SCRAPS: Scalable Collective Remote Attestation for Pub-Sub IoT Networks with Untrusted Proxy Verifier

Lukas Petzi[1], Ala Eddine Ben Yahya[1], Alexandra Dmitrienko[1], Gene Tsudik[2], Thomas Prantl[1], and Samuel Kounev[1]

[1]University of Würzburg, Germany
[2]UC Irvine

Motivation

E-Health

Smart Factory

Smart Home

Smart City

Environmental Monitoring

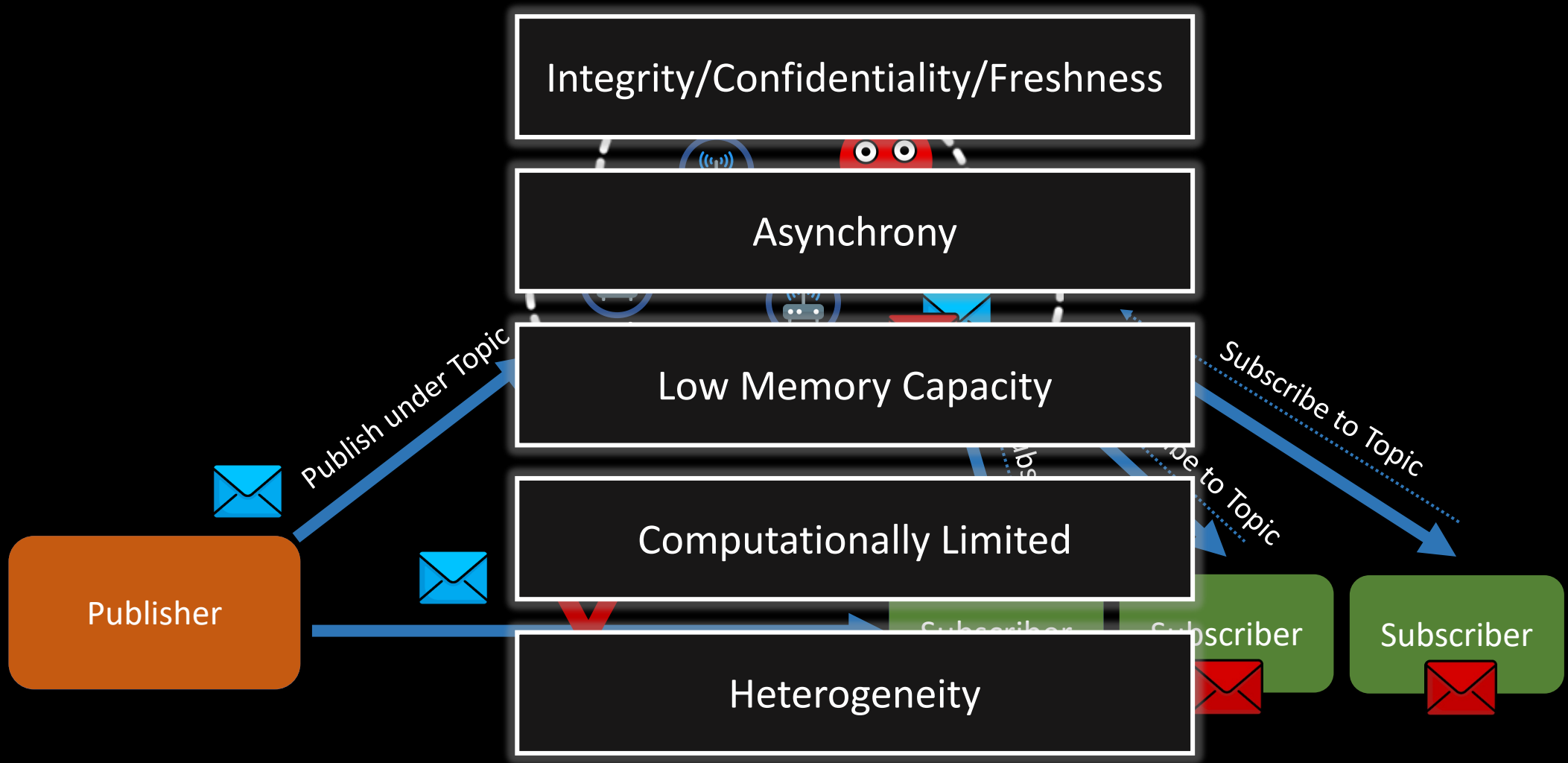
IoT

User A

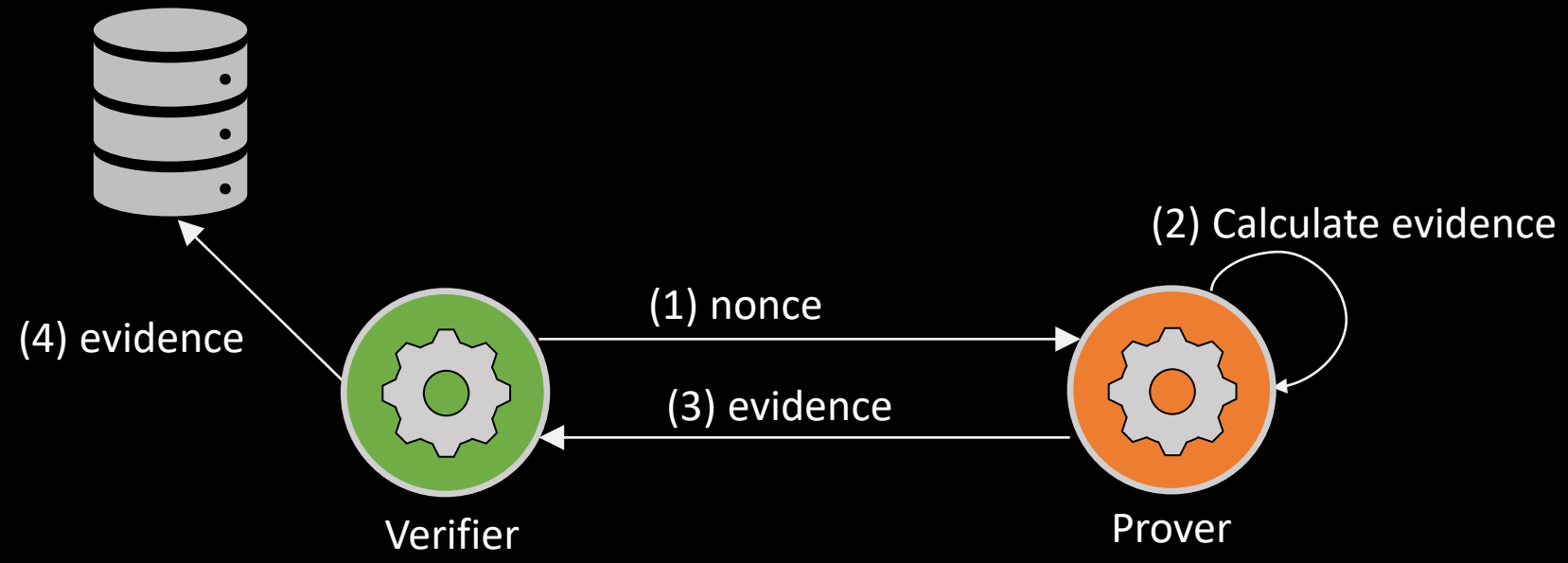
User B

User C

Challenges of Attestation in Pub/Sub IoT Networks



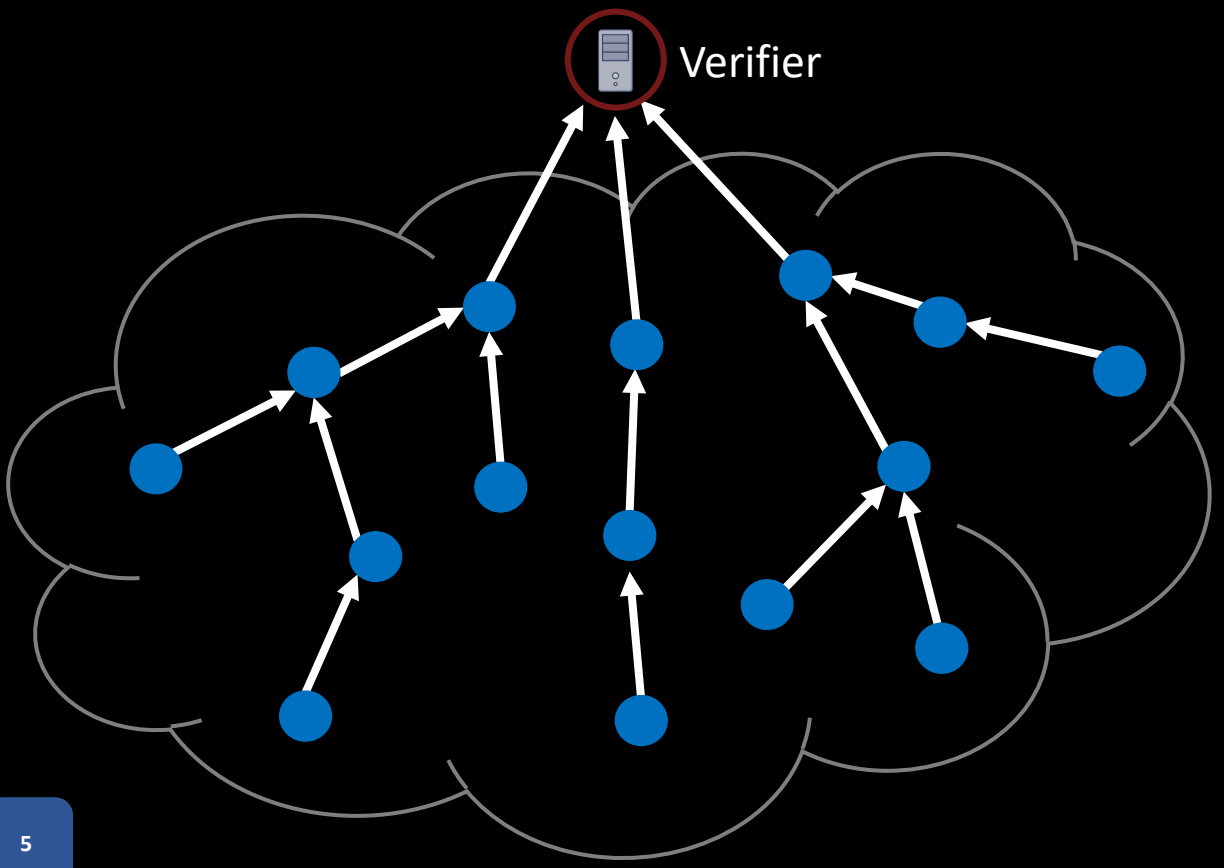
Challenges of Remote Attestation in IoT



- Poor Scalability
- Complex Key Management
- Synchronous Communication
- Uninterrupted availability
- Device Heterogeneity

Collaborative Remote Attestation Schemes

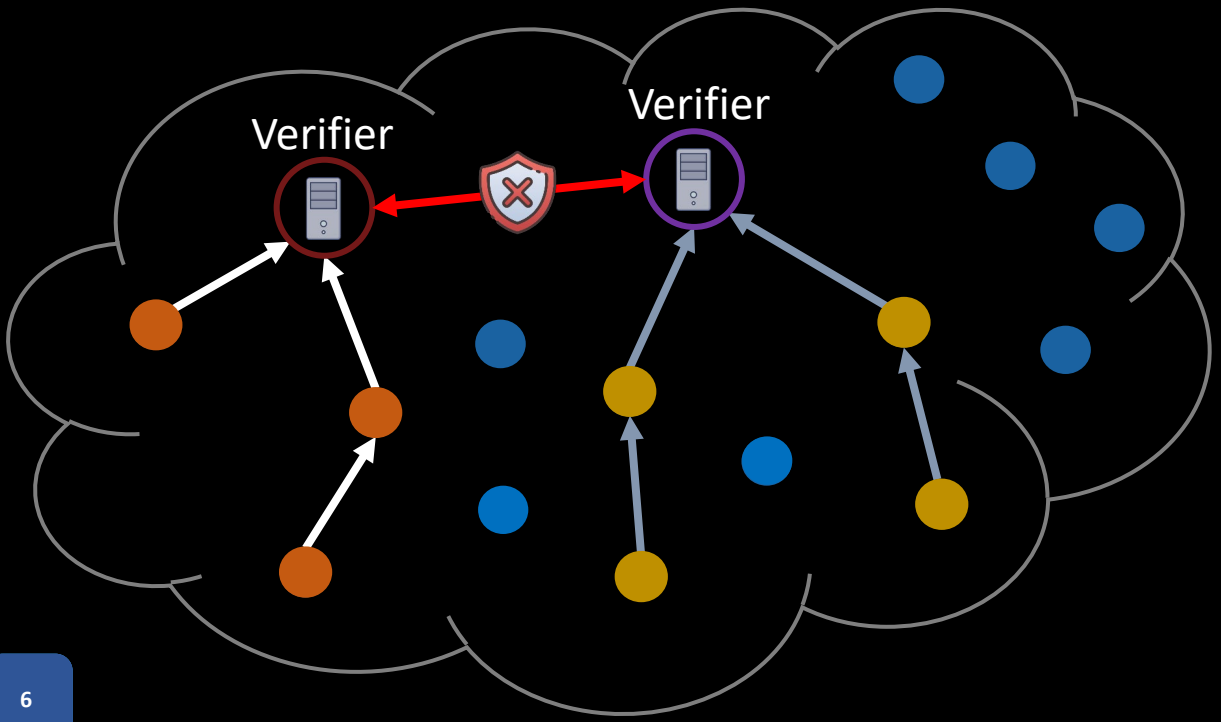
One Verifier – Many Provers



Properties	One Verifer – Many Provers
Scalability	✓
On-Demand Attestation	(✓)
Heterogeneity	(✓)
Suitable for asynchronous communication	✗
Support for Sleeping Devices	✗

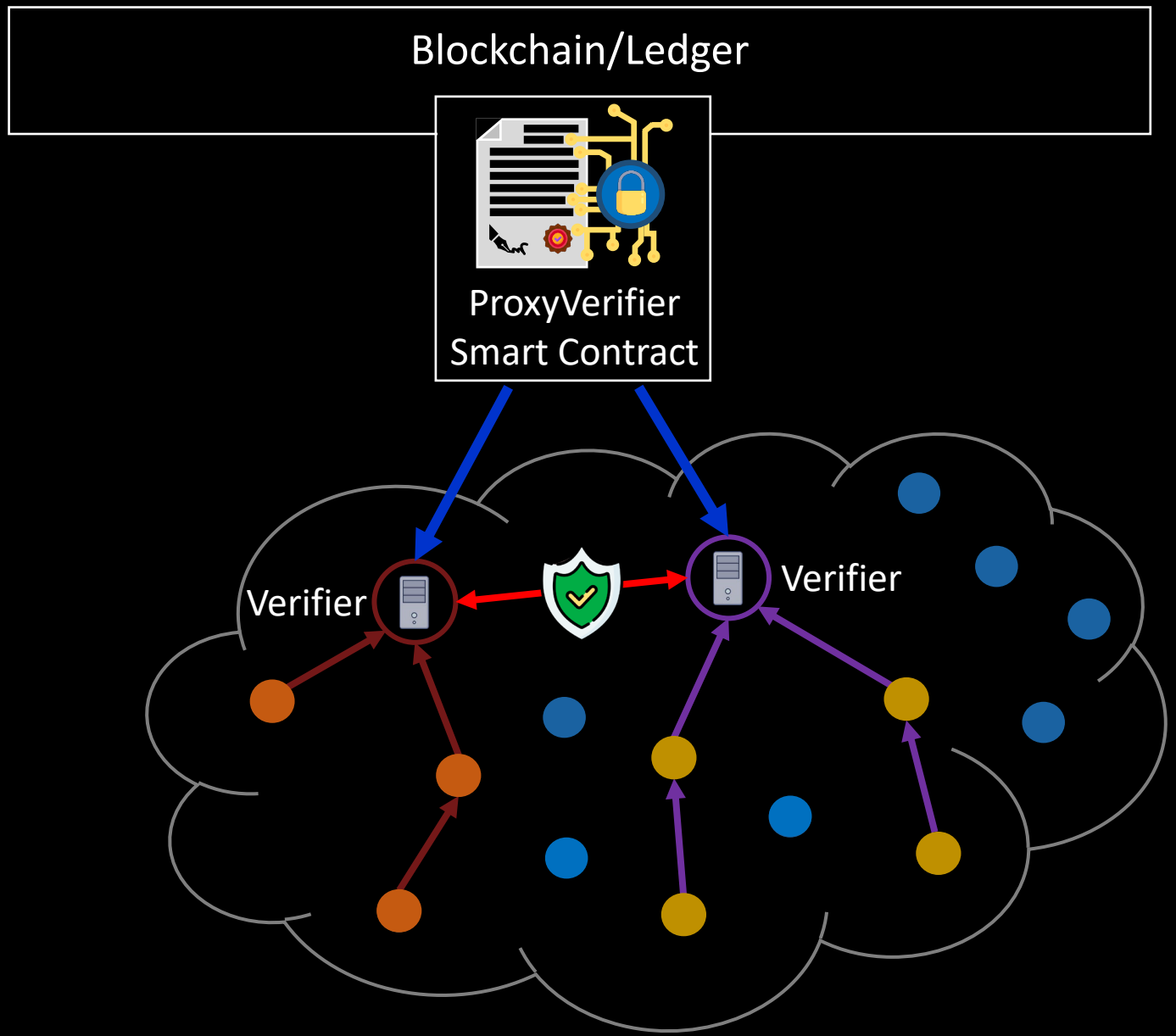
Collaborative Remote Attestation Schemes

Many Verifiers – Many Provers



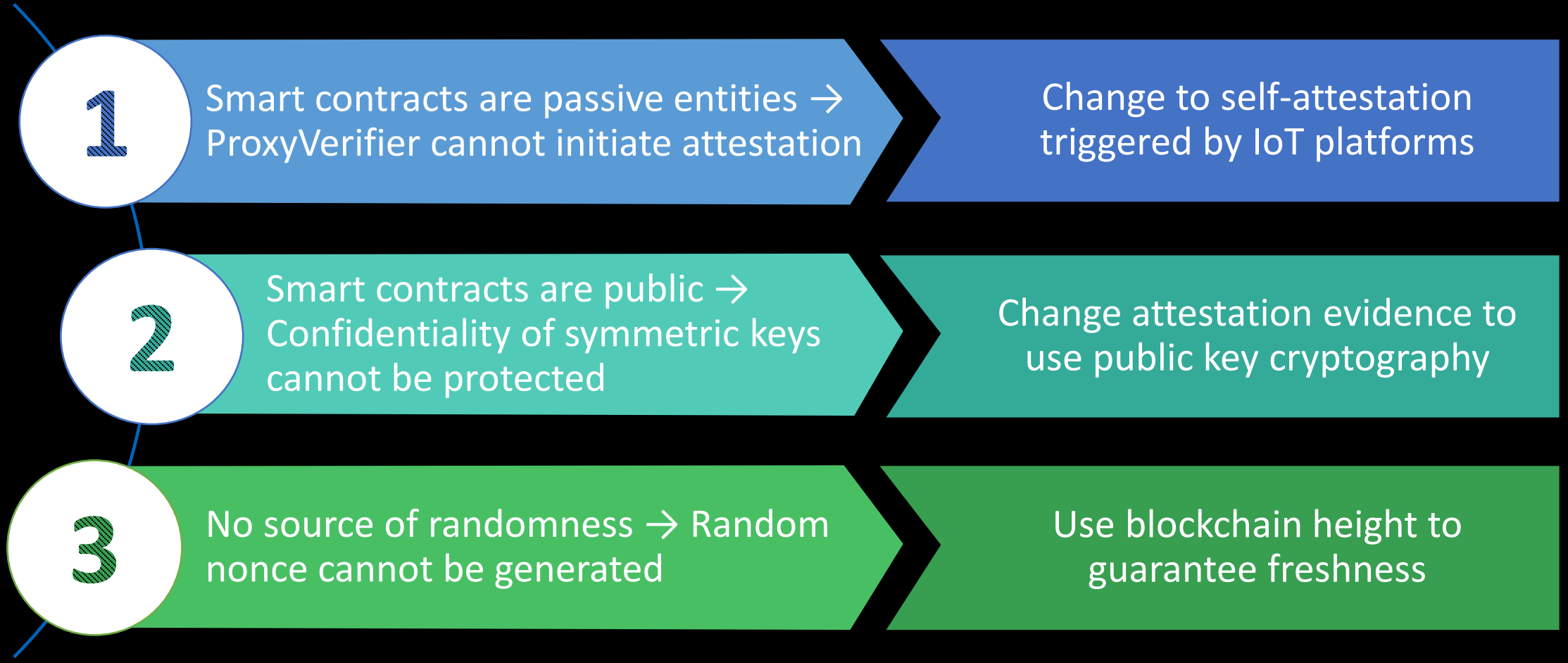
Properties	Many Verifers – Many Provers
Scalability	(✓)
On-Demand Attestation	✓
Heterogeneity	✓
Suitable for asynchronous communication	✗
Support for Sleeping Devices	✗

Hybrid Approach: SCRAPS General Idea

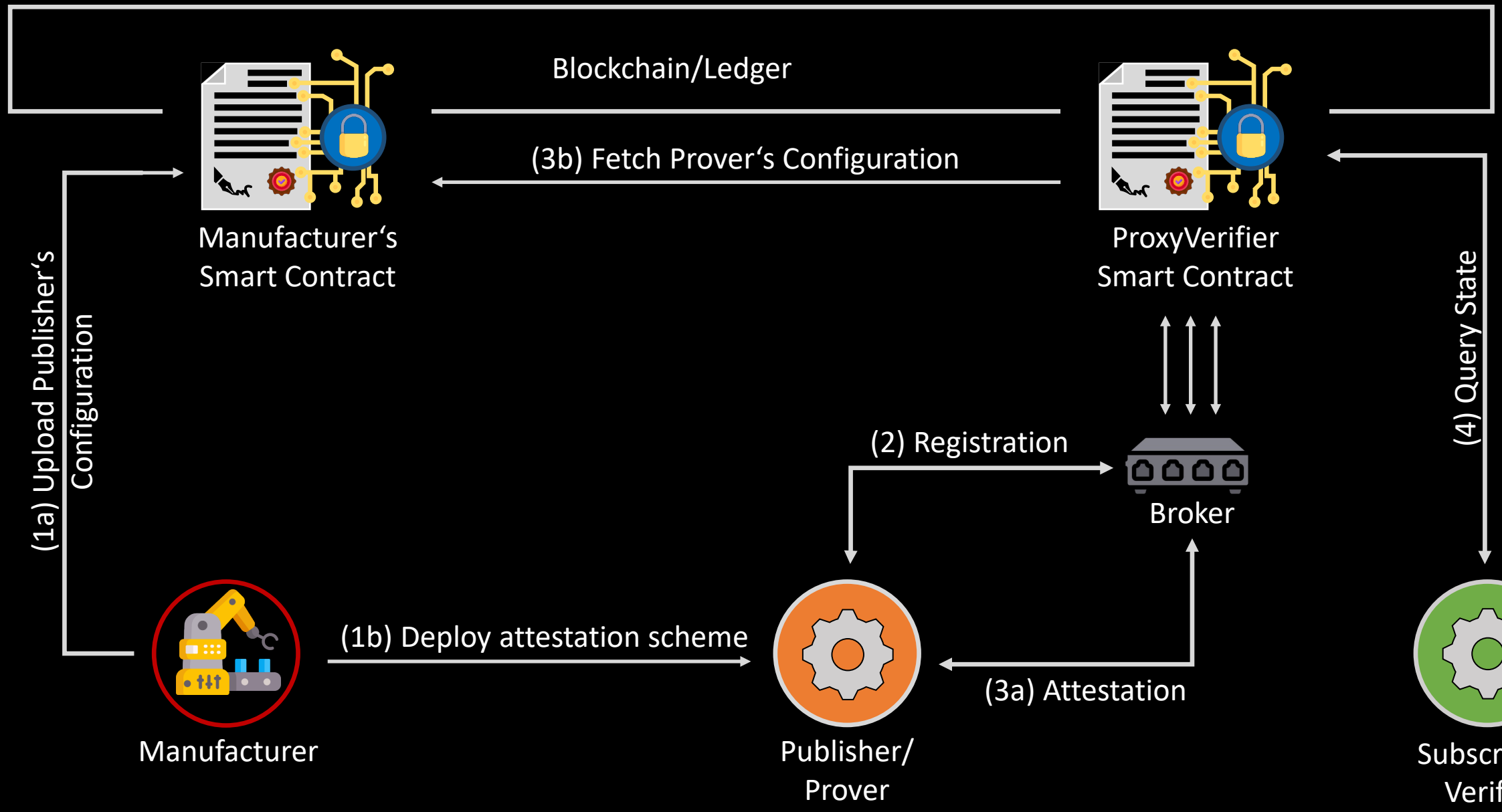


- Approach:
  - Combine both approaches
- ProxyVerifier
  - Always online – never sleeps
  - Trustless

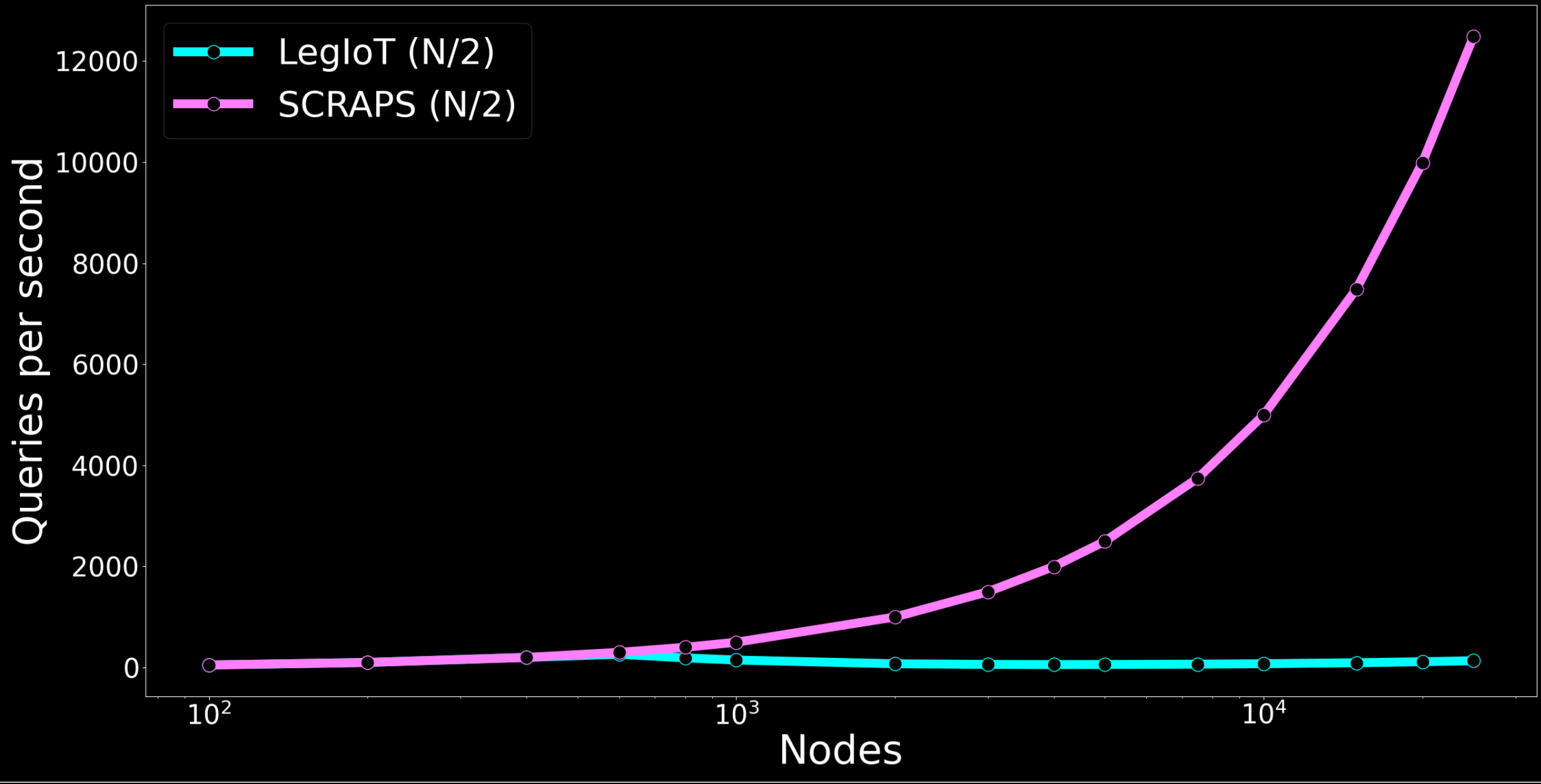
ProxyVerifier Instantiation: Technical Challenges



SCRAPS Design

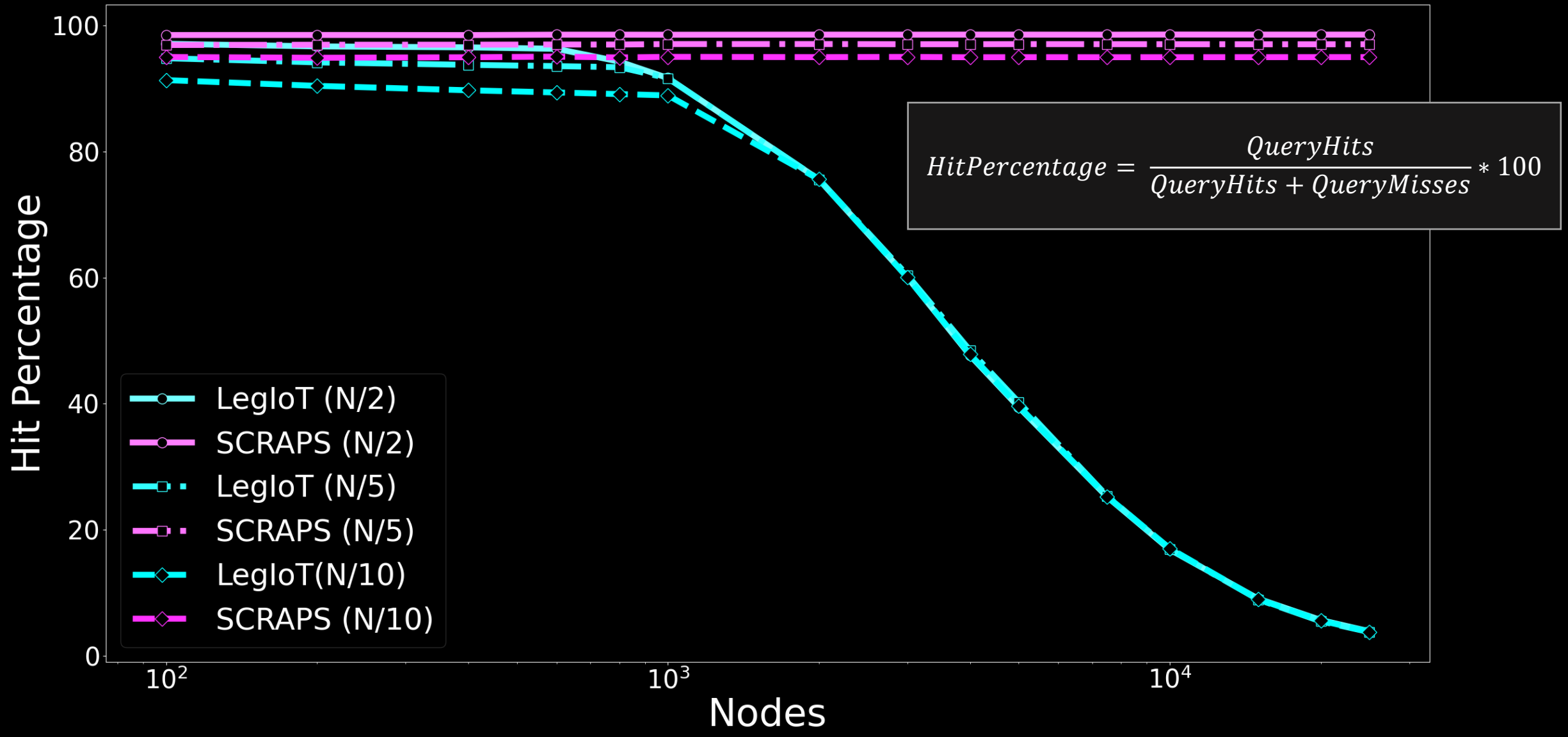


Evaluation: SCRAPS vs. LegIoT[1]



[1] Neureither et al., LegIoT: Ledgered trust management platform for IoT. In European Symposium on Research in Computer Security (ESORICS), 2020

Evaluation: SCRAPS vs. LegIoT[1]



[1] Neureither et al., LegIoT: Ledgered trust management platform for IoT. In European Symposium on Research in Computer Security (ESORICS), 2020

Conclusion

Schemes	One Verifer – Many Provers	Many Verifiers – Many Provers	Hybrid Approach (SCRAPS)
Scalability	✓	(✓)	✓
On-Demand Attestation	(✓)	✓	✓
Heterogeneity	(✓)	✓	✓
Suitable for asynchronous communication	✗	✗	✓
Support for Sleeping Devices	✗	✗	✓

First suitable solution for Pub/Sub Environments