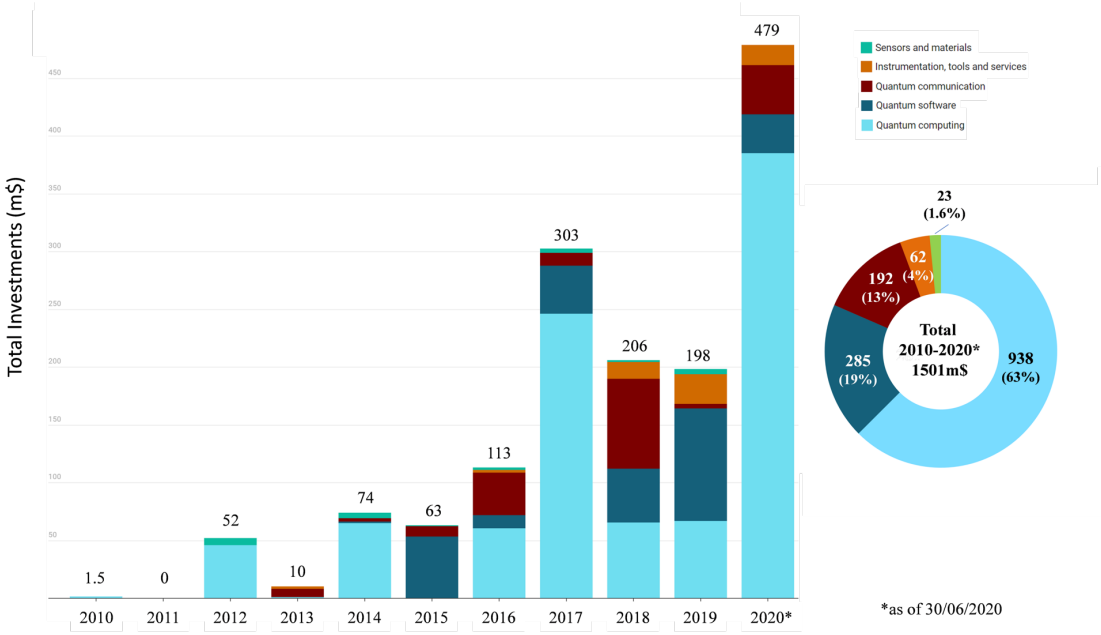
Quantum Communication Challenges in Scaling Quantum Computers

Sam Samuel
Director of Engineering ET&I
June 2022

Quantum “X” (why now?)

There is no doubt that there is investment interest in Quantum Startups

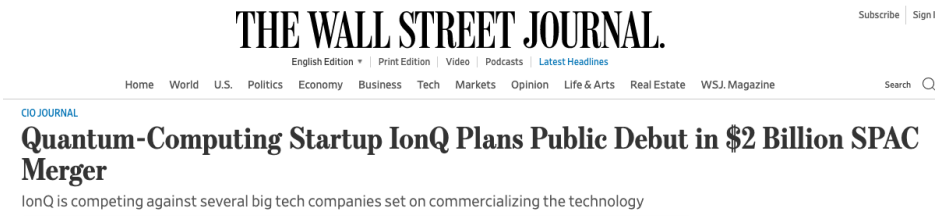


Total: $1.5B

Quantum Computing Hardware: $950M

Quantum Software: $300M

Quantum Communication/Internet: $200M


THE WALL STREET JOURNAL.

Subscribe | Sign I

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine Search

CIO JOURNAL

Quantum-Computing Startup IonQ Plans Public Debut in $2 Billion SPAC Merger

IonQ is competing against several big tech companies set on commercializing the technology

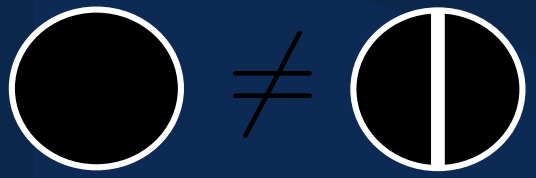
What is Quantum Computing?

Superposition (of qubits)

classical
0100110101

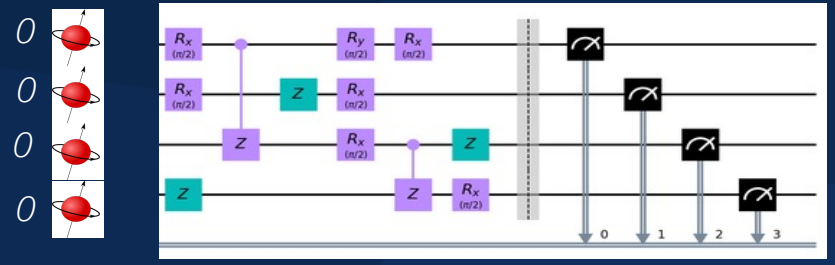
quantum
$$p_0 0000000000$$
$$+p_1 0000000001$$
$$+p_2 0000000010$$
$$\bullet\ \bullet\ \bullet$$
$$+p_{2^N} 1111111111$$

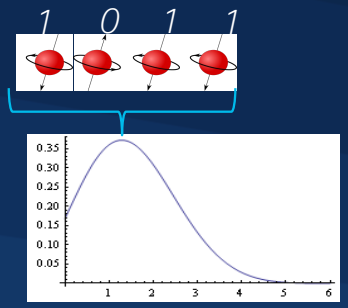
Entanglement (strange correlations)



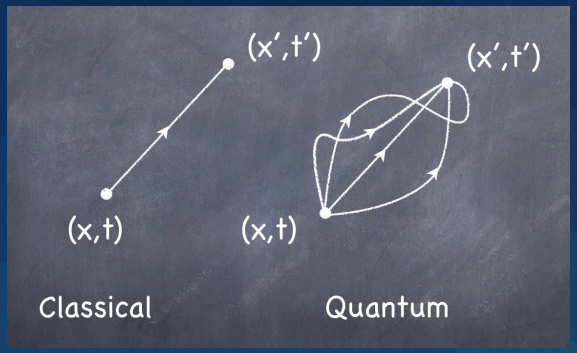
We know the state of the system as a whole, not the individual pieces

Quantum circuits are probabilistic in nature





A quantum computer explores all possible configurations. Simultaneously!



What are the possible implications?

Potential Problem … or Opportunity

Quantum Computer potency follows a double exponential law on the number of Qubits

Generation	0	1	2	3	4	5	…	N
Exponential E.g. Moore's Law (2^G)	1	2	4	8	16	32	…	2^N
Double Exponential E.g. Nevin's Law (2^{2^G})	2	4	16	256	65546	~4.3*10^9	…	2^{2^N}

Hartmut Neven: Observed that quantum computers are gaining computational power at a doubly-exponential rate

Shor's algorithm does comply with Neven's law

If Quantum Computing delivers on its promise then there could be a threat to the security of a network

In Practical Terms

… It is a matter of time before Quantum Impacts us

AES key-length k	RSA Bits	Elliptic Curve (bits length)	Notes
48	480	96	**DO NOT USE (trivial)**
50	512		
56	640	112	Advised against
62	768		
64	816	128	
73	1024		Caution – well funded criminal gangs
80	1248	160	
89	1536		
103	2048		Nation state ?
112	2432	224	
128	3248 (or 3072)	256	2030's
160	5312 (or 4096)	320	Beyond 2030's
192	7936 (or 7680)	384	
256	15424 (or 15360)	512	

Neven's Law

Quantum acceleration?

Do we see this as a threat or an opportunity?

In Practical Terms

… It is a matter of time before Quantum Impacts us

AES key-length k	RSA Bits	Elliptic Curve (bits length)	Notes
48	480	96	**DO NOT USE (trivial)**
50	512		
56	640	112	Advised against
62	768		
64	816	128	
73	1024		Caution – well funded criminal gangs
80	1248	160	
89	1536		
103	2048		Nation state ?
112	2432	224	
128	3248 (or 3072)	256	2030's
160	5312 (or 4096)	320	Beyond 2030's
192	7936 (or 7680)	384	
256	15424 (or 15360)	512	

Impacted by Shor's algorithm

Probably OK

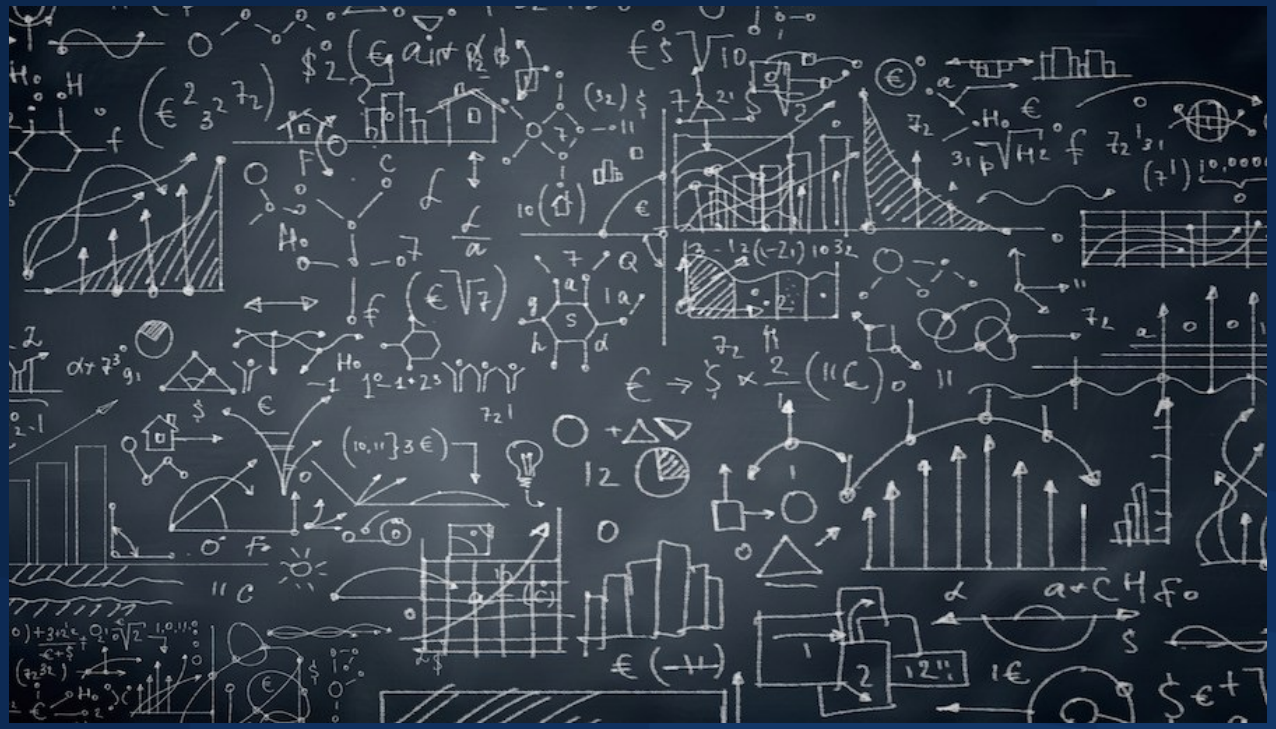
OK

Not OK – Impacts any key exchange

Neven's Law

Quantum acceleration?

Or, we can use it to solve really complex problems …

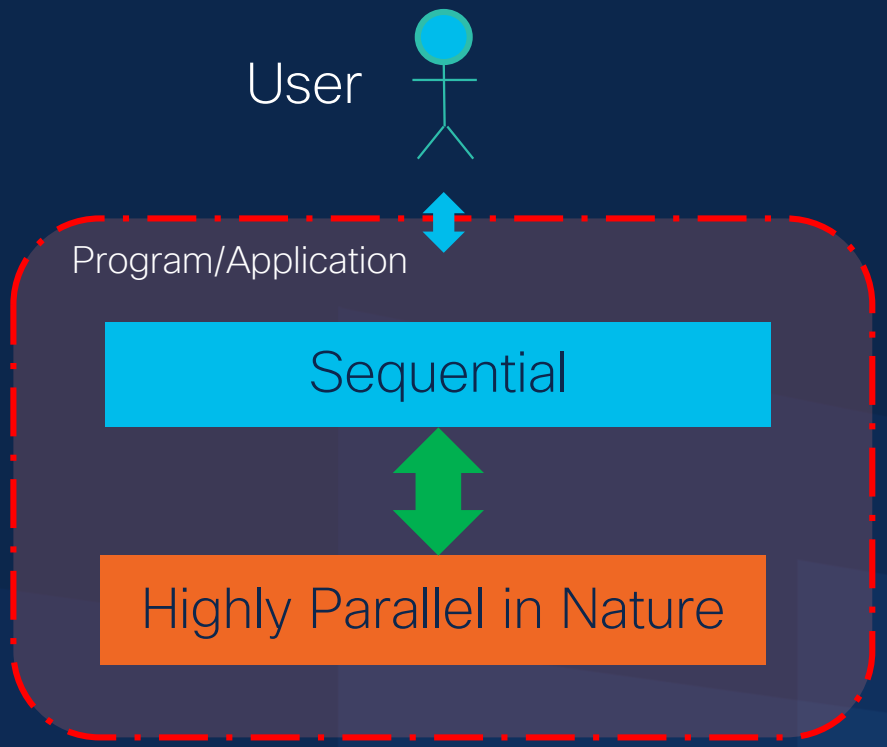


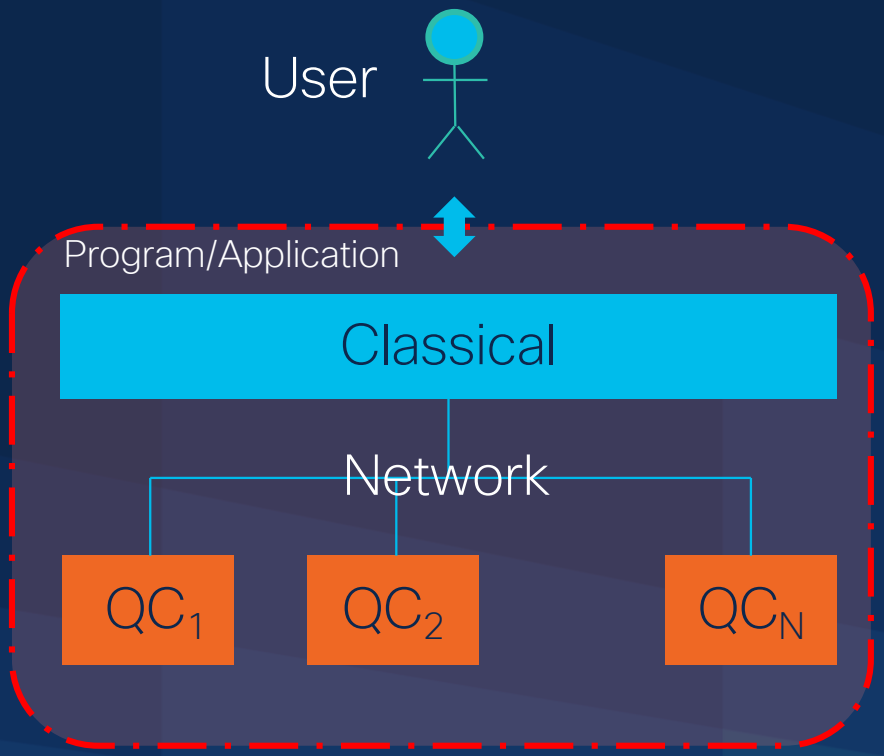
= ?

Stating the obvious ...

You can always join computers together to make a bigger computer

… And applications can be distributed too





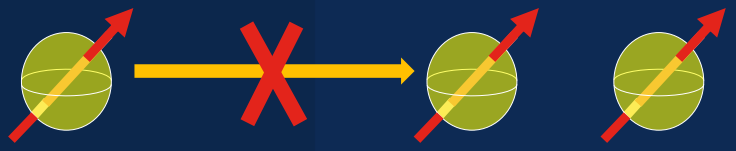
Different types of Quantum Computer are good at different things

Some new concepts for communications

Quantum State and No Cloning

A **quantum state** is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a system.

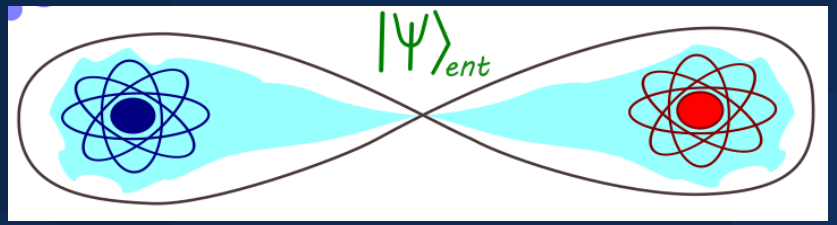
There is a "**No cloning**" theorem



A quantum state cannot be measured nor copied without the state being destroyed

Entanglement

A term to describe the quantum state of two or more particles that cannot be described independently from each other



Entangled particles separated by a great distance remain entangled (Einstein's "spooky action at distance")

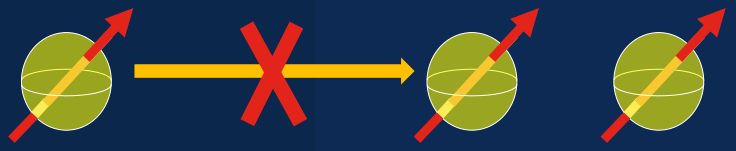
Different kind of particles (matter or flying qubit) can be entangled together

Some new concepts for communications

Quantum State and No Cloning

A **quantum state** is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a system.

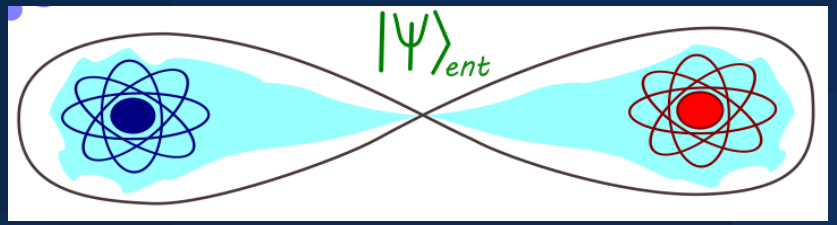
There is a "**No cloning**" theorem



A quantum state cannot be measured nor copied without the state being destroyed

Entanglement

A term to describe the quantum state of two or more particles that cannot be described independently from each other

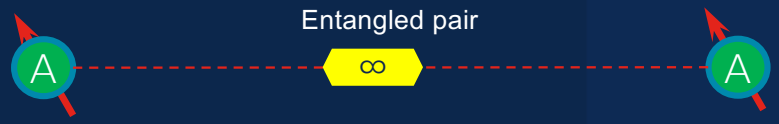


Entangled particles separated by a great distance remain entangled (Einstein's "spooky action at distance")

Different kind of particles (matter or flying qubit) can be entangled together

Teleporting: the alternative for long distance transmission

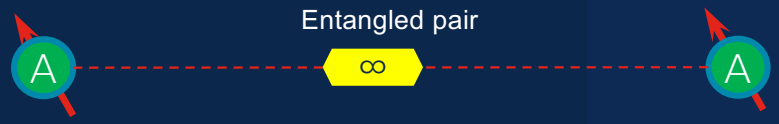
Assuming we can generate two remote entangled particles in particular state "Maximally entangled Bell state" (EPR pairs)



quantum physics enables the possibility to transfer (teleport) a quantum state via local operations and transmissions of 2 classical bits

Teleporting: the alternative for long distance transmission

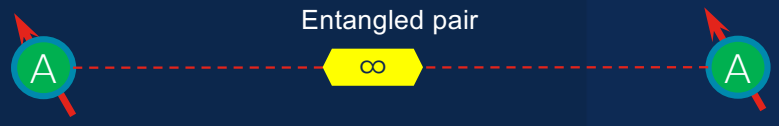
Assuming we can generate two remote entangled particles in particular state “Maximally entangled Bell state” (EPR pairs)



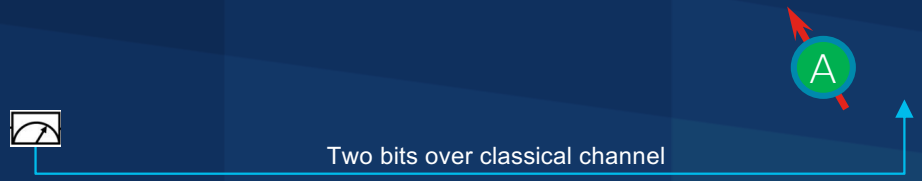
quantum physics enables the possibility to transfer (teleport) a quantum state via local operations and transmissions of 2 classical bits

Teleporting: the alternative for long distance transmission

Assuming we can generate two remote entangled particles in particular state “Maximally entangled Bell state” (EPR pairs)

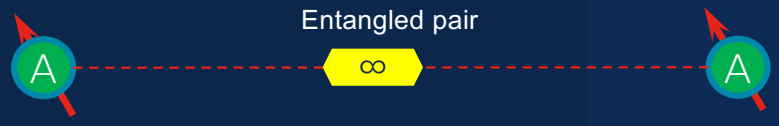


quantum physics enables the possibility to transfer (teleport) a quantum state via local operations and transmissions of 2 classical bits



Teleporting: the alternative for long distance transmission

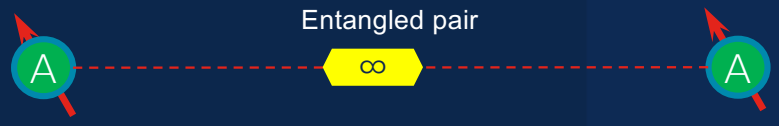
Assuming we can generate two remote entangled particles in particular state “Maximally entangled Bell state” (EPR pairs)



quantum physics enables the possibility to transfer (teleport) a quantum state via local operations and transmissions of 2 classical bits

Teleporting: the alternative for long distance transmission

Assuming we can generate two remote entangled particles in particular state “Maximally entangled Bell state” (EPR pairs)

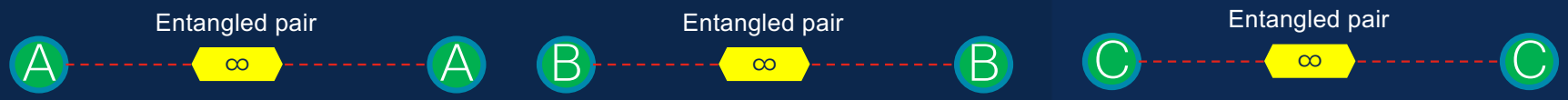


quantum physics enables the possibility to transfer (teleport) a quantum state via local operations and transmissions of 2 classical bits

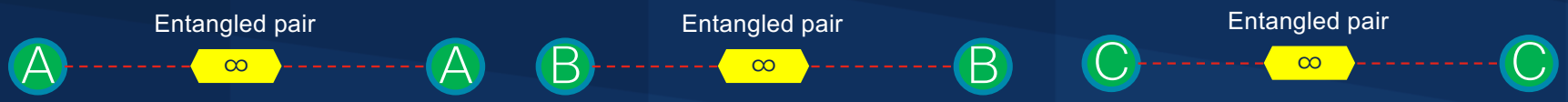
Communication

Entanglement swapping enables teleporting qubit over distance

Once we have multiple maximally entangled pair segments,

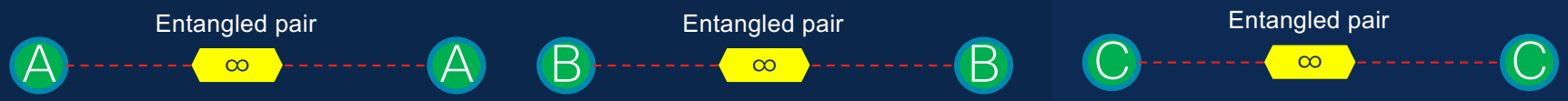


it is possible to get end to end entanglement via local operation and classical trasmission.



Entanglement swapping enables teleporting qubit over distance

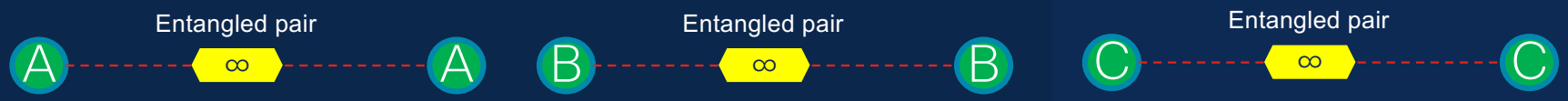
Once we have multiple maximally entangled pair segments,



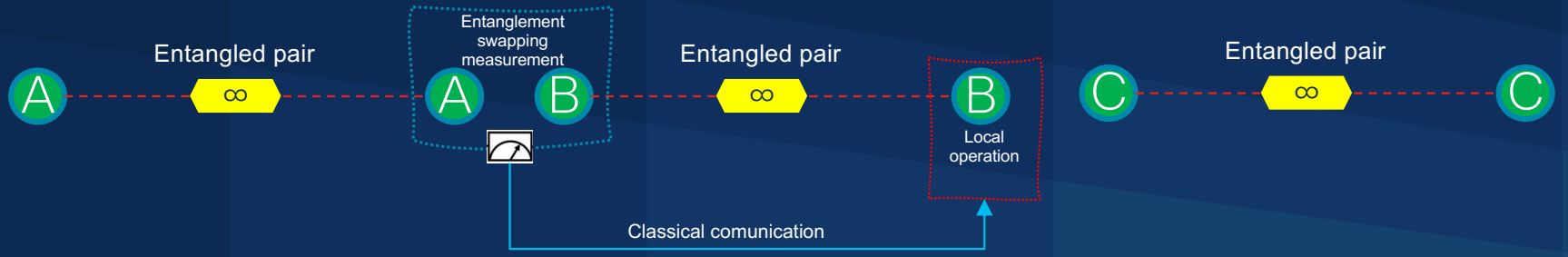
it is possible to get end to end entanglement via local operation and classical trasmission.

Entanglement swapping enables teleporting qubit over distance

Once we have multiple maximally entangled pair segments,

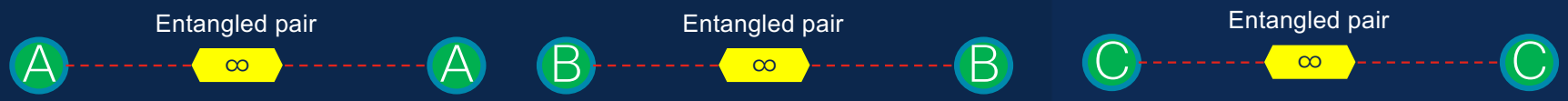


it is possible to get end to end entanglement via local operation and classical trasmission.

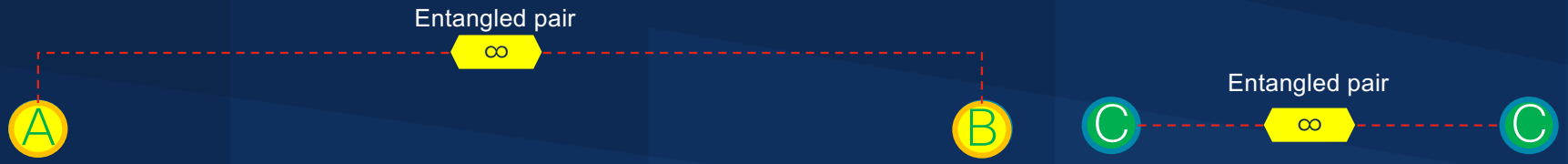


Entanglement swapping enables teleporting qubit over distance

Once we have multiple maximally entangled pair segments,

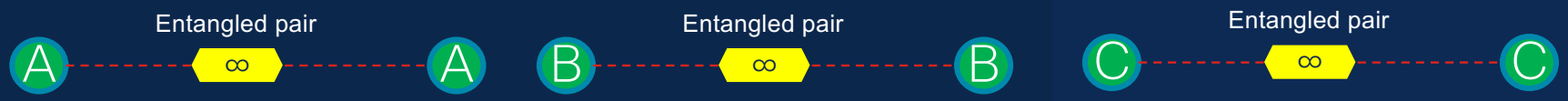


it is possible to get end to end entanglement via local operation and classical trasmission.

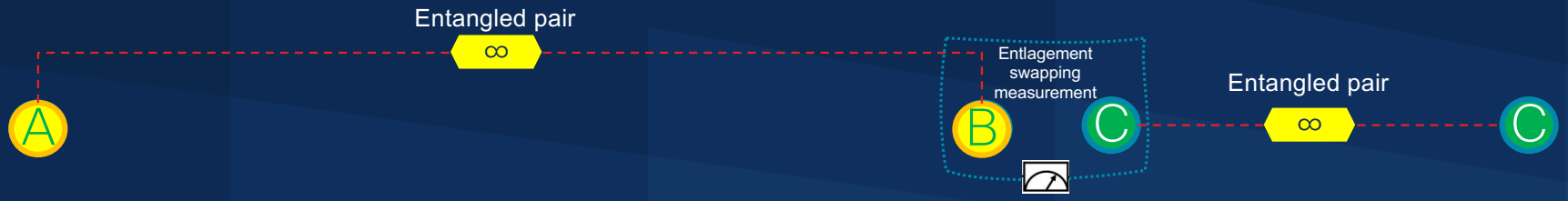


Entanglement swapping enables teleporting qubit over distance

Once we have multiple maximally entangled pair segments,

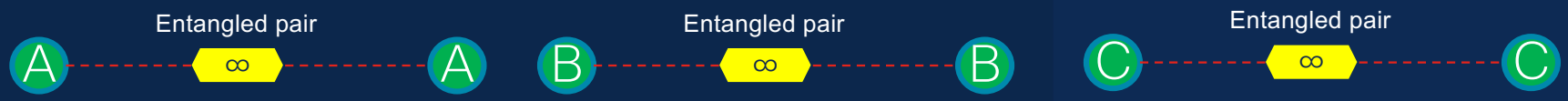


it is possible to get end to end entanglement via local operation and classical trasmission.

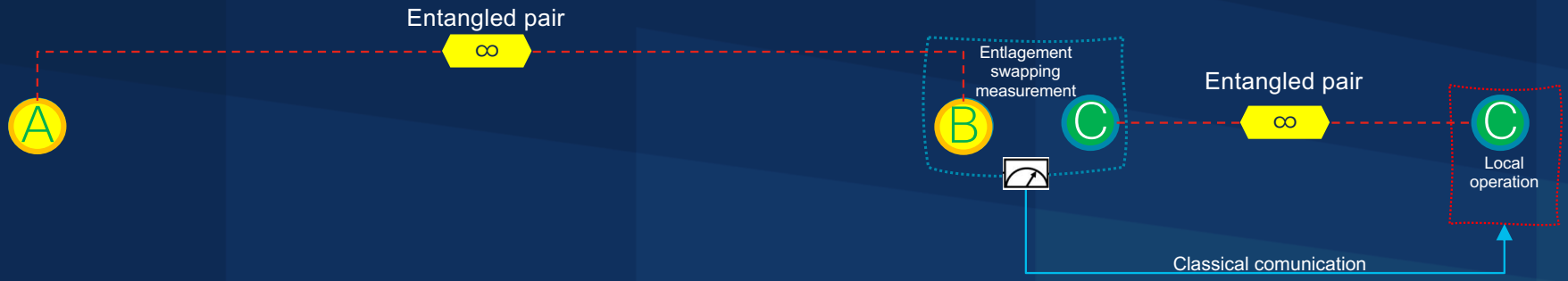


Entanglement swapping enables teleporting qubit over distance

Once we have multiple maximally entangled pair segments,

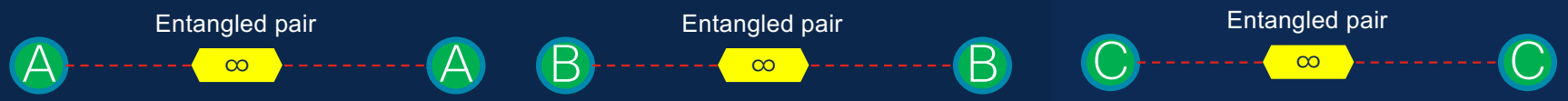


it is possible to get end to end entanglement via local operation and classical trasmission.

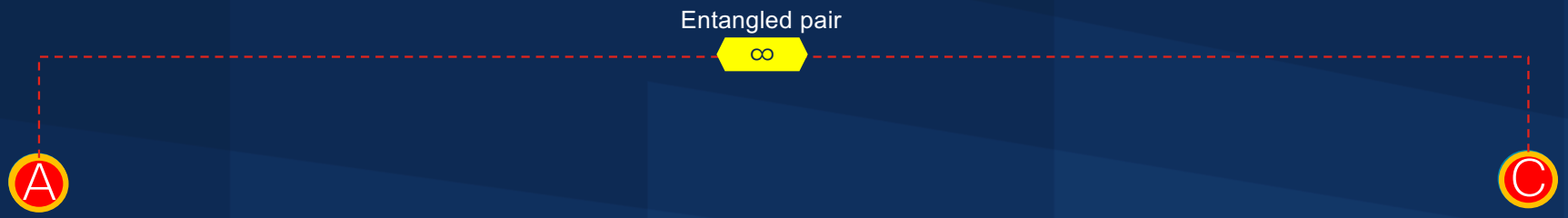


Entanglement swapping enables teleporting qubit over distance

Once we have multiple maximally entangled pair segments,

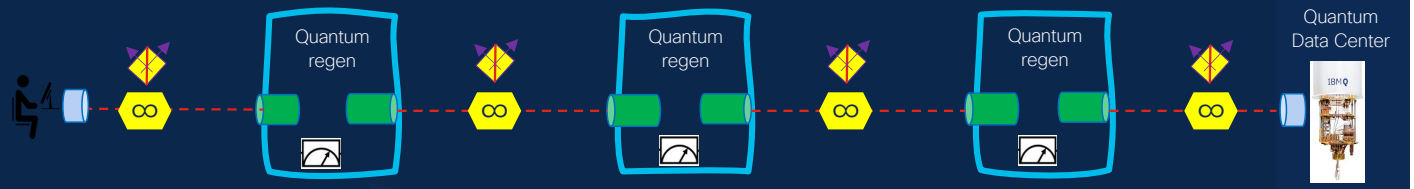


it is possible to get end to end entanglement via local operation and classical trasmission.

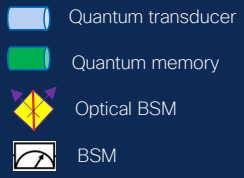


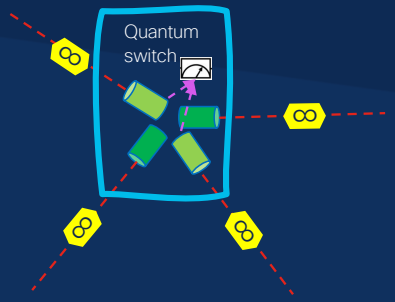
Quantum networking using teleporting

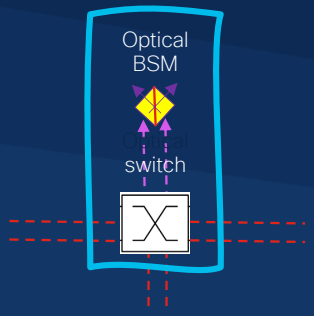
- Long distance teleportation – chaining segments with quantum regeneration

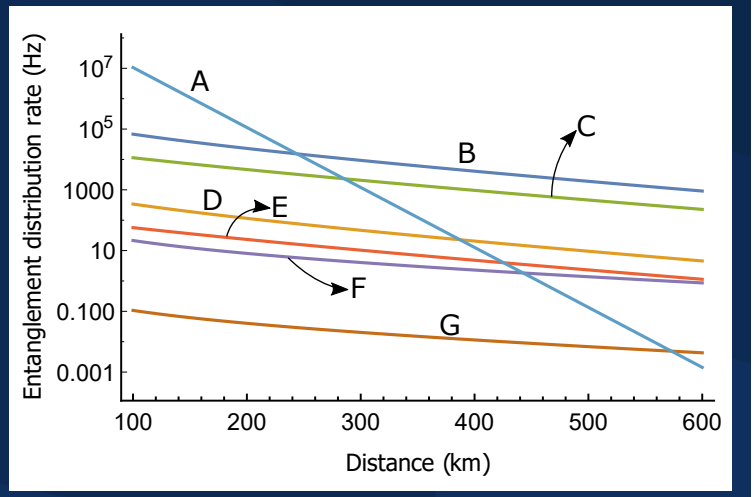


- Quantum networking needs
  - appropriate Entanglement Distribution Rate for teleporting
  - path switching achievable performing entanglement swapping on the appropriate quantum memory.









Sourabh Kumar, ikolao Lauk and Christoph Simon
Towards long-distance quantum networks with superconducting processors and optical links (2019)
https://arxiv.org/pdf/1812.08634.pdf

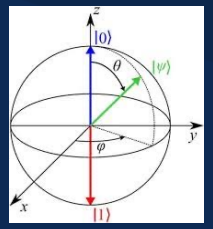
Note: we can envision routing done also optically but memory would be anyhow required somewhere to perform entanglement swapping quantum regeneration.

Challenges

Qubit challenges

Matter qubits:

- Error during programming of initial states
- Coupling with environment causing decoherence



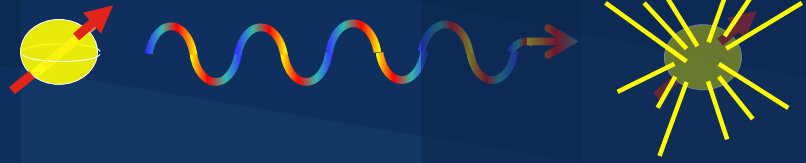
- Limited lifetime (us, ms)

Quantum Gate accuracy:

- Operation error

Flying qubits:

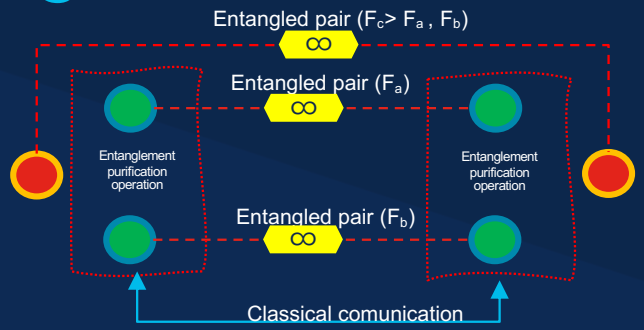
- Photon losses

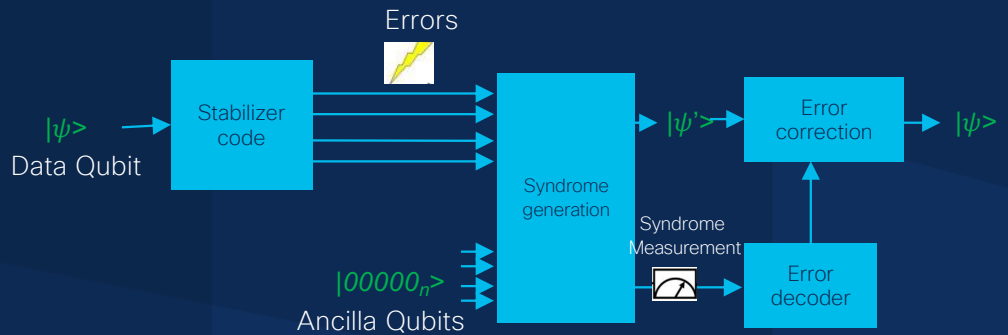


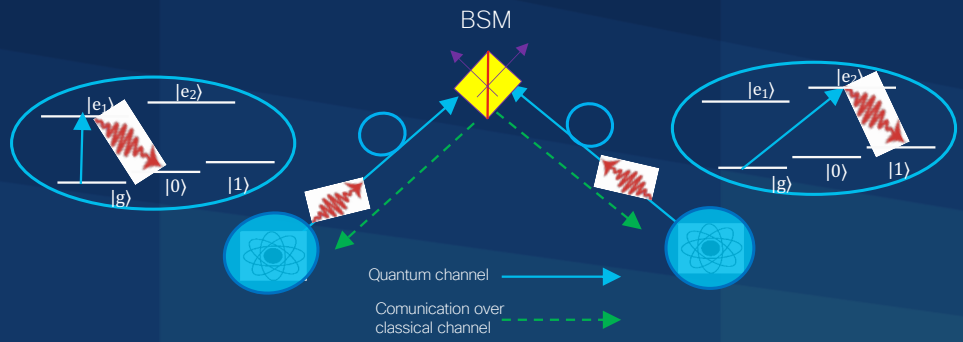
*Fidelity: a value between 0 and 1 that is a measure of the "closeness" of two **quantum** states.*

Network Challenges

- Entangled pair generation rate
  - With high fidelity and purity
- Quantum Error Correction
  - Protects against decoherence, quantum noise photon loss
  - Good idea but requires even more Qubits
- Network Synchronisation
  - Entanglement requires wave functions to overlap in time – detected via Bell State Measurement
  - Wavelength, synchronization and polarization alignement must be controlled tightly
  - Once available entanglement must be consumed before decoherence destroy it.
  - Quantum memory coherence – Qubits have a shelf life







Pragmatic way forward

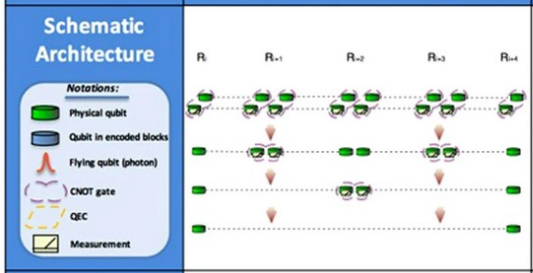
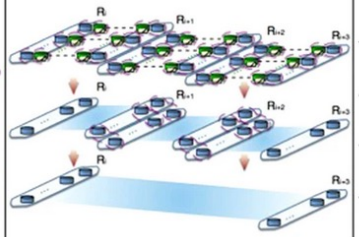
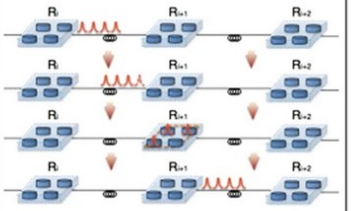
Quantum regenerator generations and network implications

Literature aligning around 3 possible quantum regen "generation" using HEG, purification and QEC to address either/or losses or operation error.

QEC offers the advantage of faster transmission but regen distances limited below 3dB.

Third generation regenerator will be more suitable for short distance quantum network

QR – Quantum Regenerator
HEG – Heralded Entanglement Generation
HEP – Heralded Entanglement Purification
QEC – Quantum Error Correction

	First Generation QR	Second Generation QR	Third Generation QR
Schematic Architecture			
Loss Error	HEG (two-way signaling)	HEG (two-way signaling)	QEC (one-way signaling)
Operation Error	HEP (two-way signaling)	QEC (one-way signaling)	QEC (one-way signaling)
Procedure	1. Create entangled pairs over L_0 between adjacent stations 2. At k-th level, connect two pairs over L_k and extend to $L_{k+1}=2L_k$, followed by HEP. 3. After n nesting levels, obtain high-fidelity pair over $L_{tot}=2^n \times L_0$	1. Prepare encoded states $\|0\rangle_L$ and $\|+\rangle_L$ 2. Use teleportation-based non-local CNOT gates to create encoded Bell pairs between adjacent stations. 3. Connect intermediate stations to create long distance encoded Bell pair	1. Encode information with a block of qubits that are sent through a lossy channel 2. Use QEC to correct both loss and operation errors 3. Relay the encoded information to the next station; and repeat steps 2 & 3.
Characteristic time scale	$\text{Max}(L_{tot}/c, t_0)$	$\text{Max}(L_0/c, t_0)$	t_0
Cost Coefficient (C')	$\text{Poly}(L_{tot})$	$\text{PolyLog}(L_{tot})$	$\text{PolyLog}(L_{tot})$

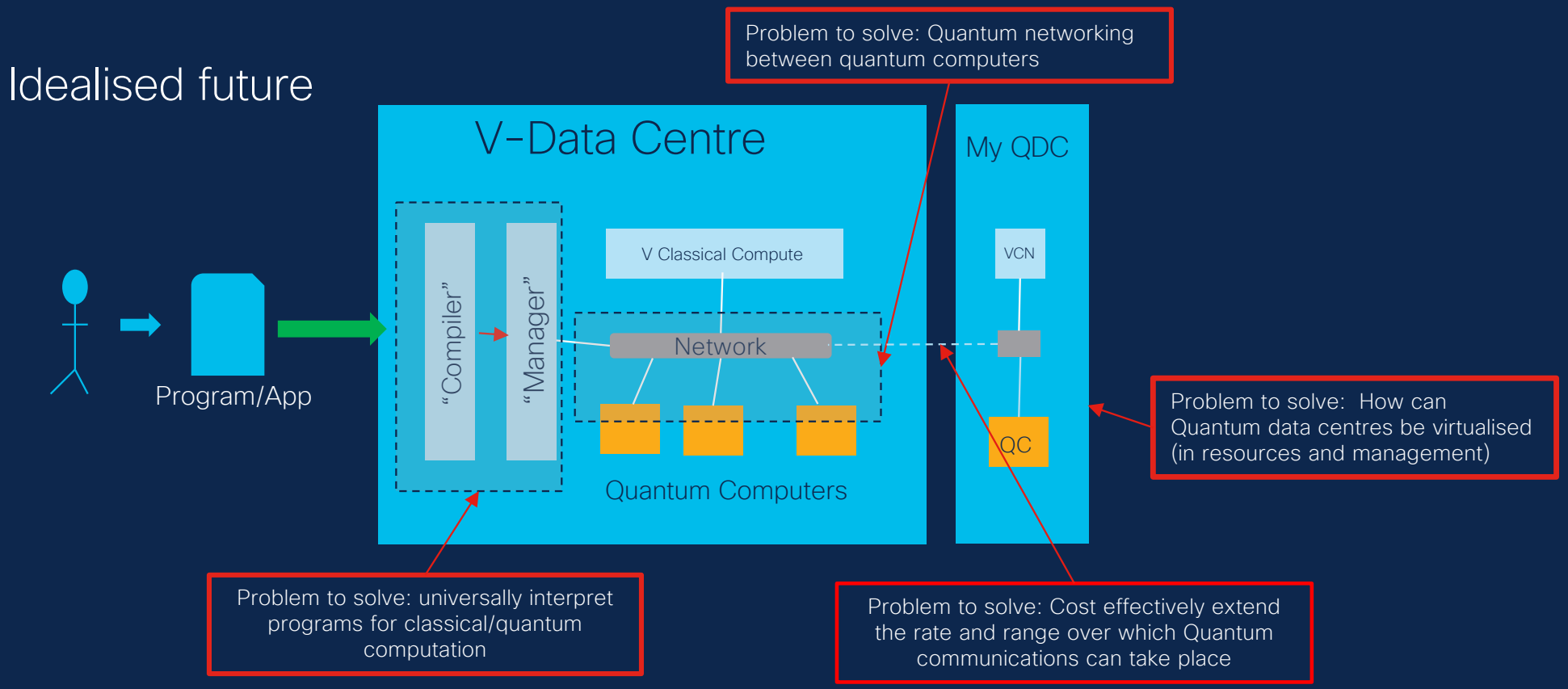
Seraman Muralidharan, et al: Optimal Architectures for Long Distance Communication (2016)
https://www.nature.com/articles/srep20463

Quantum internet

- Will manage regen of different generation/technologies:
  - Direct transmission with QEC or teleporting via entanglement pairs generation and eventually purification.
- In case of teleporting:
  - Fidelity and use of purification affect the entanglement rate need.
  - A “pseudo” path routing is selected via entanglement swapping.
  - A parallel classical network is required to vehicle control, entanglement swapping and purification informations.

Wrap up

Possible end state and problems to solve



THANK YOU!