8th Distributed Ledger Technology Workshop (DLT 2026)

Pula – June 6th, 2026

Quantum-Assisted Validator Selection for Proof-of-Stake Based Blockchains

Alberto Leporati

University of Milano-Bicocca

Department of Informatics, Systems, and Communication

alberto.leporati@unimib.it

The problem

- In Proof-of-Stake (PoS), validator selection probability is proportional to stake
- This can amplify stake concentration over time
- It may also enable collusion, economic cartels, and strategic manipulation

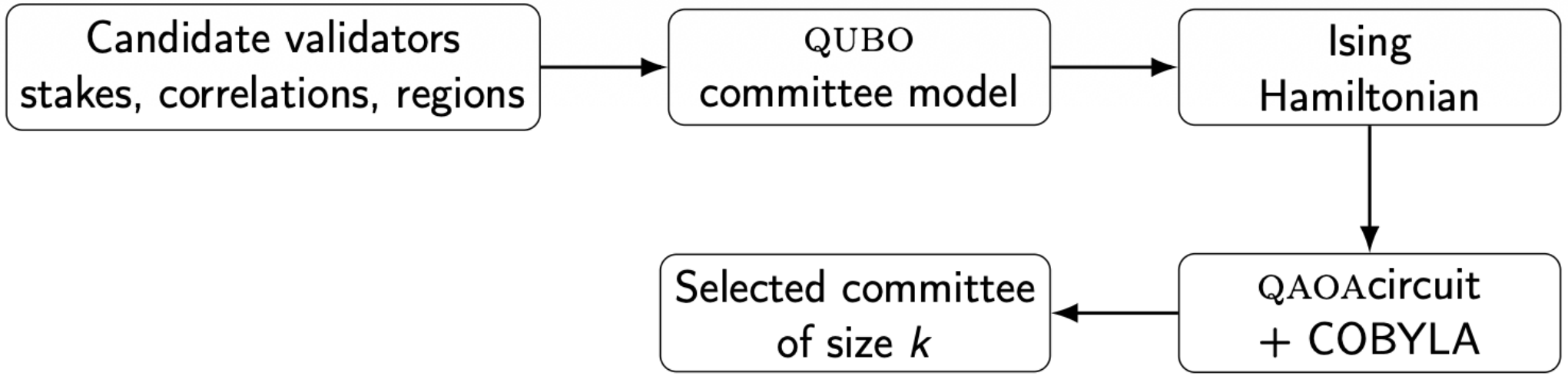
---

When selecting the validators committee, we would like to consider also economic correlations and geographic clustering

We obtain an NP-hard combinatorial optimization problem

Main idea

- Formalize validator selection as a Quadratic Unconstrained Binary Optimization (QUBO) problem, and solve it through a hybrid quantum-classical technique based on the Quantum Approximate Optimization Algorithm (QAOA)



Committee Selection as an Optimization Problem

- Let $V = \{v_1, \ldots, v_n\}$ be the candidate validators and k the committee size

Decision variable:

$$x_i = \begin{cases} 1 & \text{if } v_i \text{ is selected} \\ 0 & \text{otherwise} \end{cases}$$

Available information:

- Stake s_i of candidate v_i
- Economic correlation $c_{ij} \in [0,1]$
- Geographic matrix $G_{ij} \in \{0,1\}$

Goal: choose exactly k validators while discouraging concentration and correlated selections

The QUBO objective

The problem becomes a Quadratic Unconstrained Binary Optimization (QUBO) problem

$$H(x) = \alpha \sum_{i=1}^{n} s_i^2 x_i + \beta \sum_{1 \le i < j \le n} c_{ij} x_i x_j + \gamma \sum_{1 \le i < j \le n} G_{ij} x_i x_j + \lambda \left(\sum_{i=1}^{n} x_i - k \right)^2$$

Stake: penalizes excessive stake concentration

Economics: penalizes correlated validators

Geography: penalizes validators in the same region

Cardinality: forces exactly k selected validators

From QUBO to Ising Hamiltonian

- Each binary variable is mapped to a qubit observable:

$$x_i = \frac{1 - Z_i}{2}$$

- This yields the QAOA cost Hamiltonian:

$$H_C = \sum_{i=1}^{n} h_i Z_i + \sum_{i<j} J_{ij} Z_i Z_j$$

Each one implemented as a sequence of gates

- Single-qubit terms encode linear costs and penalties
- Two-qubit terms encode economic, geographic, and cardinality interactions
- The ground state corresponds to the minimum-cost committee

Quantum Approximate Optimization Algorithm (QAOA)

1. Prepare a uniform superposition
2. Alternate cost and mixer layers
3. Measure candidate committees
4. Use a classical optimizer to update parameters

QAOA samples a probability distribution over validator committees, biased toward low-cost solutions

- The circuit implements the following unitary operator:

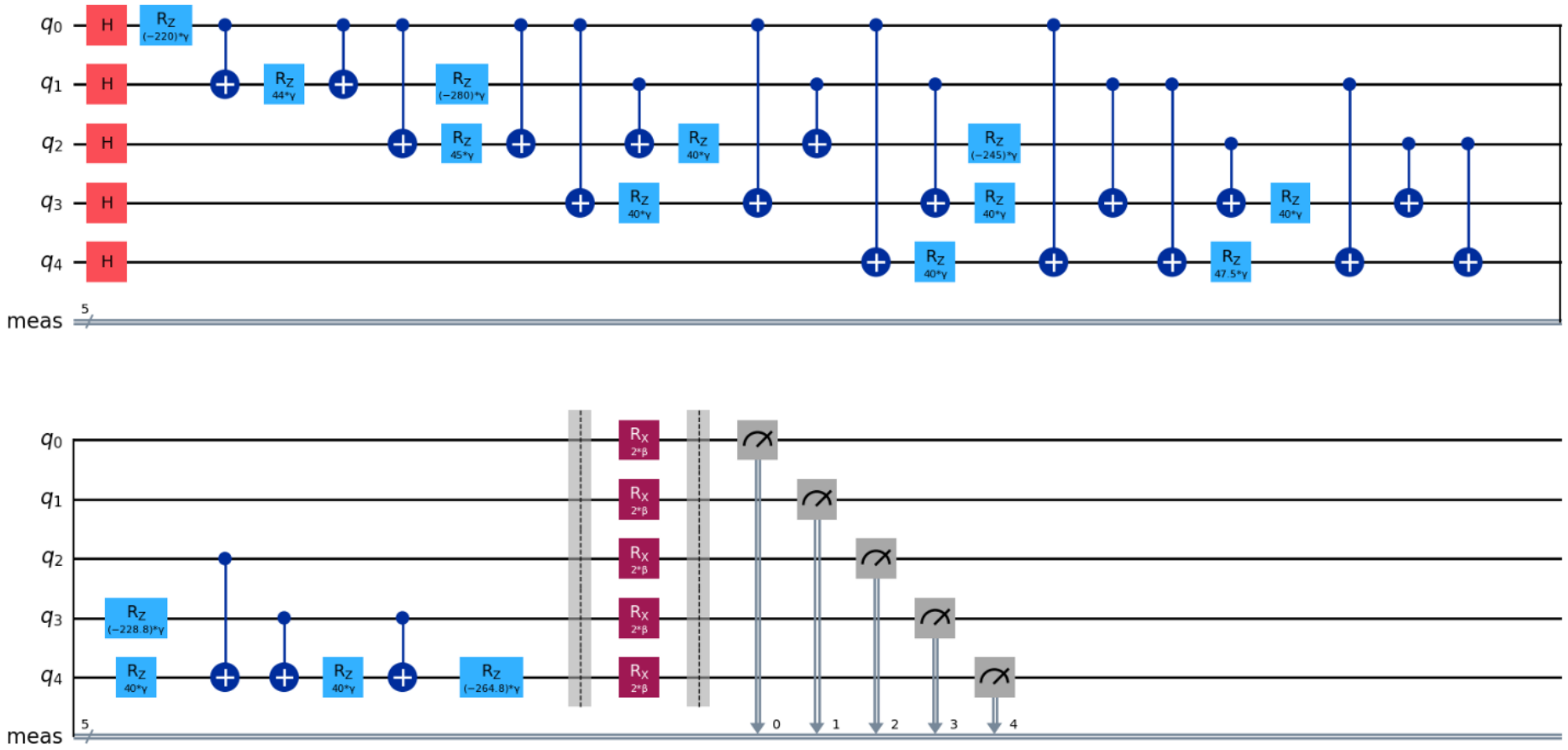
$$U(\gamma, \alpha) = e^{-i\alpha_p H_M} e^{-i\gamma_p H_C} \cdots e^{-i\alpha_1 H_M} e^{-i\gamma_1 H_C}$$

Mixer Hamiltonian: $H_M = \sum_{i=1}^{n} X_i$ (explores new solutions)

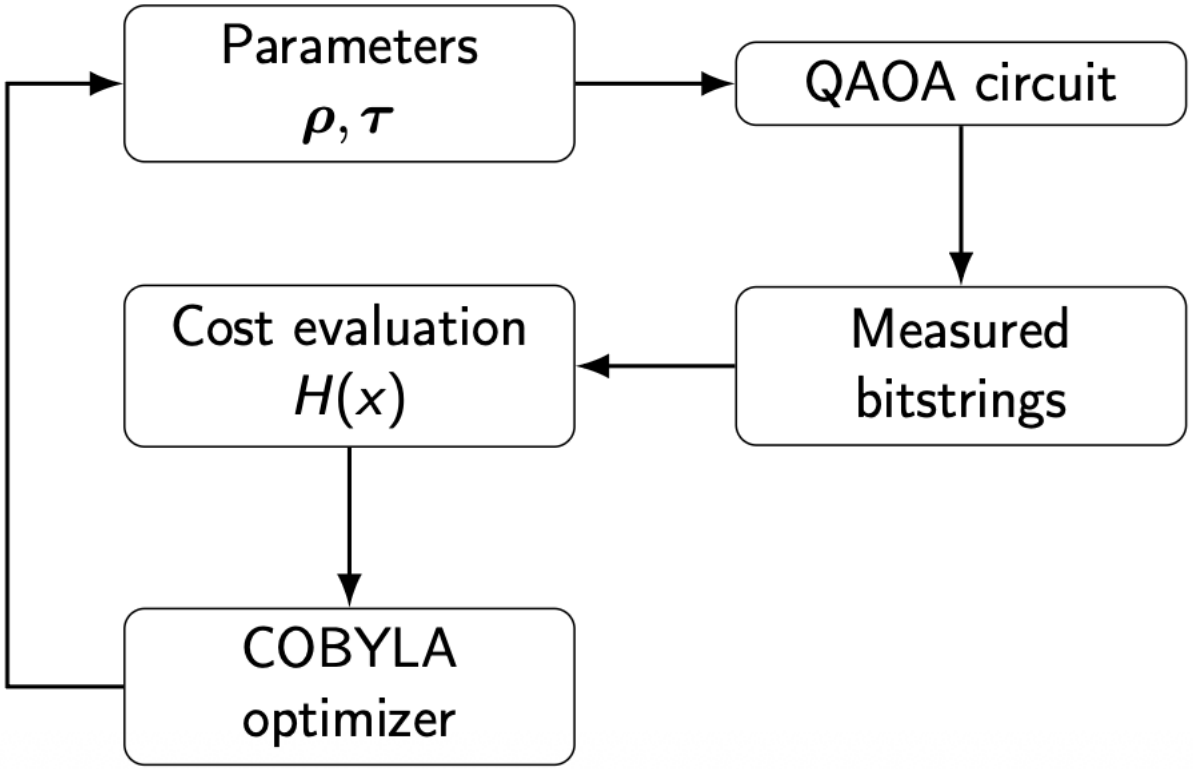
Cost Hamiltonian: $H_C = \sum_{i=1}^{n} h_i Z_i + \sum_{i<j} J_{ij} Z_i Z_j$

Quantum Approximate Optimization Algorithm (QAOA)

- Circuit for $n = 5$ candidates and $k = 3$ selected validators:



Hybrid Classical–Quantum Loop



Stopping criterion: Stop after a fixed number of iterations or when the observed energy is sufficiently low

Experimental Setup

- Implementation: Qiskit
- Classical simulation of quantum circuits
- Candidate sets: $n = 5, \ldots, 10$
- Stake of each candidate: random, between 1 and 100
- $n^2/2$ elements of matrix c set to random float number in [0,1]
- n elements of matrix G set to 1
- Committee size: $k = 3, \ldots, 6$
- 100 runs per configuration

Baselines:

- Traditional random PoS selection
- Brute-force optimal selection

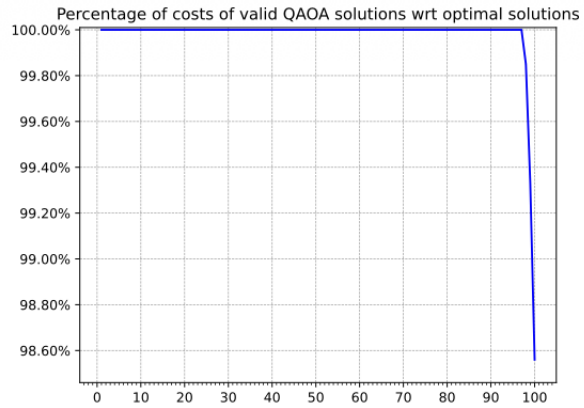
Typical parameters:

$\alpha = -0.1, \quad \beta = 1, \quad \gamma = 1, \quad p = 2$

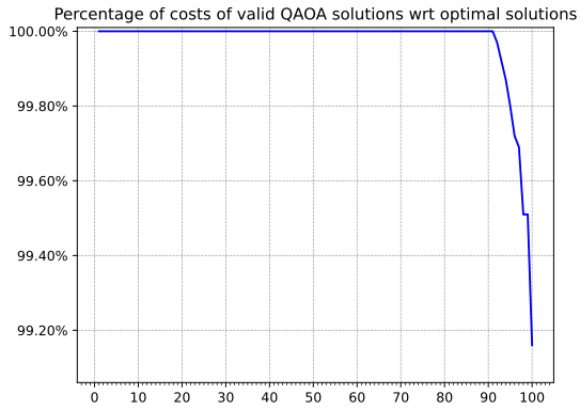
Main results: QAOA vs Random PoS (k = 3)

n	λ	# of optimal hybrid solutions	min % of hybrid vs. optimal solutions	# of optimal random solutions	min % of random vs. optimal solutions	Avg. time (s) for hybrid	Max. time (s) for hybrid	Time (s) brute force
5	2000	97	98.56%	32	94.71%	5.54	7.35	0.00005
6	2000	91	99.16%	19	93.40%	11.14	15.66	0.00010
7	2000	78	97.75%	10	93.06%	23.19	28.17	0.00015
8	2000	67	96.17%	9	92.61%	59.41	185.14	0.00026
9	4000	41	98.22%	5	96.44%	308.17	395.55	0.00041
10	4000	27	98.89%	3	95.10%	821.76	1774.45	0.00059

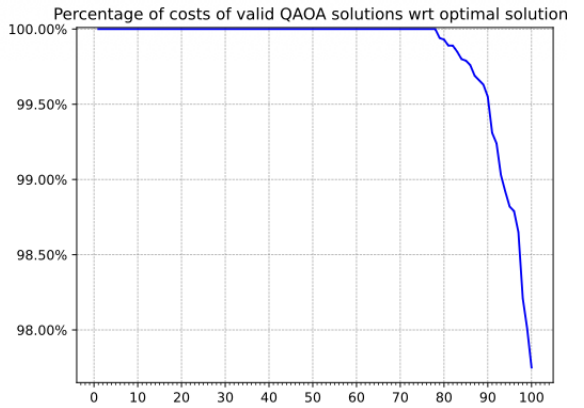
Main results: Cost of QAOA solutions vs Optimal Solutions



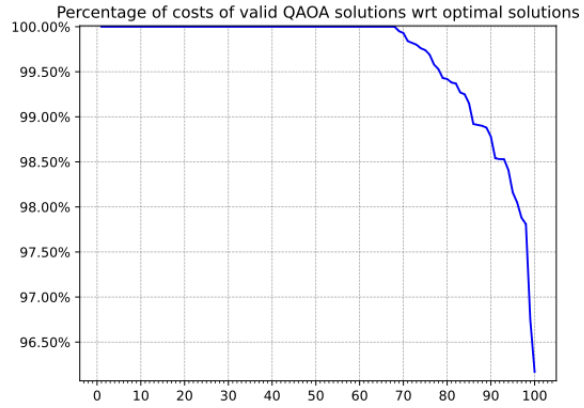
(a) $n = 5$ and $k = 3$



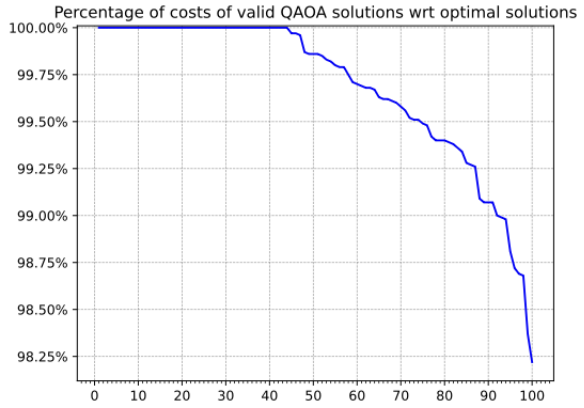
(b) $n = 6$ and $k = 3$



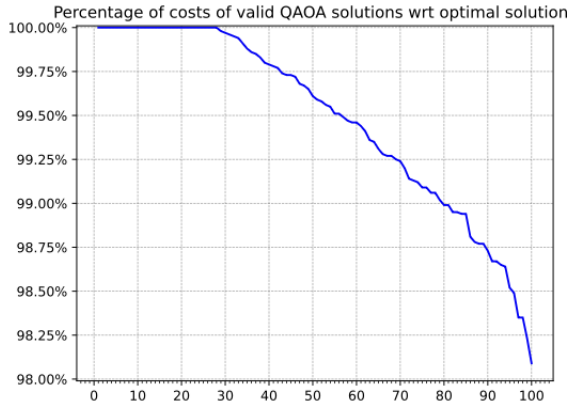
(c) $n = 7$ and $k = 3$



(d) $n = 8$ and $k = 3$

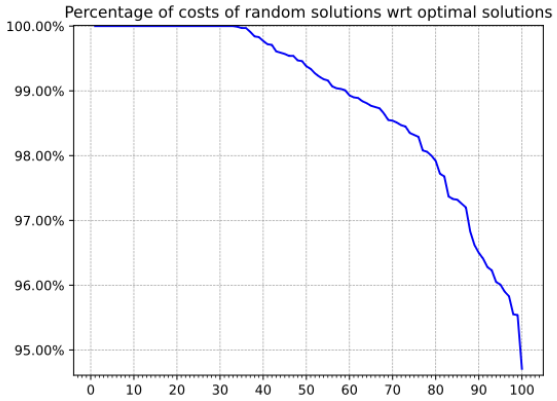


(e) $n = 9$ and $k = 3$

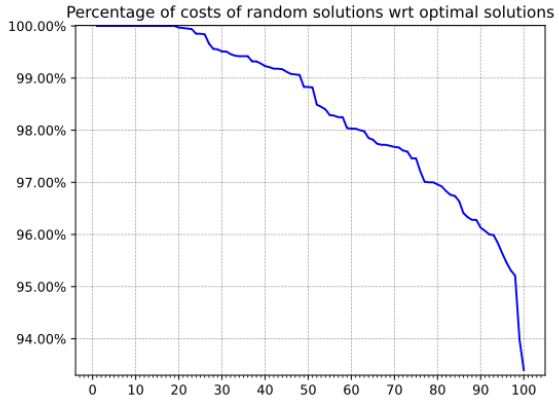


(f) $n = 10$ and $k = 3$

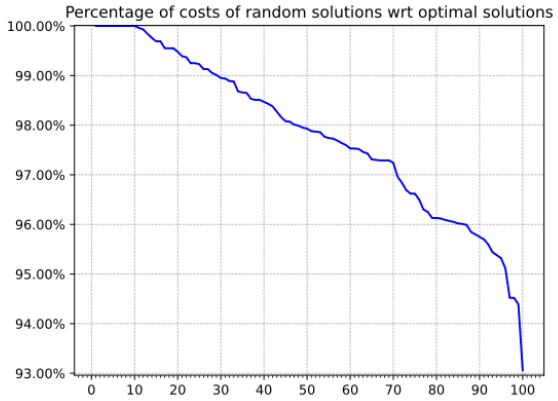
Main results: Cost of Random PoS solutions vs Optimal Solutions



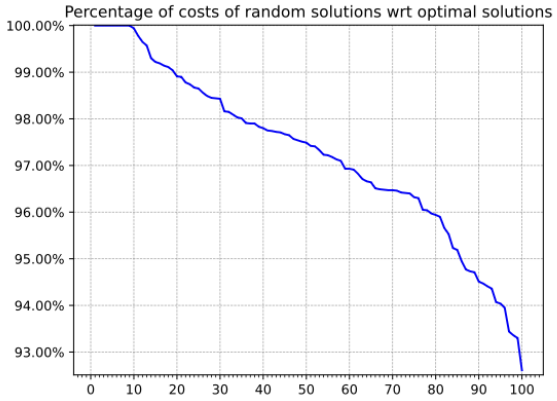
(a) $n = 5$ and $k = 3$



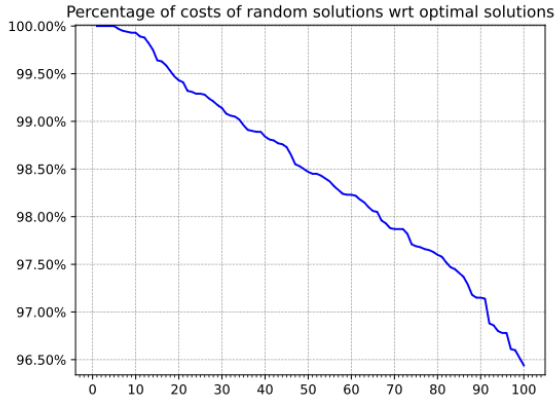
(b) $n = 6$ and $k = 3$



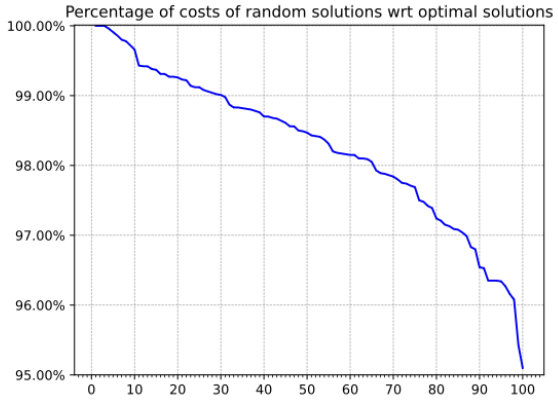
(c) $n = 7$ and $k = 3$



(d) $n = 8$ and $k = 3$



(e) $n = 9$ and $k = 3$



(f) $n = 10$ and $k = 3$

Effect of Circuit Depth

p	λ	# of optimal hybrid solutions	min % of hybrid vs. optimal solutions	# of optimal random solutions	min % of random vs. optimal solutions	Avg. time (s) for hybrid	Max. time (s) for hybrid	Time (s) brute force
2	2000	62	97.05%	7	92.12%	51.78	76.90	0.00026
3	2000	65	97.59%	11	92.65%	103.58	131.15	0.00027
4	2000	65	97.14%	13	91.90%	163.82	197.25	0.00027
5	2000	68	97.06%	10	91.99%	229.00	309.18	0.00027
6	2000	63	96.96%	5	92.43%	334.19	722.25	0.00037
7	2000	62	97.84%	11	92.92%	419.49	972.57	0.00026

Effect of Committee Size (n = 9)

k	λ	# of optimal hybrid solutions	min % of hybrid vs. optimal solutions	Avg. time (s) for hybrid	Max. time (s) for hybrid	Time (s) brute force
3	4000	39	98.19%	172.04	224.37	0.00044
4	4000	48	99.11%	175.06	218.35	0.00094
5	4000	39	99.09%	172.09	232.97	0.00133
6	4000	41	99.65%	175.41	244.16	0.00114

Conclusions, and directions for future work

Current constraints:

- Classical simulation time grows exponentially
- Simulating large networks is currently unfeasible

Future implementation:

- Real quantum hardware will resolve these circuits in milliseconds
- Zero-Knowledge (ZK) Proof of the QAOA execution will be stored on the blockchain to prevent provider cheating

Future algorithmic experiments:

- Explore variants of the QUBO formulation
- Solve with (simulators of) quantum annealers
- Compare with classical greedy algorithm
- Sensitivity analysis over $\alpha, \beta, \gamma, \lambda, p$
- Study density and structure of economic/geographic matrices

Thank you for your attention !

Gràtzias a totus po s'atentzione