LighTx: a lightweight transactions transfer system

Imane El Abid

imane.elabid@um6p.ma

Mohammed VI Polytechnic University

Yahya Benkaouz

yahya.benkaouz@um5.ac.ma

Mohammed V University in Rabat

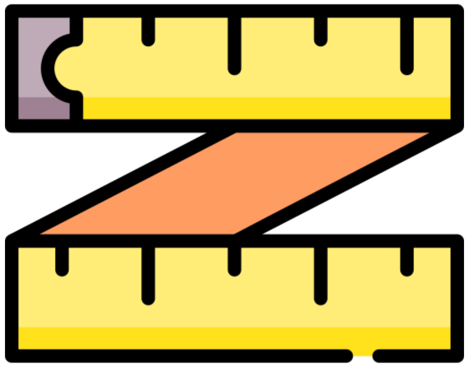
IEEE ICBC, May 2021

Outline

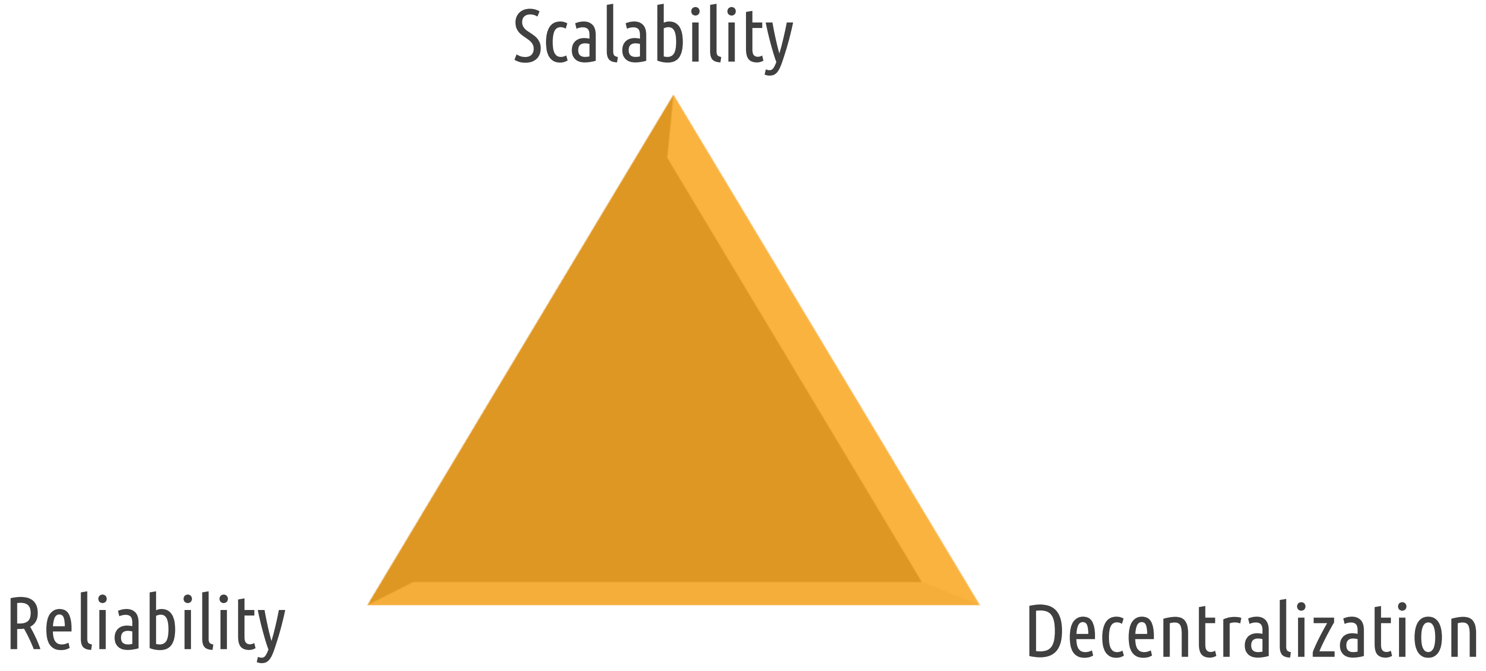
- Objectives & Motivation
- Approach
- Key Results
- Conclusion & Perspectives
- References

Objectives & Motivation

Objectives & Motivation



Objectives & Motivation



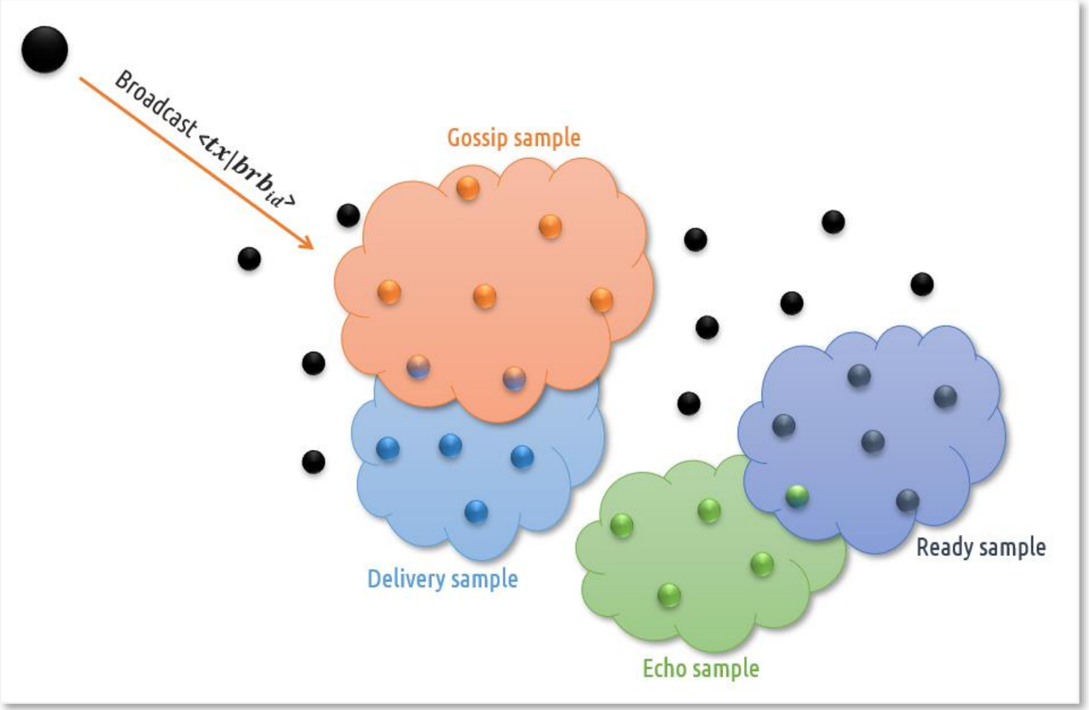
Approach

Approach

1 Byzantine Reliable Broadcast extension [1]

- Stochastic communication samples instead of quorums
- Concurrent transaction transfers via broadcast channels identifications

Broadcast channel ID	Broadcast instance
ID: A	brb_A



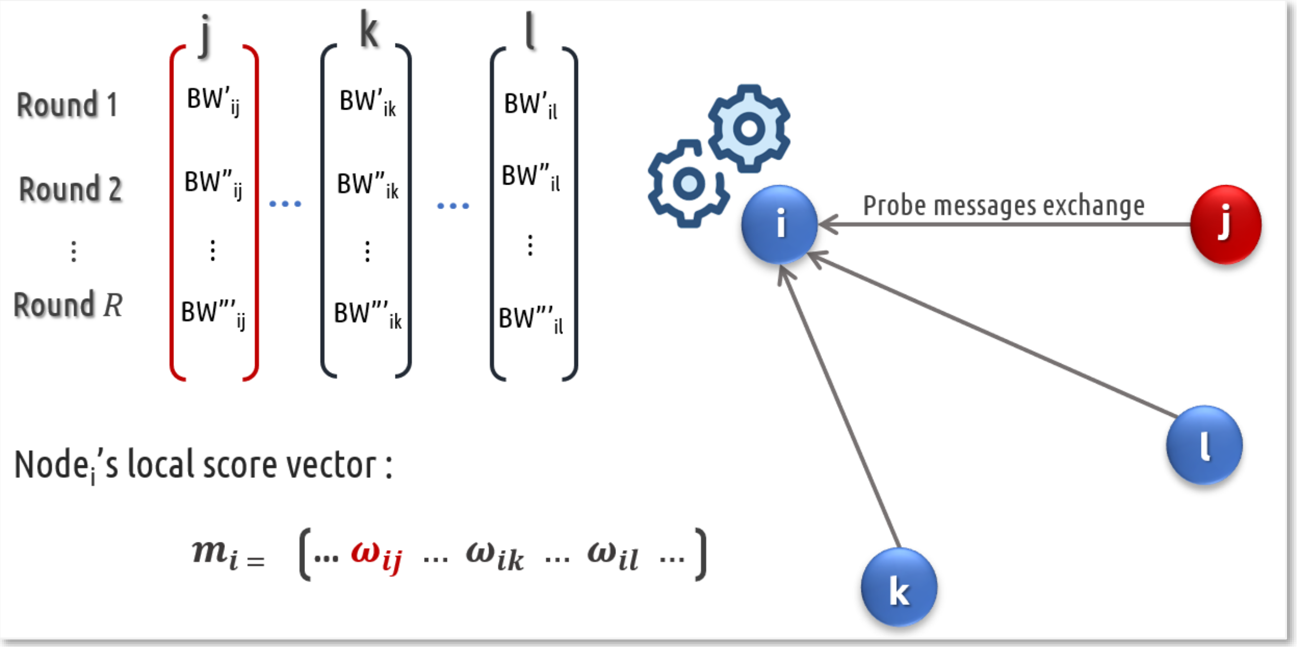
Byzantine reliable broadcast samples

Byzantine Agreement at reduced communication

Approach

2 Proof-of-Bandwidth-based Reputation system

- Measure available bandwidth of peers over rounds
- Detect fluctuations of bandwidth
- Assign local scores accordingly
- Aggregates the local scores over the network into global ones via a reputation system [2]



$$\begin{array}{cccccc} & j & & k & & l \\ \text{Round 1} & BW'_{ij} & & BW'_{ik} & & BW'_{il} \\ \text{Round 2} & BW''_{ij} & \cdots & BW''_{ik} & \cdots & BW''_{il} \\ \vdots & \vdots & & \vdots & & \vdots \\ \text{Round } R & BW'''_{ij} & & BW'''_{ik} & & BW'''_{il} \end{array}$$

Node$_i$'s local score vector :

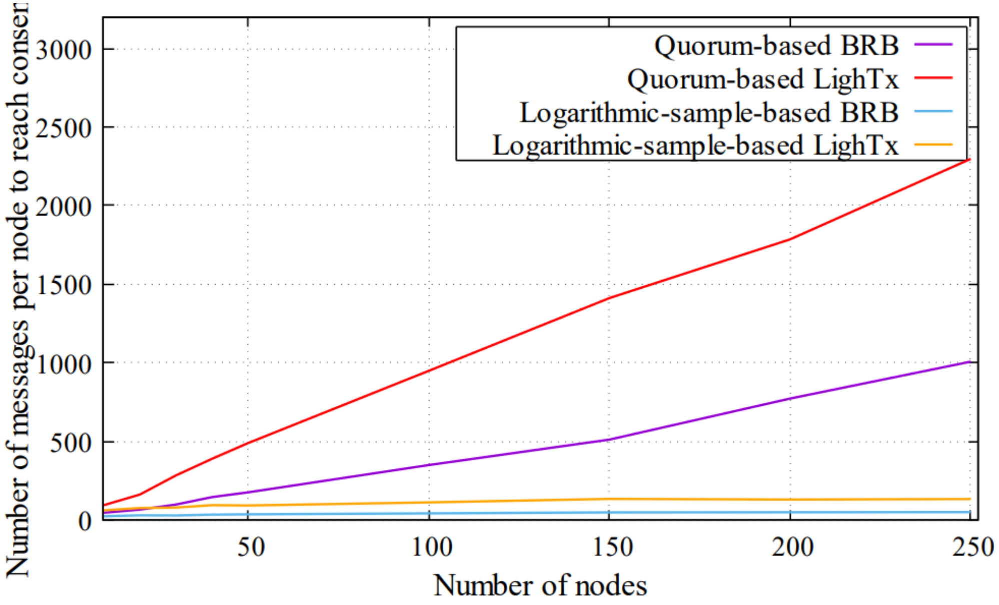
$$m_i = [\ldots\ \omega_{ij}\ \ldots\ \omega_{ik}\ \ldots\ \omega_{il}\ \ldots]$$

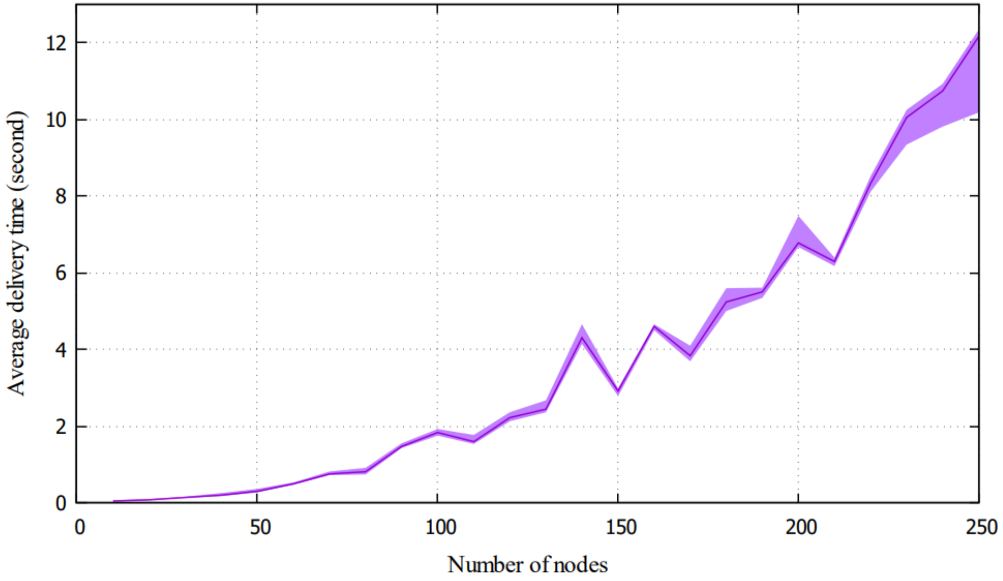
Proof-of-Bandwidth scheme

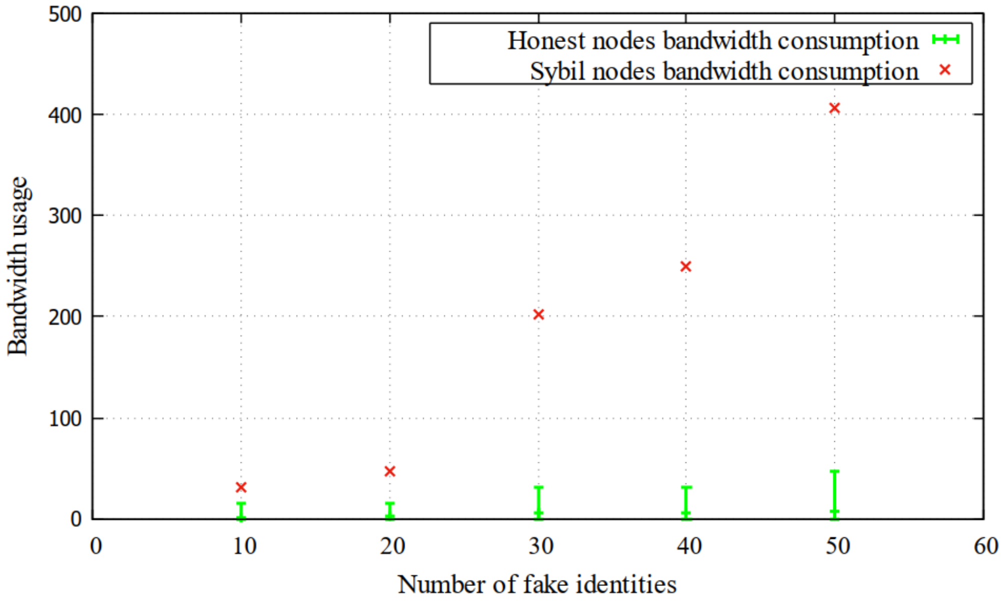
→ Sybil attack defense

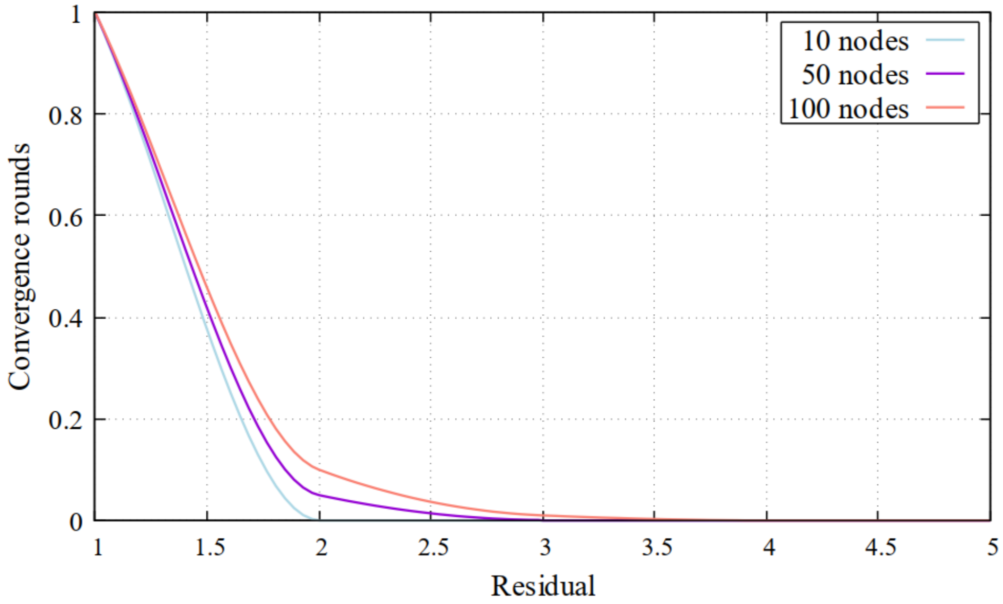
Key Results

Preliminary Results









Conclusion & Perspectives

Conclusion & Perspectives

Our proposition

- Solve double spending at a low cost
- Provide a defense to Sybil attack
- Suitable for public environments

Perspectives

- Formal analysis
- Supplementary features

References

- [1]. Guerraoui, R., Kuznetsov, P., Monti, M., Pavlovic, M., & Seredinschi, D.-A. (2019). Scalable Byzantine Reliable Broadcast (Extended Version). https://doi.org/10.4230/LIPIcs.DISC.2019.22

- [2]. Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003, May). The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the 12th international conference on World Wide Web (pp. 640-651).