned segments and preventing blockchain forks; the same testbed shows SCION achieving a mean failover of 110 ms on link failure versus 495 ms for BGP with Bidirectional Forwarding Detection (BFD).**

***Index Terms*—SCION, Bitcoin, BGP hijacking, network security, partitioning attacks, blockchain**

## I. Introduction

As a global peer-to-peer overlay over the public Internet, Bitcoin is exposed to network-layer adversaries; in particular, Border Gateway Protocol (BGP) hijacking attacks can divert and partition its traffic [1]–[3]. In April 2018, attackers exploited BGP vulnerabilities to hijack Amazon Route 53 DNS traffic, redirecting cryptocurrency users to malicious servers and stealing approximately $150,000 within two hours [4]. While this attack targeted DNS, similar BGP techniques can partition the Bitcoin network into disjoint segments that maintain separate blockchain histories. Such partitions enable double-spending: payments accepted on one side are reversed when partitions reconverge on the longest chain. Miners in smaller partitions also waste computational power on orphaned blocks.

Despite efforts to secure BGP through RPKI, BGPsec, and ROV++ [5], deployment remains limited and vulnerabilities persist. RPKI requires coordinated adoption across thousands of independent network operators, and partial deployment provides incomplete protection since attackers can route through non-validating ASes [6]. These routing-layer gaps are compounded by an orthogonal trend in the Bitcoin overlay itself: AS-level centralization. Apostolaki et al. [1] found that 50% of Bitcoin nodes were hosted by 50 ASes in 2016; by 2023, Saad et al. [3] reported only 14 ASes (measured on 2022 data). Saad et al. [2] further demonstrated that hijacking 15 IP prefixes could disrupt 95% of traffic to an AS hosting 1,000 nodes. To address these routing security challenges, we propose to leverage SCION [7], a secure Internet architecture offering path-aware networking and cryptographic path verification (Section II). Unlike BGP, SCION paths are assembled from cryptographically signed segments produced during beaconing, and per-hop MACs ensure that on-path ASes cannot deviate from the path the sender selected. Attackers cannot forge valid path signatures for ASes they do not control, making SCION traffic resistant to BGP hijacking. SCION has recently reached production maturity (70 ASes globally, with Sui as the first major blockchain to adopt it [8]), making it timely to ask whether the same protection extends to Bitcoin.

We adopt SABRE's [9] threat model and routing-security analysis but take a fundamentally different defense. Instead of relay nodes positioned by BGP route preference (which remain vulnerable to sub-prefix hijacking), we integrate SCION directly into Bitcoin nodes for cryptographic path verification independent of BGP. Because SCION today reaches only a small fraction of Bitcoin-hosting ASes, we make deployment feasibility a central focus of our analysis: how few SCION-enabled ASes suffice for substantial protection of today's Bitcoin overlay, and what coverage is achievable as deployment grows?

We make the following contributions:

1) A hybrid IP/SCION Bitcoin node based on btcd, with dual-stack operation and SCION-native peer discovery.
2) An AS-level routing analysis on December 2025 Bitnodes and CAIDA topology data showing that 5 strategically placed SCION bridges already provide 81% routing-secure coverage, while full infrastructure deployment in 198 ASes achieves 80% direct coverage immune to all BGP attacks including sub-prefix (/25) hijacking.
3) Experimental evaluation in the SEED emulator [10] demonstrating that SCION connections remain unaffected during BGP hijacking and prevent blockchain forks, and that SCION achieves 4.5× faster failover than BGP+BFD on link failure (110 ms vs. 495 ms mean).

ISBN 978-3-903176-82-9 

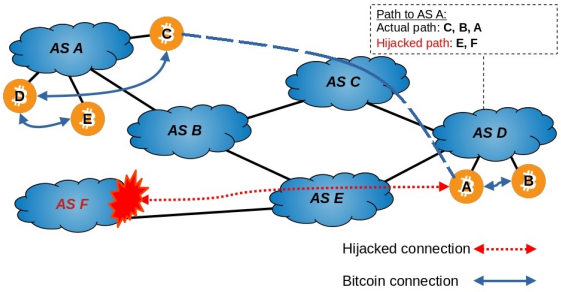



Fig. 1: AS F hijacks connection of node A to C, resulting in a partition

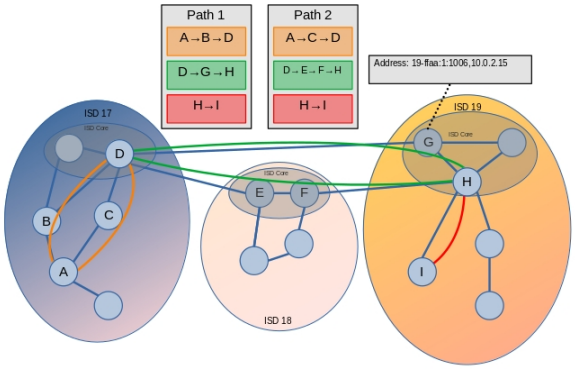



Fig. 2: SCION example topology

## II. Background

### A. Border Gateway Protocol (BGP)

BGP [11] enables Autonomous Systems (ASes) to exchange routing information. Each AS selects routes based on local policies, considering AS path length, business relationships, and traffic engineering preferences.

BGP lacks origin validation: any AS can advertise arbitrary IP prefixes, enabling hijacking attacks that divert traffic to malicious destinations. These routing-layer vulnerabilities enable network partitioning attacks against distributed systems (Section II-B).

Route Origin Validation (ROV) using RPKI [5] provides partial protection by binding ASes to authorized IP prefixes, but remains vulnerable to more-specific prefix hijacking. BGPsec limitations are discussed in Section III.

### B. Bitcoin Network

The Bitcoin network operates as a peer-to-peer (P2P) overlay where over 24,000 reachable nodes globally exchange transactions and blocks directly. Its increasing AS-level centralization [3] creates a significant attack surface for routing-layer adversaries.

BGP hijacking attacks can partition the network by isolating groups of nodes [1], [2]: an attacker hijacks IP prefixes containing victim nodes, intercepts diverted traffic, identifies Bitcoin connections (typically on port 8333), and drops them. BIP324 [12] introduced opportunistic encryption for Bitcoin's P2P protocol but does not defend against such routing-layer attacks, as an adversary can still drop encrypted connections. These attacks differ from eclipse attacks [13], which monopolize a victim's peer connections at the application layer.

Figure 1 illustrates this attack: *AS F* announces a hijacked prefix, intercepts traffic between partitions, and drops Bitcoin connections to isolate the victim AS. The impact depends on isolated hash rate: partitioning significant mining power causes blockchain forks that can enable double-spending.

### C. SCION

SCION [7] addresses BGP's limitations through *isolation domains*, *path-aware routing*, and *beaconing*.

Isolation Domains (ISDs) group ASes under a common trust root, enabling trust isolation between domains. SCION identifies end hosts by ISD, AS, and IP address (Figure 2).

Through *beaconing*, network paths are discovered as beacons propagate across ASes, accumulating cryptographically signed path-segments at each hop. This prevents unauthorized path modification and enables *path-aware routing*: senders select paths (e.g., choosing between two routes to *AS I* in Figure 2) with the guarantee that packets follow the chosen path. SCION operates independently of BGP and can function alongside IP routing, enabling incremental deployment.

Path and AS trust in SCION is rooted in the Control-Plane PKI: each ISD certifies its member ASes via a Trust Root Configuration, and beacon segments carry signatures verifiable against those certificates. Endpoints thus see a set of authenticated end-to-end paths and apply local policy (latency, AS-path length, ISD membership, avoidance of untrusted ASes) to select among them; per-hop MACs prevent on-path ASes from splicing or extending paths beyond what the control plane authorized.

SCION is deployed in production across 70 ASes globally [14], serving financial institutions, government entities [15], and research networks [16].

## III. Related Work

### A. Routing Attacks on Cryptocurrencies

Apostolaki et al. [1] demonstrated that attackers can partition the Bitcoin network with fewer than 100 hijacked prefixes, enabling delay attacks that disrupt block propagation by 20 minutes. This work established the threat model for routing-layer defenses.

Heilman et al. [13] introduced eclipse attacks, showing how attackers can monopolize a victim's peer connections to enable double-spending without majority hashpower. Yang et al. [17] combined these vectors with BGP hijacking in the BGP Hijacking Eclipse (BHE) attack.

Saad et al. [2] confirmed continued feasibility of partitioning attacks in 2019; in 2023 [3], they showed Bitcoin, Ethereum, and Ripple can be targeted by the same attacks due to

centralization. Doumanidis et al. [18] demonstrated Proof-of-Stake systems are equally vulnerable, with their StakeBleed attack causing $\sim$300 ETH losses within two hours by hijacking only 30 IP prefixes.

### B. Proposed Defenses

Apostolaki et al. [9] proposed SABRE, a network of distributed relay nodes across trusted ASes protecting against BGP hijacking with six nodes. Tran et al. [19] showed that SABRE's reliance on trusted ASes could be exploited by malicious operators.

Detection-based approaches such as BEAM [20], a semantics-aware BGP anomaly detection system deployed at a large ISP (497 true anomalies, 1.65 false alarms/day), are complementary: they raise alerts on suspicious announcements but do not, by themselves, keep traffic flowing during an active hijack.

### C. RPKI and BGPsec Limitations

RPKI covers approximately 50% of global prefixes [21], but only 27% of networks actively enforce filtering [6]. Mirdita et al. [21] found 56% of RPKI validators have documented vulnerabilities. Morillo et al. [5] proposed ROV++ for security under partial deployment. BGPsec [22] provides cryptographic path validation but requires universal deployment and introduces computational overhead hindering adoption.

### D. SCION Internet Architecture

SCION [7] provides path-aware networking with built-in path validation and isolation domains that prevent routing attacks by design. Birge-Lee et al. [23] introduced Secure Backbone AS (SBAS), abstracting a secure routing backbone as a virtual AS for incremental deployment. Krähenbühl et al. [24] extended SCION with FABRID for user-defined path preferences, achieving 160 Gbps on commodity hardware.

The Sui blockchain integrated SCION into its validator network [8], becoming the first major blockchain to adopt SCION for production. Vorkapic [25] proposed SCION for Ethereum security but provided no quantitative evaluation.

### E. Bitcoin Network Improvements

BIP324 [12] adds opportunistic P2P encryption but does not protect against routing-layer attacks. Active topology monitoring [26] provides another defense, though topology inference attacks limit obfuscation effectiveness.

## IV. SCION-Bitcoin Design

### A. Threat Model

We consider an AS-level adversary capable of: (i) manipulating BGP announcements, (ii) announcing hijacked sub-prefixes to exploit longest-prefix matching, (iii) intercepting and dropping traffic traversing their AS, and (iv) identifying Bitcoin traffic via port analysis or traffic patterns. This model follows prior work [1], [2] and covers BGP prefix hijacking, partition attacks, delay attacks, and BGP Hijacking Eclipse attacks [17].

The attacker aims to partition the Bitcoin network, enabling double-spending, wasting mining power on orphaned blocks, or gaining selfish-mining advantages. The primary attack surface is the BGP routing layer, which lacks origin validation; RPKI provides only partial protection and is bypassed by sub-prefix hijacking [27] (Section III). The Bitcoin P2P layer is vulnerable because inter-AS connections traverse multiple ASes and can be intercepted along the path, and Bitnodes data shows that 7 ASes host 30% of reachable nodes [28], making these connections critical targets.

**Colluding and Nation-State Adversaries.** Our threat model assumes a single AS-level adversary. Colluding adversaries controlling multiple ASes pose a greater threat, as they can mount coordinated attacks from multiple vantage points. However, SCION's path selection allows endpoints to choose paths avoiding known adversarial ASes. For nation-state adversaries who may control SCION infrastructure within their jurisdiction, SCION's ISD (Isolation Domain) model provides trust boundaries: traffic can be routed to avoid ISDs under adversarial control. Full analysis of nation-state adversaries is beyond scope; we focus on the common case of single AS-level attackers that prior work has shown to be effective against Bitcoin.

### B. Defense Strategy

SCION eliminates BGP-based attack vectors through cryptographic path verification and BGP-independent routing (Section II). Traffic between SCION-enabled endpoints follows cryptographically verified paths regardless of BGP manipulation, and endpoints can select paths avoiding untrusted ASes. SCION provides cryptographic authentication of paths but does not itself maintain a global AS reputation; trust labels are an operator-policy input. In a Bitcoin-specific deployment, this input can come from admin-configured deny lists, ISD-membership filters (e.g., excluding ISDs known to host hostile transit), or feeds from external BGP-anomaly monitors such as BEAM [20].

Against partition attacks, our approach provides resilience through hybrid connectivity: nodes with both SCION and IP connectivity serve as bridges during attacks, so when BGP hijacking disrupts IP connections, SCION connections maintain reachability and as long as at least one SCION path exists between would-be partitions, block propagation continues. Even partial deployment helps: strategically placed SCION nodes prevent network-wide partitions. Overall, our approach provides two security guarantees: (i) BGP hijack resistance for SCION paths (assuming SCION infrastructure integrity), as cryptographic verification ensures packets follow intended paths; and (ii) partition resilience with sufficient deployment (Section VI).

### C. Deployment Approach

Figure 3 illustrates a Bitcoin overlay during a BGP hijacking attack: the overlay remains connected because the SCION connection is unaffected. SCION operates a separate, BGP-independent control plane that traverses SCION-enabled ASes,

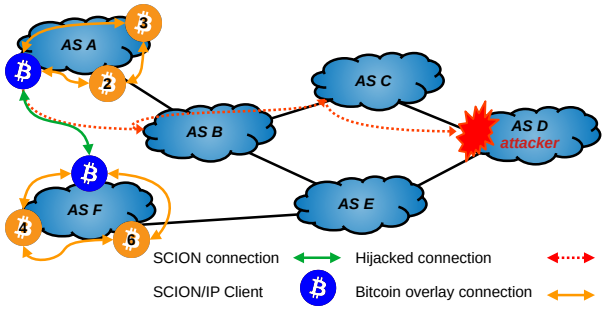



Fig. 3: During a BGP hijack, SCION-enabled Bitcoin nodes stay connected, preventing a partition.

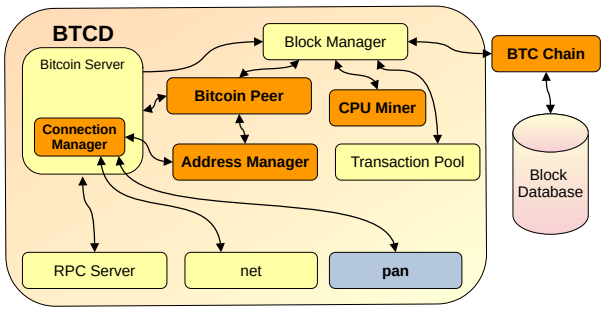



Fig. 4: SCION-enabled btcd architecture. Orange: btcd modifications; Blue: SCION additions.

so the absence of a direct BGP path between AS A and AS F does not preclude communication: SCION beacons traverse SCION-enabled intermediate ASes and assemble cryptographically signed end-to-end paths that are independent of BGP announcements. Even when the attacker hijacks the IP-layer path between A and F, the SCION path between the SCION-enabled endpoints continues to forward traffic, so blocks and transactions still propagate across the bridged segment. SCION also provides improved link-failure resilience and lower-latency paths [7].

Given limited current SCION deployment, we propose a two-phase approach: (1) strategic placement of SCION-enabled Bitcoin nodes as bridges, similar to SABRE relays [9], providing immediate protection; and (2) broad adoption where most Bitcoin nodes use SCION natively.

**Limitations.** Two key limitations exist. First, effectiveness depends on SCION infrastructure availability, currently concentrated in Switzerland [15]. Second, during attacks, nodes must trust SCION bridges to relay transactions faithfully; we discuss this trust concern and mitigations in Section VII.

## V. Implementation

We implemented our SCION-enabled Bitcoin node based on btcd, a Go-based full-node implementation. Figure 4 shows the architecture: orange indicates btcd modifications (network parameters, address handling for SCION formats); blue represents SCION additions via the PAN library[1].

### A. Base Implementation

We selected btcd because its Go codebase provides native compatibility with the SCION libraries, and its modular architecture separates network handling from blockchain logic, facilitating targeted modifications. btcd also includes a built-in RPC server and CPU miner, enabling our experimental evaluation.

### B. Module Modifications

Adapting btcd for our experimental environment required modifications to several modules:

- **Network parameters:** We created a custom network definition with modified magic bytes and port numbers to isolate our testbed from production networks.
- **Genesis block and difficulty:** We defined a custom genesis block and reduced the initial mining difficulty to enable CPU mining within reasonable timeframes. The difficulty adjustment algorithm remains unchanged.
- **CPU miner:** We enabled and configured the built-in CPU miner with adjustable thread counts to distribute mining power across testbed nodes.
- **DNS seeding:** We disabled DNS-based peer discovery, replacing it with predetermined bootstrap node addresses to ensure deterministic network formation in our experiments.
- **Address handling:** We extended the address parsing and storage logic to accommodate SCION address formats alongside traditional IP addresses.

### C. SCION Integration

SCION addresses use the format `ISD-AS,IP:port` (e.g., `1-ff00:0:110,10.0.0.1:8666`). We propagate these addresses through Bitcoin's extended `addrv2` messages, which support arbitrary address formats. The default SCION port is 8666 (configurable via command-line flags).

**Bootstrap and Peer Discovery.** A new node has no SCION peer addresses at first start, so we pre-configure each node with a small list of well-known bootstrap SCION addresses, analogous to Bitcoin Core's hardcoded fixed seeds and DNS seeds. After the first SCION connection, the standard `addrv2` peer-exchange (PEX) takes over: peers gossip both IP and SCION addresses, which are persisted to disk and used on subsequent restarts. A SCION-capable peer can therefore be discovered organically via any IP-only peer that has already learned of it. If all bootstrap SCION addresses are unreachable, the node falls back to its IP-only bootstrap path and acquires SCION addresses later through PEX. For the experiments in Section VI we disable DNS seeding and use a fixed bootstrap list so that network formation in the SEED emulator is deterministic.

**QUIC Transport:** We use QUIC as the transport protocol for SCION connections. QUIC provides three key benefits for

[1]https://github.com/netsec-ethz/scion-apps/tree/master/pkg/pan

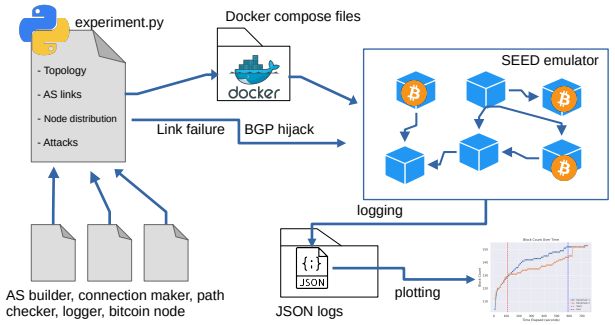



Fig. 5: Automated pipeline for the BGP hijack and link failure experiments.

our application: (i) connection migration, which enables transparent path switching without disrupting ongoing sessions; (ii) built-in TLS 1.3 encryption, providing confidentiality and integrity for Bitcoin messages; and (iii) multiplexed streams over a single connection, reducing connection establishment overhead.

**Path Selection:** The path selector probes available SCION paths every 5 seconds (configurable). If the active path latency exceeds a configurable threshold, it switches to the lowest-latency alternative. Path switching is transparent to the Bitcoin protocol via QUIC connection migration.

### D. Connection Management

**Dual-Stack Operation.** The node connects to both IP (port 8333) and SCION (port 8666) peers concurrently, preferring SCION connections for their security properties. This dual-stack approach enables nodes to bridge partitions during BGP attacks: when IP routing is compromised, SCION connections remain functional.

The connection manager maintains separate peer pools for IP and SCION connections, preferring SCION-capable peers for outbound connections. Peer addresses (both IP and SCION) are stored persistently and exchanged with peers, enabling organic discovery of SCION-capable nodes.

## VI. Evaluation

We evaluate SCION-Bitcoin through three complementary analyses: a **BGP hijacking experiment** demonstrating partition prevention with SCION-enabled bridges, a **link failure experiment** comparing failover times between SCION and BGP with BFD, and a **large-scale routing analysis** quantifying deployment requirements across the live AS-level topology.

### A. Experiment Design

Figure 5 shows the experimental components. We deployed the testbed using the SEED emulator [10], constructing the Internet topology, Bitcoin network, and attack scenarios programmatically with the SEED Python framework.

### B. Mixed Topology in the SEED Emulator

The SEED emulator enables small-scale Internet emulation including Internet Exchange Points (IXPs), ASes, and BGP/SCION infrastructure. Our topology comprises 8 ISDs (5 regional, 3 cloud/hosting) running BGP and SCION concurrently over separate links. Each AS comprises one border router, one internal network, a SCION control service, and Bitcoin nodes.

*1) Node Deployment:* To approximate real-world distribution, we placed approximately 50% of nodes in Tier-1 cloud ASes and distributed the remainder across Tier-3 stub ASes following Bitnodes data [28]. Bootstrap nodes seed the P2P network formation.

*2) Blockchain Configuration:* We adopt mainnet parameters with reduced block time and difficulty targets to accelerate block production and enable CPU mining. All nodes mine to distribute hash power uniformly. Each experiment starts from the genesis block with empty peer lists to ensure reproducibility.

### C. The BGP Hijack

We executed the BGP hijack using BIRD[2], the Internet routing daemon. Listing 1 shows the configuration for hijacking AS 130. The experiment proceeds in three phases: (1) a two-minute warm-up period for the Bitcoin network to establish peer connections, (2) an eight-minute BGP hijack targeting one AS to partition its nodes, and (3) a two-minute recovery period for reconnection and chain synchronization.

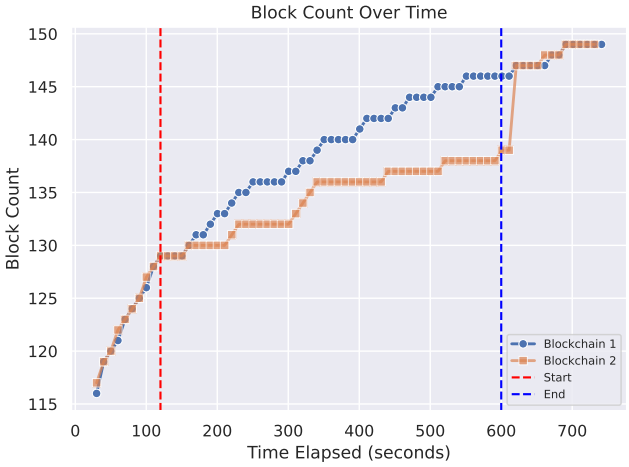
```
protocol static hijacks {
    ipv4 {
        table t_bgp;
    };
    route 10.130.0.0/25 blackhole   {
    ↪   bgp_large_community.add(LOCAL_COMM);
    ↪   };
    route 10.130.0.128/25 blackhole {
    ↪   bgp_large_community.add(LOCAL_COMM);
    ↪   };
}
```

Listing 1: Bird configuration for a BGP hijack of victim AS 130

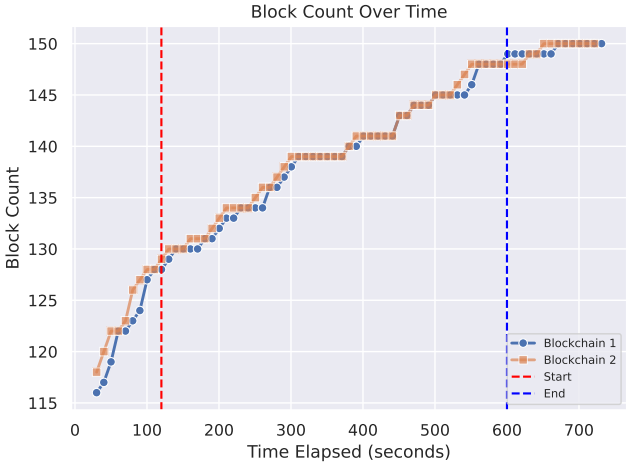
### D. The Link Failure

We induced link failures between two nodes connected over both SCION and BGP. Each node sends probe packets at one-millisecond intervals with sequence numbers; gaps in the received sequence indicate the failover duration. We disrupted and restored the link 50 times using Linux Traffic Control (TC). For BGP, we configured BFD with a 200 ms interval and a multiplier of three, which is more aggressive than Google's production recommendation (1000 ms interval, multiplier of five [29]), thereby favoring BGP in this comparison.

[2]https://bird.network.cz/




(a) **Without** SCION.




(b) **With** SCION.

Fig. 6: Block height per node during the BGP hijack. The hijack starts at $t = 120\,\text{s}$ and is retracted after 8 minutes.

### *E. Data Collection and Environment*

Each Bitcoin node reports its latest block height, block hash, peer count, and peer addresses via RPC at ten-second intervals. Experiments ran on Ubuntu 22.04.3 LTS with an AMD Ryzen 7 5800X (8-core, 32 GB DDR4). Software versions: Go 1.17.13, Python 3.10.12, Docker Engine 24.0.6, Docker Compose 2.21.0.

### *F. Hijacking Mitigation*

Figure 6 shows block heights per node during the BGP hijack experiment, verified via block hash comparisons. Orange indicates a node within the attacked AS (partitioned) and blue indicates a node outside both the attacked and attacker ASes.

Without SCION (Figure 6a), a fork emerges shortly after the attack begins, with the partitioned segment advancing more slowly because its reduced mining power operates against the network-wide difficulty target; after retraction, nodes rejoin and adopt the longer chain, discarding the forked blocks. With

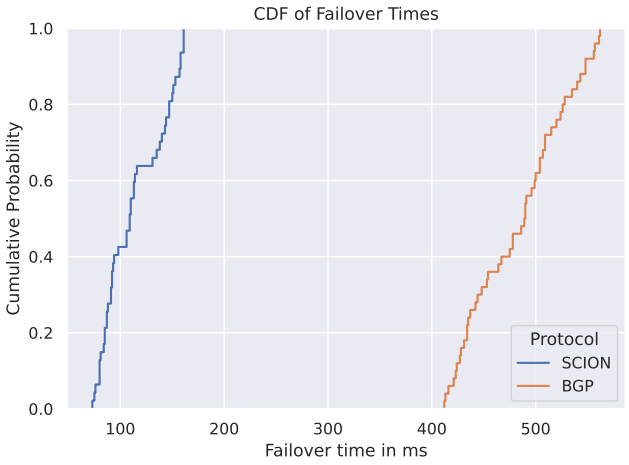



Fig. 7: Failover time (in ms) for BGP and SCION.

SCION (Figure 6b), two SCION-enabled nodes bridge the partition and no fork occurs (minor block-height variations reflect normal P2P propagation delays). Although the BGP hijack still succeeds at the routing layer, the Bitcoin overlay remains logically connected through SCION paths, preventing forks and double-spending. Multi-AS attacks would partition more nodes at the IP layer, but the protection holds as long as at least one SCION path connects the would-be partitions; Section VI-H quantifies how bridge placement achieves this for most Bitcoin nodes. Trust implications of relying on bridges during attacks are discussed in Section VII.

### *G. Link Failure Mitigation*

Figure 7 shows the failover time distribution over 50 iterations. Mean failover time is 495 ms for BGP with BFD versus 110 ms for SCION (4.5× improvement). The gap stems from where the failover decision is made: in SCION, an endpoint already holds a set of cryptographically verified alternative paths discovered via beaconing and continuously probed by our PAN-based path selector, so on detecting failure of the active path the host immediately switches to a pre-validated backup with no control-plane convergence. BGP+BFD, by contrast, must withdraw the failed prefix, propagate the update through the AS-graph, and let neighboring ASes recompute and install an alternative route before traffic flows again; even with our aggressive 200 ms BFD interval, control-plane propagation dominates the mean, and reducing the BFD interval to 50 ms did not significantly change BGP's distribution. While failover latency is less critical for Bitcoin's gossip protocol than for latency-sensitive applications, faster path recovery reduces the window during which block propagation is disrupted.

### *H. Large-Scale Deployment Analysis*

The emulation establishes that SCION-enabled nodes *can* prevent partitions and exhibhit lower failover latency than BGP; the harder question, central to any non-BGP defense, is whether such protection is reachable at scale. We therefore

quantify, on the live December 2025 Bitnodes population and the January 2026 CAIDA AS-relationship topology, how many SCION-enabled ASes are needed to protect a substantial fraction of Bitcoin nodes, using two coverage models: *direct protection*, where the node's AS is SCION-enabled, and *bridge protection*, where a routing-secure BGP path connects the node to a SCION-enabled bridge AS, following SABRE's model [9].

*1) Data Sources and Methodology:* Bitcoin node distribution comes from the Bitnodes archive [28] (December 2025): 24,392 reachable addresses comprising 8,861 clearnet (IPv4/IPv6) across 1,213 ASes and 15,531 Tor (.onion). These populations overlap substantially, as Bitcoin Core 0.21.0 [30] automatically creates Tor hidden services for clearnet nodes. Dual-stack nodes remain exposed to BGP attacks on their clearnet connections, and even Tor-only nodes face AS-level traffic correlation [31]. Our analysis covers the 8,861 clearnet nodes, representing the complete BGP-exposed attack surface.

AS-level topology data comes from the CAIDA AS relationship dataset [32] (January 2026), comprising 78,673 ASes with 160,864 provider-customer and 563,565 peer-to-peer links. After filtering Bitcoin-hosting ASes to those present in the CAIDA topology, our analysis covers 8,856 nodes in 1,208 ASes.

For the bridge coverage analysis, we classify AS-level routes using the Gao-Rexford valley-free routing model [33], widely adopted in routing security research including SABRE [9]. Route security depends on the business relationship between node and bridge: routes are ranked by local preference (CUSTOMER $>$ PEER $>$ PROVIDER), with higher-preference routes being more resistant to hijacking.

*2) Coverage Models:* **Direct Coverage (Infrastructure-Based).** A Bitcoin node receives direct protection if and only if its AS is SCION-enabled. This model provides the strongest guarantees: immunity to all BGP-based attacks, including sub-prefix (/25) hijacking. We define:

$$\text{Coverage}_{\text{direct}} = \frac{\text{Bitcoin nodes in SCION-enabled ASes}}{\text{Total clearnet Bitcoin nodes}}$$

**Bridge Coverage (Routing-Secure 1-Hop).** Bitcoin nodes in non-SCION ASes can benefit from SCION bridges if the BGP path from the node to at least one bridge is resistant to hijacking. Per SABRE's analysis [9], a route is considered routing-secure when it has high local preference and short AS-path length, making it difficult for an attacker to offer a more attractive alternative. Specifically:

- **Peer routes** (node peers with bridge AS): The node learns a 1-hop route with PEER local preference. An attacker must offer a CUSTOMER route (higher preference) or an equally-preferred shorter path to hijack this route, both of which are difficult for most AS-level adversaries.
- **Customer routes** (bridge AS is node's customer): The node learns a CUSTOMER route with the highest local preference. This is the most resistant to hijacking, as no route type has higher preference.

TABLE I: Top 10 ASes by Bitcoin node count (total: 8,861 clearnet nodes in 1,213 ASes).

| Rank | AS Name | Type | Nodes | Cumul. |
|---|---|---|---|---|
| 1 | Hetzner (AS24940) | Cloud | 872 | 9.8% |
| 2 | OVH (AS16276) | Cloud | 423 | 14.6% |
| 3 | Google Cloud (AS396982) | Cloud | 359 | 18.7% |
| 4 | AWS (AS16509) | Cloud | 352 | 22.6% |
| 5 | Comcast (AS7922) | ISP | 334 | 26.4% |
| 6 | AT&T (AS7018) | ISP | 232 | 29.0% |
| 7 | DigitalOcean (AS14061) | Cloud | 218 | 31.5% |
| 8 | Verizon (AS701) | ISP | 198 | 33.7% |
| 9 | Deutsche Telekom (AS3320) | ISP | 192 | 35.9% |
| 10 | Contabo (AS51167) | Cloud | 188 | 38.0% |

TABLE II: Minimum ASes for direct coverage targets (greedy placement).

| Target | ASes | Nodes | Composition |
|---|---|---|---|
| 50% | 24 | 4,448 | Top cloud + major ISPs |
| 60% | 46 | 5,328 | + Regional providers |
| 70% | 96 | 6,215 | + Mid-size hosting |
| 80% | 198 | 7,090 | + Long-tail begins |
| 90% | 463 | 7,975 | + Significant long-tail |

- **Provider routes** (bridge AS is node's provider): The node learns a PROVIDER route with the lowest local preference. Any attacker offering a PEER or CUSTOMER route can hijack this path. We *exclude* provider routes from safe bridge coverage.

**SCION Advantage over SABRE.** Unlike SABRE relays, which must maintain mutual $k$-connectivity via routing-secure BGP paths, SCION bridges communicate over cryptographically verified SCION paths. This eliminates the inter-relay connectivity constraint, broadening the candidate set for bridge placement.

*3) Bitcoin Node Distribution:* Bitcoin nodes exhibit significant concentration in cloud providers and residential ISPs. Table I shows the top 10 ASes by node count. The top 5 ASes host 26.4% of all clearnet nodes, while approximately 50% of ASes host only a single node, creating a long-tail distribution.

*4) Direct Coverage Analysis:* We apply a greedy placement algorithm that iteratively selects the AS hosting the most unprotected Bitcoin nodes. Table II shows the ASes required to reach direct coverage targets.

Reaching 80% requires 198 ASes (16.3% of Bitcoin-hosting ASes) and 90% requires 463 (38.3%), reflecting the long-tail distribution.

*5) Routing-Secure Bridge Coverage:* We apply a greedy algorithm that iteratively selects the AS maximizing marginal safe 1-hop coverage (peer and customer routes only, excluding easily-hijacked provider routes). Table III shows one example of the resulting placement: 5 ASes achieve 81.0% coverage, with heavily-peered ASes providing broad routing-secure reach and cloud ASes contributing direct node coverage. While 14 alternative 5-AS sets also reach 80%, all contain the same two heavily-peered core ASes (i3D.net and Hurricane Electric). These figures are conservative, as only direct 1-hop

TABLE III: Greedy SCION bridge placement by safe 1-hop coverage. Coverage is cumulative and excludes provider-route (easily hijacked) links.

| # | AS (Name) | Peers | Coverage |
|---|---|---|---|
| 1 | AS49544 (i3D.net) | 6,616 | 64.4% |
| 2 | AS6939 (Hurricane Elec.) | 7,712 | 73.2% |
| 3 | AS396982 (Google Cloud) | 0† | 77.2% |
| 4 | AS51167 (Contabo) | 0† | 79.4% |
| 5 | AS3356 (Lumen/Level3) | 74 | 81.0% |

†No peers; selected for direct Bitcoin node coverage.

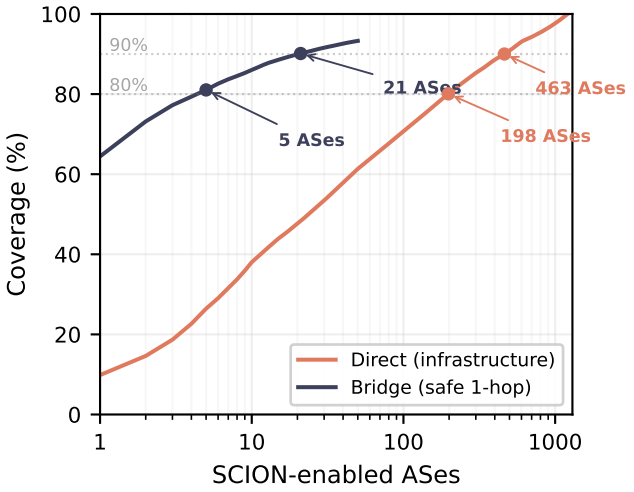



Fig. 8: Coverage progression with greedy AS placement. Bridge coverage reaches 80% with only 5 ASes and 90% with 21; direct coverage requires 198 ASes for 80% and 463 for 90%, reflecting the long-tail AS distribution.

links with safe relationship types are counted; multi-hop paths resistant to hijacking would increase coverage further.

*6) Deployment Strategy:* Figure 8 compares the two coverage models, mapping to the two-phase strategy in Section IV-C and summarized in Table IV. Current SCION production deployment (approximately 70 ASes, primarily Swiss ISPs and European research networks [14]) provides only 1.3% direct coverage, as these ASes host few Bitcoin nodes. However, the safe 1-hop model reveals that these same ASes already cover 52.4% of Bitcoin nodes through routing-secure paths from well-peered Swiss ISPs. Independently, deploying SCION in just 5 well-chosen ASes (Table III) achieves 81.0% safe 1-hop coverage. Extending deployment to major cloud providers and residential ISPs transitions protection from bridge-based to infrastructure-based: 198 ASes yield 80% direct coverage, immune to all BGP-based attacks including sub-prefix (/25) hijacking. This progression aligns with the SBAS model [23].

*7) Comparison with State of the Art:* Table V compares SCION-Bitcoin with SABRE and RPKI across both coverage models.

**SABRE** [9] achieves high coverage with 6 relays by exploiting BGP route preferences (May 2018 topology), but

TABLE IV: Coverage under deployment phases.

| Phase | Model | ASes | Coverage |
|---|---|---|---|
| Current | Direct | ∼70 | 1.3% |
| Current | Safe 1-hop | ∼70 | 52.4% |
| Bridges | Safe 1-hop | 5 | 81.0% |
| Cloud/ISPs | Direct | 198 | 80.0% |
| Cloud/ISPs | Direct | 463 | 90.0% |

TABLE V: Comparison of approaches for protecting Bitcoin against BGP attacks.

| Property | SABRE | RPKI/ROV | SCION |
|---|---|---|---|
| Protection model | BGP pref. | Origin val. | Infrastructure |
| Sub-prefix (/25) | Vulnerable | Vulnerable† | Immune |
| Path verification | None | Origin AS | Cryptographic |
| Bridge 80% cov. | 6[a] | N/A | 5[b] |
| Direct 80% cov. | N/A | N/A | 198 |
| Inter-relay sec. | $k$-conn. | N/A | SCION paths |
| Deployment | None reported | Partial‡ | Production |

[a]BGP preference model, May 2018 data; $k$=1 connectivity.
[b]Safe 1-hop model, Dec 2025 data; no $k$-connectivity needed.
†Vulnerable when hijacked prefix is more specific than ROA.
‡25–33% of ASes enforce ROV filtering [6].

relays must satisfy structural constraints (no customer ASes, mutual $k$-connectivity, /24 prefix announcements) and remain vulnerable to sub-prefix (/25) attacks. Using the same routing model on December 2025 data, 5 SCION bridges achieve 81.0% safe 1-hop coverage. The key structural advantage is that SCION eliminates the $k$-connectivity constraint, as bridges communicate over SCION paths rather than BGP.

**RPKI/ROV** [27] validates route origins but cannot prevent path manipulation or sub-prefix attacks, and deployment remains incomplete (Section III).

## VII. Discussion

**Cost Analysis.** SABRE [9] requires dedicated P4-based relay nodes deployed solely for Bitcoin protection. In contrast, SCION is general-purpose Internet infrastructure that benefits all applications in an AS. In ASes that already support SCION, a Bitcoin bridge node runs on commodity hardware at cost comparable to a standard full node. For non-SCION ASes, the border-router and Anapaya CORE licensing cost is amortized across all SCION-enabled services, not borne by Bitcoin alone, and yields operational benefits (fast failover, flexible path selection) beyond hijack protection.

**Trust and Decentralization.** During active attacks, Bitcoin nodes depend on SCION-enabled bridges for block and transaction relay, introducing three trust requirements: bridges must be (i) *available* (reachable and forwarding without indefinite delay), (ii) *complete* (relaying all valid blocks without selective censorship), and (iii) *timely* (forwarding promptly to prevent stale-block mining). These parallel SABRE's trusted relay model [9]. Bitcoin's protocol provides inherent safeguards: bridges cannot forge blocks or transactions (all nodes independently verify proof-of-work and signatures), stalling bridges are detected and disconnected through existing timeout mechanisms, and selective censorship is mitigated by connecting

to multiple independently operated bridges. Concentrating bridges in only 5 ASes does create some centralization; deploying more than the minimum coverage threshold mitigates this, and as SCION adoption broadens, bridge dependence diminishes in favor of direct SCION connections.

## VIII. Conclusion and Future Work

We presented a SCION-enabled Bitcoin node based on btcd that resists BGP hijacking through cryptographic path verification, eliminating reliance on BGP-layer routing security. Our AS-level analysis on December 2025 Bitnodes and CAIDA data shows that meaningful coverage is reachable with a small number of SCION-enabled ASes: 5 strategically placed SCION bridges cover 81% of Bitcoin nodes via routing-secure paths. As SCION grows, deployment in 198 ASes achieves 80% direct, infrastructure-based coverage immune to all BGP hijacks including sub-prefix (/25) attacks. In SEED-emulator experiments, SCION connections remained functional during active BGP hijacks, enabling SCION-enabled nodes to bridge partitions and prevent blockchain forks; the same testbed showed a 4.5× failover speedup over BGP+BFD on link failure (110 ms vs. 495 ms mean). Taken together, these results suggest that effective protection of Bitcoin against BGP hijacking is reachable through targeted SCION deployment.

Future work includes latency optimization for miners via SCION path selection, multi-path block propagation, extension to other vulnerable cryptocurrencies [3], and real-world deployment studies.

## References


[1] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392, IEEE, 2017.

[2] M. Saad, V. Cook, L. Nguyen, M. T. Thai, and A. Mohaisen, "Partitioning attacks on Bitcoin: Colliding space, time, and logic," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1175–1187, IEEE, 2019.

[3] M. Saad and D. Mohaisen, "Three birds with one stone: Efficient partitioning attacks on interdependent cryptocurrency networks," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 1404–1418, IEEE Computer Society, 2023.

[4] BGPStream, "BGP Leak Causing Major Traffic Routing Issues for Amazon, Google and Others." https://bgpstream.crosswork.cisco.com/, Apr. 2018. Amazon Route 53 BGP hijack incident affecting MyEtherWallet users.

[5] R. Morillo, J. Furuness, C. Morris, J. Breslin, A. Herzberg, and B. Wang, "ROV++: Improved deployable defense against BGP hijacking," *Proceedings 2021 Network and Distributed System Security Symposium*, 2021.

[6] T. Hlavacek *et al.*, "Keep your friends close, but your routeservers closer: Insights into RPKI validation in the internet," in *Proceedings of the 32nd USENIX Security Symposium*, USENIX Association, 2023.

[7] L. Chuat, M. Legner, D. Basin, D. Hausheer, S. Hitz, P. Müller, and A. Perrig, *The Complete Guide to SCION*. Springer, 2022.

[8] Sui Foundation, "Sui advances network security and performance with SCION," 2025. Blog post.

[9] M. Apostolaki, G. Marti, J. Müller, and L. Vanbever, "SABRE: Protecting Bitcoin against Routing Attacks," in *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS)*, The Internet Society, 2019.

[10] W. Du, H. Zeng, and K. Won, "SEED emulator: An internet emulator for research and education," in *Proceedings of the 21st ACM Workshop on Hot Topics in Networks*, pp. 101–107, 2022.

[11] Y. Rekhter, S. Hares, and T. Li, "A Border Gateway Protocol 4 (BGP-4)." RFC 4271, Jan. 2006.

[12] D. Mehta, T. Ruffing, J. Schnelli, and P. Wuille, "BIP 324: Version 2 P2P encrypted transport protocol," 2019.

[13] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," in *Proceedings of the 24th USENIX Conference on Security Symposium*, pp. 129–144, USENIX Association, 2015.

[14] Anapaya Systems, "SCION AS Registry." https://learn.anapaya.net/docs/resources/assignments/ases/, 2024. Accessed: 2024.

[15] C. Krähenbühl, S. Tabaeiaghdaei, C. Gloor, J. Kwon, A. Perrig, D. Hausheer, and D. Roos, "Deployment and scalability of an inter-domain multi-path routing infrastructure," in *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies*, pp. 126–140, Association for Computing Machinery, 2021.

[16] F. Wirz, M. Gartner, J. van Bommel, E. Ehsani Moghadam, G. H. Cimaszewski, A. He, Y. Zhang, H. Birge-Lee, F. Kottmann, C. Krähenbühl, J. Kwon, K. Mavromati, L. Wang, D. Bertolo, M. Canini, B. Cho, R. A. Ferreira, S. P. Green, D. Hausheer, J. Hur, X. Jia, H. Lee, P. Mittal, O. Oaiya, C. Park, A. Perrig, J. Sobieski, Y. Sun, C. Wang, and K. Wierenga, "Scaling sciera: A journey through the deployment of a next-generation network," in *Proceedings of the ACM SIGCOMM 2025 Conference*, SIGCOMM '25, (New York, NY, USA), p. 720–741, Association for Computing Machinery, 2025.

[17] J. Yang, G. Sun, R. Xiao, and H. He, "Detectable, Traceable, and Manageable Blockchain Technologies BHE: An Attack Scheme against Bitcoin P2P Network," *Wireless Commun. Mobile Comput.*, vol. 2022, Aug. 2022.

[18] C. Doumanidis and M. Apostolaki, "Routing attacks in Ethereum PoS: A systematic exploration," *arXiv preprint arXiv:2505.07713*, 2025.

[19] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A stealthier partitioning attack against bitcoin peer-to-peer network," in *2020 IEEE symposium on security and privacy (SP)*, pp. 894–909, 2020.

[20] Y. Chen *et al.*, "Learning with semantics: Towards a semantics-aware routing anomaly detection system," in *Proceedings of the 33rd USENIX Security Symposium*, USENIX Association, 2024. Distinguished Paper Award, Internet Defense Prize.

[21] D. Mirdita, H. Shulman, and M. Waidner, "SoK: An introspective analysis of RPKI security," in *Proceedings of the 34th USENIX Security Symposium*, USENIX Association, 2025.

[22] M. Lepinski and K. Sriram, "BGPsec Protocol Specification." RFC 8205, Sept. 2017.

[23] H. Birge-Lee, J. Wanner, G. H. Cimaszewski, J. Kwon, L. Wang, F. Wirz, P. Mittal, A. Perrig, and Y. Sun, "Creating a secure underlay for the internet," in *Proceedings of the 31st USENIX Security Symposium*, pp. 2601–2618, USENIX Association, 2022.

[24] C. Krähenbühl, M. Wyss, D. Basin, V. Lenders, A. Perrig, and M. Strohmeier, "FABRID: Flexible attestation-based routing for inter-domain networks," in *Proceedings of the 32nd USENIX Security Symposium*, USENIX Association, 2023.

[25] A. Vorkapic, "Secure blockchain network communication using SCION," 2018. Master thesis.

[26] F. Franzoni, X. Salleras, and V. Daza, "AToM: Active topology monitoring for the Bitcoin peer-to-peer network," *Peer-to-Peer Networking and Applications*, vol. 15, pp. 408–425, 2022.

[27] Y. Gilad, A. Cohen, A. Herzberg, M. Schapira, and H. Shulman, "Are we there yet? on RPKI's deployment and security," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2017.

[28] A. Yeow, "Bitnodes: Global Bitcoin nodes distribution." https://bitnodes.io/, 2026. Accessed: January 9, 2026.

[29] "Bidirectional forwarding detection (bfd) overview," 2023.

[30] Bitcoin Core, "Bitcoin Core 0.21.0 released." https://bitcoincore.org/en/releases/0.21.0/, January 2021. Added support for Tor v3 onion addresses.

[31] Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang, and P. Mittal, "RAPTOR: Routing attacks on privacy in Tor," in *Proceedings of the 24th USENIX Security Symposium*, pp. 271–286, USENIX Association, 2015.

[32] Center for Applied Internet Data Analysis (CAIDA), "AS Relationships Dataset." https://www.caida.org/catalog/datasets/as-relationships/, 2026. Serial-2 format, Accessed: January 2026.

[33] L. Gao and J. Rexford, "Stable internet routing without global coordination," *SIGMETRICS Perform. Eval. Rev.*, vol. 28, p. 307–317, jun 2000.