

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

Lukas Petzi¹, Ala Eddine Ben Yahya¹, Alexandra Dmitrienko¹, Gene Tsudik²,
Thomas Prantl¹, and Samuel Kounev¹

¹University of Würzburg, Germany

²UC Irvine

Motivation



E-Health



Smart Factory



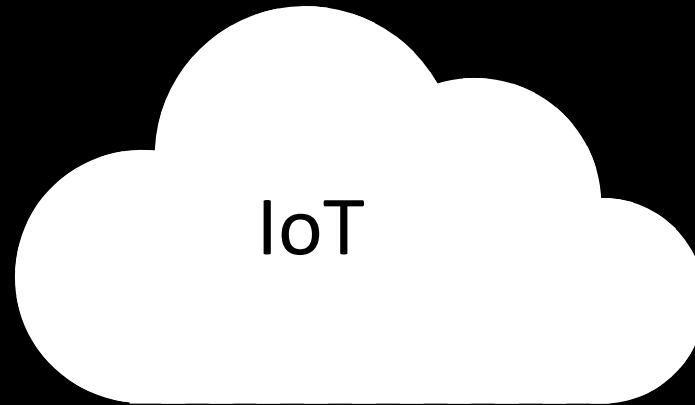
Smart Home



Smart City



Environmental
Monitoring



User A



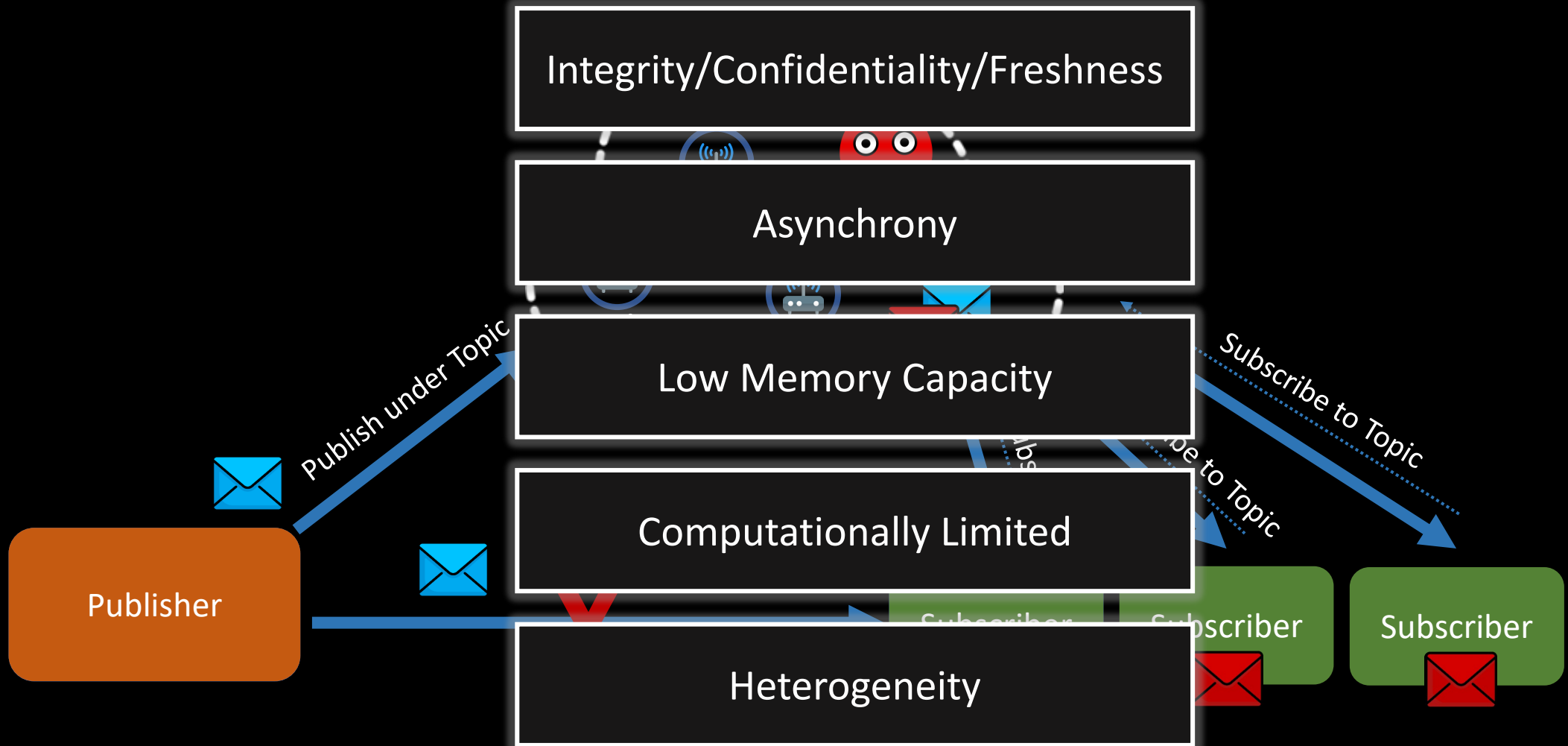
User B



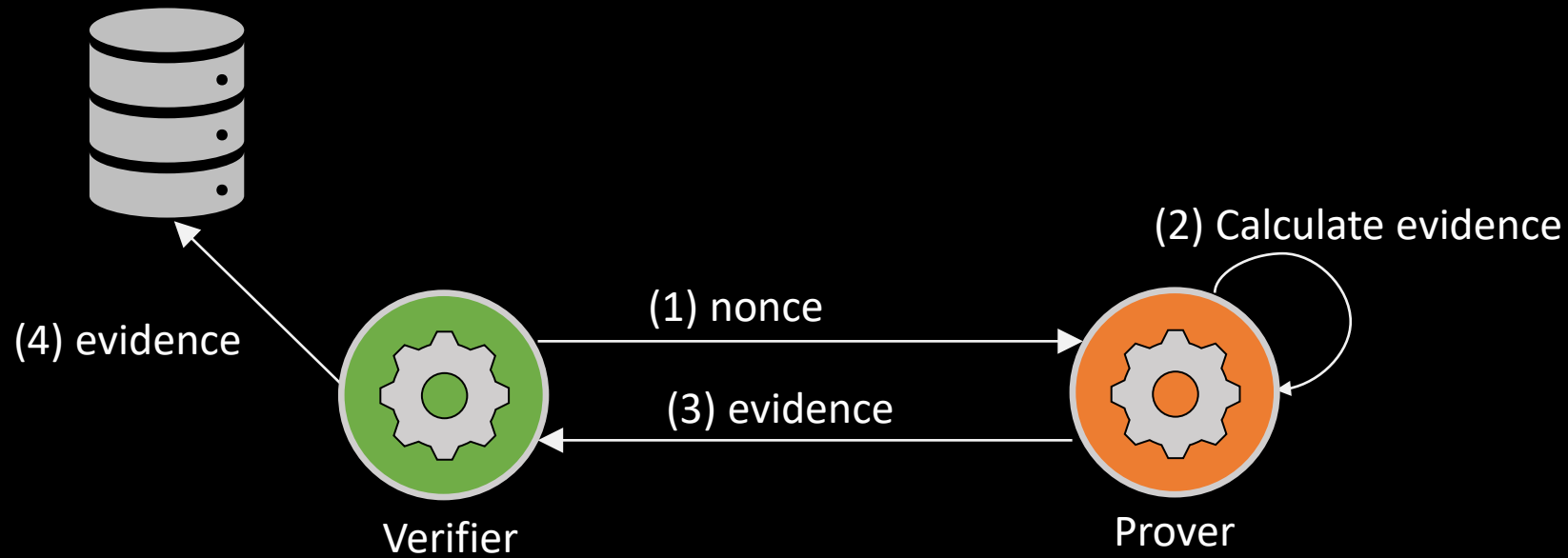
User C



Challenges of Attestation in Pub/Sub IoT Networks



Challenges of Remote Attestation in IoT



👎 Poor Scalability

👎 Complex Key Management

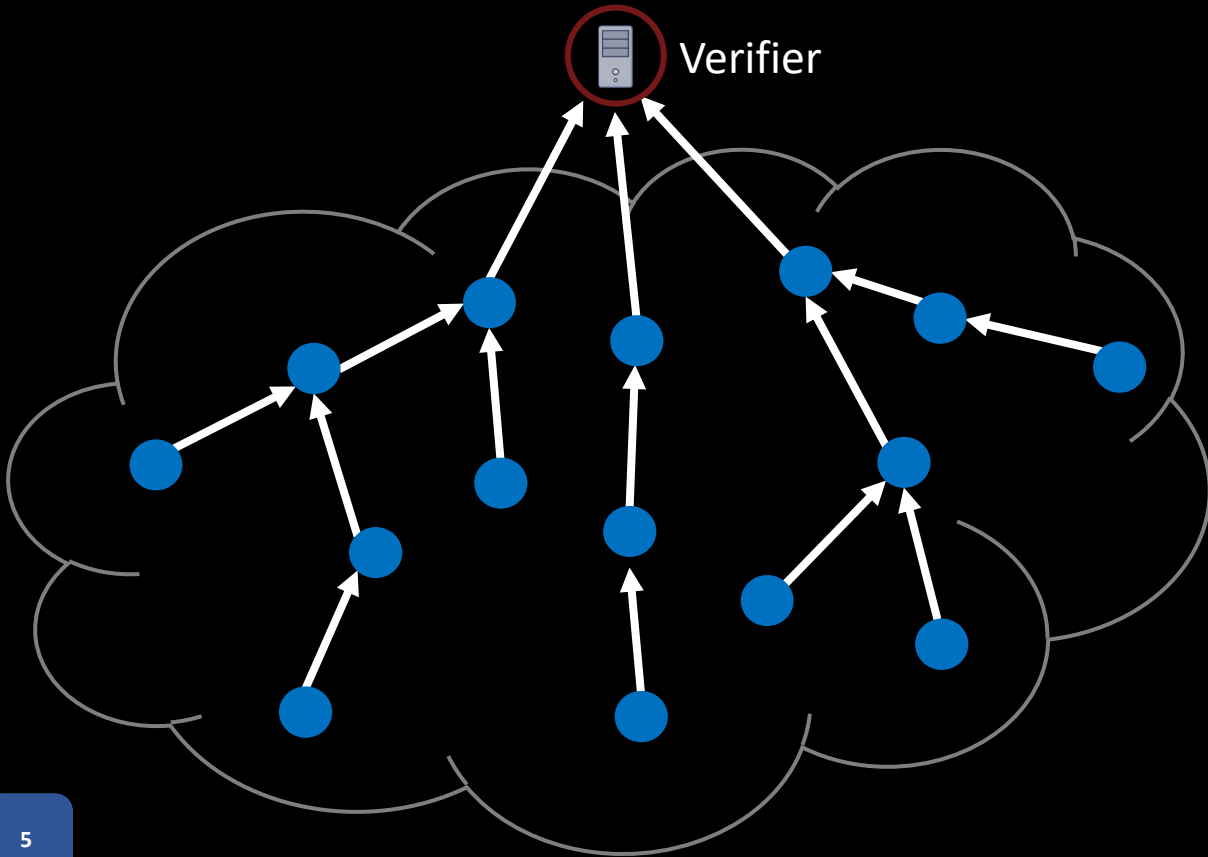
👎 Synchronous Communication

👎 Uninterrupted availability

👎 Device Heterogeneity

Collaborative Remote Attestation Schemes

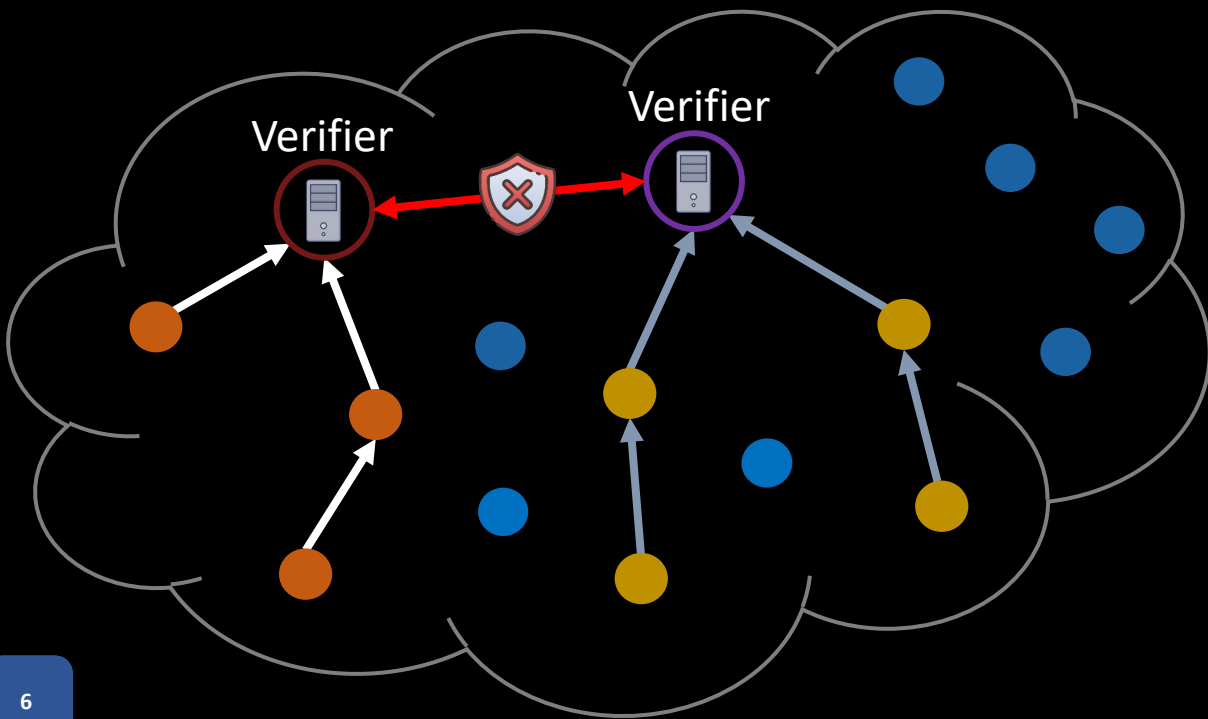
One Verifier – Many Provers



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

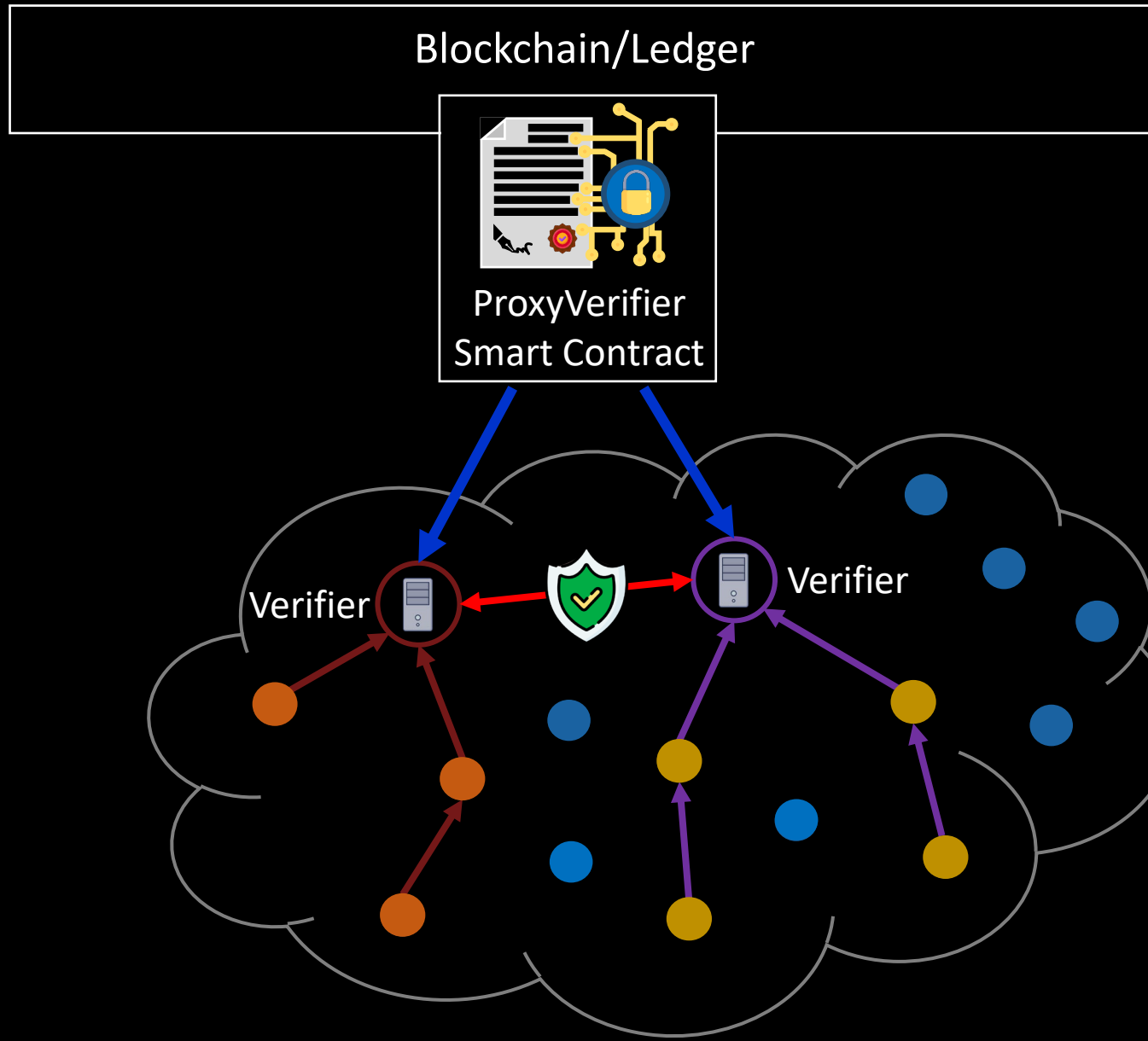
Collaborative Remote Attestation Schemes

Many Verifiers – Many Provers



Properties	Many Verifiers – 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

1

Smart contracts are passive entities → ProxyVerifier cannot initiate attestation

Change to self-attestation triggered by IoT platforms

2

Smart contracts are public → Confidentiality of symmetric keys cannot be protected

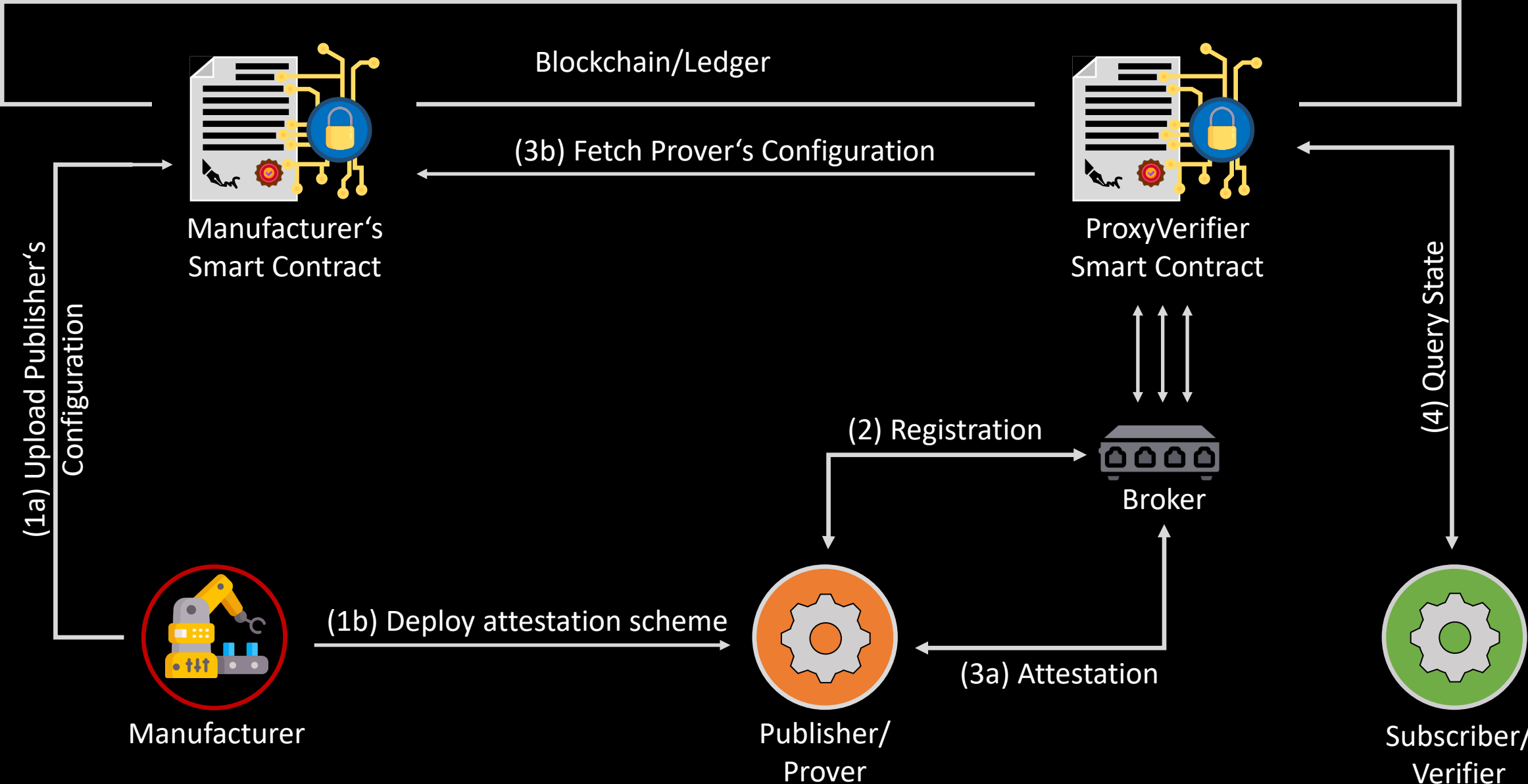
Change attestation evidence to use public key cryptography

3

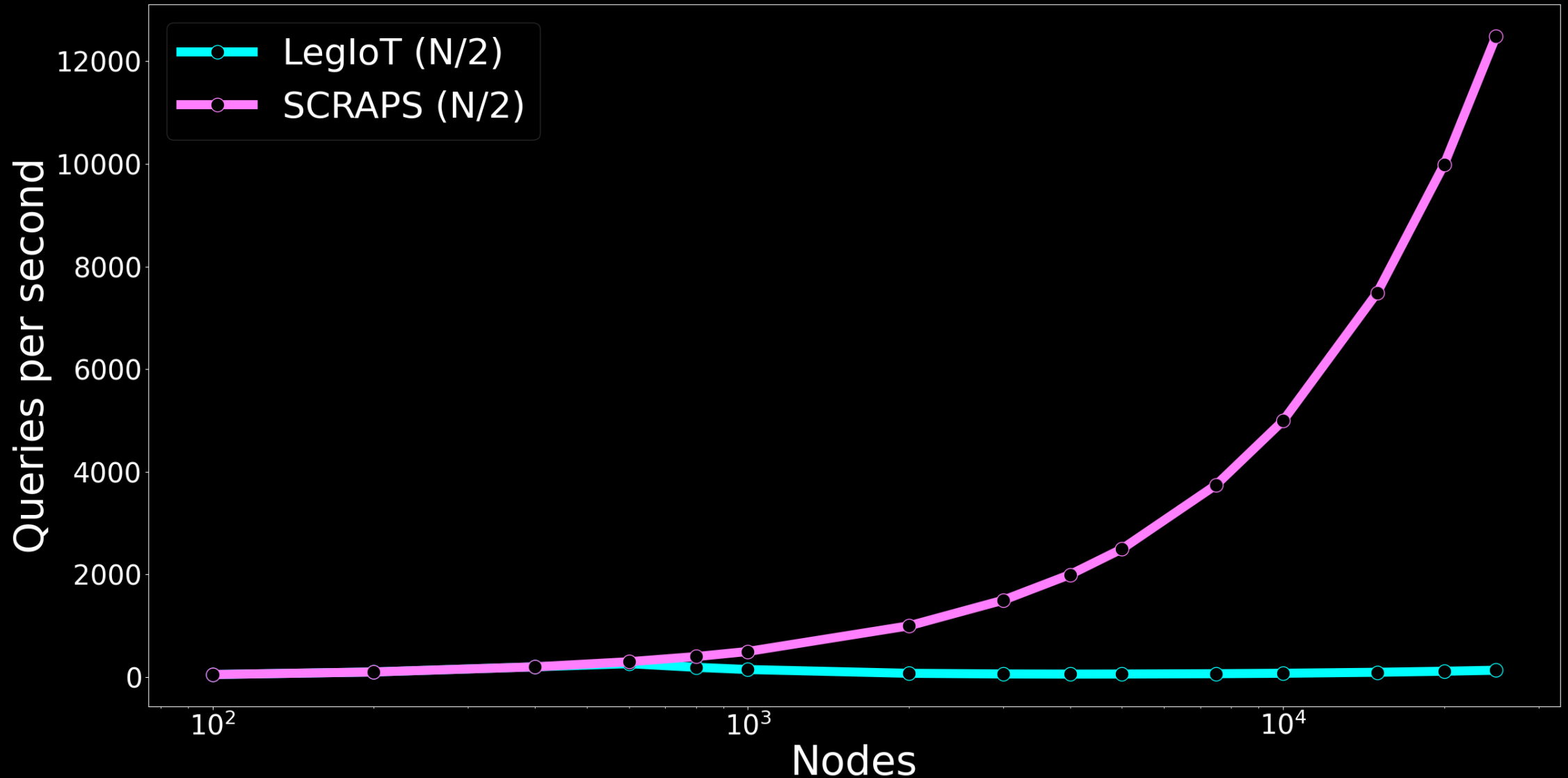
No source of randomness → Random nonce cannot be generated

Use blockchain height to guarantee freshness

SCRAPS Design

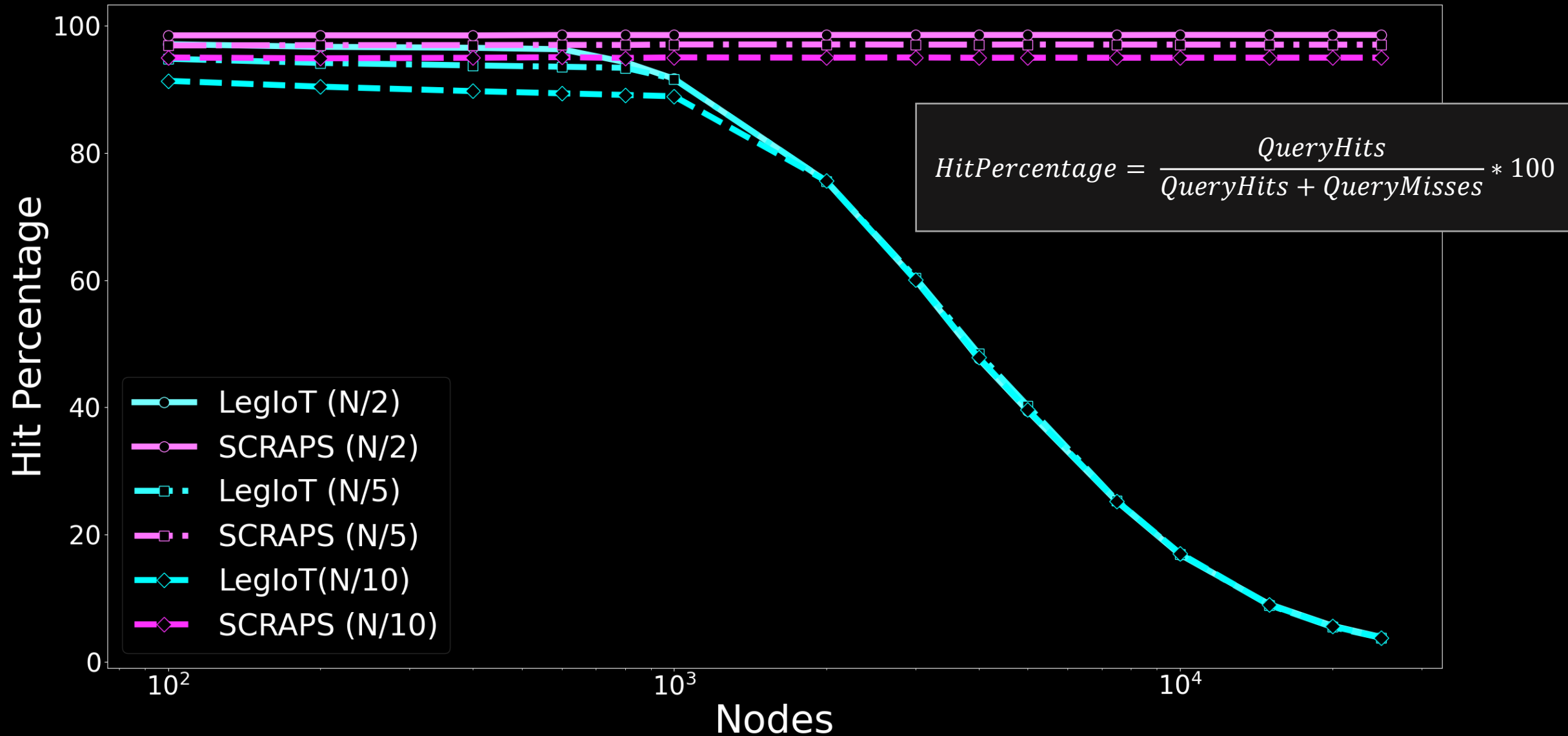


Evaluation: SCRAPS vs. LegIoT[1]



[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