The Quantum Blockchain Cloud
(or: buzzword compliance in the age of quantum computing)

Roland van Rijswijk-Deij
The H-word

Quantum Computing Hype Cycle Just Getting Started
Quantum computing could be to the 2020s what cloud computing was to the 2010s

By Dana Blankenhorn, InvestorPlace Contributor  Jul 25, 2018, 1:24 am EST

Quantum Computing Under Hype Cycle and Market Clock Scrutiny
With new technology come the plaudits and the critics. Quantum computing is no different from any other sector

By James Dargan - August 1, 2019  46  3

Quantum computing is not a cure-all for business computing challenges

By James Sanders in Innovation B.  On May 18, 2016, 11:05 AM PST
Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

The hype isn't helpful!

- The amount of hyperbole is mind boggling
  - Google's "quantum supremacy" was compared to the Wright brothers' first flight moment

- How can we know what is true or not?

- Is quantum computing really happening? Is our public key cryptography really no longer safe? **Hopefully this talk will help.**
Hackernoon sez it better...

Quantum Computing: Is it the end of blockchain?

June 3rd 2018
Some facts

• Quantum computers have *qubits*, which - as many of you may already know - can simultaneously encode any value between 0 and 1 at the same time (in superposition)

• The trick with *qubits* is that they can be *entangled*, that is: their quantum states can be linked

• This leads to some weird properties, such as "quantum teleportation"

• It also plays a role in breaking classic public key cryptography
Building a qubit

• It turns out there are many ways in which qubits can be created

• Think of this as "hard drive" vs. "tape drive" vs. "flash drive"

• Many of these methods have some extreme requirements (very very cold environments, diamonds, powerful lasers, ...)

• The holy grail is keeping qubits stable; current records are in the order of a minute
Physical vs. logical qubit

• It turns out quantum computers are inherently noisy and unreliable; consequently, you need many *physical* qubits to create one *logical* qubit

• To perform error-free computations on a quantum computer, you need quantum error correction, to get from physical unreliable qubits to reliable logical qubits

• This can cause serious confusion; when the claims start flying that we need hundreds or millions or billions of qubits to break cryptography, what type of qubits are they talking about?
OK, but what about D-Wave?

- D-Wave regularly shows up in discussion about quantum computing

- Current model is claimed to have 2048 qubits, with a new model claiming 5000 qubits by mid-2020

- So are we done by mid-2020? No more RSA or Elliptic Curves? Some news outlets seem to think so (the picture on the right is from a scare-tactic Forbes article on quantum)
Not so fast (after all)

- D-Wave is not a general purpose QC, instead it does something called "adiabatic quantum computing"
- The jury is still out on whether this provides a real speed-up over classic computing, experts disagree
- The documentation is also unclear, but it appears that the 2048/5000 qubit claim talks about physical qubits
- Most importantly, though, D-Wave's systems cannot run Shor's algorithm (more about that in a minute)
Time for a quick summary

• Making stable qubits is really hard
• Qubits are highly unreliable
• You need orders more physical qubits to create logical qubits
• The state of the art are machines with some 50-ish logical qubits with limited stability
**Shor's algorithm**

- In 1994 prof. Peter Shor (see picture) devised an algorithm to factor very large numbers (think: RSA) much more efficiently on quantum computers.

- This was touted as the "killer app" for quantum computers (which many claim had been a niche interest until then).

- His algorithm requires a stable general purpose quantum computer to execute; let's assume that exists for the sake of argument.
Research to improve Shor

- Researchers are trying to improve Shor's algorithm
- To drive down the requirements to break common public key algorithms
- They do this without actual access to a working QC (awesome!)
- Take, for example, this table from [6] (references at end of deck):

<table>
<thead>
<tr>
<th>Historical cost estimate at ( n = 2048 )</th>
<th>Physical gate error rate</th>
<th>Cycle time (microseconds)</th>
<th>Reaction time (microseconds)</th>
<th>Physical connectivity</th>
<th>Approach</th>
<th>Estimated costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fowler et al. 2012 [9]</td>
<td>0.1%</td>
<td>1</td>
<td>0.1</td>
<td>planar</td>
<td>Distillation strategy: 1200 T; Execution strategy: single threaded</td>
<td>Physical qubits (millions): 1000; Expected runtime (days): 1.1; Expected volume (megaqubitdays): 1100</td>
</tr>
<tr>
<td>O’Gorman et al. 2017 [18]</td>
<td>0.1%</td>
<td>10</td>
<td>1</td>
<td>arbitrary</td>
<td>block CCZ; single threaded</td>
<td>230; 3.7; 850</td>
</tr>
<tr>
<td>Gheorghiu et al. 2019 [19]</td>
<td>0.1%</td>
<td>0.2</td>
<td>0.1</td>
<td>planar</td>
<td>1100 T; single threaded</td>
<td>170; 1; 170</td>
</tr>
<tr>
<td>(ours) 2019 (1 factory)</td>
<td>0.1%</td>
<td>1</td>
<td>10</td>
<td>planar</td>
<td>1 CCZ; serial distillation</td>
<td>16; 6; 90</td>
</tr>
<tr>
<td>(ours) 2019 (1 thread)</td>
<td>0.1%</td>
<td>1</td>
<td>10</td>
<td>planar</td>
<td>14 CCZ; single threaded</td>
<td>19; 0.36; 6.6</td>
</tr>
<tr>
<td>(ours) 2019 (parallel)</td>
<td>0.1%</td>
<td>1</td>
<td>10</td>
<td>planar</td>
<td>28 CCZ; double threaded</td>
<td>20; 0.31; 5.9</td>
</tr>
</tbody>
</table>
Research to improve QECC

• Researchers are not just trying to improve Shor

• More fundamentally (because it is required for other quantum algorithms) they are trying to improve error correction

• One of the latest developments is called "surface codes"; these purportedly work better on "noisy" qubits

• In the context of Shor: they require approximately 15,000 physical qubits per logical qubit for qubits with an error rate of $10^{-3}$ (state of the art)
So where are we with Shor?

<table>
<thead>
<tr>
<th>Public Key System</th>
<th>Key size</th>
<th>Security</th>
<th>Logical qubits required</th>
<th>Physical qubits required</th>
<th>Running time</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>1024 bits</td>
<td>80 bits</td>
<td>2,050</td>
<td>8.05x10^6</td>
<td>3.58h</td>
</tr>
<tr>
<td></td>
<td>2048 bits</td>
<td>112 bits</td>
<td>4,098</td>
<td>8.56x10^6</td>
<td>28.63h</td>
</tr>
<tr>
<td></td>
<td>4096 bits</td>
<td>128 bits</td>
<td>8,194</td>
<td>1.12x10^7</td>
<td>229h</td>
</tr>
<tr>
<td>ECC</td>
<td>256 bits</td>
<td>128 bits</td>
<td>2,330</td>
<td>8.56x10^6</td>
<td>10.5h</td>
</tr>
<tr>
<td></td>
<td>384 bits</td>
<td>192 bits</td>
<td>3,484</td>
<td>9.05x10^6</td>
<td>37.67h</td>
</tr>
<tr>
<td></td>
<td>512 bits</td>
<td>256 bits</td>
<td>4,719</td>
<td>1.13x10^7</td>
<td>55h</td>
</tr>
</tbody>
</table>

Source: [2] -- terms and conditions apply 😊
That previous slide...

- Has a *lot* of assumptions, none of which hold today

- So the $64 million question is: when, if ever, will these assumptions hold?

- An oft-quoted person is Michele Mosca, whose most recent prediction puts the likelihood of a quantum computer that can break RSA 2048 in the next decade at *one in six*
So what do the experts agree on?

• **Nobody** really *knows if a quantum computer* good enough to run Shor will ever be built

• *Equally*, **nobody claims** that it can never be built

• There is **lots and lots of parallel research** going on, all of which **requires major breakthroughs** to get there

• *The best thing you can do:* **keep a keen eye on post-quantum crypto!**
Mosca's Inequality

- A handy way to reason about when you should really take action is what is often referred to as "Mosca's Inequality": \( X + Y > Z \)

  where:
  - \( X \) = the amount of time you want to keep your data secret
  - \( Y \) = the amount of time you take to transition to PQC
  - \( Z \) = when we expect QC's to be able to run Shor

- The problem, again, here is that nobody really knows a sensible value for \( Z \) in this equation
The experts are on it

President Donald J. Trump signs the "National Quantum Initiative" into law
Quantum Key Distribution

• I assume most (if not all?) of you are familiar with One-Time Pads?

From: A History of U.S. Communications Security (Vols. I and II);
the David G. Boak Lectures, National Security Agency, 1973
QKD relies on the observer effect

- QKD is used to distribute a one-time pad from A to B
- Security relies on the fact that you can tell if the message was observed
- Common implementation: polarised light through a fibre-optic cable
Conceptual QKD in two slides

Basis 1: Rectilinear

<table>
<thead>
<tr>
<th></th>
<th>→</th>
<th>⬤ = 0</th>
<th>⬤ = 1</th>
</tr>
</thead>
</table>

Basis 2: Diagonal

<table>
<thead>
<tr>
<th></th>
<th>⬤</th>
<th>⬤ = 0</th>
<th>⬤ = 1</th>
</tr>
</thead>
</table>

Alice

<table>
<thead>
<tr>
<th>message</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmitted</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>basis</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

Bob

<table>
<thead>
<tr>
<th>message</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>basis</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>received</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

Shared secret = 0 0 1 0 0
## Conceptual QKD in two slides

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Bob</th>
<th>Eve</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>message</strong></td>
<td>0 1 0 0 1 1 1 0 1 0 0</td>
<td>0 1 0 1 0 1 1 0 0 0 1</td>
<td>0 1 0 1 0 1 1 0 0 0 1</td>
</tr>
<tr>
<td><strong>transmitted</strong></td>
<td>× × → ↑ × × × × × × ↑ →</td>
<td>× × ↑ × × × × × × ↑ ×</td>
<td>× × → × × × × × ↑ ×</td>
</tr>
<tr>
<td><strong>basis</strong></td>
<td>× × ↓ ↑ × × × × × × ↑ ×</td>
<td>× × ↑ × × × × × × ↑ ×</td>
<td>× × → × × × × × ↑ ×</td>
</tr>
<tr>
<td><strong>received</strong></td>
<td>× × ↑ × × × × × × × ×</td>
<td>× × ↑ × × × × × × ↑ ×</td>
<td>× × → × × × × × ↑ ×</td>
</tr>
<tr>
<td><strong>message</strong></td>
<td>1 1 0 1 0 1 1 0 0 0 1</td>
<td>1 1 0 1 0 1 1 0 0 0 1</td>
<td>1 1 0 1 0 1 1 0 0 0 1</td>
</tr>
</tbody>
</table>
Issues with QKD

- It requires "classic" cryptography to authenticate the communicating parties (am I really sending something to Bob?)

- More importantly, though, it is vulnerable to attacks

  - Photon-splitting attack *(doesn't that sound awesome?!)*
    QKD relies on single photon emission, but that is actually impossible

  - Trojan attack
    Shining a very bright light at the message source, attack can infer chosen polarisation from reflection with 90% accuracy [7]
Do we really need QKD?

- It is expensive
  - order of €25K/device, you need two!
  - oh, and you need dark fibre

- It is inefficient (bit rate in the order of 1Mbit/s over 50km)

- And there are known attacks, how many are still to come?

- Never underestimate the bandwidth of a truck full of one-time pads 😄
Wrapping up

• There is a lot of hype and hyperbole about quantum computing

• Just as there is about blockchain (hence the title of this talk)

• So we have two takeaways for you:
Takeaway #1

DON'T PANIC

picture source: Wikimedia Commons
Takeaway #2

- Pay attention to Post Quantum Cryptography
- ...and give people like Andreas more €€€ for their research!

Photo by Марьян Блан | @marjanblan on Unsplash
So what is the QBC?

Well that, as they say, is simple:

It's a computer system in someone else's data centre that you don't find out actually exists until you make a transaction that needs to be persisted on a ledger after which it sets fire to said data centre, belching out more pollutants than a brown coal fired power plant in Germany.
Thank you! Questions?

LinkedIn: nl.linkedin.com/in/rolandvanrijswijk

Twitter: @reseauxsansfil

Email: roland@nlnetlabs.nl


