Suggestions for building quantum programs

Harold Ollivier

2022-03-31

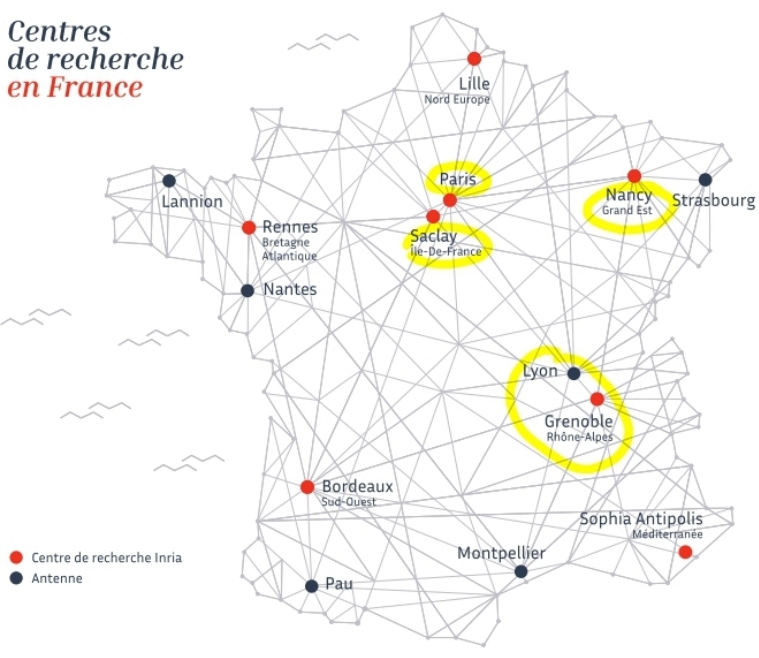
Séminaire TQCI

Overview of QuantumTech@INRIA

Overview of QuantumTech@INRIA

Timeline

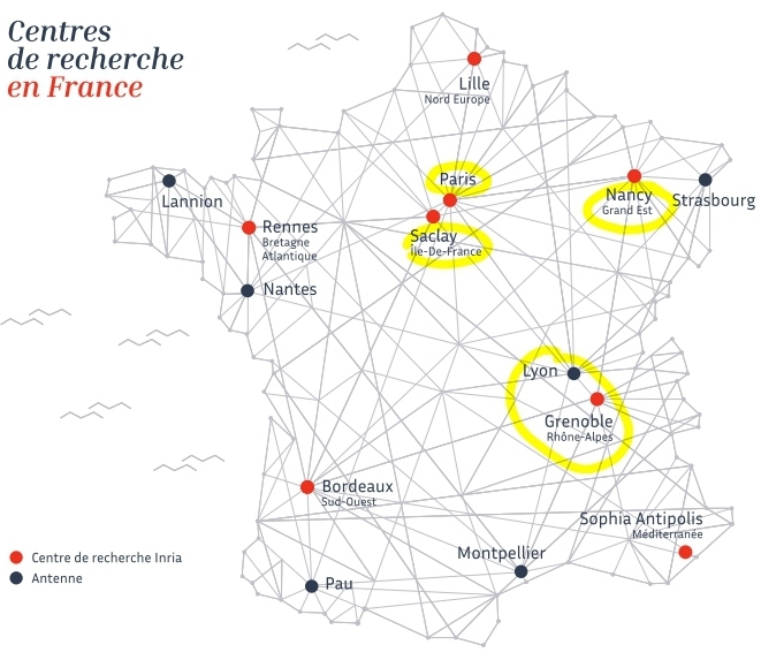
- Started in 2001
- Since 2018, the number of permanent researchers has doubled
- 2020: 5 new PIs
- 2021: 4 new PIs
- 5 Active teams
- 2 are being created



Overview of QuantumTech@INRIA

Timeline

- Started in 2001
- Since 2018, the number of permanent researchers has doubled
- 2020: 5 new PIs
- 2021: 4 new PIs
- 5 Active teams
- 2 are being created



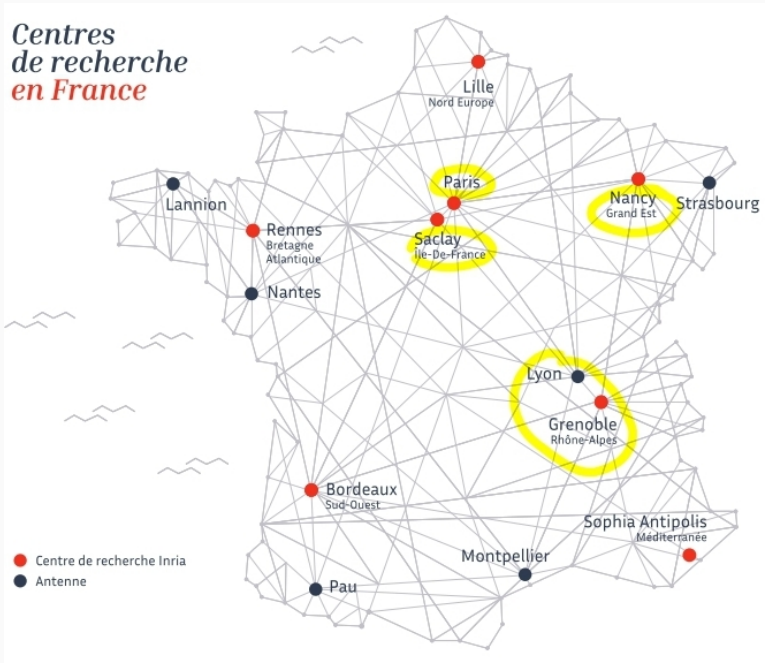
Main topics

- Controlling qubits
- Error correction and fault-tolerance
- Compilation / Languages
- Cryptography (q. & post q., cryptanalysis)
- Quantum information theory

Overview of QuantumTech@INRIA

Timeline

- Started in 2001
- Since 2018, the number of permanent researchers has doubled
- 2020: 5 new PIs
- 2021: 4 new PIs
- 5 Active teams
- 2 are being created



Main topics

- Controlling qubits
- Error correction and fault-tolerance
- Compilation / Languages
- Cryptography (q. & post q., cryptanalysis)
- Quantum information theory

Action plan

- Spread the word internally (Defi EQIP)
- Keep increasing the workforce
- Extend our coverage (architectures and applications)

Suggestions for building quantum programs

(Simplified) overview of QC development status

Dealing with (un)certainties

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup
- It will still take time ($>$ 5-10yrs) to get FTQC

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup
- It will still take time ($>$ 5-10yrs) to get FTQC
- Need to rethink algorithms

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup
- It will still take time ($>$ 5-10yrs) to get FTQC
- Need to rethink algorithms
- NISQ machines are available

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup
- It will still take time ($>$ 5-10yrs) to get FTQC
- Need to rethink algorithms
- NISQ machines are available
- Few guarantees are available for NISQ compatible algorithms

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup
- It will still take time ($>$ 5-10yrs) to get FTQC
- Need to rethink algorithms
- NISQ machines are available
- Few guarantees are available for NISQ compatible algorithms

What does it mean for end-users?

(Simplified) overview of QC development status

Dealing with (un)certainties

- Fault-tolerant QC provide speedup
- It will still take time ($>$ 5-10yrs) to get FTQC
- Need to rethink algorithms
- NISQ machines are available
- Few guarantees are available for NISQ compatible algorithms

What does it mean for end-users?

- We don't know when nor by how much QC will be useful

(Simplified) approach to quantum programs

A single (not so simple) objective

(Simplified) approach to quantum programs

A single (not so simple) objective

- Computing an ROI for QC investments should be the main objective of quantum programs

(Simplified) approach to quantum programs

A single (not so simple) objective

- Computing an ROI for QC investments should be the main objective of quantum programs
  - When do we have breakeven performance?

(Simplified) approach to quantum programs

A single (not so simple) objective

- Computing an ROI for QC investments should be the main objective of quantum programs
  - When do we have breakeven performance?
  - How much is gained past breakeven performance?

(Simplified) approach to quantum programs

A single (not so simple) objective

- Computing an ROI for QC investments should be the main objective of quantum programs
  - When do we have breakeven performance?
  - How much is gained past breakeven performance?

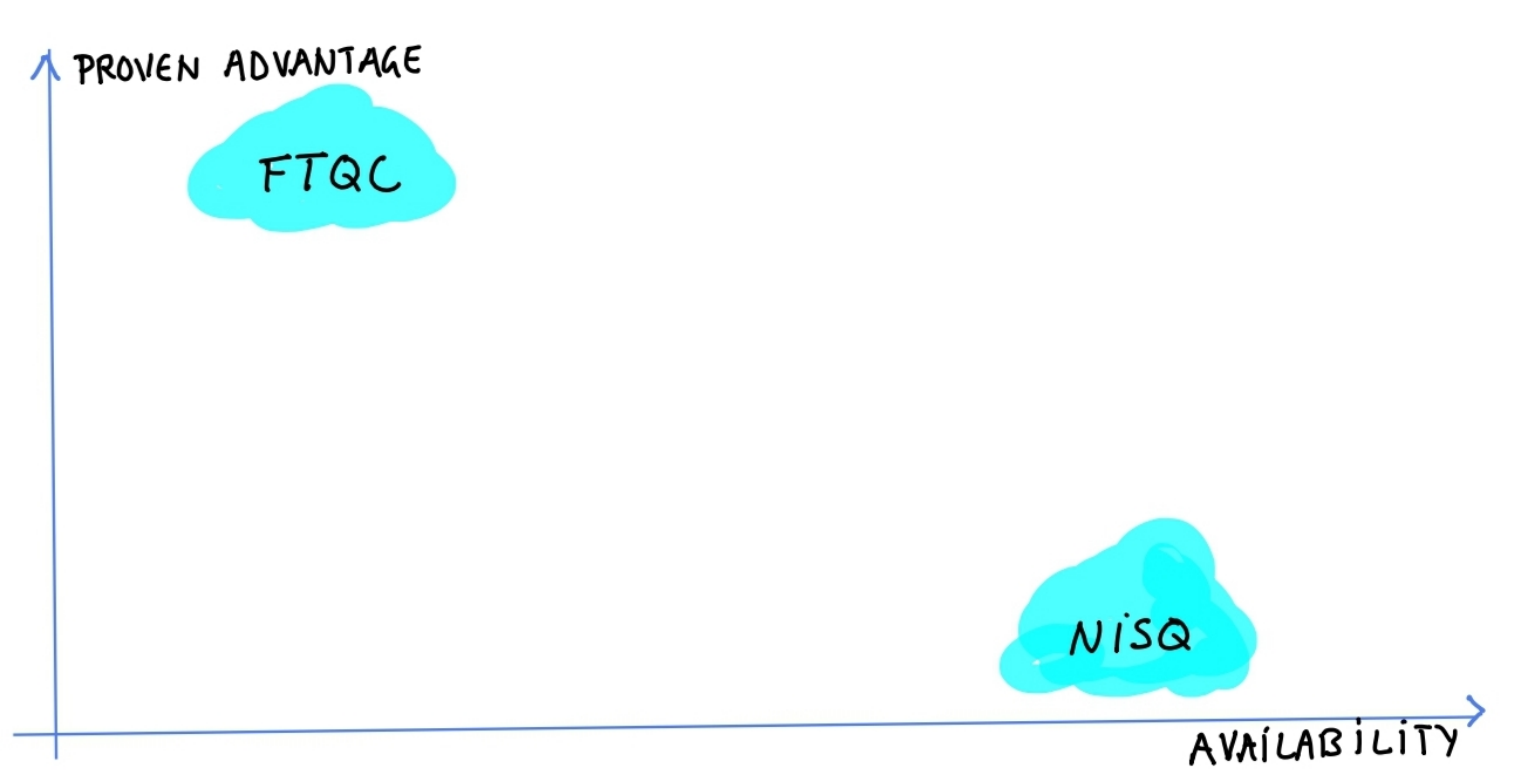
The national quantum strategy is no exception

(Simplified) approach to quantum programs

A single (not so simple) objective

- Computing an ROI for QC investments should be the main objective of quantum programs
  - When do we have breakeven performance?
  - How much is gained past breakeven performance?

The national quantum strategy is no exception

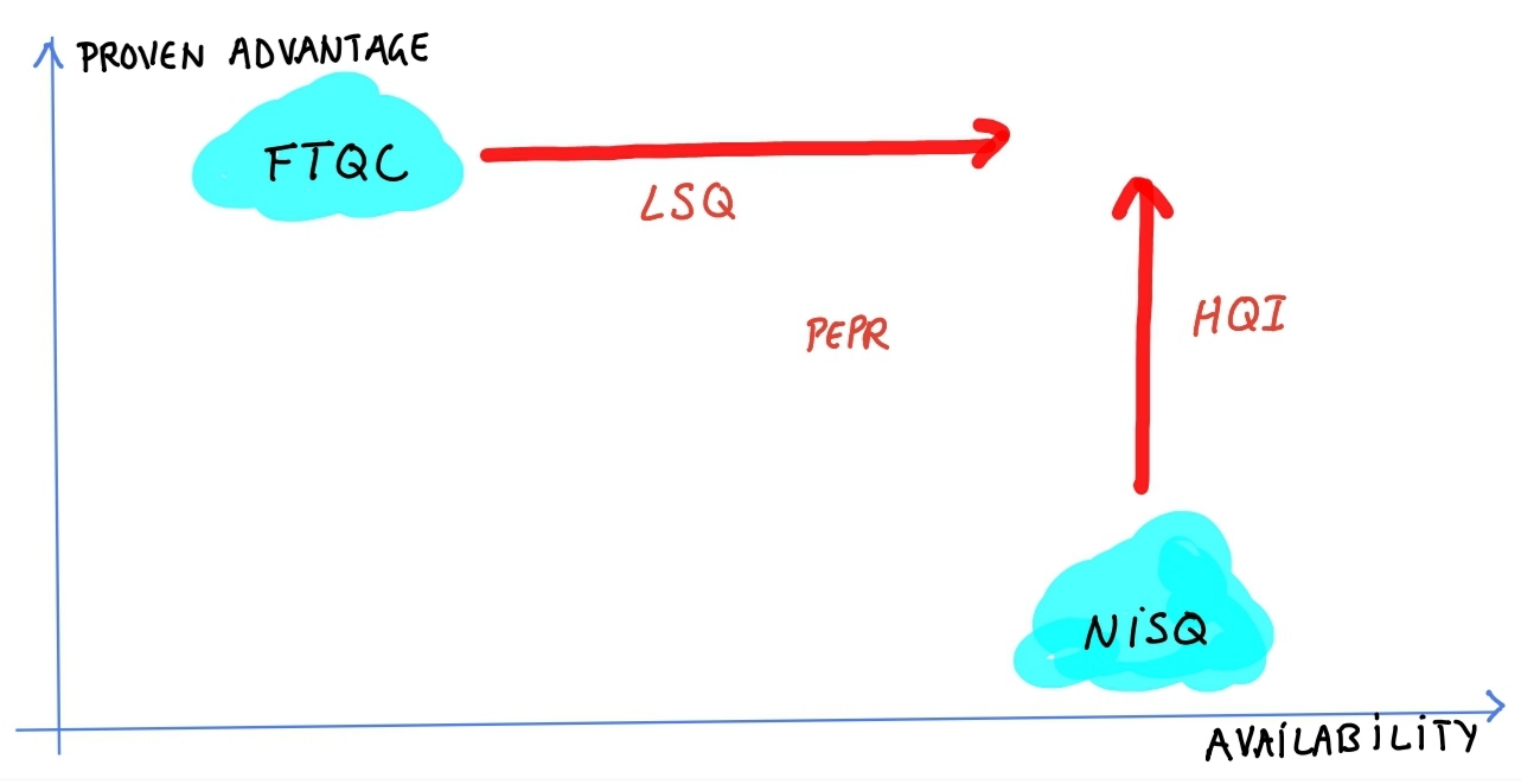


(Simplified) approach to quantum programs

A single (not so simple) objective

- Computing an ROI for QC investments should be the main objective of quantum programs
  - When do we have breakeven performance?
  - How much is gained past breakeven performance?

The national quantum strategy is no exception



What can be done?

Building expertise

Building expertise

Why

- Linking external knowledge to internal know-how

Building expertise

Why

- Linking external knowledge to internal know-how
- Know where to look for quantum advantage
  - Smaller datasets
  - Quantum data...

Building expertise

Why

- Linking external knowledge to internal know-how
- Know where to look for quantum advantage
  - Smaller datasets
  - Quantum data...
- Bring value out of proof of concepts
  - Do I reduce the uncertainty about when performance is at breakeven and/or how much will be gained?

Building expertise

Why

- Linking external knowledge to internal know-how
- Know where to look for quantum advantage
  - Smaller datasets
  - Quantum data...
- Bring value out of proof of concepts
  - Do I reduce the uncertainty about when performance is at breakeven and/or how much will be gained?

How

- Public events (Hackathons) allow to have a quick look at the field

Building expertise

Why

- Linking external knowledge to internal know-how
- Know where to look for quantum advantage
  - Smaller datasets
  - Quantum data...
- Bring value out of proof of concepts
  - Do I reduce the uncertainty about when performance is at breakeven and/or how much will be gained?

How

- Public events (Hackathons) allow to have a quick look at the field
- Small dedicated team able to interact with academia and/or service providers

Building expertise

Why

- Linking external knowledge to internal know-how
- Know where to look for quantum advantage
  - Smaller datasets
  - Quantum data...
- Bring value out of proof of concepts
  - Do I reduce the uncertainty about when performance is at breakeven and/or how much will be gained?

How

- Public events (Hackathons) allow to have a quick look at the field
- Small dedicated team able to interact with academia and/or service providers
- Find partners that are aligned with your interests

Building expertise

Why

- Linking external knowledge to internal know-how
- Know where to look for quantum advantage
  - Smaller datasets
  - Quantum data...
- Bring value out of proof of concepts
  - Do I reduce the uncertainty about when performance is at breakeven and/or how much will be gained?

How

- Public events (Hackathons) allow to have a quick look at the field
- Small dedicated team able to interact with academia and/or service providers
- Find partners that are aligned with your interests
- Value is created with longer projects

Building commitment

Building commitment

Why

- It's a long journey: difficult to answer to the question "how much can be gained?"
  - Understanding where improvements can be made in existing workflows
  - Understanding what are the requirements on the machines to bring concrete advantage

Building commitment

Why

- It's a long journey: difficult to answer to the question "how much can be gained?"
  - Understanding where improvements can be made in existing workflows
  - Understanding what are the requirements on the machines to bring concrete advantage

How

- Look for algorithmic choices and improvements in existing workflows
  - expensive but might bring gains before QC / identify building blocks that could be possibly be replaced by Q Algorithms

Building commitment

Why

- It's a long journey: difficult to answer to the question "how much can be gained?"
  - Understanding where improvements can be made in existing workflows
  - Understanding what are the requirements on the machines to bring concrete advantage

How

- Look for algorithmic choices and improvements in existing workflows
  - expensive but might bring gains before QC / identify building blocks that could be possibly be replaced by Q Algorithms
- Go for PoC, simulations, analytic x simulations to get an sense of required parameter sets

Short focus on making the best out of PoCs

Step-by-step approach

Methodology

1. Survey existing approaches
2. Which ones are the most profitables for the program
3. Adapt to real hardware
4. Study requirements for obtaining the required functionality / advantage

Step-by-step approach

Methodology

1. Survey existing approaches
2. Which ones are the most profitables for the program
3. Adapt to real hardware
4. Study requirements for obtaining the required functionality / advantage

Practice

1. Applications for quantum networks

Protocol Library

Functionality	Protocols
Anonymous Transmission	GHZ-based Quantum Anonymous Transmission
	Verifiable Quantum Anonymous Transmission
Authentication of Classical Messages	Uncloneable Encryption
Authentication of Quantum Messages	Purity Testing based Quantum Authentication
	Polynomial Code based Quantum Authentication
	Clifford Code for Quantum Authentication
	Trap Code for Quantum Authentication
	Auth-QFT-Auth Scheme for Quantum Authentication
	Unitary Design Scheme for Quantum Authentication
	Naive approach using Quantum Teleportation
Byzantine Agreement	Fast Quantum Byzantine Agreement

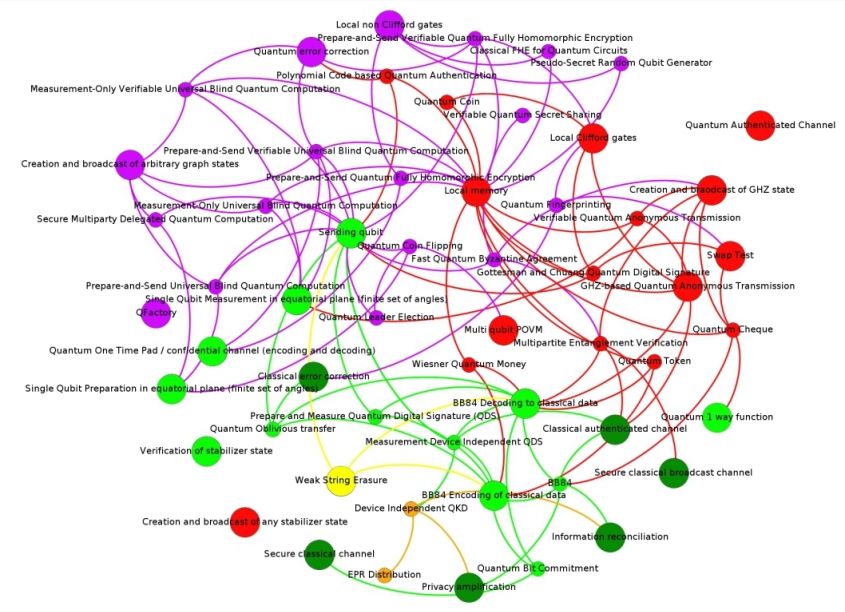
Step-by-step approach

Methodology

1. Survey existing approaches
2. Which ones are the most profitables for the program
3. Adapt to real hardware
4. Study requirements for obtaining the required functionality / advantage

Practice

1. Applications for quantum networks
2. Deconstruction and routines analysis



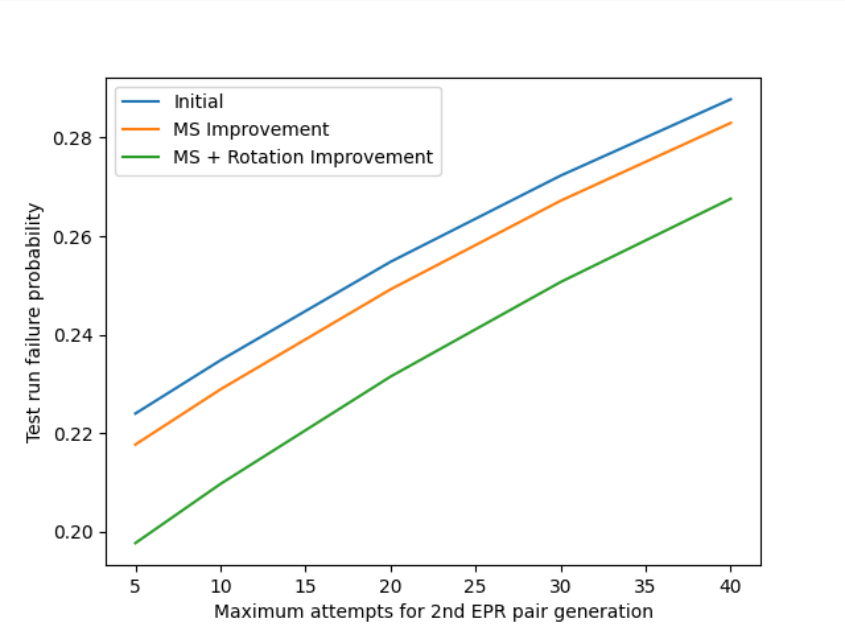
Step-by-step approach

Methodology

1. Survey existing approaches
2. Which ones are the most profitables for the program
3. Adapt to real hardware
4. Study requirements for obtaining the required functionality / advantage

Practice

1. Applications for quantum networks
2. Deconstruction and routines analysis
3. Complete protocol rewriting



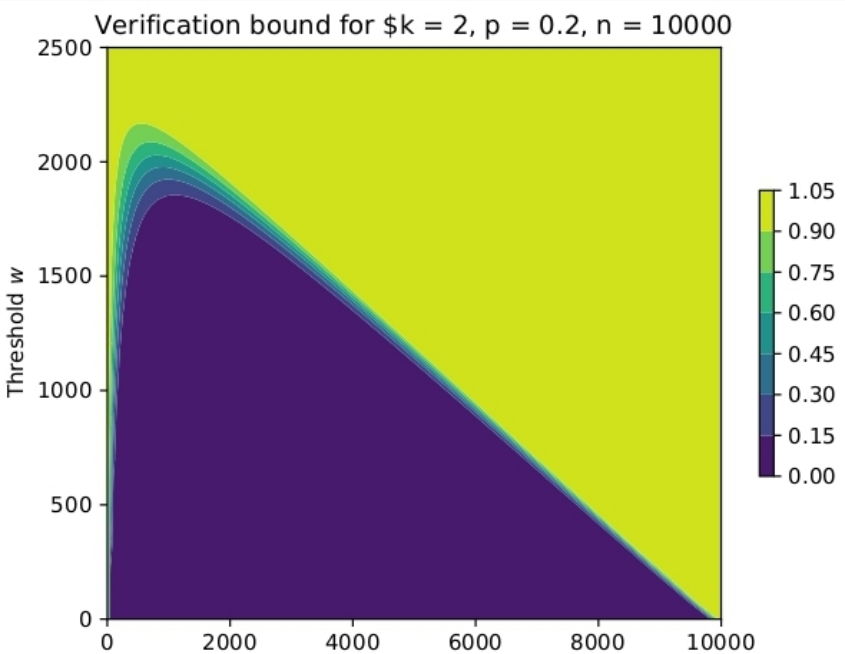
Step-by-step approach

Methodology

1. Survey existing approaches
2. Which ones are the most profitables for the program
3. Adapt to real hardware
4. Study requirements for obtaining the required functionality / advantage

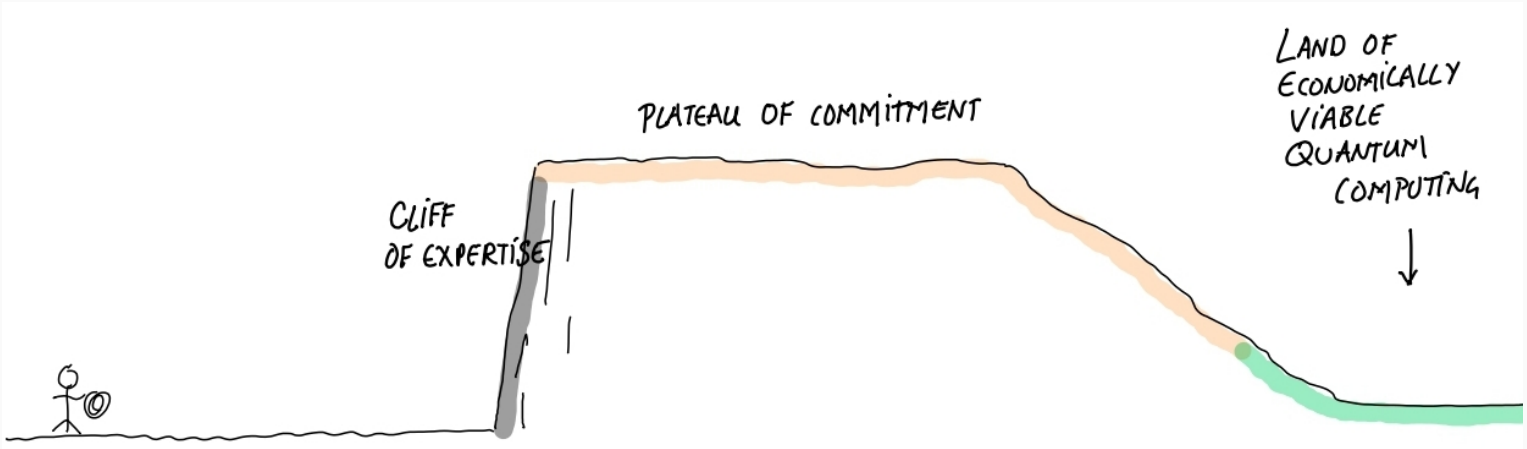
Practice

1. Applications for quantum networks
2. Deconstruction and routines analysis
3. Complete protocol rewriting
4. Overhead analysis and requirements to get functionning PoC

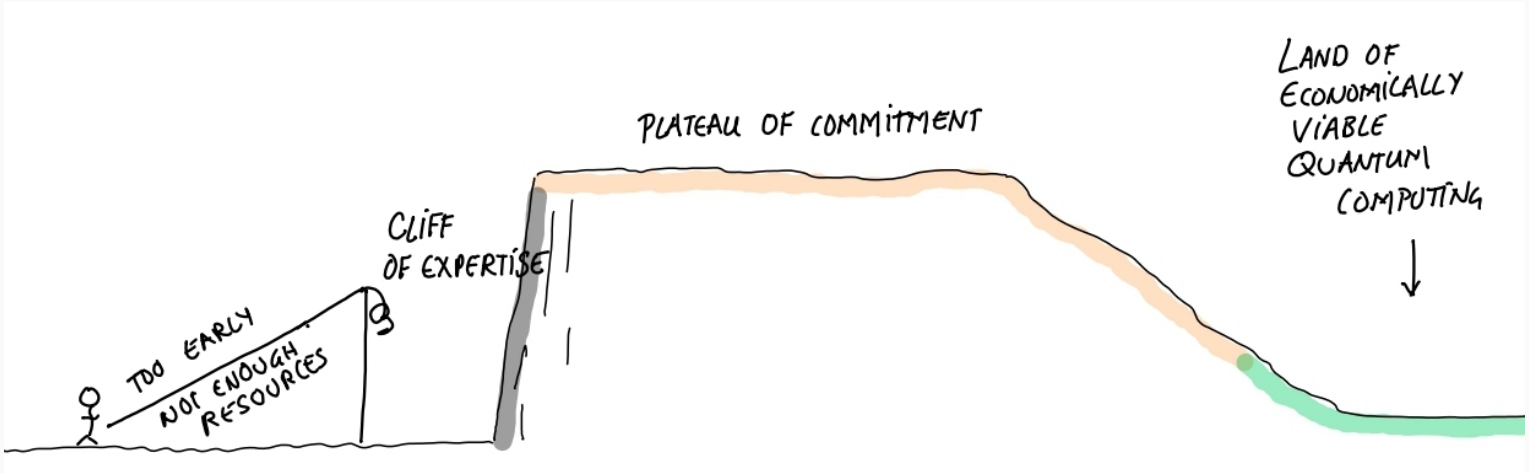


When to start?

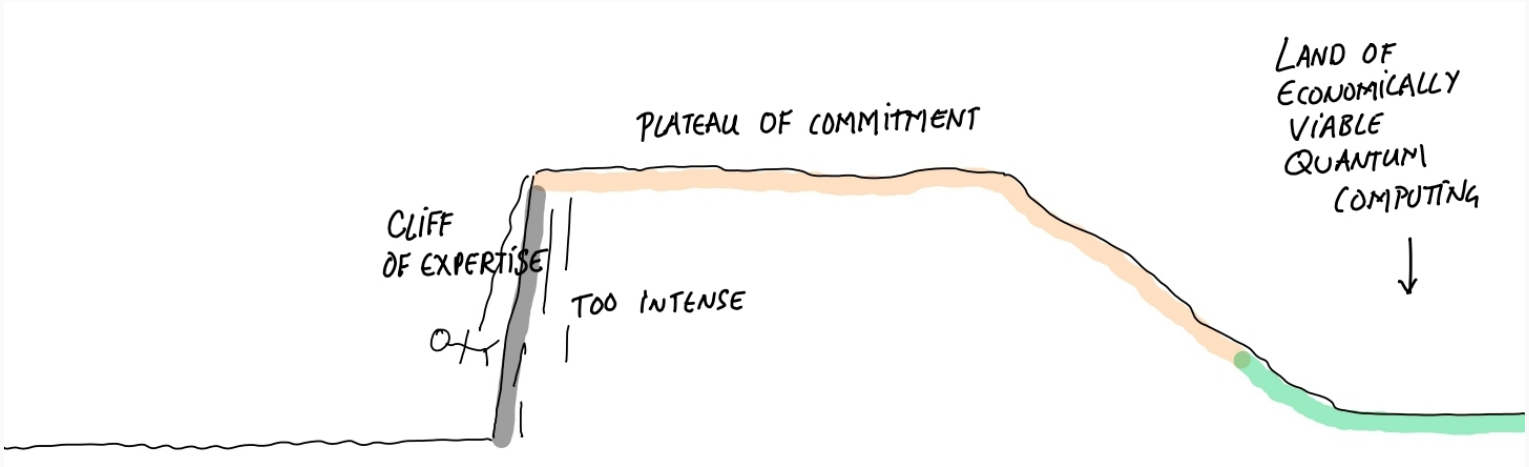
Well in advance, but think that you need to keep the motivation high for a long time



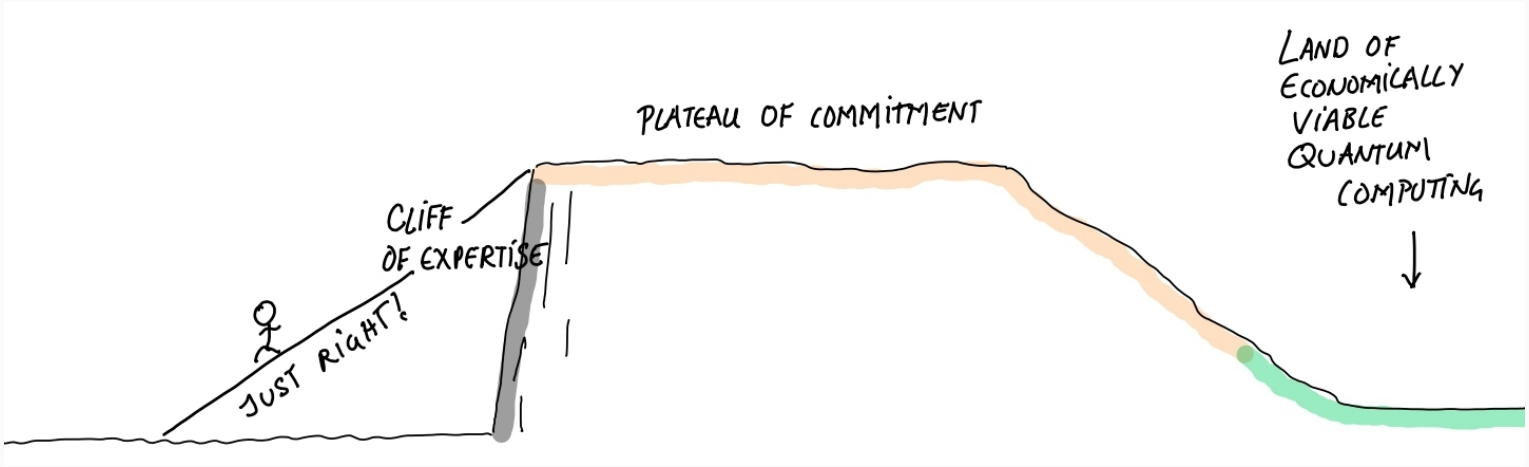
Well in advance, but think that you need to keep the motivation high for a long time



Well in advance, but think that you need to keep the motivation high for a long time



Well in advance, but think that you need to keep the motivation high for a long time



Thank you