

Studying the Applicability of Proof of Reputation(PoR) as an alternative consensus mechanism for Distributed Ledger Systems

Oladotun Aluko ¹ Anton Kolonin ¹

May 11, 2021

¹Department of Mathematics and Mechanics,
Novosibirsk State University

- Background
- Contributions
- Related Work
- Method
- Experiments and Results
- Conclusion

Background on Distributed Ledger Systems and Consensus

- A Distributed Ledger is a data structure replicated over a set of network nodes and comprises of an ordered list of transactions grouped and chained together in a block
- Cryptographic principles are employed within these systems to guarantee ledger's integrity - ability to detect data tampering
- Consensus within Distributed Ledger Systems refer to how some shared data can be agreed upon by a set of distributed nodes

- Several crucial issues to consider when designing a consensus mechanism
 - Node failure
 - Network latency
 - Network partition
 - **Node behaviour** [1]
 - Out-of-order inputs

- In our scheme, the behaviour of a node affects its overall reputation value
- Also, our approach also uses a social choice function during the consensus consensus
- Finally, we develop an experimental implementation and evaluate its performance in terms of consensus latency and the throughput of the system.

Related Work (Consensus Mechanisms)

- Proof-of-Work (PoW) is by far the most widely used consensus mechanism. The generation of new data blocks however requires the use of a huge amount of computational power
- Proof-of-State (PoS) was proposed as an alternative to PoW. With PoS, nodes who like to participate in the block creation process must prove ownership of a certain amount of stake

Related Work (Reputation Based Consensus)

- Reputation-based consensus mechanism based on the proof-of-work consensus algorithm by Yu et al. [2]
- Reputation-based consensus mechanism for peer-to-peer networks by Gai et al. [3]

Method (Consensus Mechanism)

- Assume N nodes in a network, an individual node is represented as $p_i, i \in N$
- In addition, each node i is identified by a key pair, pk_i is the public key and sk_i is the corresponding secret key
- Each node during regular interaction can either be the sender or recipient of a rating w.r.t a service
- We denote this interaction where node i is the rater and node j is the recipient as follows:

$$T = (E_{sk_i}, p_j, r) \quad (1)$$

$$\{r : 0 < r < 1\}$$

Method (Consensus Group Election)

- At the start of a new round, members of the consensus group are selected into a committee
- Let G_r denote the consensus group for a round r
- Nodes are selected in such a way that the total reputation value of the group is more than 50% of the entire network
- A node in this group denoted as

$$pk_i \in G_r \quad (2)$$

- This group is selected at the start of every block creation round

Method (Consensus Group Election - contd.)

- To proceed, a leader is then selected at random
- After a leader is selected, it's duty is to package all transactions(data interactions) for that round, validate, calculate a new reputation list, signs and then broadcast to the consensus group

$\langle \textit{Commit}, l_r, \textit{Block}_r \rangle \quad (3)$

- Other nodes in this committee re-validate these data interactions and the calculated reputation ranks and also check the integrity of the broadcast through a weighted voting process

Method (Consensus Group Election - contd.)

- Our weighted voting process uses a social choice function as basis for decision making
- For a set of nodes in the consensus group for round G_r , each node has an associated weight w assigned which is equivalent to its reputation value from the previous round $r - 1$
- Also, there's a minimum quota which has to be reached for decisions to be made. We set this quota at $\frac{2}{3}$ of the total weight in the consensus group

$$d(G) = \begin{cases} 1 & \sum_{i \in G} w_i > q \\ 0 & \text{otherwise} \end{cases}$$

Method (Reputation System)

- Nodes selected for the consensus are usually highest ranking nodes in the network
- Let s_i denote the reputation for a node i
- All nodes in the network start with a default reputation value determined on system initialization
- During node interactions, a node's reputation value is determined by the liquid rank algorithm [4]. This approach can be used as a predictive metric to evaluate a node's behaviour

Method (Reputation System)

The principles for the design of the reputation system are

- The liquid nature of the reputation values. The reputation value computed for a node is based on the reputation value of the node providing the rating
- The temporal scoping of reputation so that reputation values collected by members in the past are less contributing to the current reputation value

Method (Reputation System - contd.)

- For each round, a node can receive multiple unique ratings

$$S_{i1\dots n} = \{S_{i1}, \dots, S_{in}\} \quad (4)$$

- Range of s_i is $[0, 1]$
- Values s_i are then normalised as follows

$$S_{i,n} = \frac{S_{i,n} - \min_i(S_{i,n})}{\max_i(S_{i,n}) - \min_i(S_{i,n})} \quad (5)$$

- To prevent null values from the set of ratings, we slightly modify the above formula as follows

$$S_{i,n} = \frac{(S_{i,n} - \min_i(S_{i,n})) + 1}{(\max_i(S_{i,n}) - \min_i(S_{i,n})) + 1} \quad (6)$$

Method (Reputation System - contd.)

- Specifically, we denote node transactions as a row vector S
- To compute new reputation values, we blend these ratings with the rater reputation values from the previous round $r - 1$
- We denote this as

$$P = \vec{S} * \vec{R} \quad (7)$$

where $\vec{S} = [s_{ij}]$ and $\vec{R} = [r_{in}]^T$

- P is now the new rank value for the current round r

Method (Reputation System - contd.)

- To calculate the reputation value for the round r

$$R_{i,r+1} = \alpha * P + (\alpha - 1) * R_r \quad (8)$$

where α is a constant value

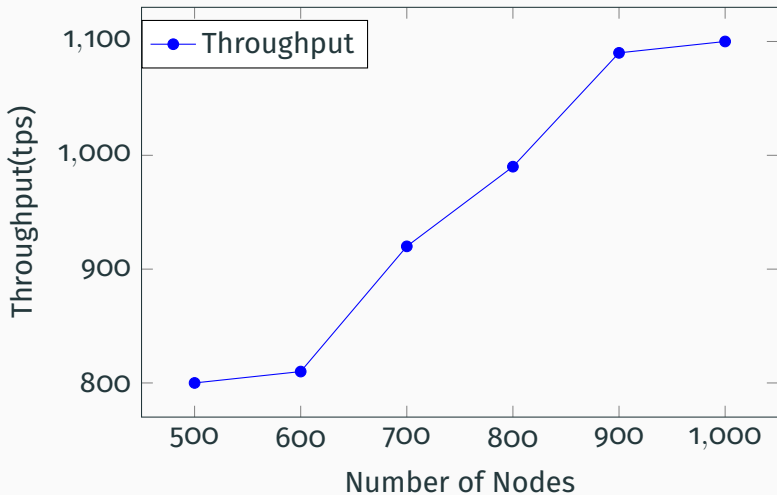
- Further, to prevent reputation values from hopping, we clamp the values using a sigmoid function as follows

$$R'_{i,r+1} = \frac{R_{i,r+1}}{\sqrt{1 + (R_{i,r+1})^2}} \quad (9)$$

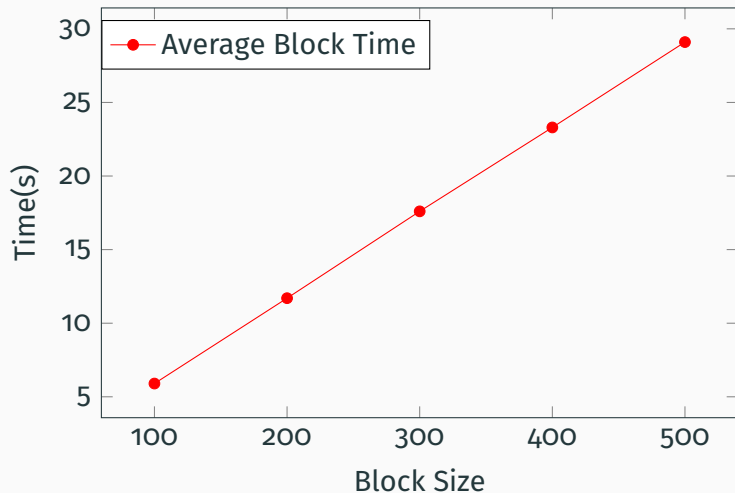
Experiments Setup

- For our prototype, we built an experimental network, implemented our mechanism and deployed nodes with AWS EC2 running on 16GM RAM with Amazon's t3 processor
- We imposed a round-trip latency of 200ms and varied node setup between 500 and 1000
- Added rate limiting to curtail excess bandwidth usage
- Finally, benchmarked with ApacheBench

Experiments and Results



Experiments and Results






Conclusion

- In our reputation-based consensus mechanism, the reputation of a node is not simply calculated by the value of the direct rating given by other nodes but by blending together a normalized set of ratings and the corresponding reputation values of the node providing the rating at a given period in time. The behaviour of a node affects its overall reputation value
- Our novel approach to reputation consensus is based on social choice functions as a means to determine integrity of data in a consensus group

Conclusion (contd.)

- Our reputation system is based on the following principles: 1) The liquid nature of the reputation values. The reputation value computed for a node is based on the reputation value of the node providing the rating. 2) The temporal scoping of reputation so that reputation values collected by members in the past are less contributing to the current reputation value
- Finally, we develop an experimental implementation and evaluate its performance of the system.

-  L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” in *Concurrency: the Works of Leslie Lamport*, pp. 203–226, 2019.
-  J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, “Repucoin: Your reputation is your power,” *IEEE Transactions on Computers*, vol. 68, no. 8, pp. 1225–1237, 2019.
-  F. Gai, B. Wang, W. Deng, and W. Peng, “Proof of reputation: A reputation-based consensus protocol for peer-to-peer network,” in *International Conference on Database Systems for Advanced Applications*, pp. 666–681, Springer, 2018.



A. Kolonin, B. Goertzel, D. Duong, and M. Ikle, “A reputation system for artificial societies,” *arXiv preprint arXiv:1806.07342*, 2018.