BLOCKCHAIN AS A DATABASE FOR STORING AND ANALYZING BGP ANNOUNCEMENTS

BGP-Sentry

Extending Trust Coverage Beyond RPKI Through Behavioral Assessment

Wayne State University

Introduction: The Problem

BGP lacks mandatory, global authentication.

- BGP route announcements are accepted without verification
- RPKI is the most widely accepted authentication mechanism
- However, only **37%** of ASes have RPKI enabled
- **63%** of Internet routing remains unverifiable

Real-World BGP Hijacking Attacks:

- YouTube (2008): Pakistan Telecom hijacked YouTube's prefix [1]
- MyEtherWallet (2018): \$150K+ stolen via BGP hijack [2]
- Amazon Route 53 (2018): Cryptocurrency theft via BGP hijack [3]

Motivation: Why Existing Solutions Fail

RPKI Limitations

- Limited coverage
- Policy barriers
- No audit trail
- Cannot assess non-RPKI

Prior Blockchain (Onboarding)

- Trust-based onboarding
- No identity verification
- Dishonest nodes can join
- Sybil vulnerability

Prior Blockchain (Consensus)

- Asymmetric observations
- Assumes symmetric views
- No scalable consensus
- No persistent intelligence

Key Insight: RPKI will never achieve 100% coverage.
We need to extend trust to the 63% outside RPKI.

Three Critical Challenges

1. **Challenge 1: Incomplete RPKI Adoption**
   - Only 37% of ASes enforce RPKI
   - Economic misalignment causes free-riding
   - 63% of routing remains unverifiable

2. **Challenge 2: No Authenticated Observers**
   - Blockchain validators are randomly selected
   - May include malicious nodes
   - Circular trust problem

3. **Challenge 3: Limited Scalable Consensus**
   - BGP observations are asymmetric across vantage points
   - Traditional consensus assumes symmetric views
   - No persistent security intelligence

How We Address Each Challenge

Challenge 1: Incomplete RPKI Adoption
$\rightarrow$ **Solution:** Expanding trust by monitoring non-RPKI ASes and assessing their behavior

Challenge 2: No Authenticated Observers
$\rightarrow$ **Solution:** RPKI verification during onboarding secures the observer network

Challenge 3: Limited Scalable Consensus
$\rightarrow$ **Solution:** Proof of Population consensus provides scalable agreement

Challenge → Solution → Contribution

#	**Challenge**	**Solution**	**Contribution**
1	Incomplete RPKI Adoption	Extended Coverage and Trust Propagation	Trust-based Routing for Non-RPKI ASes
2	No Authenticated Routing Observers	RPKI-Verified Observers with Incentives	Behavioral Monitoring and Observer Accountability
3	Limited Security Intelligence Consensus	Scalable PoP Consensus with Persistent Intelligence	Auditable Trust Rating via Post-Hoc Forensic Analysis

Our Solution: BGP-Sentry

A **permissioned consortium blockchain** that transforms **RPKI-enabled ASes** into distributed observers that monitor and rate **non-RPKI ASes**

RPKI Observer Network

Real-time detection *and* long-term post-hoc forensic analysis

Secure Onboarding

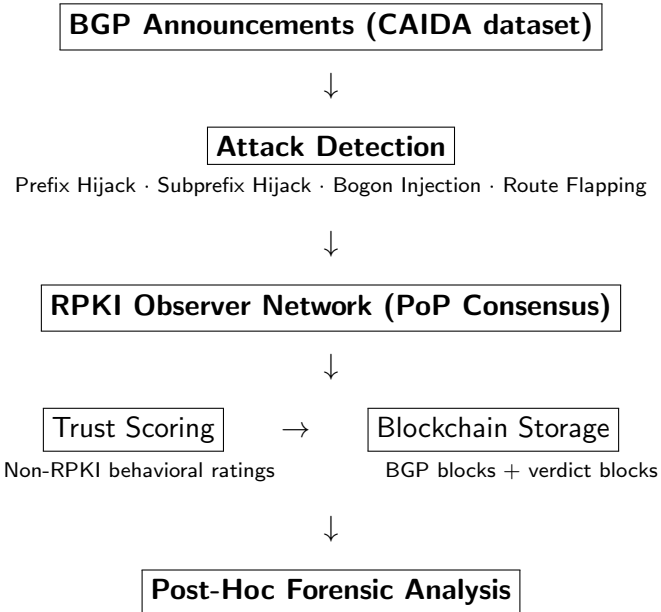
RPKI-verified identity. Token rewards incentivize honesty.

Proof of Population

Three-way voting: `approve` / `no_knowledge` / `reject`. One RPKI node = one vote.

Scalable Nodes	**PoP** Consensus	**4** Attack Types	**P2P** Network

System Architecture



Post-Hoc Forensic Analysis

Why: Real-time detection catches attacks as they happen.
Post-hoc analysis *reconstructs the full history* from immutable blockchain records.

Who runs it

- Network operators (NOC teams)
- Security researchers / CERT teams
- Automated scheduled jobs (cron)
- Regulatory auditors

How it runs

- Queries the blockchain offline
- No live network access needed
- Reproducible from any chain replica

Three analysis modules:

1. Blockchain Forensics
Attacker profiling, prefix history, observer cross-reference, audit trail generation

2. Targeted Attack Analyzer
Single-witness patterns, consensus escalation detection, temporal clustering

3. Longitudinal Behavior Analysis
Trust score trajectories, rating drift, repeat offenders, BGPCoin economy health

Post-Hoc Analysis: Output

Output	**Contents**	**Security Use Case**
Forensic Audit Report	Attacker profiles, affected prefixes, observer coverage	Incident response evidence package
Escalation Detection	Chronological vote-count patterns per (prefix, AS)	Identify learning attackers before they succeed
Trust Trajectories	Per-AS rating history over time	Flag ASes drifting toward malicious behavior
Cross-Observer Correlation	Which observers detected the same attack independently	Measure detection coverage and consensus quality

Key property: All outputs are *reproducible* from blockchain data alone.
Any party with a chain replica can independently verify every conclusion.

Summary and Contributions

Key Contributions:

1. **Trust Expansion** — Extend RPKI trust to 63% non-participating ASes
2. **Authenticated Observers** — RPKI-verified onboarding eliminates Sybil attacks
3. **Proof of Population** — Novel consensus where each RPKI node = one vote
4. **Post-Hoc Forensic Audit** — Immutable blockchain enables offline attacker profiling, escalation detection, and reproducible audit trails
5. **Economic Incentives** — BGPCoin token rewards create accountability

Thank You — Questions?

Wayne State University

References I

[1] RIPE NCC. *YouTube Hijacking: A RIPE NCC RIS Case Study*. RIPE NCC. 2008. URL: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

[2] Cloudflare. *BGP leaks and cryptocurrencies*. Cloudflare Blog. MyEtherWallet BGP hijack, $150K+ stolen. 2018. URL: https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/.

[3] BGPStream / Oracle. *Amazon Route 53 BGP Hijack*. BGPStream. Cryptocurrency theft via BGP hijack of AWS Route 53 DNS. 2018.