Classical Verification of Quantum Learning

Marcel Hinsche

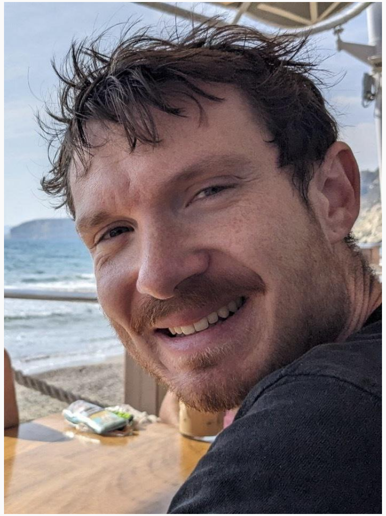
Freie Universität Berlin

Based on: arXiv:2306.04843

20/11/23 - QTML 2023

My collaborators

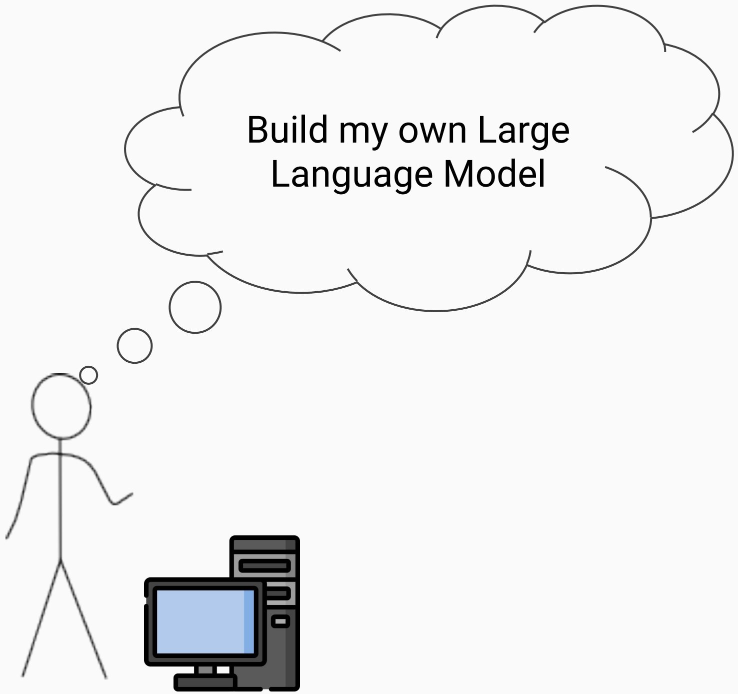
Matthias Caro

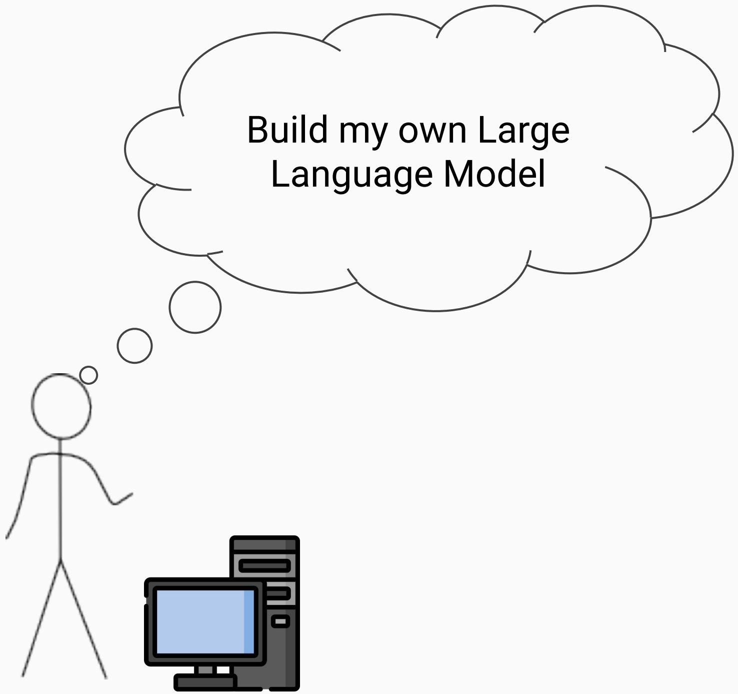


Marios Ioannou

Alexander Nietner

Ryan Sweke


Build my own Large Language Model

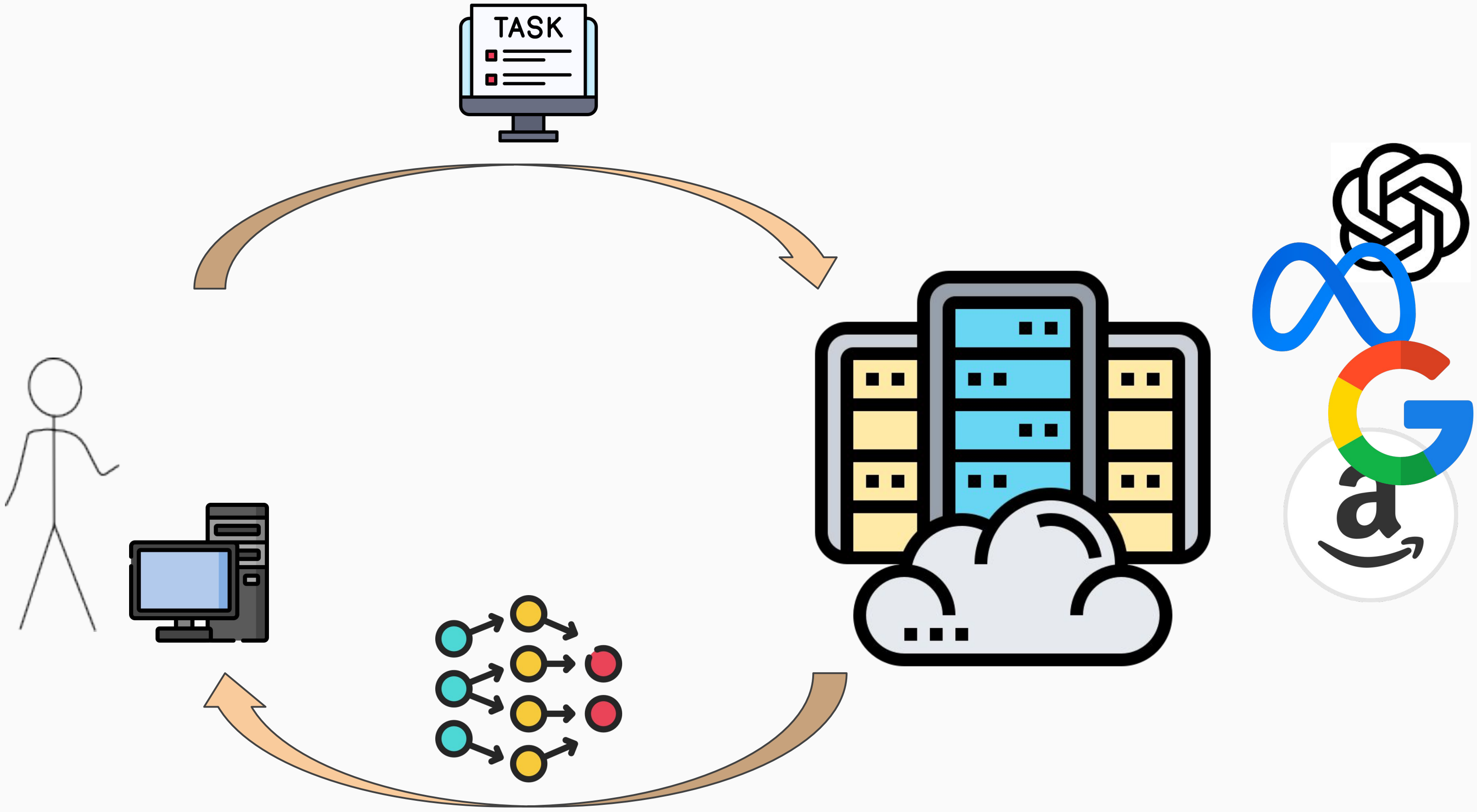


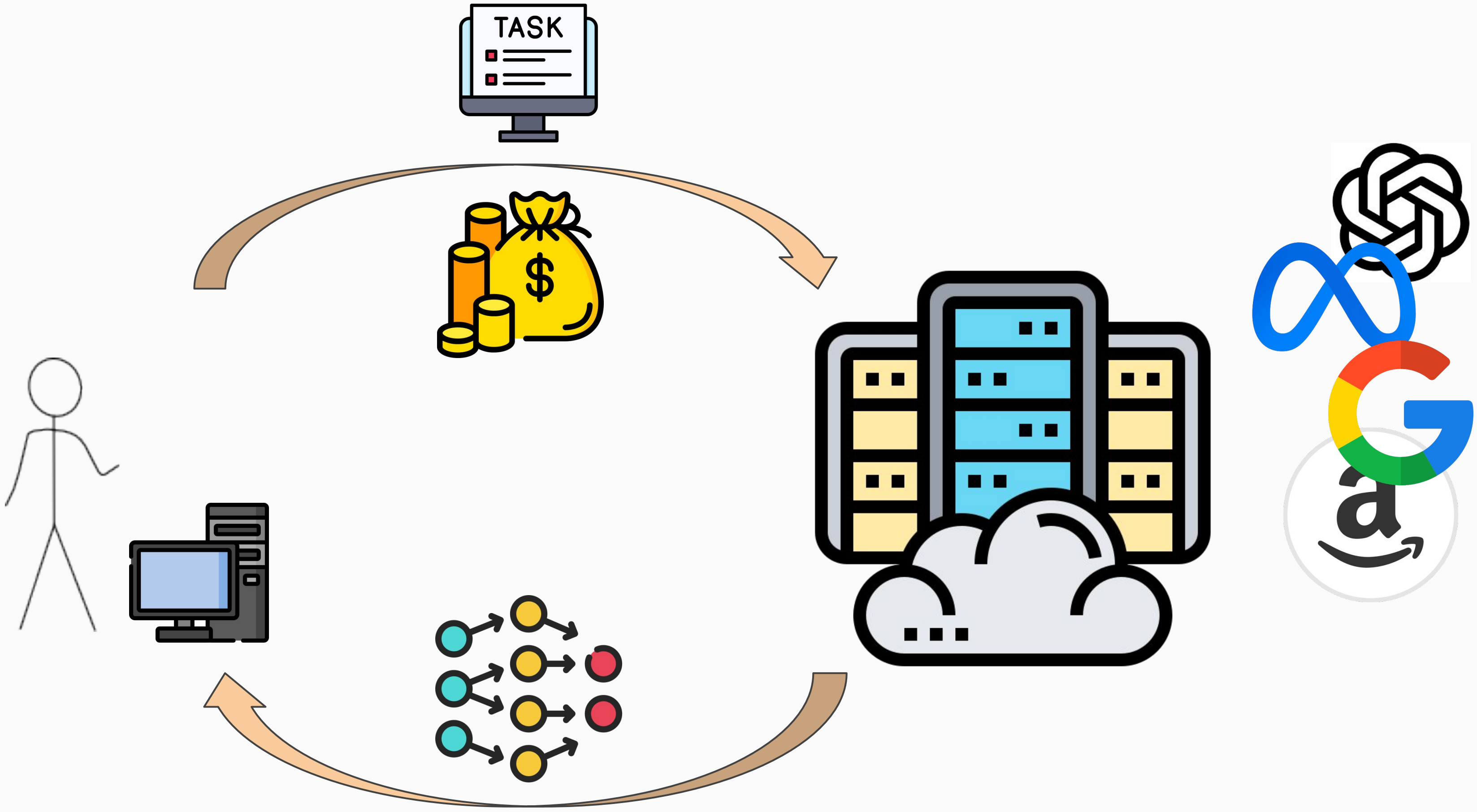
Limited amount of

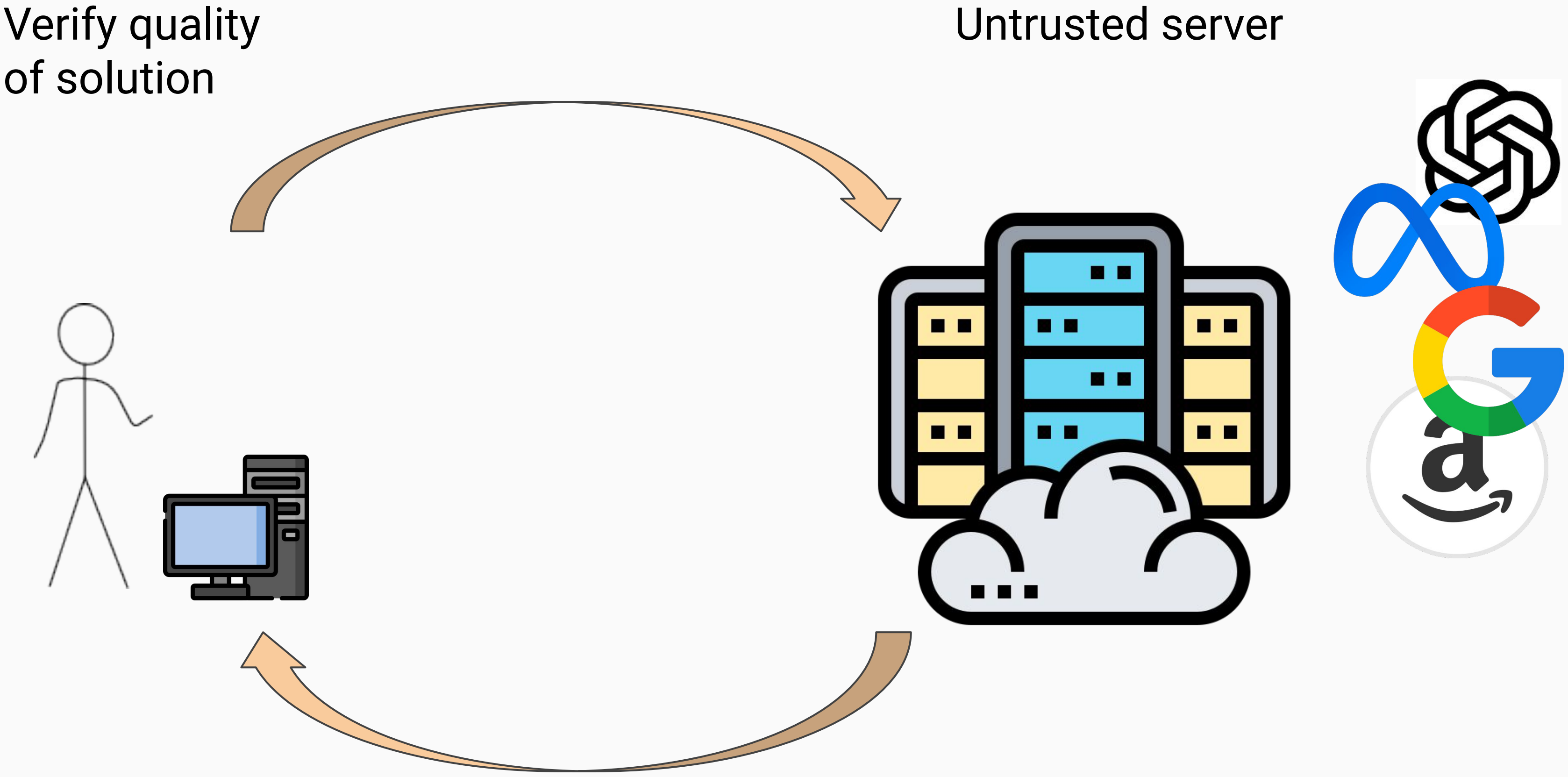
- high quality data
- compute
- expertise

More

- high-quality data
- compute
- expertise


TASK


TASK


Verify quality
of solution
Untrusted server

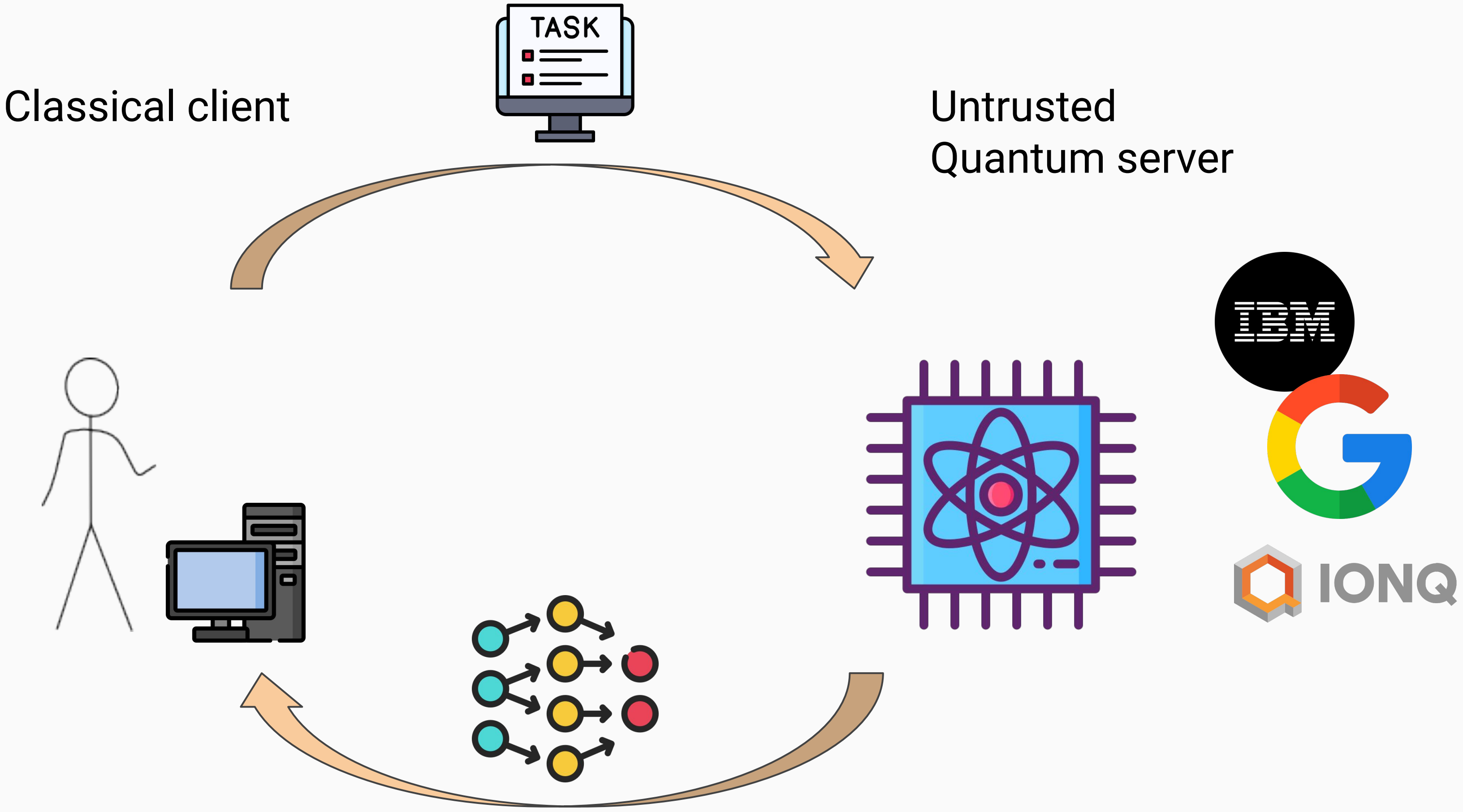
Verifying Classical Learning [1]

[1] Goldwasser et al.; ITCS 2021

“Can **verifying** be cheaper than **learning**?”

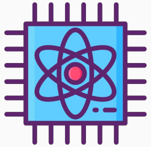
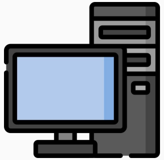
Main result: A problem such that

Cost[**verification**] << Cost[**learning**]


Classical client
TASK
Untrusted
Quantum server
IBM
IONQ

Our Work: Verifying Quantum Learning

Is there an ML problem such that

1. Learning requires a quantum computer 
2. Verification is possible with a classical computer? 

Main result: Yes, such a problem exists! 

Remark I - Other notions of delegation

This work:
Verification of
Quantum Learning

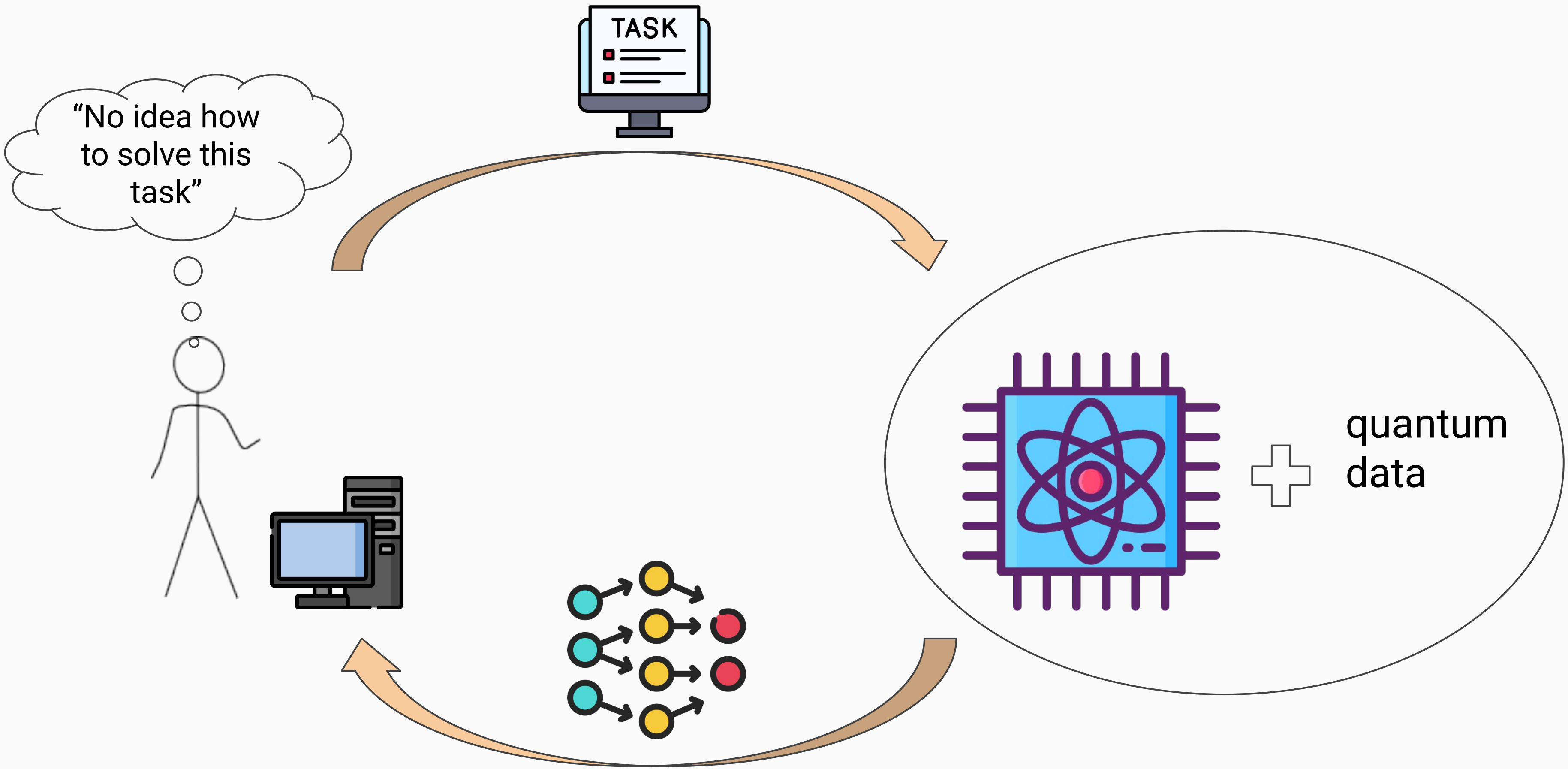
≠

Delegated quantum computing

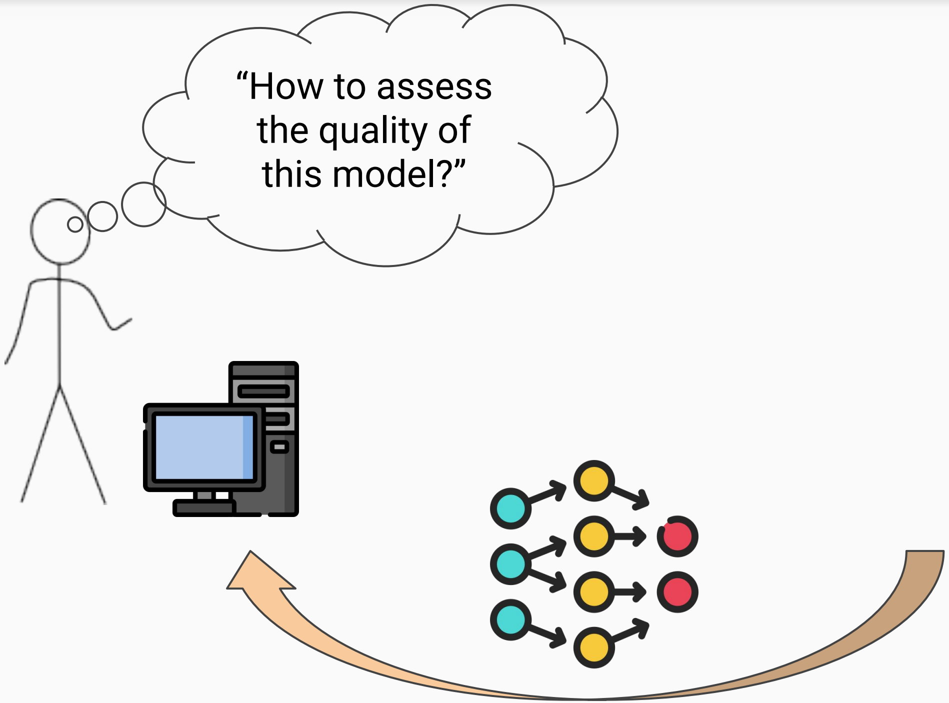
Blind quantum computing

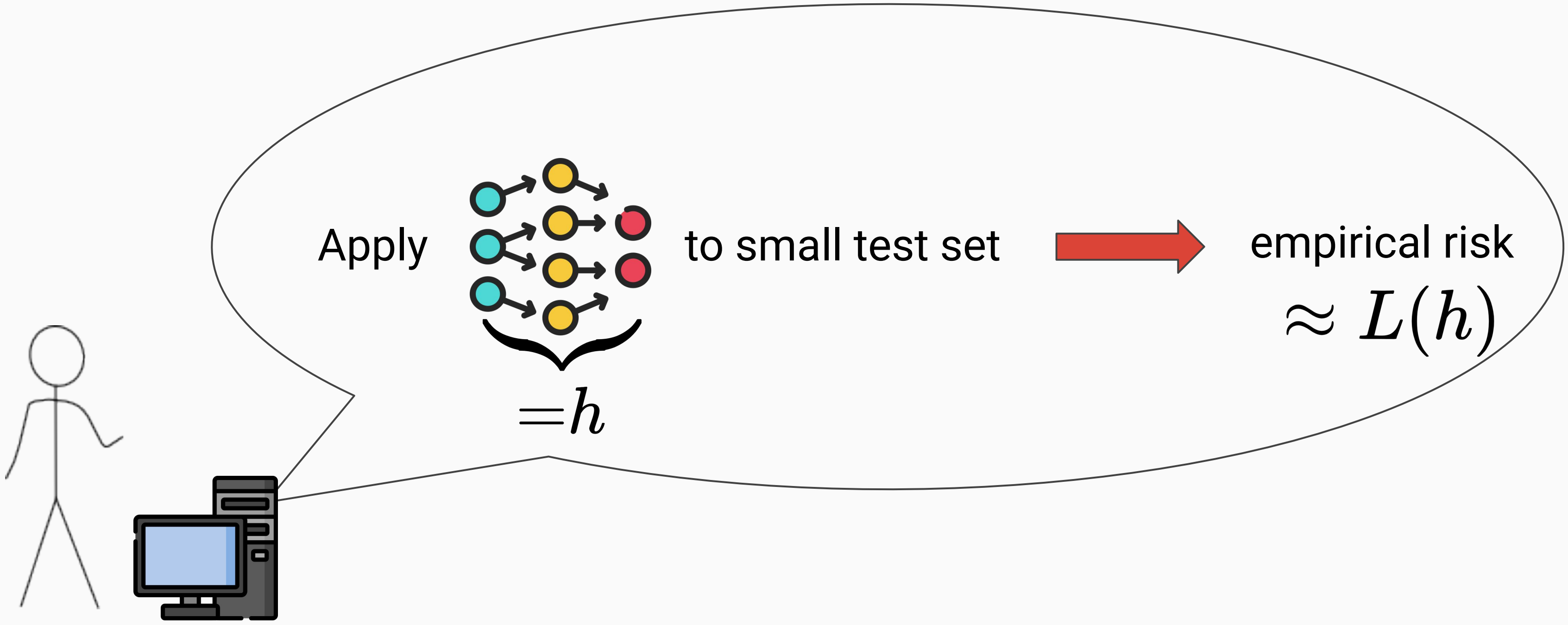
Classical Verification of Quantum Computation

Our work: Delegation of quantum **learning**



Remark II - How to measure quality?




Apply
to small test set
empirical risk
$\approx L(h)$
$=h$

Central challenge of verification

Compare to minimal risk:

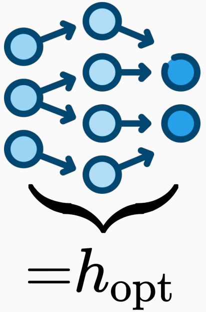
$$L(h_{\text{opt}})$$

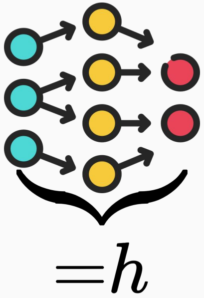
The measure of quality:

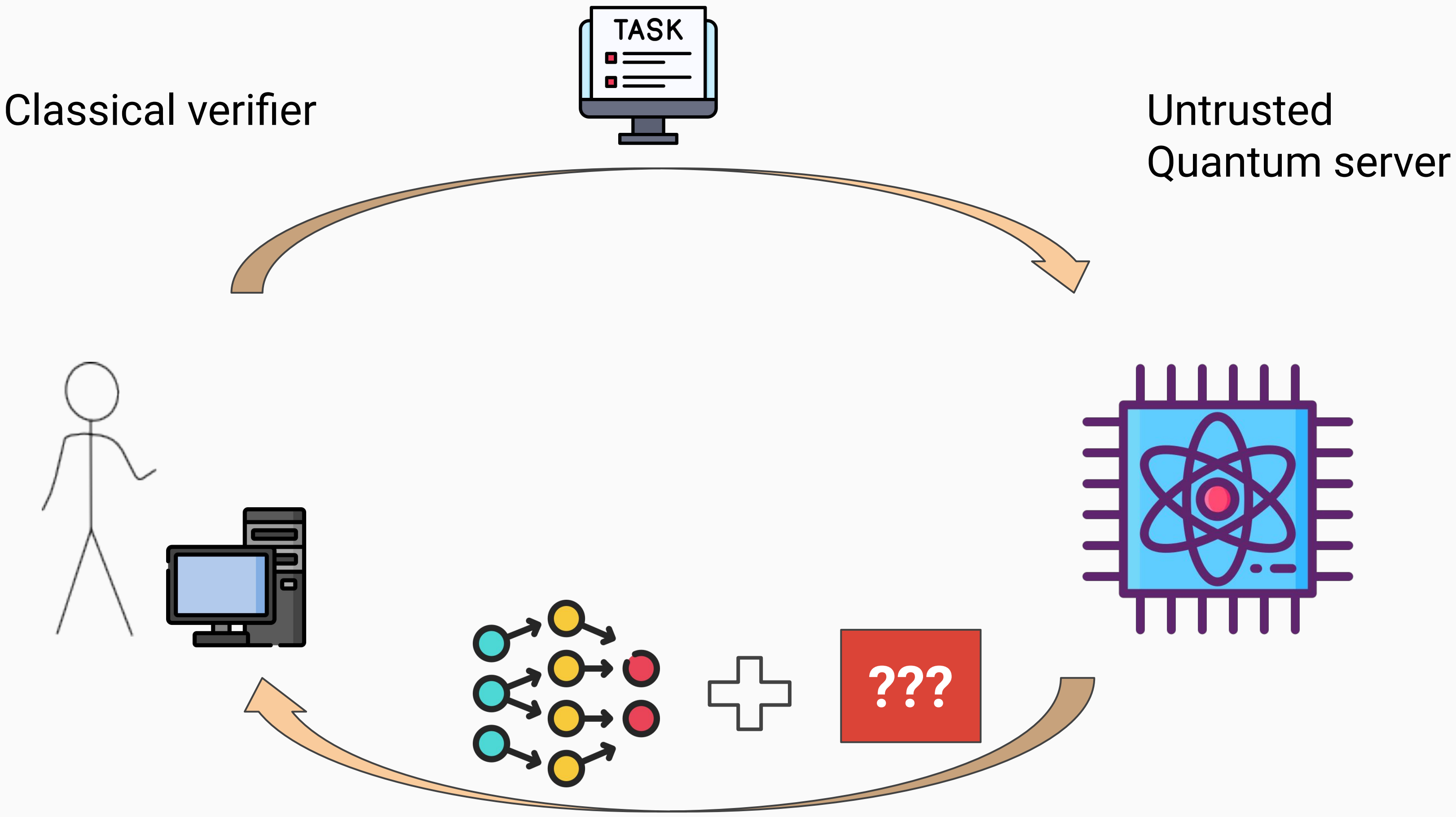
$$|L(h) - L(h_{\text{opt}})|$$

Problem with verification:

Client does not know $L(h_{\text{opt}})$

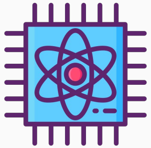
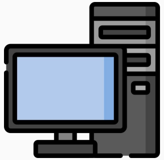





Classical verifier
TASK
Untrusted
Quantum server
???

Our Work: Verifying Quantum Learning

We show a learning problem such that

1. **Learning** requires a quantum computer 
2. **Verification** is possible with a classical computer 

Overview

- We work in the framework of agnostic PAC-learning
- We consider learning Boolean functions (≈ binary classification)

$$h : \{-1, 1\}^n \to \{-1, 1\}$$

- The concrete problem is **agnostic learning parities** under uniform distribution

$$h_S(x) = \prod_{i \in S} (-1)^{x_i}$$

Learning requires a quantum computer

Classical **hardness**:

Agnostic learning parities

≈

Learning parities with noise

believed to be hard classically

Learning requires a quantum computer

Classical **hardness**:

Agnostic learning parities

≈

Learning parities with noise

believed to be hard classically

Quantum easiness:

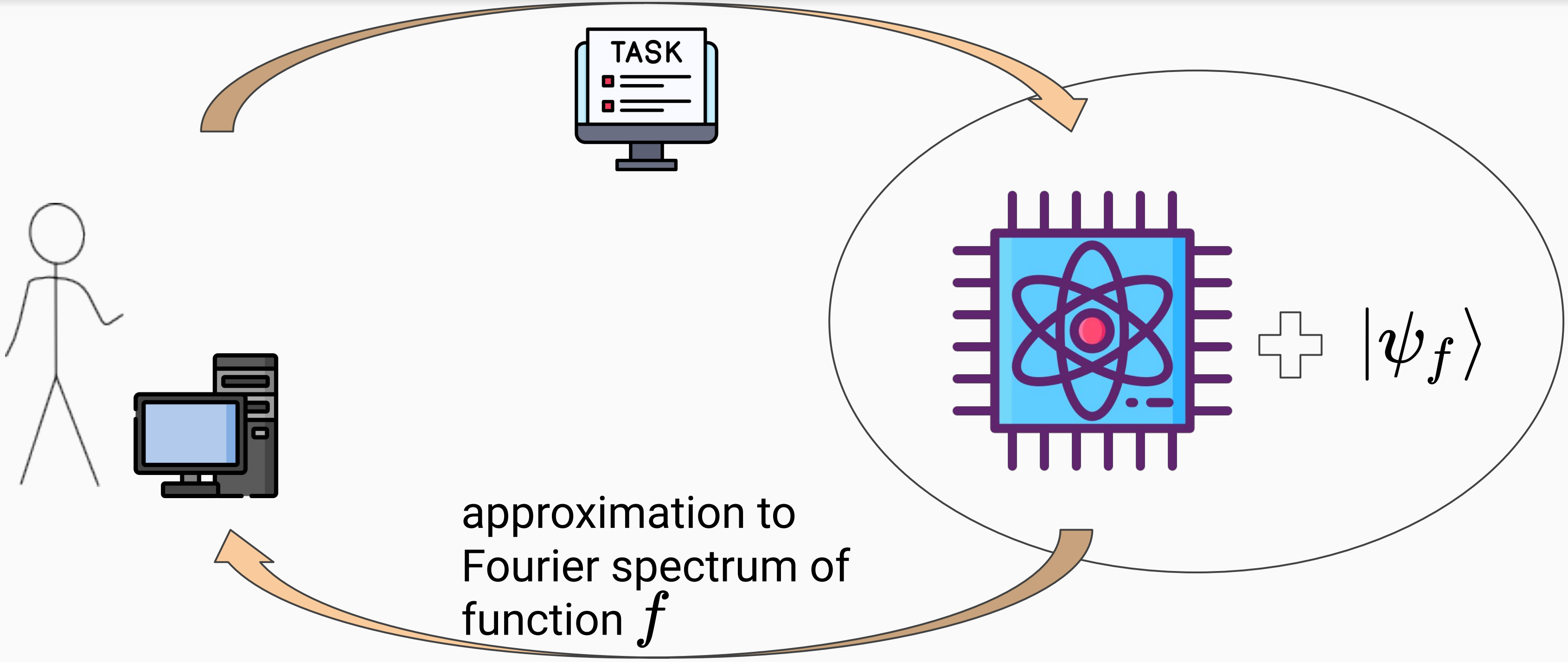
Quantum superposition oracle

$$|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x, f(x)\rangle$$

allows access to Fourier spectrum

→ can solve agnostic parity learning

Verification is possible with a classical computer



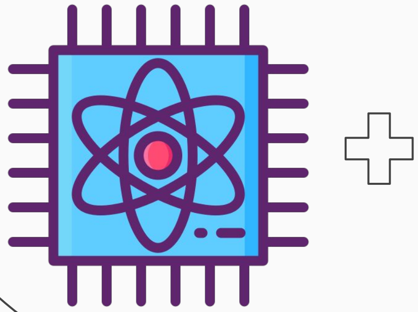
New proposal for quantum data access!

To tackle most general agnostic learning,

we introduce **Mixture-of-superpositions oracle**

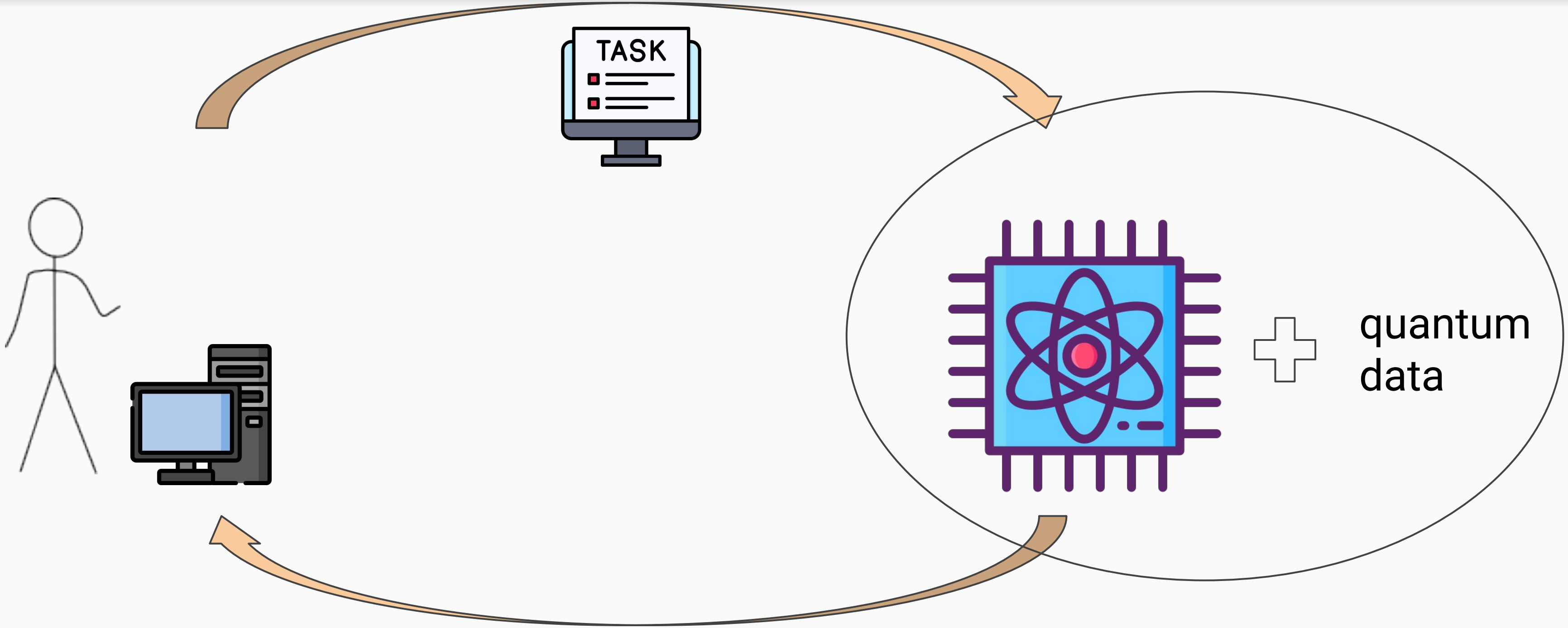
$$\rho_{\mathcal{D}} = \mathbb{E}_f \left[|\psi_f\rangle\langle\psi_f| \right]$$

where $|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x, f(x)\rangle$



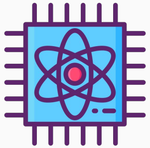
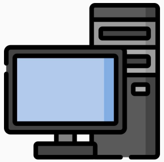
quantum data

Summary



Main result

Proof-of-principle demonstration of an agnostic learning problem where

1. Learning requires a quantum computer 
2. Verification is possible with a classical computer 

Future research

Is your favorite QML problem classically verifiable?