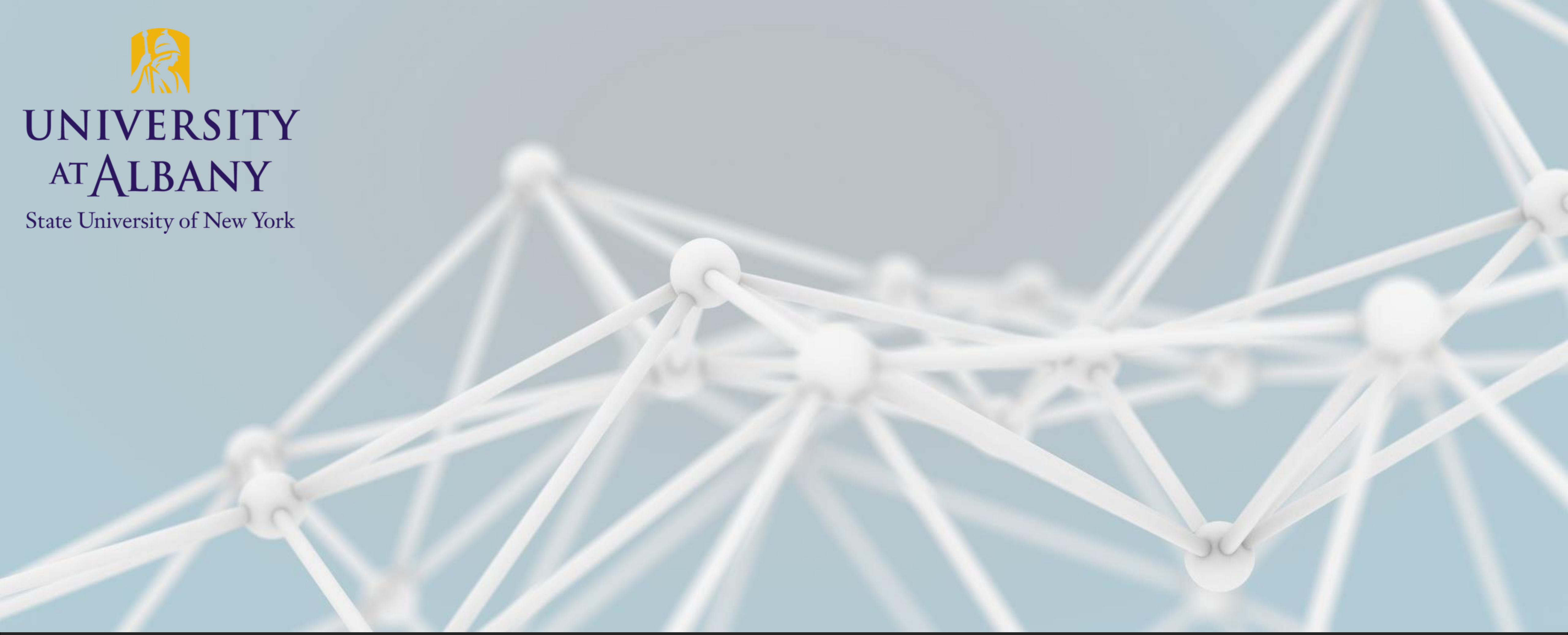


UNIVERSITY AT ALBANY
State University of New York

# SenseChain: Blockchain based Reputation System for Distributed Spectrum Enforcement

**MAQSOOD CAREEM** AND AVEEK DUTTA

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

UNIVERSITY AT ALBANY, SUNY

# Motivation

- Advent of Spectrum Sharing demands Enforcement of Spectrum policies.
- Spectrum enforcement requires fusion of sensing information from Sensors.
- Autonomous Agents - Autonomous Vehicles (UAVs, UGVs) [1], Crowd mobile users [2].

Problem: Lack of Trust → Incorrect or Biased inferences.

**SenseChain:** Distributed consensus in Blockchain to assign Reputation for sensors → Reliable & Accurate Sensing / Enforcement.

[1] **Maqsood, A. Dutta** and W. Wang, "Spectrum Enforcement and Localization Using Autonomous Agents With Cardinality," in *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 702-715, Sept. 2019.

[2] **A. Dutta** and M. Chiang, "“See Something, Say Something” Crowdsourced Enforcement of Spectrum Policies," in *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 67-80, Jan. 2016.

# I. Problem Statement: Reputation

- Malicious Nodes

Anomaly Detection

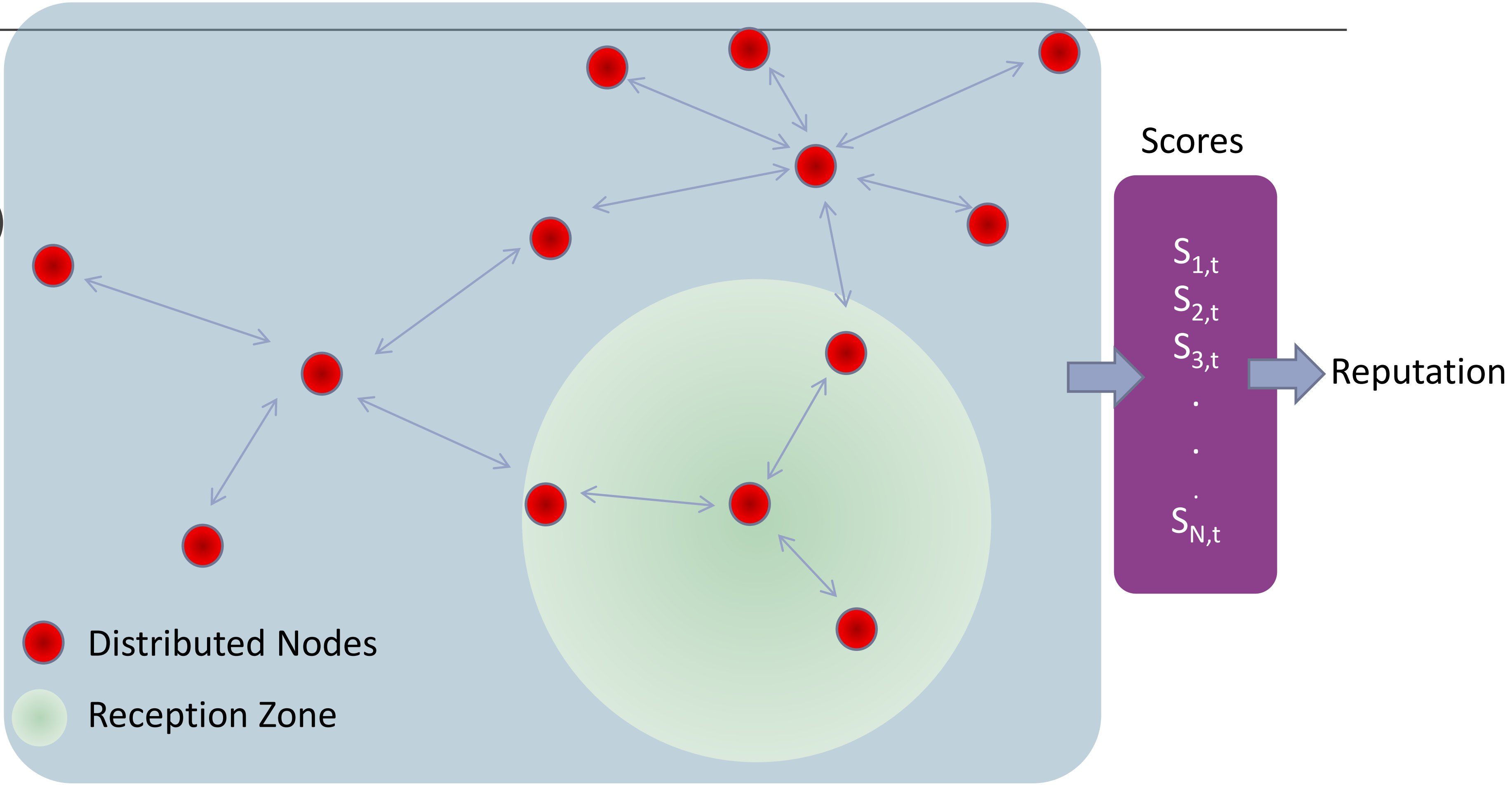
Credibility (Sensors / Validators)

- Dynamic (Mobile)

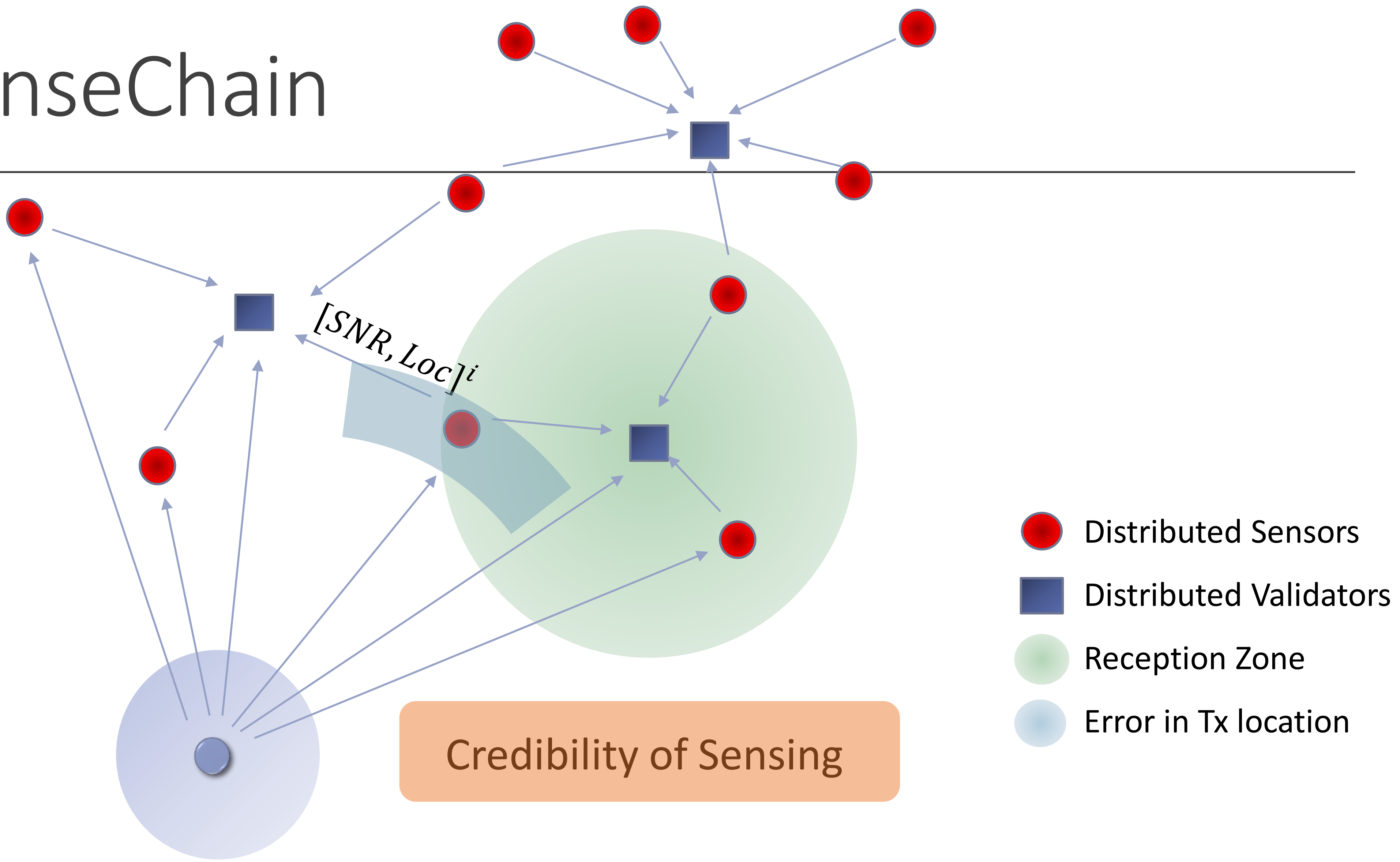
- Chaining / Aggregation

- Fully Distributed

- Consensus

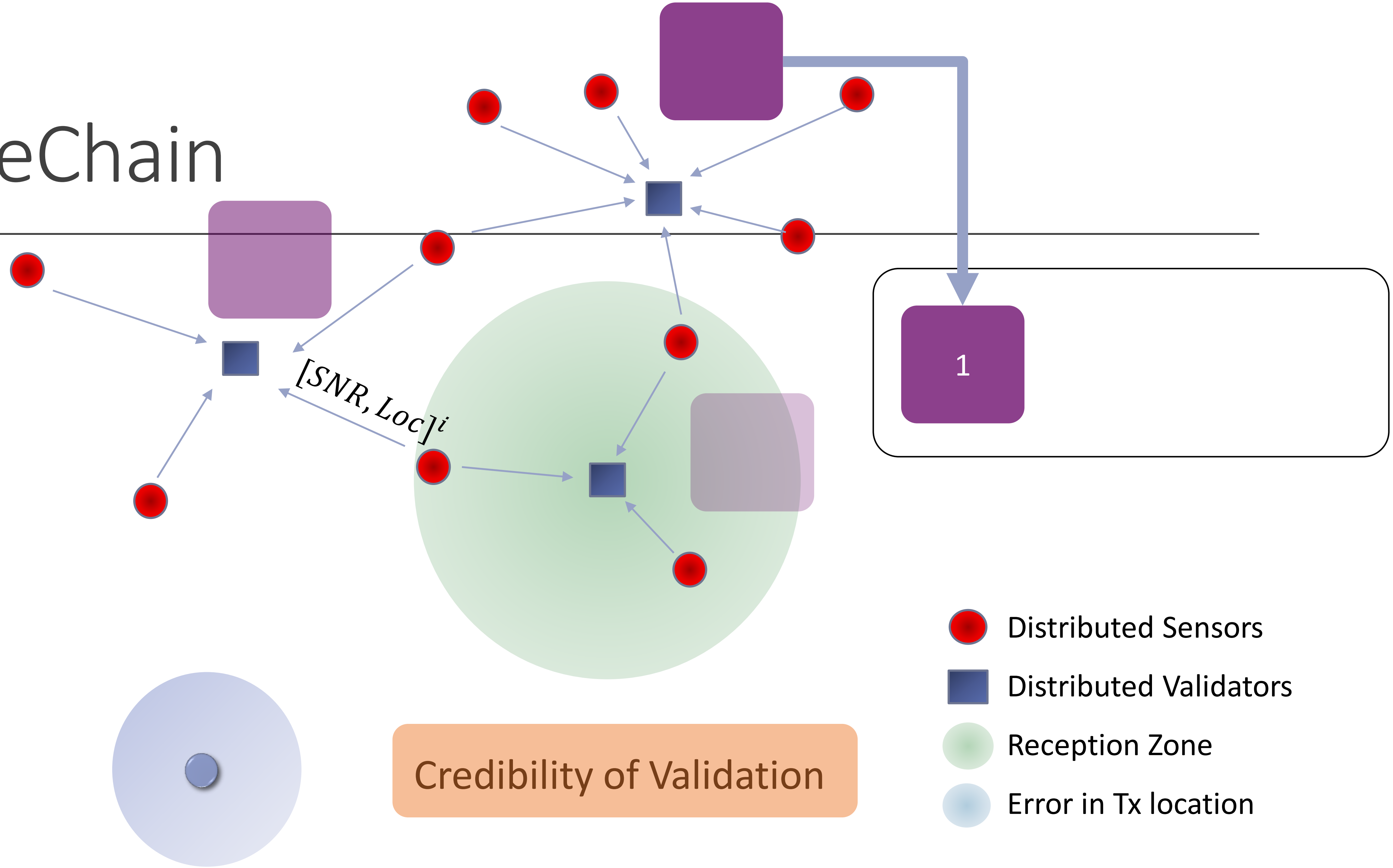


# II. SenseChain



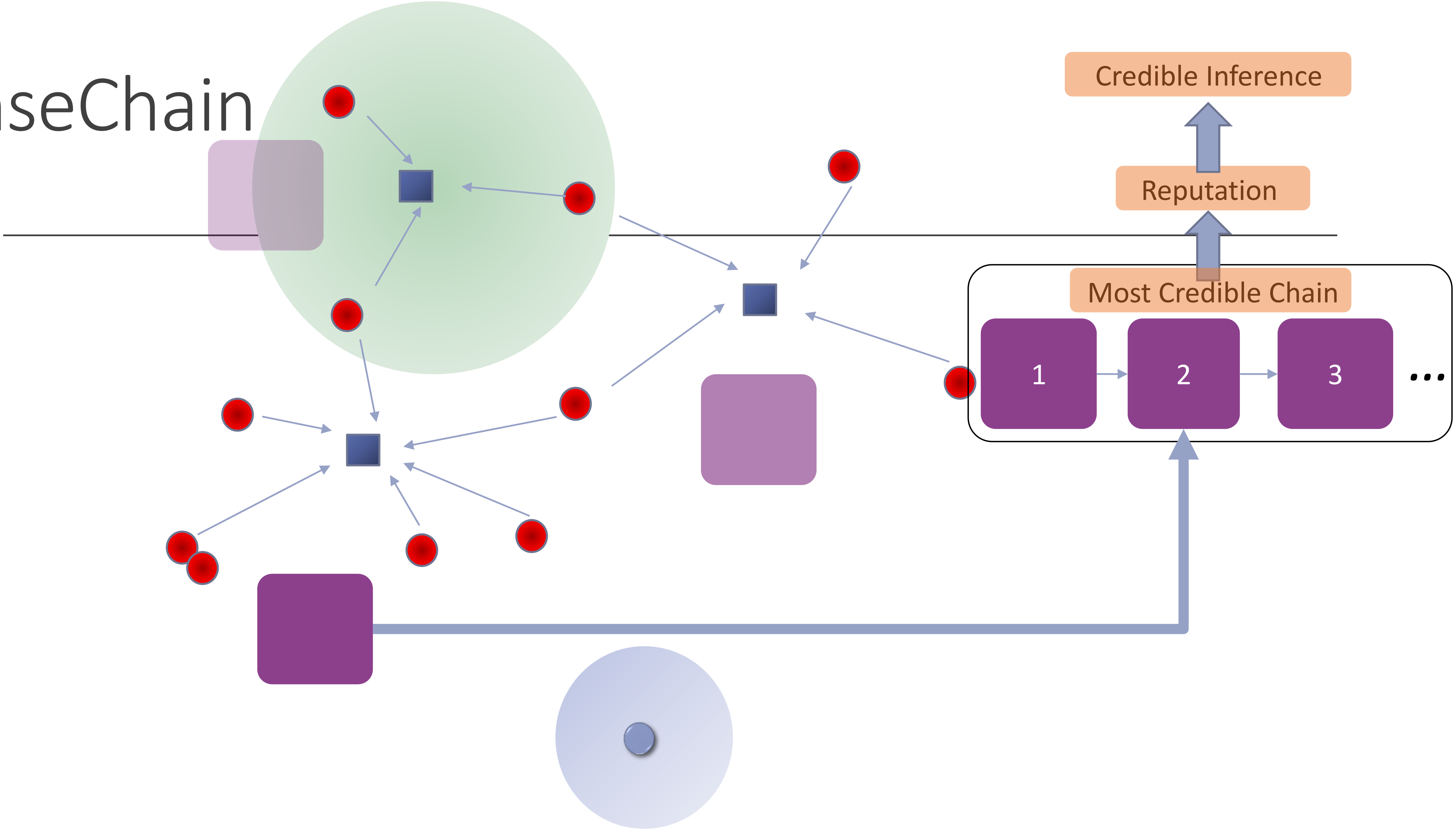

Credibility of Sensing

# SenseChain



[SNR, Loc]^i
1
Credibility of Validation
Distributed Sensors
Distributed Validators
Reception Zone
Error in Tx location

# SenseChain



# III. SenseChain: Anomaly Detection

**Log Distance Channel Model**

$$PL_{s_i} = PL_{v_j} + 10\gamma \log_{10} \frac{d_{s_i}}{d_{v_j}} + \chi \qquad PL = P_t - P_r$$

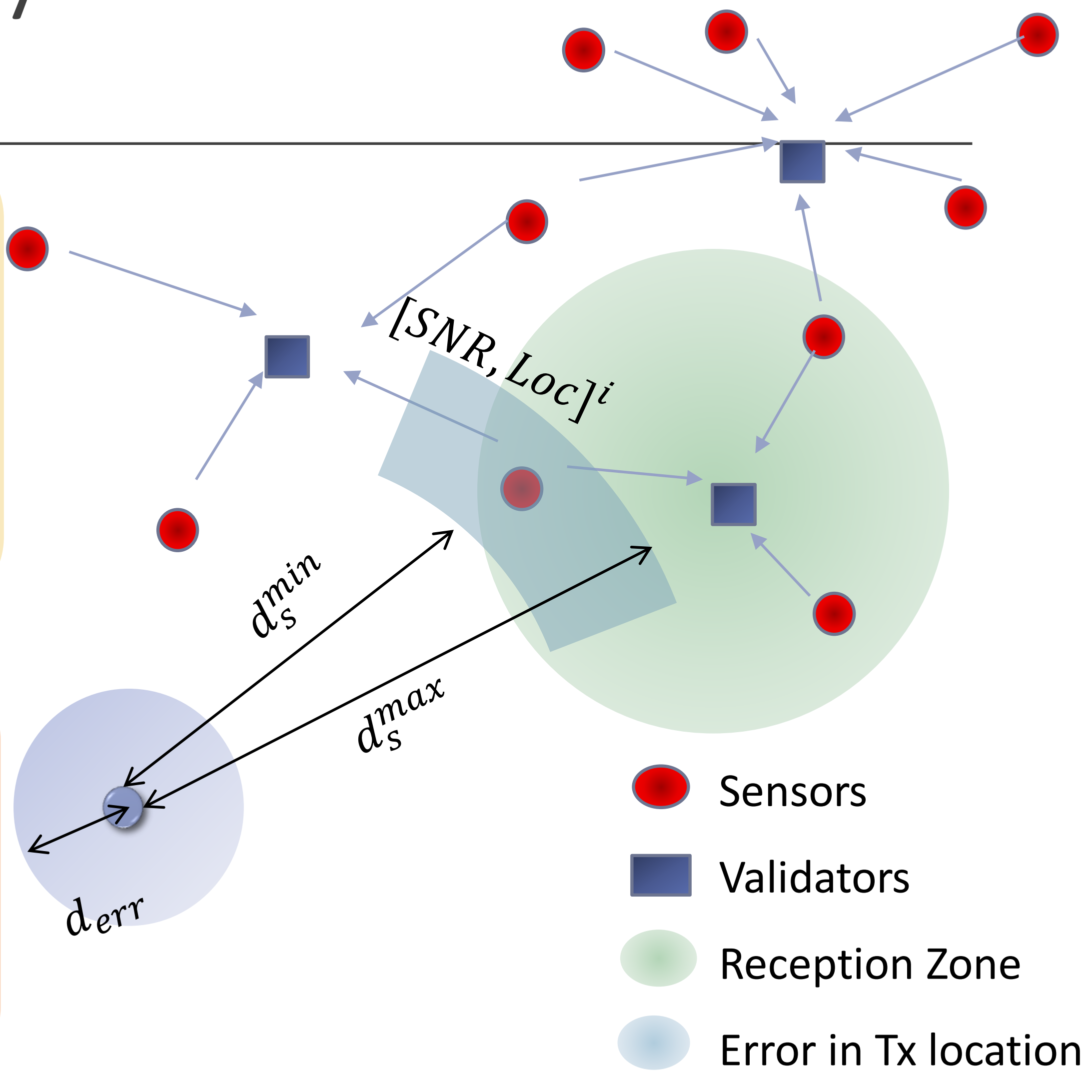
$$P_{r,s_i}(dBm) = SNR^i(dB) + NF(-96dBm)$$

$$-SNR_{s_i} = -SNR_{v_j} + 10\gamma \log_{10} \frac{d_{s_i}}{d_{v_j}} + \chi$$

**Estimated Annular Zone**

$$d_{s_i}^{min} = (d_{v_j} - d_{err}) \times 10^{\left(\frac{SNR^j - SNR^i - X_g}{10\gamma}\right)}$$

$$d_{s_i}^{max} = (d_{v_j} + d_{err}) \times 10^{\left(\frac{SNR^j - SNR^i - X_g}{10\gamma}\right)}$$



# Anomalies and confidence score

## Anomaly Detected if...

Reported location,

- Is Outside Validator Range

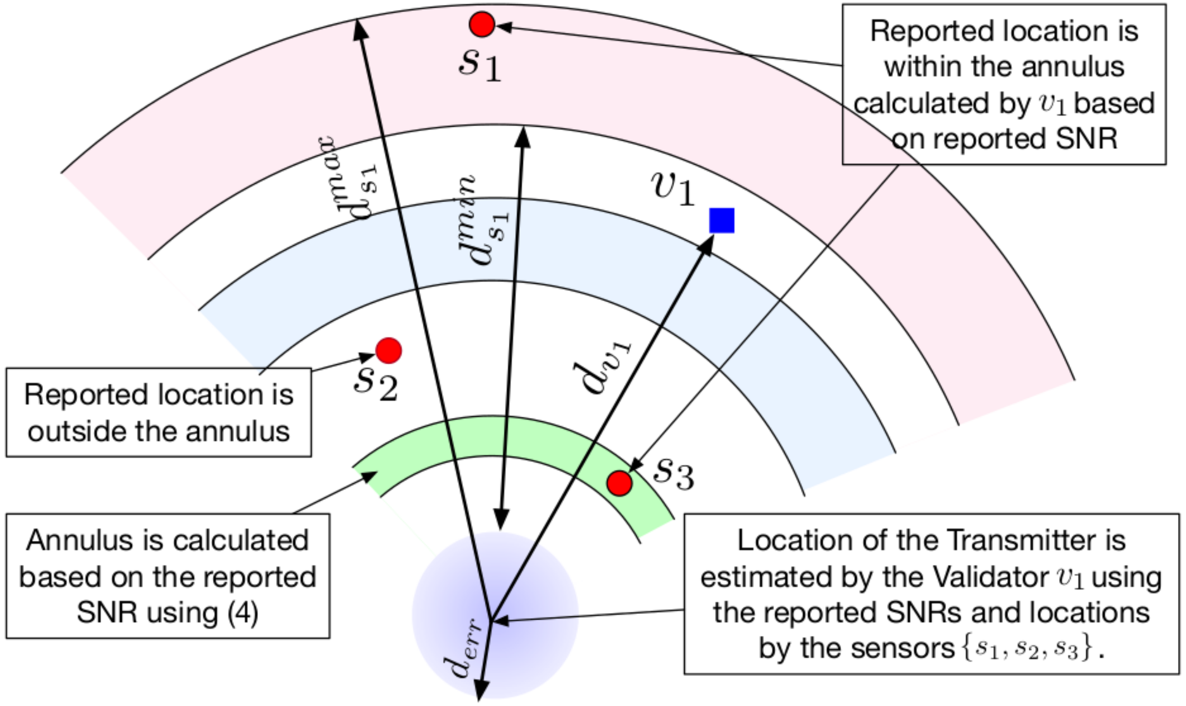
$$(d_{s_i} - d_{v_j}) > R$$

- Is Outside estimated annulus

$$\hat{d_{s_i}} < d_{s_i}^{min} \text{ or } \hat{d_{s_i}} > d_{s_i}^{max}$$

## Confidence Score

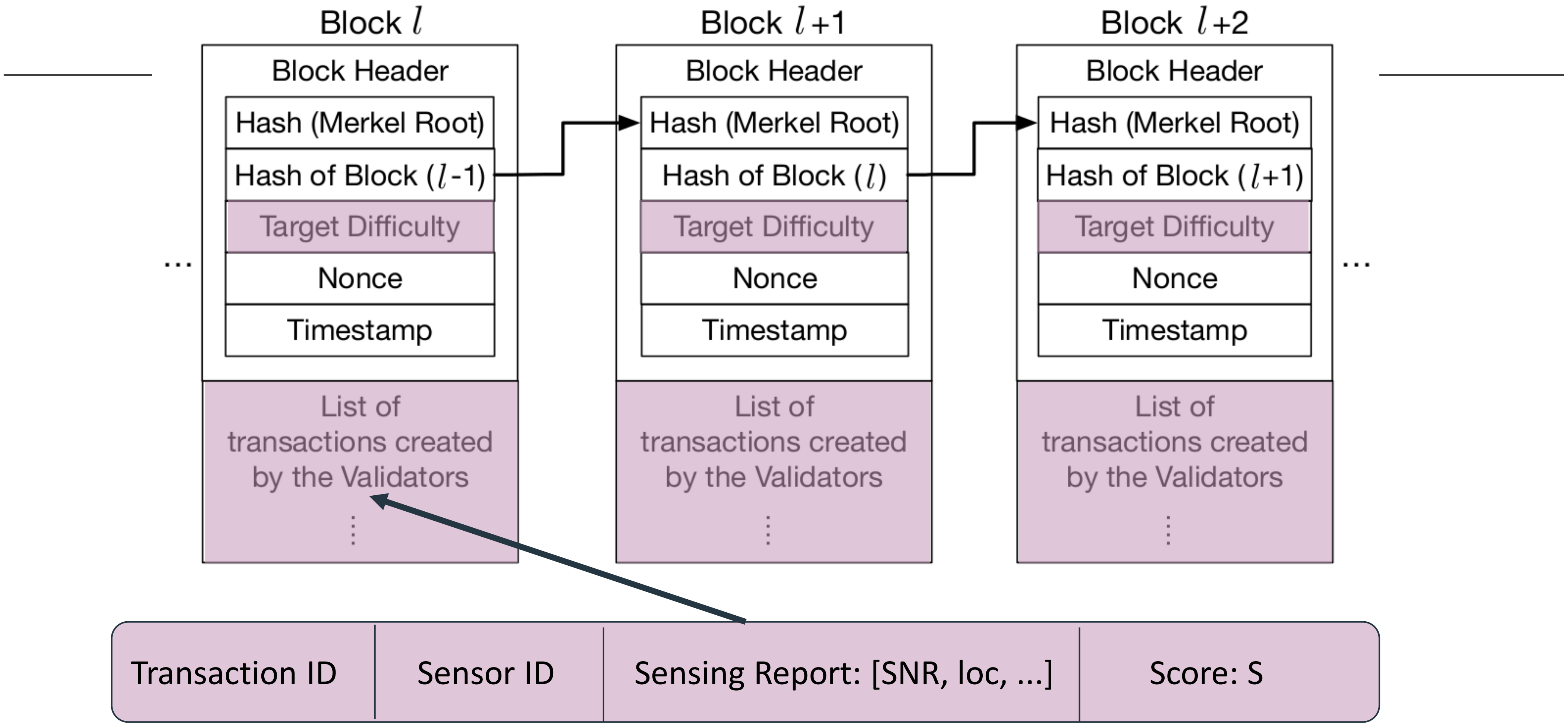
$$S_{s_i} = \begin{cases} 1 - \frac{(d_{s_i}^{max} - d_{s_i}^{min})}{d_0}, \text{if } (d_{s_i}^{min} \leq \hat{d_{s_i}} \leq d_{s_i}^{max}) \quad \& \quad (d_{s_i}^{max} - d_{s_i}^{min} < R) \\ 0 \quad \text{, otherwise} \end{cases}$$




Anomaly detected if reported sensor is outside annulus.

Else a confidence score represents its truthfulness.

# IV. SenseChain: Blockchain-based Reputation



# A. Difficulty of mining

Hardness to find a hash below a target T:

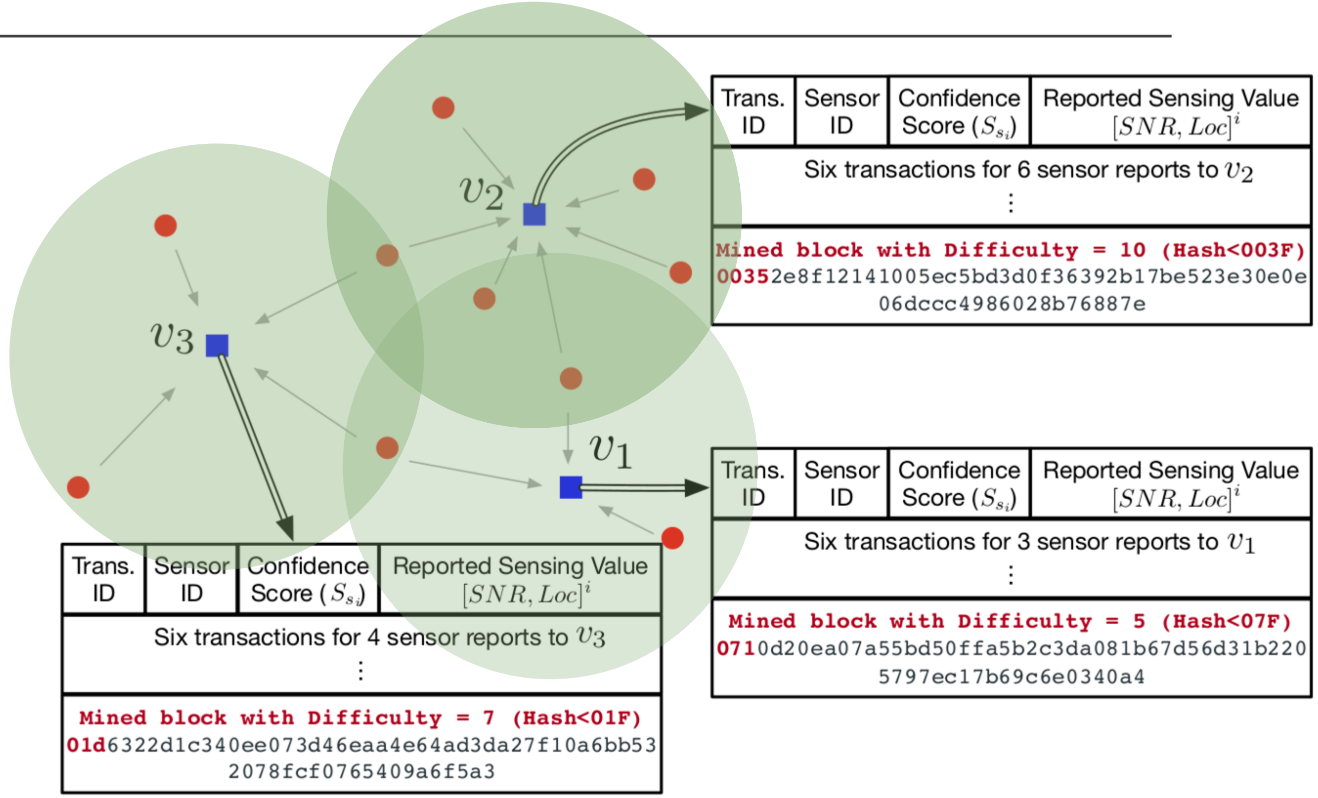
**Difficulty**

$$D_{v_j} = \left\lceil D_{max} \times \frac{n_{v_j}}{N} \right\rceil \qquad \forall v_j \in \mathcal{V}$$

$n_{v_j}$ # Sensors in Reception zone of validator

$N$ Total Number of sensors

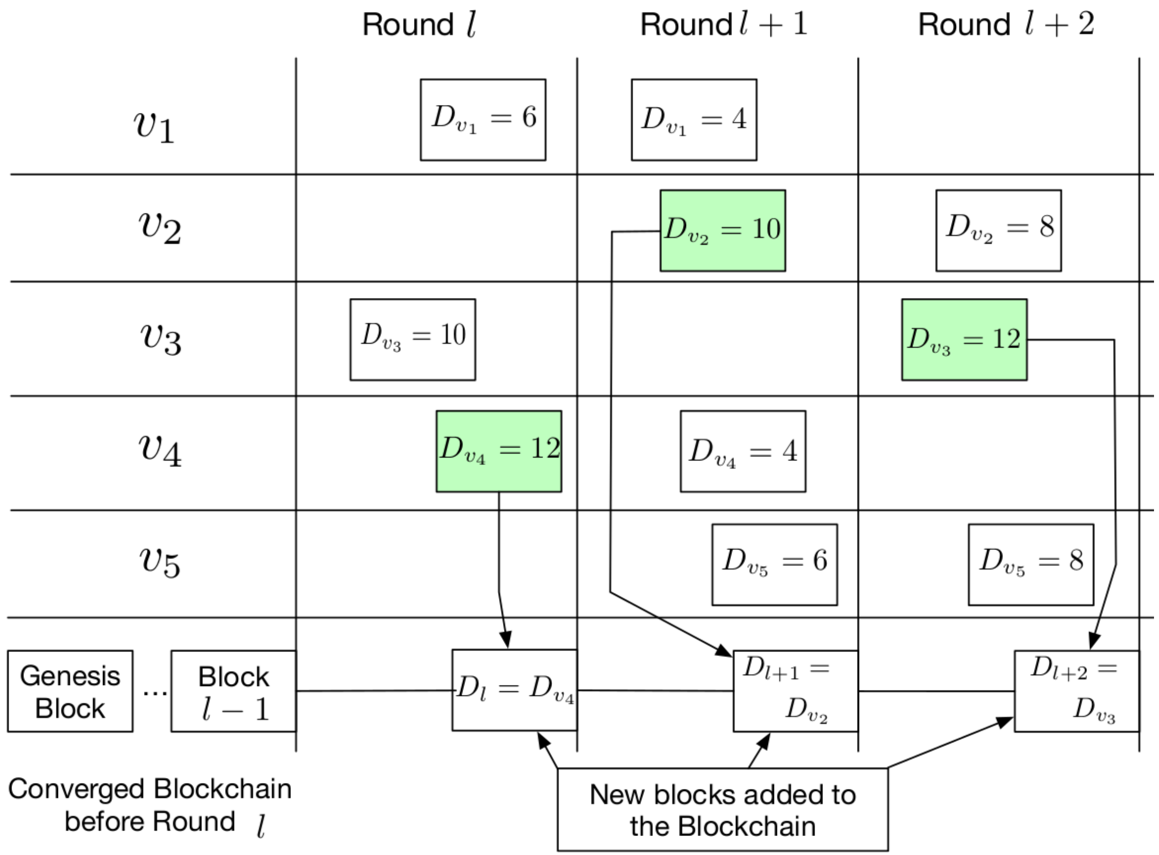
[Immutability] vs [Low Power & Fast Convergence]




Difficulty ∝ Validation Credibility (Power of the Crowd)

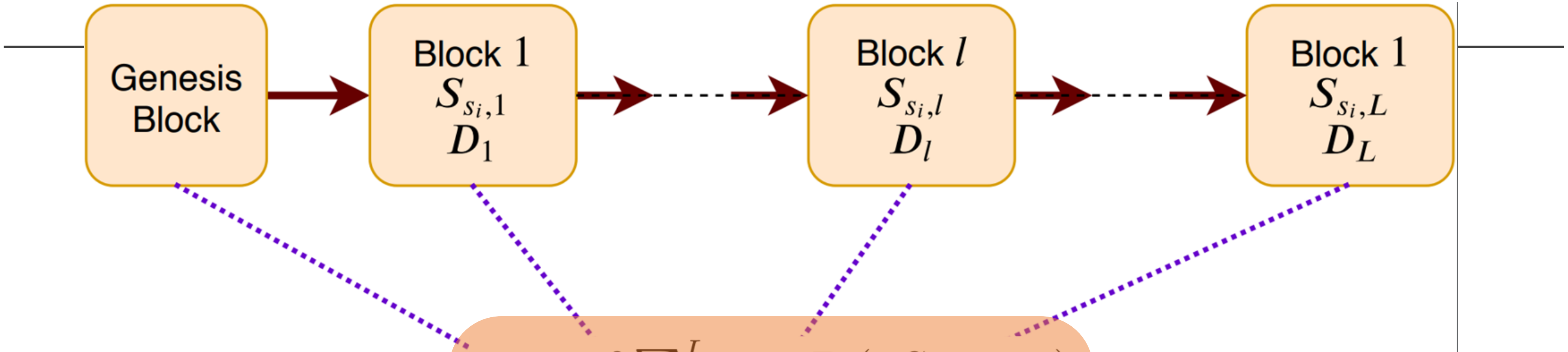
# B. Most-Difficult-Chain consensus

Validators arrive at consensus on most credible chain




Most-Difficult-Chain Consensus: At each round, the most difficult mined block is added to the blockchain.

# V. Historical Reputation & Provenance




$$\eta_{s_i} = \frac{\beta \sum_{l=1}^{L} a_{i,l} D_l (2S_{s_i,l} - 1)}{L.D_{max} \sum_{l=1}^{L} a_{i,l}}$$

$$\mathcal{R}_{s_i} = \frac{1}{1 + e^{-\eta_{s_i}}}$$

a: Availability

S: Confidence (Credibility of Sensing)

D: Difficulty (Credibility of Validation)

**Most Credible Reputation Assignment → Most Credible Inference**

# VI. Evaluation & Results

## A. Simulation Framework

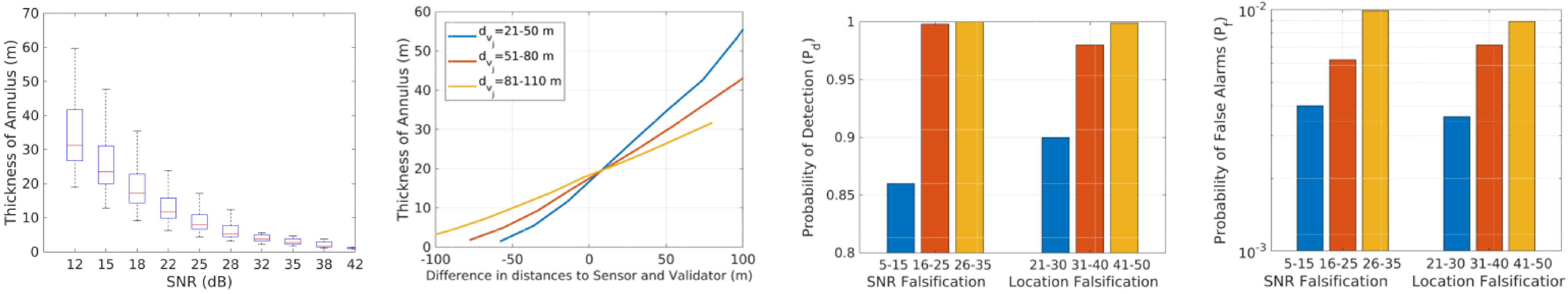
1) Sensing Environment

2) Blockchain Simulator

TABLE I: Simulation Parameters

| Parameters | Value/Model |
|---|---|
| Area | 300m × 300m |
| Node Distribution | Uniform Distribution |
| Mobility Model | Random Waypoint |
| Propagation Model | Log-distance propagation model [14] |
| Path-loss exponent ($\gamma$) | 3 (urban area) |
| Carrier Frequency (f) | 600 MHz |
| Number of Validators | 5 |
| Number of Sensors | 20 |
| Antenna Type | Omnidirectional |
| Broadcast Range | 100 |
| Maximum Difficulty ($D_{max}$) | 16 |
| Block-wait Time ($\tau_{\mathcal{B}}$) | 7 s |
| Target location error ($d_{err}$) | Uniformly distributed in [20,30] m |

# B. Performance of anomaly detection




(a) Variation of annulus width with reported SNR

(b) Annulus width with Sensor and Validator distances

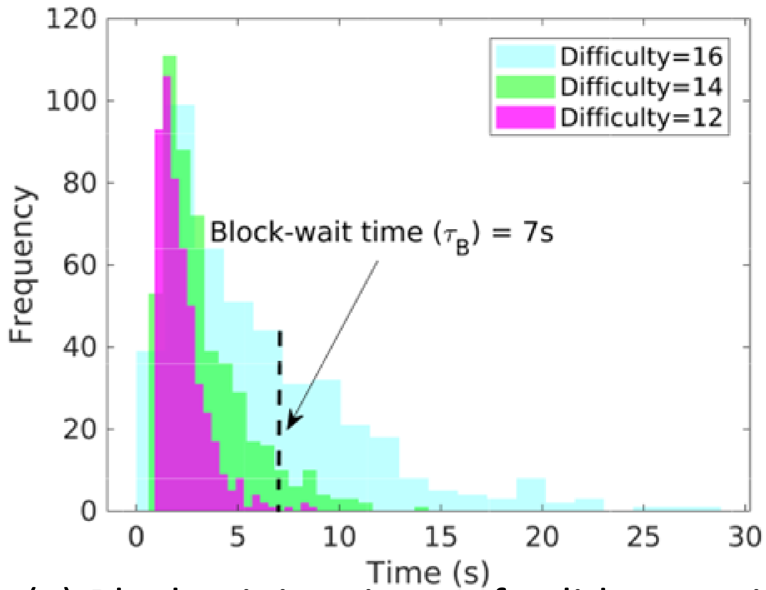
(c) Pd with falsification in SNR (dB) and Location (m)

(d) Pf with falsification in SNR (dB) and Location (m)

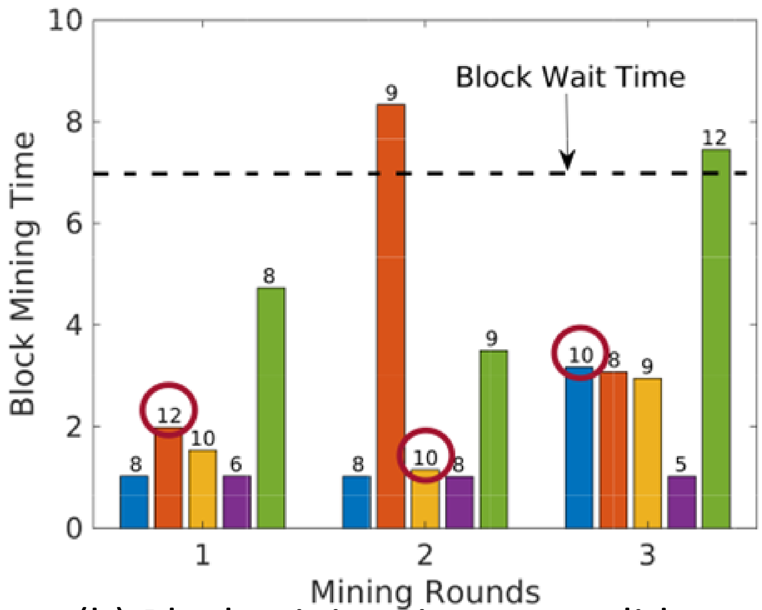
**Truthfulness of Sensors can be Accurately inferred in Distributed Manner**

# C. Performance of Blockchain based Reputation

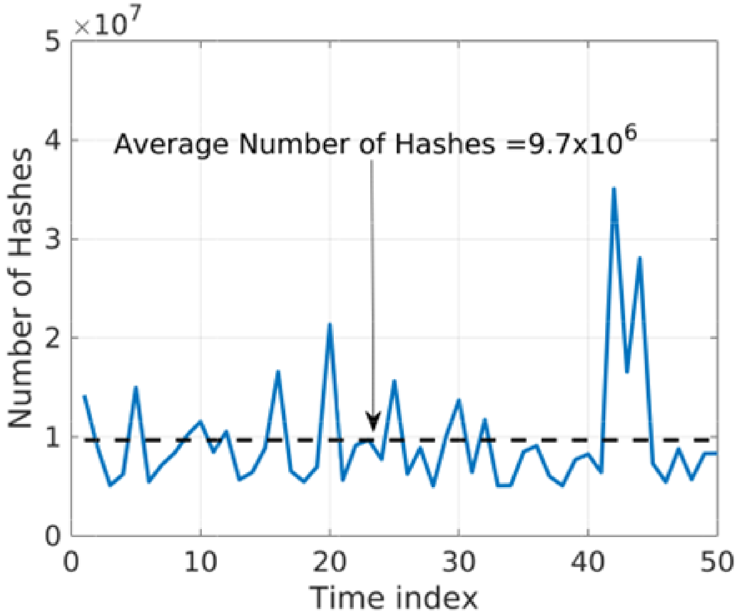
**Blockchain performance:**




(a) Block mining times of validators with varying difficulty targets

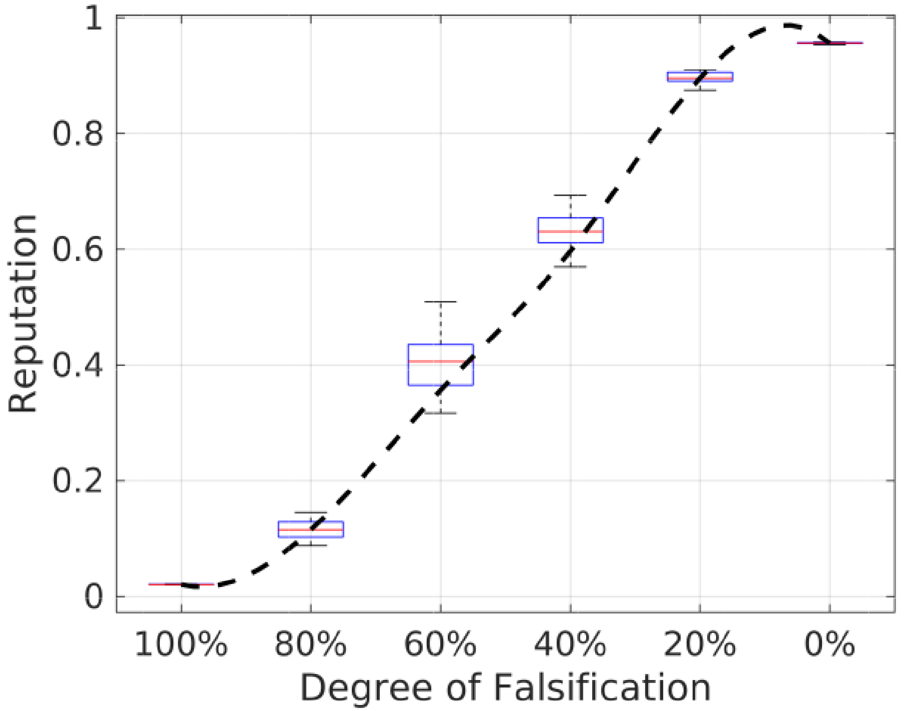



(b) Block mining time per validator and winning block in each round

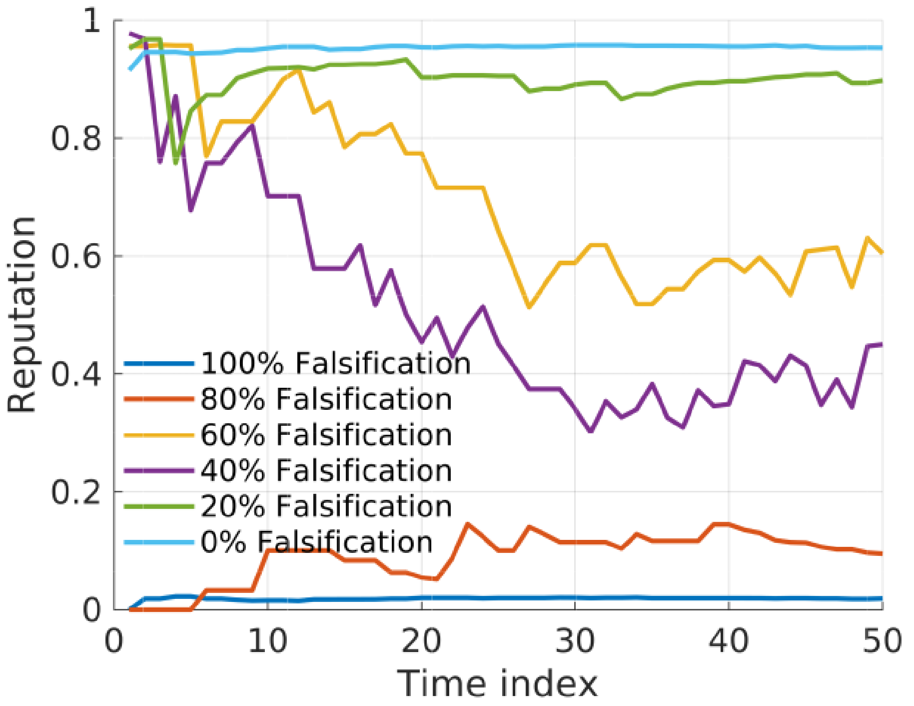



(c) The number of hashes generated by the winning validator

# Reputation Assignment:




(a) Reputation with degree of falsification




(b) Reputation of falsifying Sensors over time

**Reputation of Sensors represents the Degree of Maliciousness of Sensors**

# Conclusion

1. Distributed, peer-based **Anomaly Detection** algorithm
2. **Novel Blockchain Design:** Records Confidence scores. Difficulty of mining $\propto$ credibility of validation.
3. **Network protocol:** Achieve consensus using Most-Difficult-Chain rule.
4. **Nonlinear Reputation** metric: Aggregation of historical confidences and Difficulty.
5. Evaluation using combined Sensing and Blockchain simulator

SenseChain: Fast & Tamper-proof distributed consensus on the reputation of sensors, among trustless entities.

# Choice of Maximum Difficulty: $D_{max}$

$\mathbb{E}[t]$ Average time to mine a block

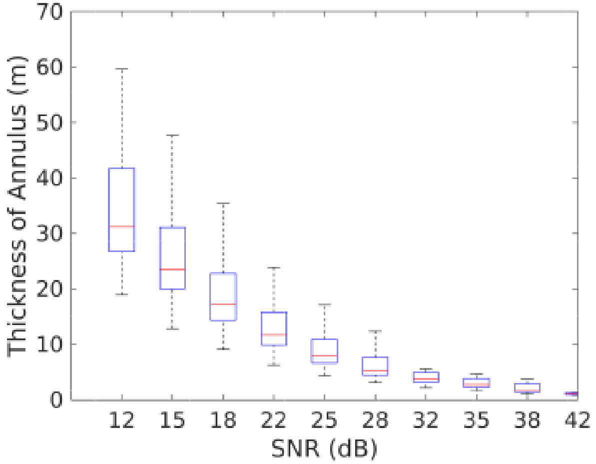
$R$ : Average Hashing or Mining Power of validators

$$\mathbb{E}[t] \propto \frac{D_{max}}{R}$$

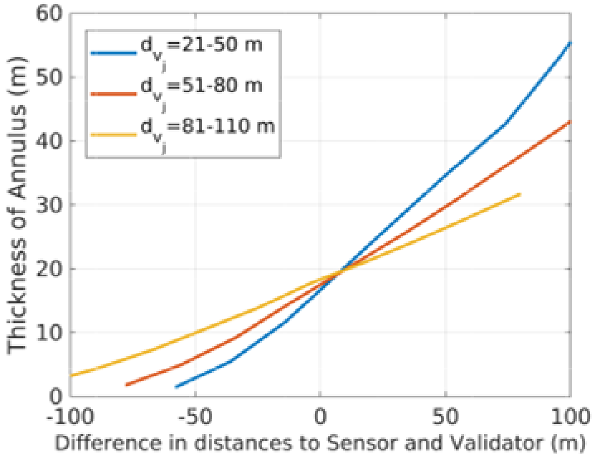
**Tradeoff**

[Immutability & Credibility] vs [Computational Power & Convergence speed]

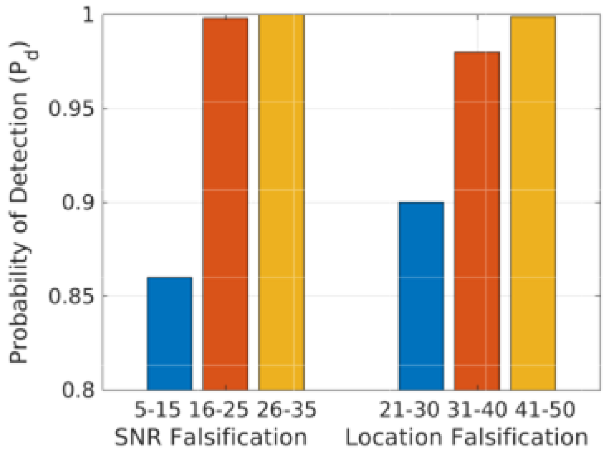
# B. Performance of anomaly detection



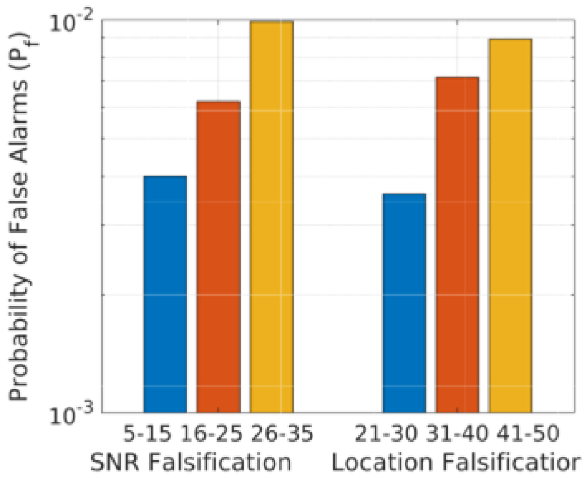

(a) Variation of annulus width with reported SNR




(b) Annulus width with Sensor and Validator distances




(c) Pd with falsification in SNR (dB) and Location (m)




(d) Pf with falsification in SNR (dB) and Location (m)

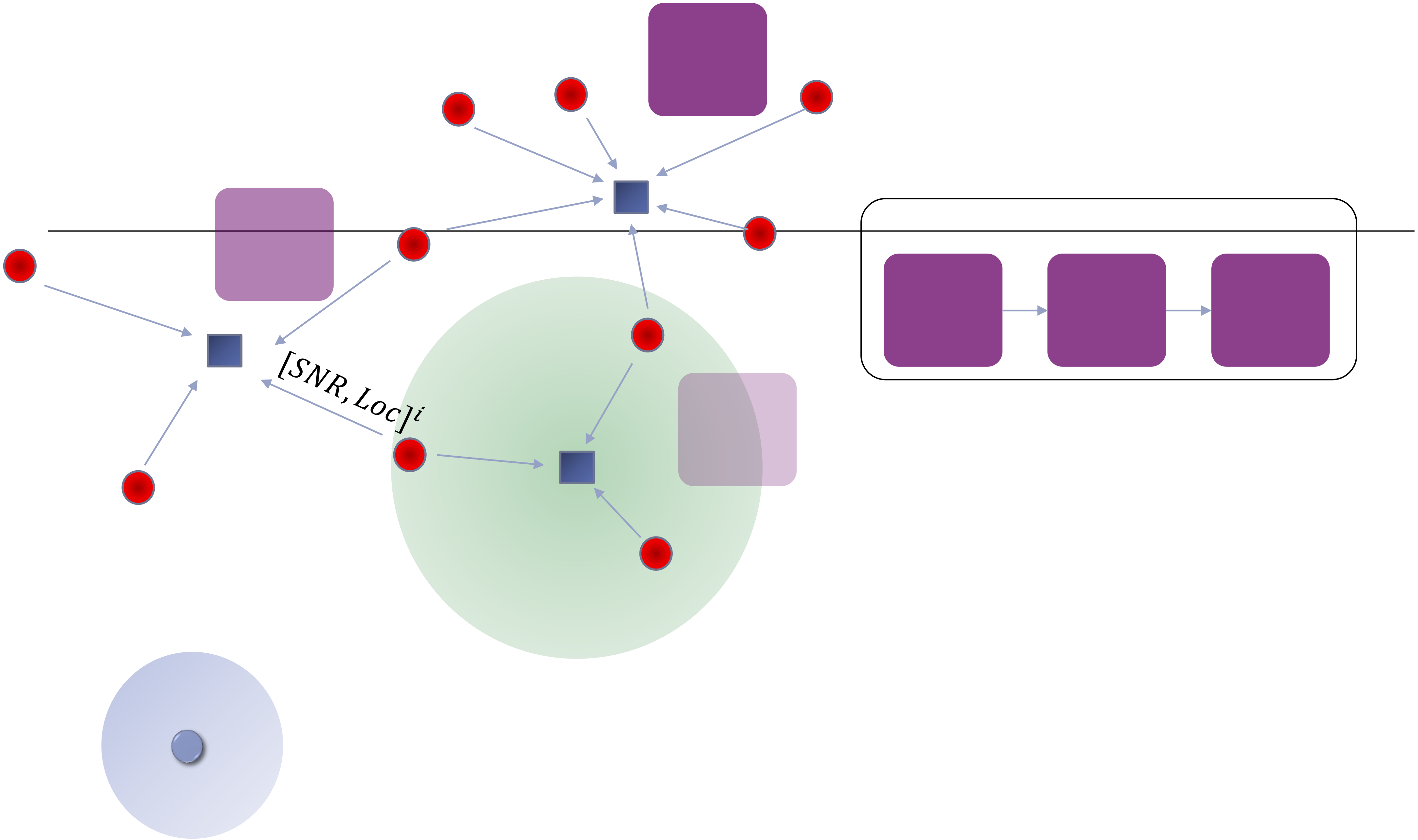
**Truthfulness of Sensors can be Accurately inferred in Distributed Manner**

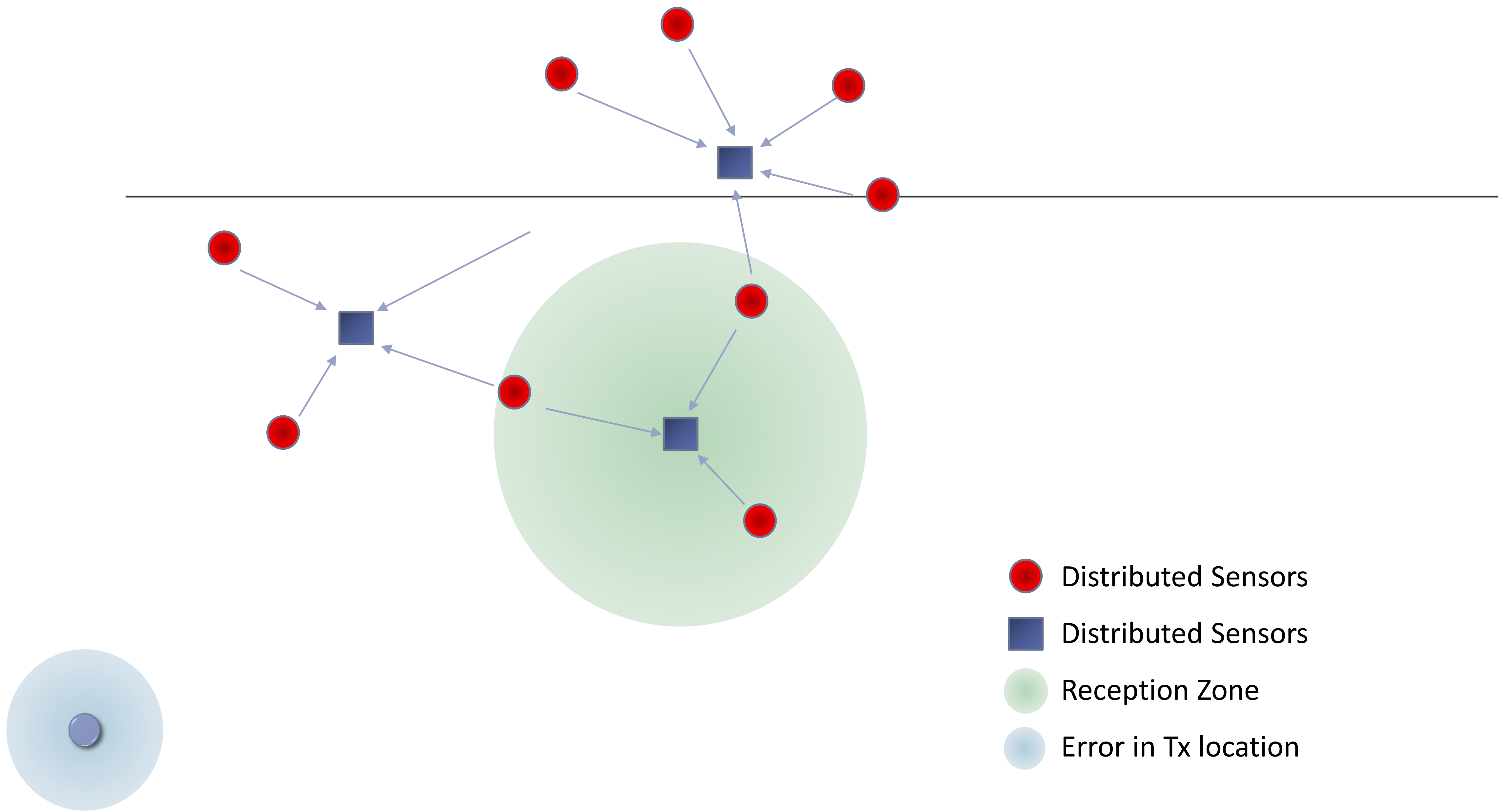
Anomaly Detection → Heterogeneous Blockchain → Most-Credible Chain Consensus → Reputation Metric → SenseChain Evaluation

# VII. Related Work

Anomalous behaviour Detection

Blockchains for sensor networks


$[SNR, Loc]^i$


Distributed Sensors
Distributed Sensors
Reception Zone
Error in Tx location

# Problem Statement