U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

May 16, 2018

TO: Members, Subcommittee on Digital Commerce and Consumer Protection

FROM: Committee Majority Staff

RE: Hearing entitled "Disrupter Series: Quantum Computing"

I. INTRODUCTION

The Subcommittee on Digital Commerce and Consumer Protection will hold a hearing on Friday, May 18, 2018, at 9:15 a.m. in 2322 Rayburn House Office Building. The hearing is entitled "Disrupter Series: Quantum Computing."

II. WITNESSES

- Michael Brett, CEO, QxBranch;
- Christopher Monroe, Chief Scientist and Founder, IonQ, Inc. and Professor of Physics, University of Maryland;
- Matthew Putman, CEO, Nanotronics. Inc.; and
- Diana Franklin, Director of Computer Science Education, the University of Chicago

III. BACKGROUND

A. Quantum Computing

Quantum computing has been described as "harnessing and exploiting the amazing laws of quantum mechanics to process information."[1] Traditional computers operate through instructions that use a binary system represented by the numbers 0 and 1; these numbers represent the "off" or "on" position of a logic gate on an integrated circuit.[2] These positions can be expressed using binary digits (or "bits") stored in a computer's memory; when expressed they represent the control of the flow of energy through the circuit. Individually a bit can exist in one of two possible states (on/off).[3]

By contrast, quantum computers "use quantum bits, or qubits, to encode information as 0s, 1s, or both at the same time. This superposition of states—along with the other quantum

[1] *Quantum Computing 101*, Institute for Quantum Computing, University of Waterloo (retrieved May 1, 2018) https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101
[2] Das, Subhasis, *How Computer Chips Work,* Gizmodo (October 13, 2014) https://gizmodo.com/how-computer-chips-work-1645654993
[3] See *Bit*, Wikipedia (retrieved May 2, 2018)https://en.wikipedia.org/wiki/Bit

mechanical phenomena of entanglement and tunneling—enables quantum computers to manipulate enormous combinations of states at once."[4] Venture capital firms have invested $147 million in quantum computing startups and governments around the world have invested $2.2 billion in technology that is expected to change how professionals in a variety of industries address problems that require a massive amount of computing power today—from stronger encryption for sensitive transactions to improving battery density technology for electric vehicles.[5]

i. Quantum Mechanics

Quantum mechanics is a theory of physics that describes the behavior of matter and light at atomic and subatomic levels. As described by Richard Feynman, one of the leading physicists of the 20th Century:

> "Quantum mechanics" is the description of the behavior of matter and light in all its details and, in particular, of the happenings on an atomic scale. Things on a very small scale behave like nothing that you have any direct experience about. They do not behave like waves, they do not behave like particles, they do not behave like clouds, or billiard balls, or weights on springs, or like anything that you have ever seen.[6]

Unlike in Classical or Newtonian physics, which allows for the prediction of the movement of bodies at a larger-than-atomic scale with accuracy to a reasonable state of approximation,[7] quantum mechanics holds that it is impossible to know both the precise position and precise momentum of a quantum object. Instead, the more that is known about one of these variables, the less that can be known of the other. This theory, know as the *Heisenberg Uncertain Principal* (HUP) after its discoverer Werner Heisenberg, is a consequence of the fact that at the most fundamental level, matter and light operate as both particle and wave.[8]

The wave-particle duality described in the HUP lies at the heart of quantum mechanics. A consequence of the theory is that at a fundamental level matter and light can only be described probabilistically; it is impossible to know both the position and momentum of a quantum object because the object exists in all possible states simultaneously until it is measured (or observed) - a concept known as *superposition.*[9]

---

[4] *Quantum Computing*, D-Wave Systems,(retrieved May 2, 2018), https://www.dwavesys.com/quantum-computing
[5] Schatsky, David and Puliyakodil, Ramya K., *From fantasy to reality- Quantum computing is coming to the marketplace,* Deloitte Insights (April 26, 2017) https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/quantum-computing-enterprise-applications.html?id=us:2ps:3gl:lookagainfy18:eng:greendot:111617:nonem:na:zX4NySth:1079921058:244804402979:b:RLSA_Innovation:RLSA_Quantum_Computing_BMM:nb#endnote-sup-1
[6] Feynman, Richard; Leighton, Robert; Sands, Matthew (1964). *The Feynman Lectures on Physics, Vol. 3.* California Institute of Technology. p. 1.1. ISBN 0201500647. http://www.feynmanlectures.caltech.edu/III_01.html
[7] Morin, David (2008). *Introduction to Classical Mechanics*. New York: Cambridge University Press
[8] *Consequences of the Uncertainty Principle*, Ohio State University Department of Physics (retrieved May 2, 2018) http://www.physics.ohio-state.edu/~ntg/H133/handouts/uncertainty.pdf
[9] *What is Superposition?,* Physics.org (retrieved May 3, 2018) http://www.physics.org/article-questions.asp?id=124

As noted by Natalie Wolchover:

> The orthodox view of quantum mechanics . . . holds that particles play out all possible realities simultaneously. Each particle is represented by a 'probability wave' weighting these various possibilities, and the wave collapses to a definite state only when the particle is measured.[10]

Another fundamental concept of quantum mechanics is the idea of *quantum entanglement*, which holds that particles can interact in such a way that a change to the quantum state of one particle will necessarily result in an equal but opposite change to its entangled twin.[11] As described by the physicist John Stewart Bell, quantum entanglement appears to violate the principle of locality, meaning that quantum entangled particles will simultaneously demonstrate changes to their quantum state regardless of the distance separating them.[12] This remains true whether the entangled particles are separated across a room or across the universe.[13]

The implications of quantum mechanics are described by Professor Feyman:

> We would like to emphasize a very important difference between classical and quantum mechanics. We have been talking about the probability that an electron will arrive in a given circumstance. We have implied that in our experimental arrangement (or even in the best possible one) it would be impossible to predict exactly what would happen. We can only predict the odds! This would mean, if it were true, that physics has given up on the problem of trying to predict exactly what will happen in a definite circumstance. Yes! physics has given up. We do not know how to predict what would happen in a given circumstance, and we believe now that it is impossible—that the only thing that can be predicted is the probability of different events. It must be recognized that this is a retrenchment in our earlier ideal of understanding nature. It may be a backward step, but no one has seen a way to avoid it.[14]

ii. The Use of Quantum Mechanics in Computing

The use of quantum mechanics as a basis for computation creates new possibilities in terms of the speed at which results can be calculated.

---

[10] Natalie Wolchover, *Have We Been Interpreting Quantum Mechanics Wrong This Whole Time?*, Wired (June 30, 2014)https://www.wired.com/2014/06/the-new-quantum-reality/

[11] See, e.g. *Quantum Entanglement*, Wikipedia (retrieved May 3, 2018), https://en.wikipedia.org/wiki/Quantum_entanglement

[12] *Bell's Theorem,* Stanford Encyclopedia of Philosophy (First published July 21, 2004; substantive revision June 11, 2009) https://plato.stanford.edu/entries/bell-theorem/

[13] For an example of this see Kaplan, Sarah, *Quantum entanglement, science's 'spookiest' phenomenon, achieved in space*, Washingtonpost.com (June 15, 2017) https://www.washingtonpost.com/news/speaking-of-science/wp/2017/06/15/quantum-entanglement-sciences-spookiest-phenomenon-achieved-in-space/?utm_term=.e5bf2a2c5dbc

[14] Feynman, Leighton and Sands at 1.7.

As noted by Joseph Altpeter:

> Quantum computers are fundamentally different from classical computers because the physics of quantum information is also the physics of *possibility*. Classical computer memories are constrained to exist at any given time as a simple list of zeros and ones. In contrast, in a single quantum memory many such combinations—even *all possible* lists of zeros and ones—can all exist *simultaneously*. During a quantum algorithm, this symphony of possibilities split and merge, eventually coalescing around a single solution.[15]

Traditional bits can at one time be in only one of two states (0 or 1; "off" or "on"). Superposition allows a qubit to exist in all states simultaneously. This means that the computational power of a qubit increases exponentially:

> (a) 2-qubit machine allows you to do four calculations at once. A 3-qubit machine can do eight calculations. A 4-qubit machine gives you 16 calculations, all simultaneously. By the time you get to 300 qubits, you've got a computer that can do more 'calculations' than there are atoms in the universe.[16]

The ability to run billions of calculations using all available data at the same time would allow analysis of problems that were previously deemed incalculable because of time constraints.[17]

B. The Current State of Quantum Computer Development

Quantum computing has attracted a great deal of interest both within the United States as well as abroad. According to a 2017 report by the consulting firm Deloitte, "in the last three years, venture capital investors have placed $147 million with quantum computing startups" and "governments globally have provided $2.2 billion in support to (quantum computer) researchers."[18] Private-sector leaders in the area include IBM, QxBranch LLC, Ionq, Google, MagiQ Technologies, Rigetti Computing, and Station Q- Microsoft, all based in the United

---

[15] Altpeter, Joseph, *A tale of two qubits: how quantum computers work*, Ars Technica (January 1, 2010) https://arstechnica.com/science/2010/01/a-tale-of-two-qubits-how-quantum-computers-work/

[16] Diamadis, Peter, *Massive Disruption*¸ Tech Blog (retrieved May 3, 2018) http://www.diamandis.com/blog/massive-disruption-quantum-computing

[17] E.g. "Today, we spend approximately 3 percent of the world's total energy output on making fertilizer. This relies on a process developed in the early 1900s that is extremely energy intensive—the reaction gas required is taken from natural gas, which is in turn required in very large amounts. However, we know that a tiny anaerobic bacteria in the roots of plants performs this same process every day at very low energy cost using a specific molecule—nitrogenase. This molecule is beyond the abilities of our largest supercomputers to analyze, but would be within the reach of a moderate scale quantum computer." Reiher, Markus, Wiebe, Nathan, Svore, Krysta,Wecker, Dave and Troyer, Matthias, *Elucidating Reaction Mechanisms on Quantum Computers*, arXiv:1605.03590v2 [quant-ph] 25 May 2016, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/05/1605.03590-2.pdf

[18] Schatsky, David and Puliyakodil, Ramya K., *From fantasy to reality- Quantum computing is coming to the marketplace*, Deloitte Insights (April 26, 2017) https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/quantum-computing-enterprise-applications.html?id=us:2ps:3gl:lookagainfy18:eng:greendot:111617:nonem:na:zX4NySth:1079921058:244804402979:b:RLSA_Innovation:RLSA_Quantum_Computing_BMM:nb#endnote-sup-1

States, as well as D-Wave Systems Inc. and 1QB Information Technologies Inc., both from Canada.[19] In addition to private sector initiatives, there are dozens of universities engaged in quantum computing research world-wide.[20] In the U.S., leading academic centers for quantum research include MIT,[21] the University of Southern California,[22] and the University of Maryland.[23]

Outside of the U.S., China is a leading source of quantum computing research. The Chinese government has invested $20 billion in a national laboratory for quantum sciences, which is scheduled to open in 2020.[24] The Chinese companies Baidu, Alibaba Group Holdings, and Tencent Group Holdings are also working on quantum computers, with Alibaba announcing in February 2018 the opening of a quantum computing cloud platform for researchers that operates on an 11-qubit processor.[25] The Chinese government has announced plans to lead the world in quantum-enable technologies: in August 2016, the country launched the world's first quantum satellite, called Micius, and used it for conducting experiments such as a quantum-secured video conference call between Beijing and Vienna, Austria.[26]

In 2016, the European Union announced a "quantum flagship" program to advance the technology in the Union. The program is aiming for achieving a "ramp-up" phase by this year, which will ultimately result in one billion euros joint public-private investment over a ten-year period.[27]

C. <u>Quantum computing applications</u>

The potential ability of a quantum computer to process multiple calculations simultaneously makes it particularly well suited to some of the most complex problems faced by programmers. These include the "optimization" problem, which involves finding the best of all possible solutions among various alternatives; machine learning derived from detecting patterns

---

[19] *Quantum Computing Market by Revenue Source, Application (Simulation, Optimization, and Sampling), Industry (Defense, Banking & Finance, Energy & Power, Chemicals, and Healthcare & Pharmaceuticals), and Geography - Global Forecast to 2023*, MarketsandMarkets.com (Aug 2017) https://www.marketsandmarkets.com/Market-Reports/quantum-computing-market-144888301.html
[20] *Quantum Computing Report-Universities* (retrieved May 4, 2018) https://quantumcomputingreport.com/players/universities/
[21] http://ctp.lns.mit.edu/research-quantum.html
[22] http://cqist.usc.edu/
[23] http://jqi.umd.edu/
[24] Decker, Susan and Yasiejko, Christopher, *Forget the Trade War. China Wants to Win Computing Arms Race*, Bloomberg (April 8, 2018) https://www.bloomberg.com/news/articles/2018-04-08/forget-the-trade-war-china-wants-to-win-the-computing-arms-race
[25] Soo, Zen *China's race for the mother of all supercomputers just got more crowded*, South China Morning Post (March 12, 2018) http://www.scmp.com/tech/science-research/article/2136669/chinas-race-mother-all-supercomputers-just-got-more-crowded
[26] Kania, Elsa, *Is China Seeking 'Quantum Surprise,'* Bulletin of the Atomic Scientists, (March 1, 2018) https://thebulletin.org/china-seeking-%E2%80%9Cquantum-surprise%E2%80%9D11552
[27] Ansip, Andrus, Vice President, *The race to quantum: taking computing to a new level in Europe*, European Commission (Oct 31, 2017)https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/race-quantum-taking-computing-new-level-europe_en

among large datasets; materials simulation, which involves the modelling of materials at the atomic and smaller level; and "Monte Carlo" simulations, which requires the repeated random sampling of simulations to predict the probability of a given outcome.[28]

Applying these advantages to real world problems, a quantum computer could help logistics companies find optimal routes for parcel delivery, reducing both time and expense;[29] personalized medicine and drug development, where it might be possible to model candidate molecules and genetic factors for faster drug discovery;[30] and other areas including financial services, aerospace engineering, data storage optimization, electric battery design and oil and gas exploration.[31]

Cryptography has the potential to be massively disrupted by quantum computing. Underlying one of the mostly widely used methods of encrypting electronic data is the use of prime factorization (the reduction of a larger number into its factorials, where those factorials are both prime numbers). Calculating the factorials of a large number scales rapidly exceeds the capacity of classical computers: for example, a 128-bit advanced encryption standard (AES) cipher is for all purposes unbreakable today given the volume of possibilities needed to guess with a brute-force attack to break the encryption.[32] However, using the power of quantum computing to decode the same 128-bit AES cipher could take as little as six months.[33] The potential of a quantum computer to decode formerly impenetrable data has spurred both public and private efforts to develop new forms of encryption.[34]

IV. ISSUES

The following issues may be examined at the hearing:

- What are some of the uses of a quantum computer, what advantages would a quantum computer hold over conventional computers, and what dangers would it present?
- What are the barriers to the development of a commercially available quantum computer?
- Where does the United States stand in relation to other nations in developing a commercially available quantum computer?

---

[28] See D-Wave Systems, *Applications*, https://www.dwavesys.com/quantum-computing/applications
[29] *Five ways quantum computing will change the way we think about computing*, IBM (May 8, 2017) https://phys.org/news/2017-05-ways-quantum.html
[30] Sandle, Tim, *Quantum Computing Initiative Advances Drug Discovery*, Digital Journal (June 29, 2017) http://www.digitaljournal.com/tech-and-science/technology/quantum-computing-initiative-advances-drug-discovery/article/496462

[31] Shatsky and Puliyakodil, *From fantasy to reality*, at "Enterprises are already seeking applications."
[32] https://medium.com/@drgutteridge/whats-the-deal-with-encryption-strength-is-128-bit-encryption-enough-or-do-you-need-more-3338b53f1e3d
[33] Wood, Lamon, *The clock is ticking for encryption*, ComputerWorld (March 21, 2011) www.computerworld.com/article/2550008/security0/the-clock-is-ticking-for-encryption.html
[34] Shatsky and Puliyakodil.

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Melissa Froelich or Gregory Zerzan of the Committee staff at (202) 225-2927.