OneConnect Financial Technology - Singapore Management University

Distributed Ledger Research Project Report

January 2021

OneConnect Financial Technology Co., Ltd.

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Vetted by

BLOCKCHAIN ASSOCIATION SINGAPORE

TABLE OF CONTENTS

PROJECT REVIEW:

The project commenced on 1st February 2020. Its objective is to develop a proof of concept (PoC) for a quantum distributed ledger to uncover potential advantages for distributed ledger technologies (DLTs). A PoC framework was created using the IBM Q quantum computers and Qiskit development kit. Details of the business requirements can be found in the project business requirement document and details of the technical components of the PoC can be found in the design and technical documents.

The researchers reviewed various types of consensus mechanisms and their suitability for quantum computation. Due to the inherent probabilistic nature of quantum phenomena, the focus should either be on the mechanism for electing a leader in proof of transfer (PoX) types of consensus, such as Proof of Work, or for leaderless consensus. As work already existed for leader election (Mazzarella 2013), the researchers explored a quantum leaderless consensus protocol based on the classical leaderless protocols presented in Ben-Or (1983).

There are several problems with DLTs, for example, with oracle data sources that can be addressed using a leaderless consensus. While it is unusual for leaderless consensus to be the main consensus mechanism in DLTs, leaderless consensus enables all nodes to agree on a value which would be useful for determining oracle values and detecting nodes which may be compromised. As there is the possibility for quantum technology to hold much larger data sizes than in classical systems, the volume of data used for consensus could also be very large.

Given the relative immaturity of quantum technology, the researchers made use of the quantum leaderless design in a hybrid model - where the variation in consensus is calculated classically. This gives greater visibility and control compared to a pure quantum model. As there are no quantum computers linked to quantum communication channels currently, all nodes in the consensus network run on the same quantum computer.

Due to the noisy characteristics of real quantum computer backends, development of the model was first initiated in simulators and then moved to real quantum backends with noise mitigation.

This document describes the results from experiments on quantum simulators and real quantum computers, as compared to classical leaderless consensus agreement using the disropt package written for the Python programming language. The disropt nodes were all run on the same computer to ensure there was no effect from networking.

All codes were run on Jupyter notebooks in Anaconda3 using Qiskit '0.15.1'.

KPI

KEY PERFORMANCE INDICATORS WERE:

- The number of rounds (Nr) to reach a majority of agreement
- The complexity of the Nr with the addition of more nodes for two topologies (Ring and Partial Mesh)

PROBLEM STATEMENTS

Current consensus algorithms for decentralised networks of peers cannot go beyond the trilemma of speed, size and security.

For example:

As network size expands, the speed of consensus is reduced and security becomes increasingly compromised.

With increased security, the speed and network size is reduced.

With increased speed, the security and size are reduced.

This in turn limits the usefulness of consensus algorithms in industry applications, as:

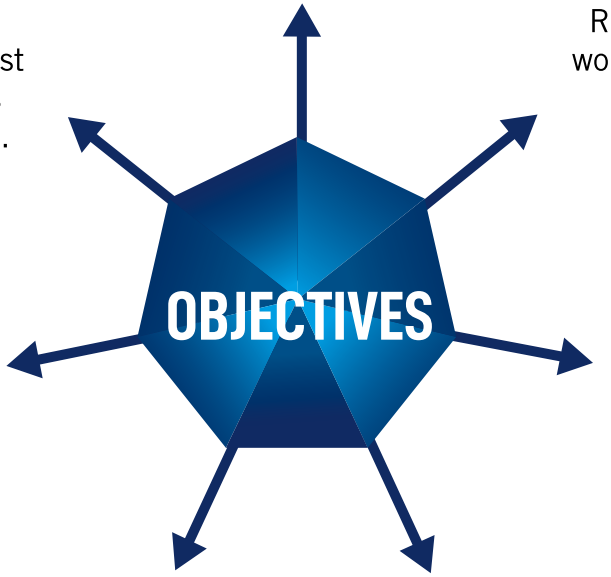
- More time is required to reach consensus for highly secure DLTs;
- Security is lowered; e.g. using RAFT consensus to increase the speed of consensus;
- DLT nodes in general only connect to around 10 other nodes with decreasing speed and lowered security as networks grow.

These problems limit potential business usage.

As data volumes continue to grow and as DLTs continue to become more prevalent, increased data will be required to be kept in consensus by more nodes with the same or better security. Quantum technologies may be explored to understand the potential for such improvements.

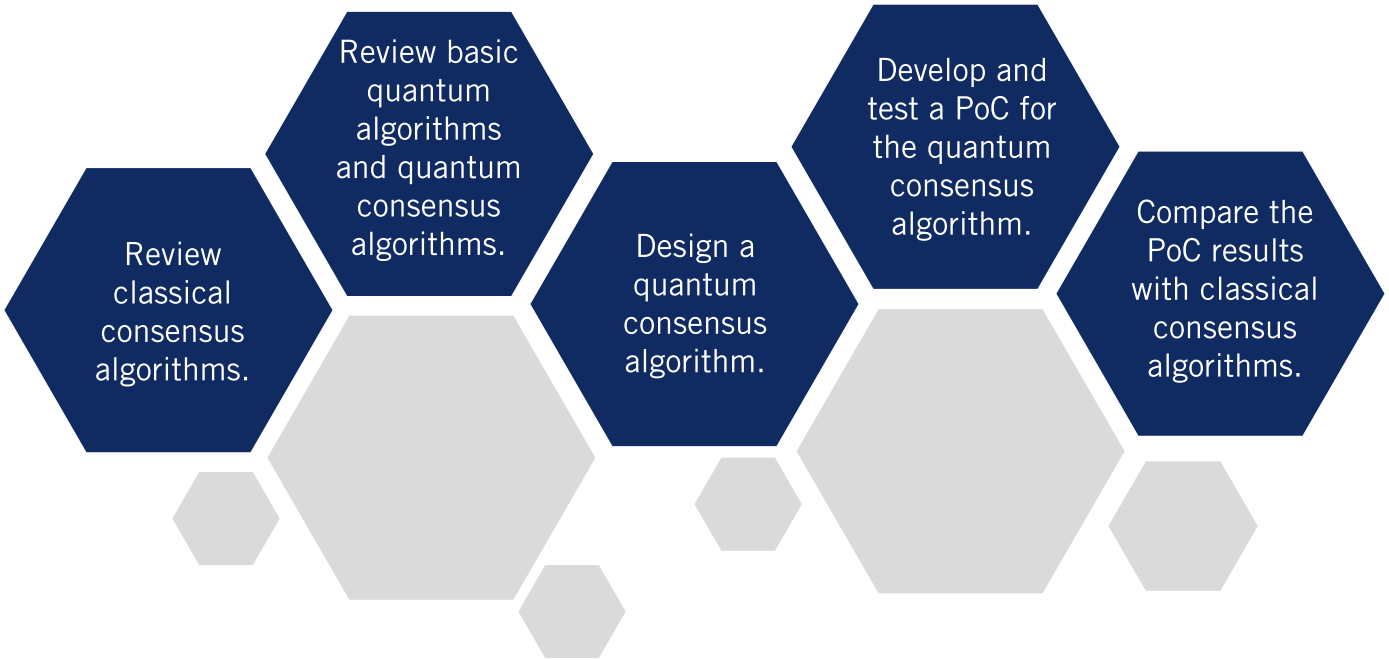
PROOF OF CONCEPT (POC)

To develop a proof of concept (PoC) for a quantum distributed ledger that can be tested for its suitability for business applications.



- Review current work on quantum distributed ledgers.
- Build on prior work on the use of quantum computer algorithms for consensus to uncover potential advantages for distributed ledgers.
- Define OneConnect's requirements for quantum distributed ledgers.
- Design a proof of concept (PoC) for an aspect of quantum distributed ledgers.
- Set up PoC development and test environments.
- Test the PoC protocol against the business requirements.

APPROACH



SUMMARY OF RESULTS

In summary, it was observed that on average, quantum leaderless consensus took the same Nr to converge to an agreement as the classical consensus. However, quantum leaderless consensus showed variation in Nr each time it was run. In contrast, the classical system showed less variation and was very reproducible (to be expected as all nodes ran on the same machine).

Discussion

While there was no advantage to be seen in the Nr taken to reach agreement for quantum over classical consensus, it is worth noting that quantum consensus does not on average take longer.

Given the enormous differences in the available states of a quantum computer (2^n where n is the number of qubits) over that of classical machines, quantum consensus could potentially agree on huge datasets such as those used in Big Data. This is something that would be impossible for classical consensus networks.

It should also be noted that the variation in Nr includes shorter as well as longer convergence times. If the shorter convergence times occurred more often, then an advantage over classical would be seen.

Details OF PoC Results:

For all the results given in this section the parameters used are:

- Threshold variance = 0.0001
- Shots for all quantum circuits executed = 8000
- Maximum rounds = 100
- N = number of nodes

Result 1

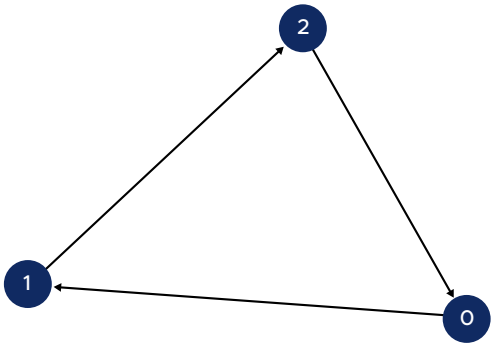
Convergence results for N=3 on QASM Simulator

In this section, we observed 3 nodes for the PoC quantum consensus model connected in one direction to form a Ring topology (Fig 1a) and executed using the QASM simulator.

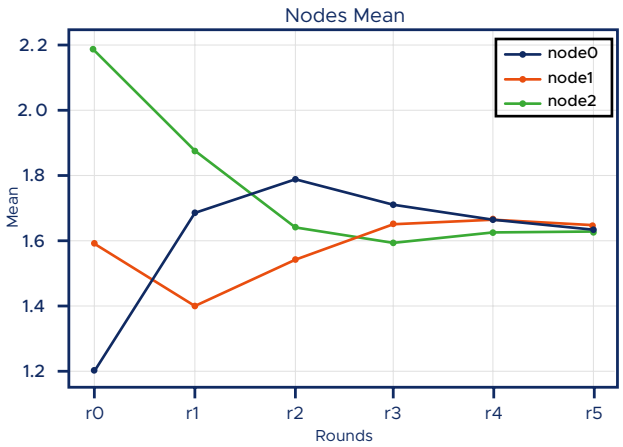
The graph in Fig 1b displays the number of rounds required to reach an agreement for the 3 nodes. It shows that for 3 nodes, a total of 6 rounds are required for all the nodes to decide on a common value and to reach an agreement within the threshold variance.

The variance for each node (Fig 1c) is seen to converge quite closely after 3 rounds (r3).

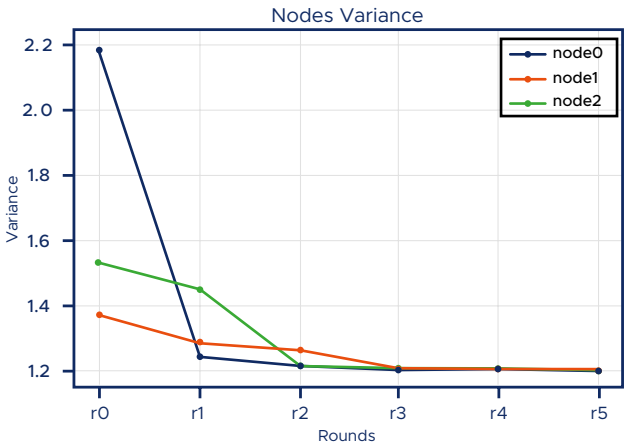
Fig 1:



(a) Ring



(b) Mean Graph



(c) Variance Graph

Conclusion:

- The expected mean for the 3 nodes is 1.67 based on an arithmetic mean of the initial values.
- The QASM simulator gives the agreed value of 1.64 with 100% nodes in agreement and within the threshold variance.

Result 2

Comparison of convergence results for N=3 on QASM Simulator and real backend.

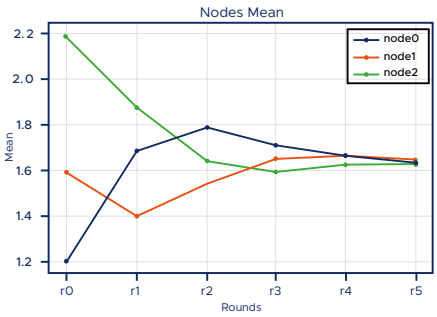
In this section, we compared the results obtained in Result 1 above with a real quantum computer backend for the same 3 nodes topology.

Fig. 2 shows the results of the QASM simulator (a) and a real backend with (b) and without (c) noise mitigation.

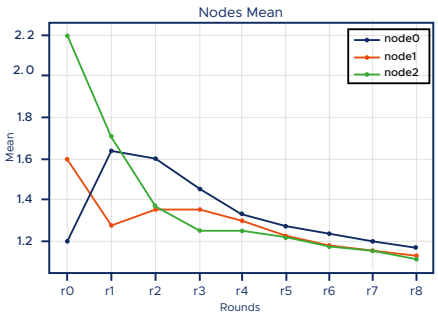
In order to obtain results from the real backend, parameters such as logical to physical qubits mapping and high optimization levels were configured. Fig. 2b shows the results without any noise mitigation.

Fig. 2c shows the results using the measurement error mitigation module for Qiskit. The calibration matrix used for the mitigation was generated from a real backend of the IBM Q system.

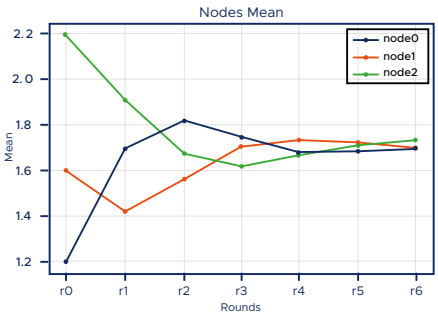
Fig 2:



(a) QASM simulator



(b) Real Backend without mitigation



(c) Real Backend with measurement error mitigation

While the nodes did reach agreement for the real backend, the agreed value was much lower than that expected. This was due to noise in the qubits, gates and measurements. However, the noise can be mitigated to a large extent bringing the agreed value much closer to that expected (Fig. 2c). Nonetheless, other runs of the consensus showed variations in the agreed value over time.

Conclusion:

- We conclude that the measurement error mitigation of the IBM Q system helps to mitigate the noisy results of the backend to some extent.
- The stability of the mitigation needs to be observed over time to explore how frequently noise calibration is required.

Result 3

Complexity for Ring topology adding more nodes for Quantum Consensus

We investigated the consensus model for a Ring topology for 50 iterations of consensus with different network sizes (from 3 to 10 nodes). Input values for the nodes were chosen from a normal distribution with a standard deviation of 0.40 (Table 1).

	N=3	N=4	N=5	N=6	N=7	N=8	N=9	N=10
1	1.7	2.2	2.1	1.3	2.2	1.1	1.1	1.1
2	2	1.6	1.8	2.2	1.3	1.7	1.7	1.7
3	1.2	2	1.5	1.8	1.1	1.1	1.1	1.1
4		1.3	1.1	2.2	1.6	2.2	2.2	2.1
5			2	1.9	1.5	1.7	1.7	1.7
6				1.3	1.4	2.1	2.1	2.1
7					2.1	1.6	1.6	1.6
8						1.9	2.1	1.7
9							1.4	2.2
10								1.3
mean	1.6333	1.7750	1.7000	1.7833	1.6000	1.6750	1.6667	1.6600
std dev	0.4041	0.4031	0.4062	0.4070	0.4082	0.7097	0.4153	0.4006

Table 1: Node values set for each of the nodes. N = number of nodes.

Fig 3 shows that when the number of nodes increase from 3 to 10, the average number of rounds taken to reach agreement for 50 iterations is seen to increase approximately linearly.

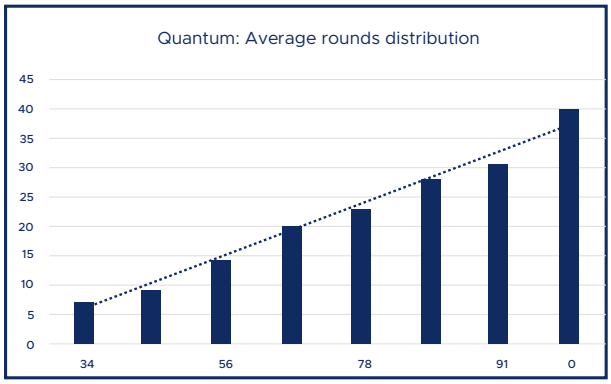


Fig. 3 : Average number of rounds taken to agree for 50 iterations.

Conclusion:

- We conclude that as the number of nodes increases, the rounds required to reach an agreement also increases.
- The number of nodes in a network and the number of rounds required to reach an agreement shows a linear relationship for a Ring topology of up to 10 nodes.

Result 4

Comparing Complexity for Quantum and Classical Consensus

In this section, we compared quantum consensus with classical consensus. For classical consensus, the Python disropt package was used.

Table 2 and Fig. 4 show the time complexity comparison for 3 to 10 nodes for quantum and classical consensus. We observed that over 50 iterations, the time complexity for classical consensus exhibited similar patterns as compared to quantum consensus.

No of nodes	Quantum	Classical
3	7.12	6
4	9.14	8
5	14.56	14
6	20.22	18
7	23.02	22
8	28.1	27
9	30.3	32
10	39.94	38

Table 2. The average number of rounds to reach agreement for quantum consensus compared to classical consensus.

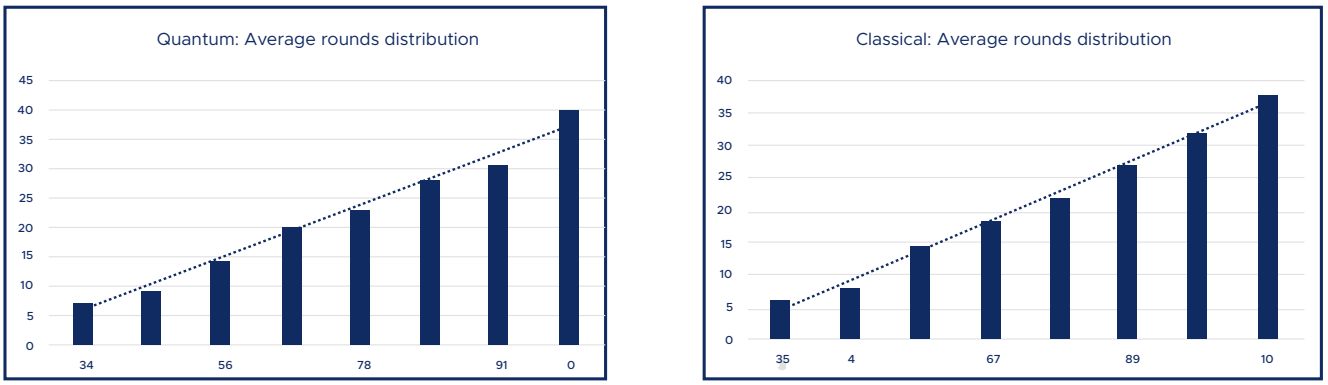


Fig 4: Comparison of quantum (left graph) and classical (right) complexity for the number of rounds increasing from 3 to 10 nodes.

Conclusion:

- When we compare the quantum and classical rounds distribution for node 3 to 10, we obtain similar results.
- For quantum consensus, we need to calculate the average the number of rounds across 50 iterations; whereas for classical consensus, the number is consistent for each iteration.

Result 5

Quantum Consensus variation in Ring topology

In this section, we observed the mean and median for the distribution of the number of rounds needed to reach an agreement - when the quantum consensus model was executed for 50 iterations in the Qiskit, across 3 nodes and a Ring topology.

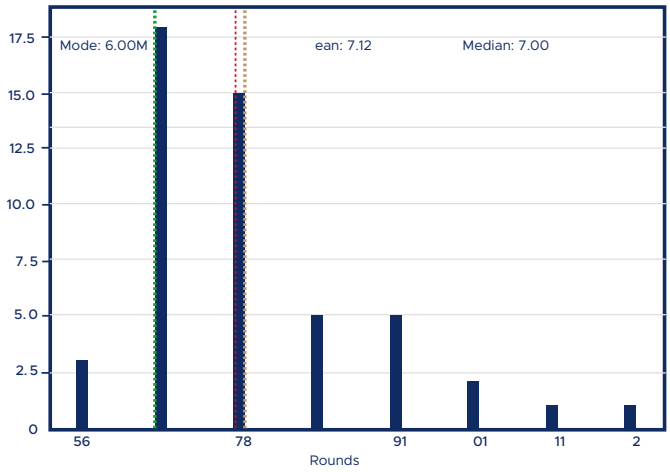


Fig 5: A histogram plot for the distribution of the number of rounds to reach an agreement for 3 nodes. The mode (= 6, green dotted line), the median (= 7, red dotted line) and the mean (= 7.12, black dotted line) are shown on the graph.

Table 3 displays the mean, median and mode that quantum consensus required to reach an agreement for 3 to 10 nodes, comparing them with the rounds required for classical consensus.

Nodes	mean	Median	Mode	Classical number of rounds required to terminate	Quantum average number of rounds required to terminate
3	7.12	7.0	6	6	7.12
4	9.14	9.0	10	8	9.14
5	14.56	14.0	14	14	14.56
6	20.22	20	18	18	20.22
7	23.02	22.50	21	22	23.02
8	28.10	27	25	27	28.1
9	30.3	30	33	32	30.3
10	39.94	39.50	38	38	39.94

Table 3: Comparison of mean, mode, median for quantum consensus with classical mean for nodes 3 to 10

Conclusion:

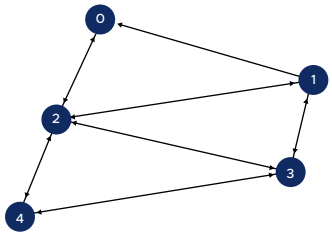
- The difference in mode, median and mean implied the data was skewed.
- The mode obtained in quantum consensus for 3 nodes and the number of rounds required to reach agreement in classical consensus are the same.
- The mode value for most of the quantum consensus is similar to the number of rounds required to reach agreement in the classical consensus.

Result 6

Comparing Quantum and Classical Consensus for Partial Mesh Topology

We compared the number of rounds required to reach an agreement for quantum and classical consensus for a partial mesh topology.

A full mesh topology is a network where all the nodes are connected to each other. To mimic a real- world scenario, we designed a partial mesh network where all nodes are not directly connected to each other.



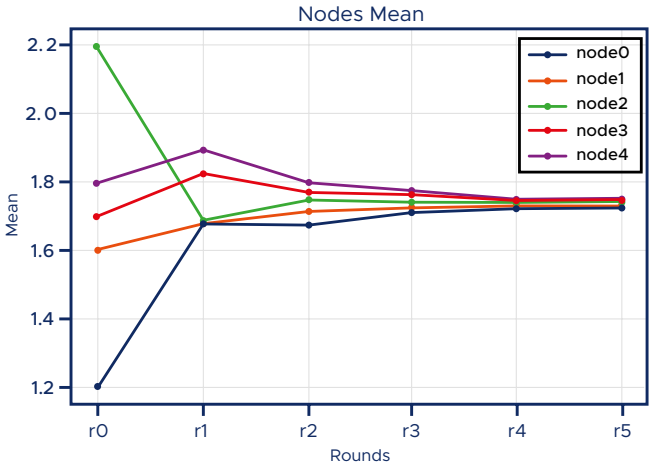
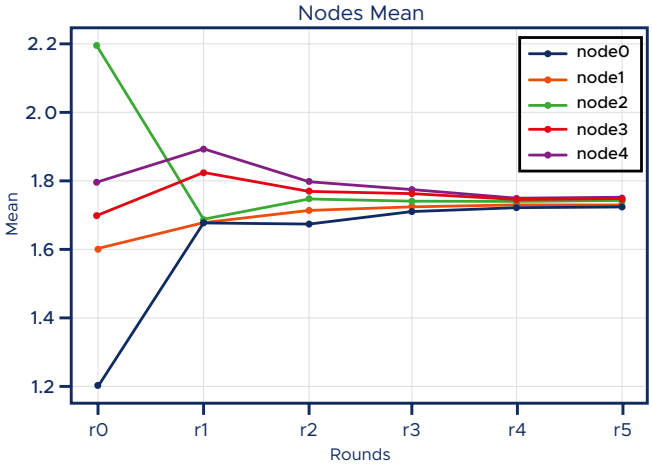


Fig 6. Average distributed consensus for N=5, Partial Mesh Topology and node mean values.



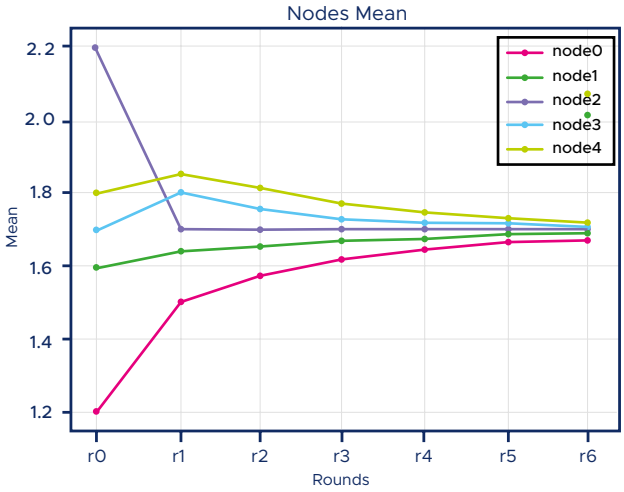


Fig 7: Comparison of the node mean values for each round quantum (left) and classical (right).

For this example with 5 nodes, classical consensus reached majority in 7 rounds and quantum in 6 rounds.

Conclusion:

- We observed that the number of rounds needed to reach an agreement for a partial mesh topology is similar for both classical and quantum consensus.

REFERENCES

Luca Mazzarella, Alain Sarlette and Francesco Ticozzi, *Consensus for Quantum Networks:From Symmetry to Gossip Iterations, ar*Xiv:1303.4077v1 [quant-ph] 17 Mar 2013

Michael Ben-Or ,*Another Advantage of Free Choice: Completely Asynchronous Agreement Protocols (Extended Abstract)* PODC '83: Proceedings of the second annual ACM symposium on Principles of distributed computing, https://doi.org/10.1145/800221.806707.