LighTx: A Lightweight Proof-of-Bandwidth Transactions Transfer System

Imane El Abid

imane.elabid@um6p.ma

Mohammed VI Polytechnic University, Morocco

Yahya Benkaouz

yahya.benkaouz@um5.ac.ma

LCS, Faculty of Sciences
Mohammed V University, Morocco

Ahmed Khoumsi

Ahmed.Khoumsi@usherbrooke.ca

University of Sherbrooke, Canada

NETYS, May 2021

Outline

Objectives & Motivation

Objectives & Motivation

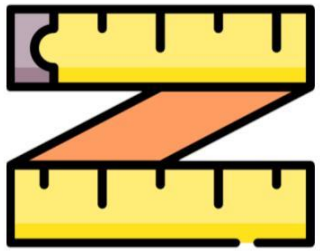
Objectives & Motivation

High energy consumption

Consensus

Lack of fairness

Low scalability



Centralization

Objectives & Motivation

Scalability

Security

Decentralization

Consensus families

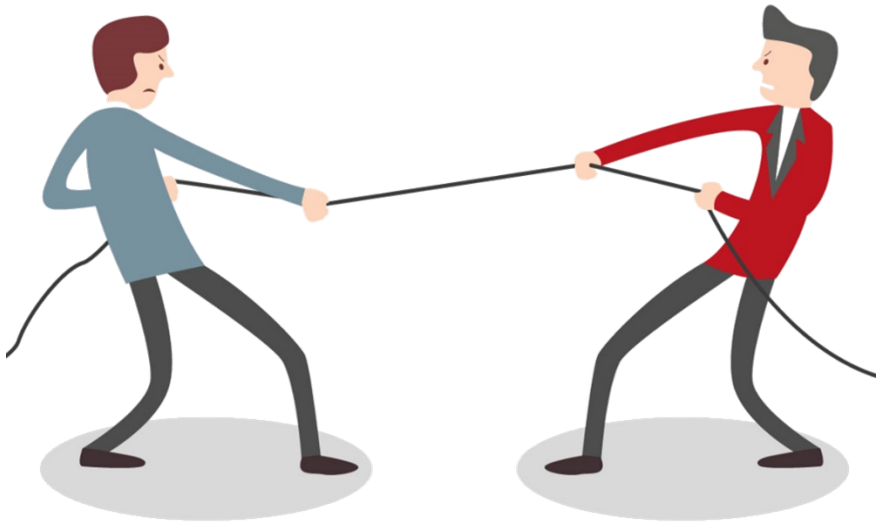
Consensus families

Nakamoto's consensus

++ Robust
++ Suitable or public environments

-- Energy exhaustive
-- High latency
-- Less scalable

- Proof of stake
- Proof of Elapsed Time
- Proof-of-Activity
- Proof of Burn
- …



Byzantine Fault Tolerance consensus

++ Reduction in energy
++ Fast

-- Poor scalability
-- High communication complexity
-- Permissioned only

- Practical Byzantine fault tolerance
- Simplified Byzantine fault tolerance
- Delegated Byzantine Fault Tolerance
- …

Contribution

System Model

We consider :

- A public peer to peer system
- Authenticated reliable point-to-point communication links
- All nodes have direct access to a sampling service to pick their communication samples
- Participating nodes are recommended to dedicate their bandwidth resources for the application
- Nodes newly joining the network are not assigned any reputation score
- A set of high-ranked nodes (Pre-trusted nodes)

Byzantine Reliable Broadcast [1]

- Layer I

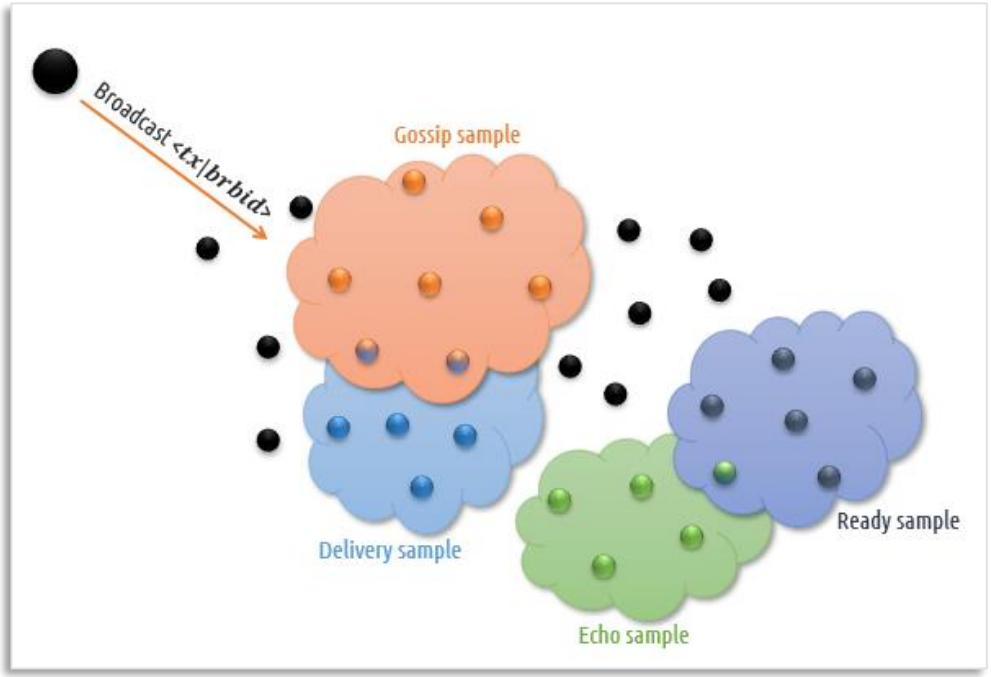
  Murmur ➔ Gossip to a *gossip sample* and deliver the first received message.

- Layer II

  Sieve ➔ Check consistency of gossiped messages among an *echo sample* (via echoes: what did you hear from layer I?)

- Layer III

  Contagion ➔ Deliver message when enough nodes are ready for it (Double echoes: Are you ready to deliver? I am ready)



Byzantine reliable broadcast samples

Byzantine Reliable Broadcast extension

+ Reach agreement
+ Scalable
+ Fast
+ Green
+ Reduced communication
+ Byzantine robust

But ..

- Abstraction
- Poor handling of concurrent events
- Sybil attack prone

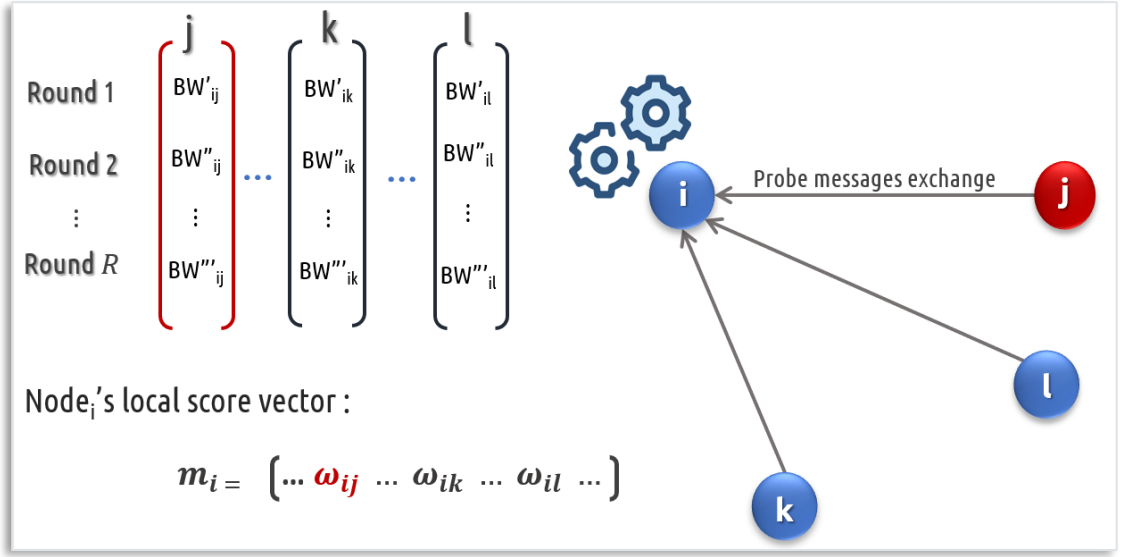
- Identification of broadcast channels
- Upon receipt of any BRB message, route through corresponding broadcast channel
- Map each broadcast instance to its corresponding message
- Each broadcast channel carries one single transaction

Broadcast channel ID	Broadcast instance
ID: A	brb_A
ID: B	New brb_B

Routing table

Proof-of-Bandwidth-based Reputation system

- Measure available bandwidth of peers over rounds
- Detect fluctuations of bandwidth
- Assign local scores accordingly
- Compare the variance of the bandwidth records σ_{BW} of each node to the fluctuation tolerance factor α and update local score as follows.



Proof-of-Bandwidth scheme

$$\omega_{ij} = \begin{cases} \omega_{ij}^{(0)} - \sigma_{BW}.BW_{max} : & if \quad \sigma_{BW} > \alpha \\ \omega_{ij}^{(0)} : & otherwise \end{cases}$$

- Normalize local scores

Proof-of-Bandwidth-based Reputation system

- Aggregate the local scores over the network into global ones via a reputation system [2]
- Compute global scores including evaluations of remote nodes weighted to their local scores

Node i trust in node k

$$m_{ik} = \sum_j m_{ij} \cdot m_{jk}$$

Node j trust in node k (remote trust)

Node i trust in node j (weight)

Iteratively, we converge to a global score in the form:

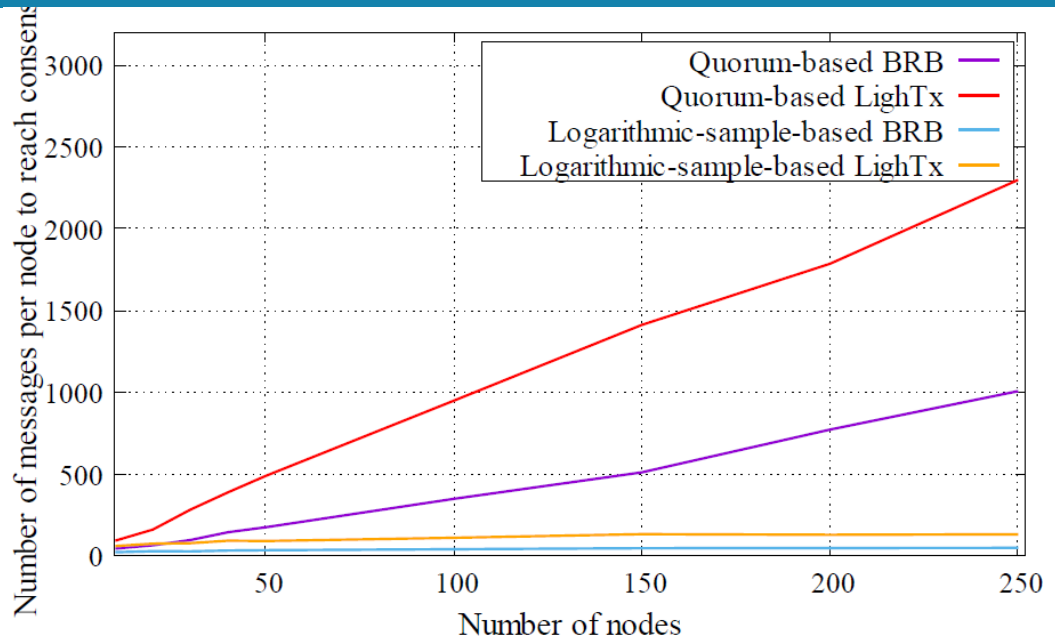
$$m = dmglobal + (1 - d)m_{local}$$

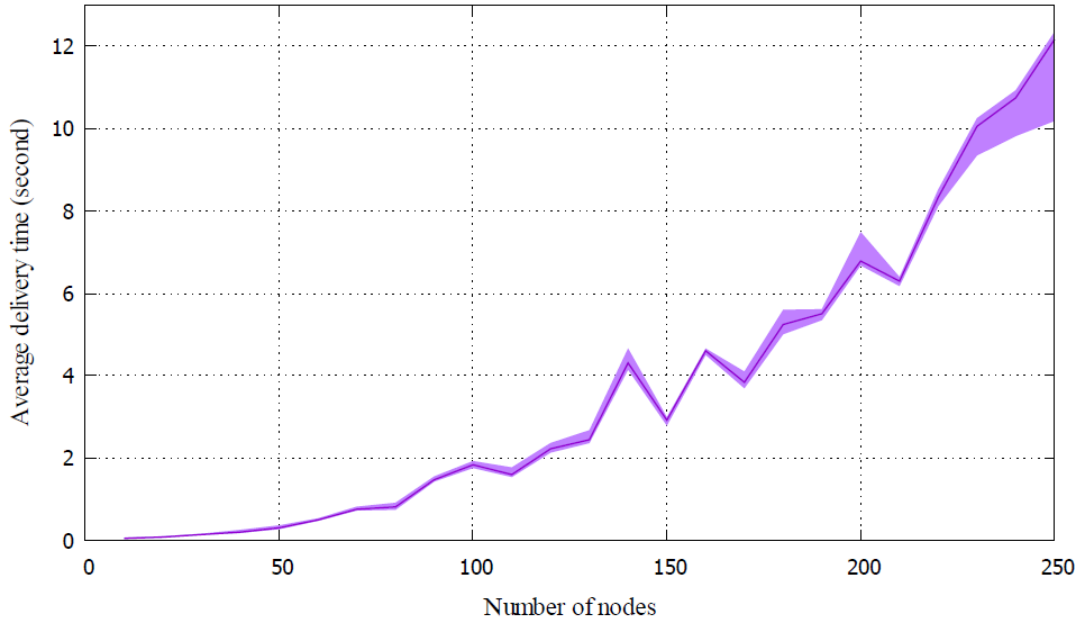
We say that we converged to a global score when:

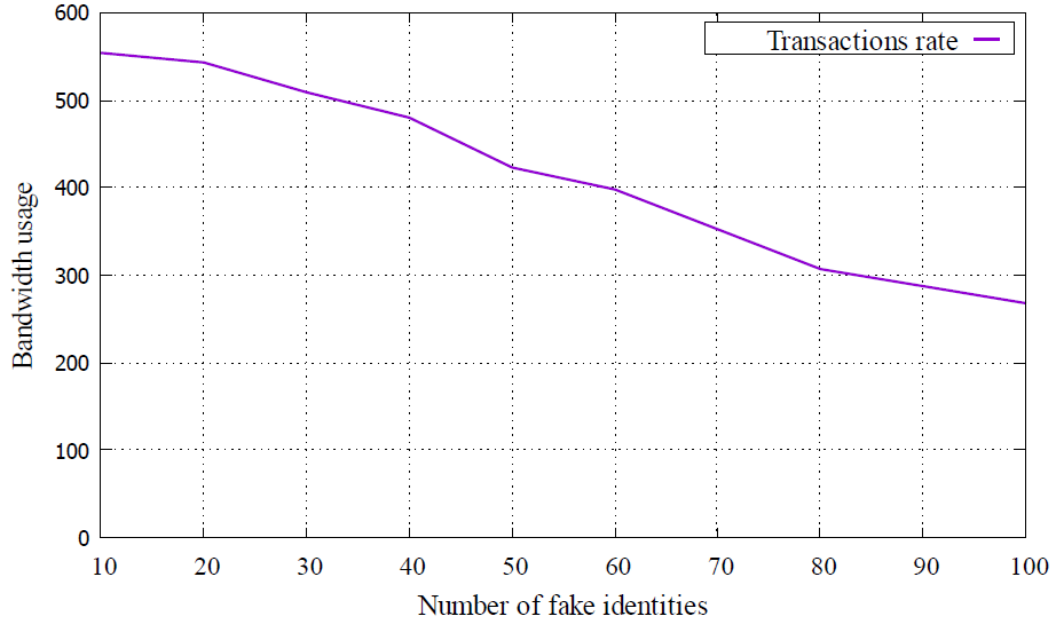
$$||\vec{\mathrm{m}}^{(k+1)} - \vec{\mathrm{m}}^{(k)}|| < \phi$$

Evaluation

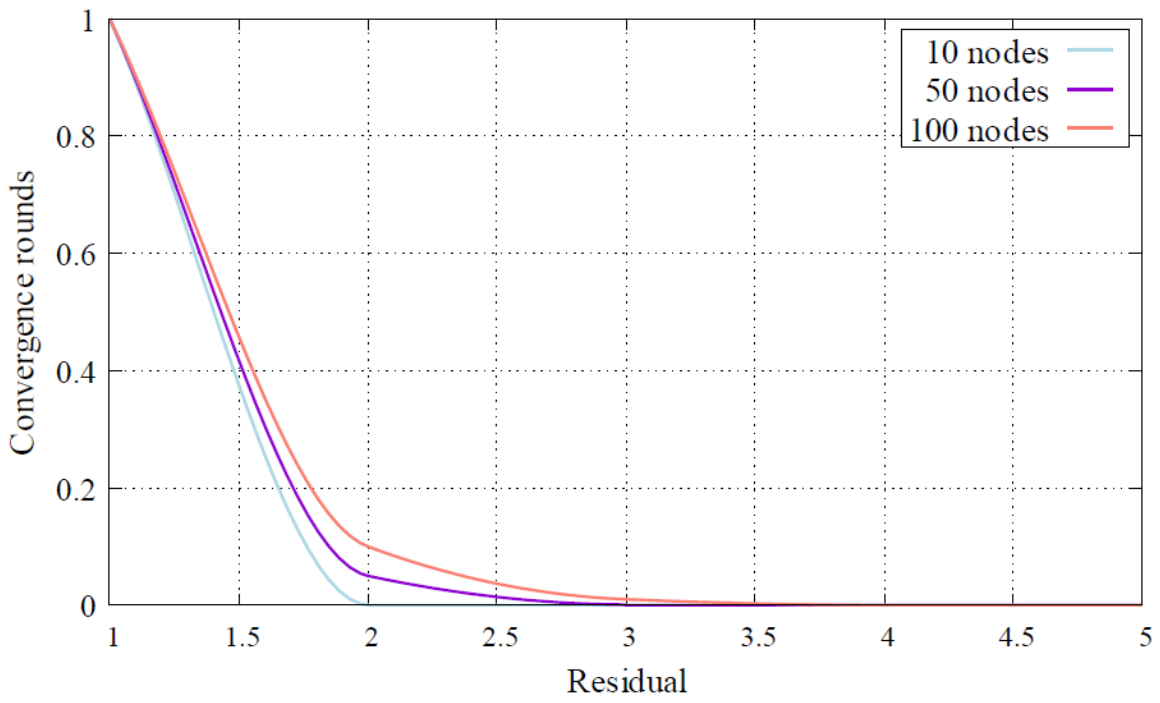
Evaluation

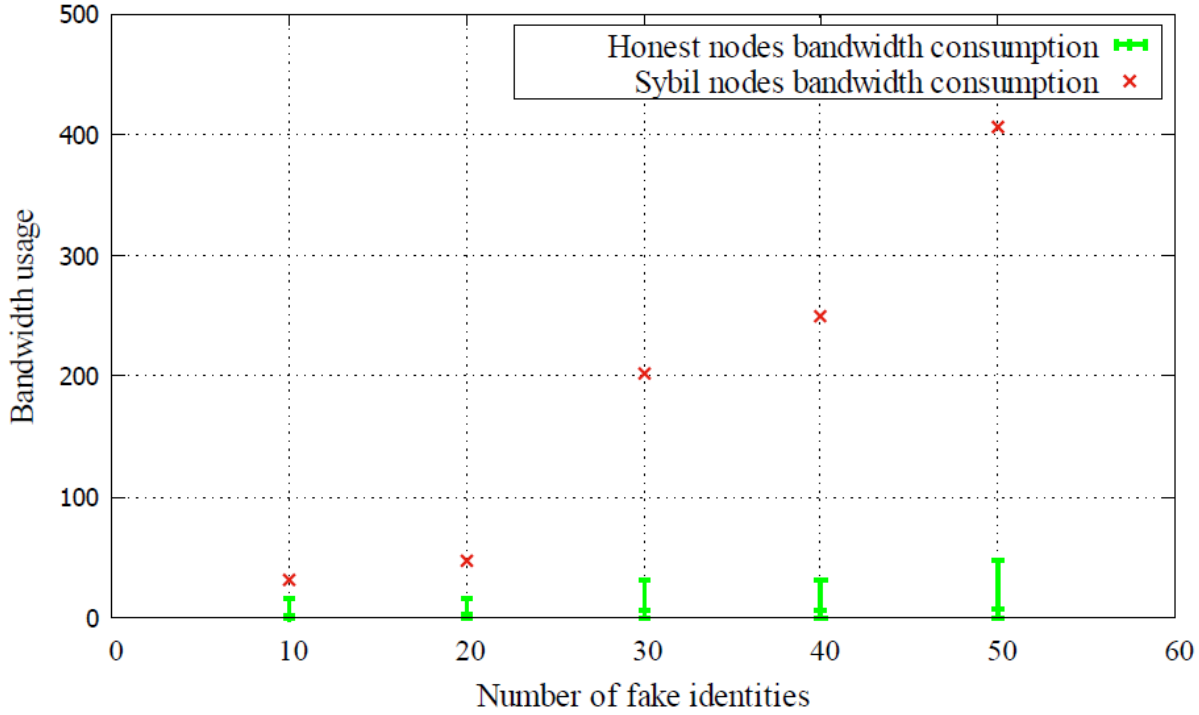

Quorum-based BRB
Quorum-based LighTx
Logarithmic-sample-based BRB
Logarithmic-sample-based LighTx
Number of messages per node to reach consens
Number of nodes
0
500
1000
1500
2000
2500
3000
50
100
150
200
250


Average delivery time (second)
Number of nodes
0
2
4
6
8
10
12
0
50
100
150
200
250


Transactions rate
Bandwidth usage
Number of fake identities
0
100
200
300
400
500
600
10
20
30
40
50
60
70
80
90
100

Evaluation


10 nodes
50 nodes
100 nodes
Convergence rounds
Residual
1
0.8
0.6
0.4
0.2
0
1
1.5
2
2.5
3
3.5
4
4.5
5


Honest nodes bandwidth consumption
Sybil nodes bandwidth consumption
Bandwidth usage
Number of fake identities
500
400
300
200
100
0
0
10
20
30
40
50
60

Conclusion & Perspectives

Conclusion & Perspectives

Our solution

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

Perspectives

- Wide network simulation
- 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).

Thank you.