American University of Armenia **Vani Mardirossian**
Introduction to Quantum Computing **Project Task #01**
Prof. Hakob Avetisyan **May 11, 2020**

According to the article, how do ambitions for quantum networks differ across nation-states around the world, and why? Include your own convictions about what role quantum networks should play.

In 2004, Vienna's city hall and the Bank of Austria made an attempt at making a quantum encrypted bank transfer. In 2007, Swiss authorities tried to use quantum encryption to send vote tallies from polling stations to state government bodies in Geneva. In Japan, Toshiba researchers sent quantum encrypted genomic data to a University located 7 kilometers away. In the UK, a quantum network is being deployed between Bristol and Cambridge, which are about 290 kilometers apart. In the capital of Australia, Canberra, a closed quantum government network is being built. China built a quantum network linking Beijing and Shanghai, users of this network include China Industrial and Commercial Bank, the China Banking Regulatory Commission, and the Xinhua news agency, which is the official state press agency of China. Essentially, all of these are attempts at creating a quantum internet, a network of quantum processors which would send and receive data regardless of the distance between them. What makes the classical internet a utility parallel to electricity and water is its ability to transmit large quantities of data over very long distances, having many senders and receivers. Quantum networks are responsible for sending information in the form of qubits from one quantum processor to another, and in order to achieve a working quantum internet, quantum networks will be essential in transmitting the necessary information between quantum processors, over an arbitrarily long distance, and having many senders and receivers.

We see multiple examples of governments investing in quantum network projects, more or less for the same reasons: securing exchange of sensitive information. Most countries also seem to share the type of information that they are interested in exchanging via these quantum networks. Austria, Switzerland, China, and others have an interest in using these technologies to provide more secure financial transactions between large institutions, although the inclusion of the Xinhua news agency in this network adds a new layer, one which seems to strengthen the centrality of the Chinese government. Switzerland, on the other hand, put quantum networks to a more democratic use in their 2007 elections, although their network later proved to be vulnerable to tampering. Japan's interests seem to be more research oriented.

Of course, there can be many uses for a quantum internet, from safe financial transactions, to safe elections, to non-governmental level exchanges of information. But it is an important question whether it will do more good than harm if such quantum capabilities became commercially available to any user. Most importantly, I believe that governments should have a vested interest in investing these quantum technologies for national security matters, because the development of quantum internet is a double edged sword, while it will give governmental institutions the ability to securely encrypt sensitive information, it will also give bad faith actors the ability to hack into classically encrypted older information, and I think that governmental resources are best spent trying to prevent such events in the future.

Give four reasons why corporations and governments believe "the time for investment, all agree, is now" for quantum computation, according to the article. Comment on which of the reasons you believe are most convincing.

Financial Incentives: This might sound obvious, but of course, corporations and governments do not want to miss out on potential future revenue streams that are predicted with high certainty. Whether quantum technology is put to use for high profile purposes by large institutions, or whether its applications are made available for commercial use, there is no doubt that it's lucrative, and governments want to get in on the action while it's still early. While no one is expecting fully functioning products anytime soon, the success of early attempts make the future for quantum computing promising, which simply attracts investments.

Post-Quantum Ciphers: Another obvious reason is security concerns. It is abundantly clear that quantum computing promises security of information, unparalleled by classical computers, as well as the ability to surpass barriers that currently make classical encryption approaches safe from hacking, "what got researchers going in the first place was the fear that global encryption standards would crumble in the face of quantum computing." Governments and research groups alike are working to come up with protocols, that would protect current data from hacking in a post-quantum world. It is not enough to worry about future information, if quantum computing is inevitable, then governments need to act quick in protecting all sensitive information from future hacking.

Enhancements of Existing Technologies: It is known that quantum computers will solve problems faster than classical computers, but the article mentions that a wider part of the appeal is not only due to the speed up on classical computers, but also due to the fundamental differences in the way quantum and classical computers work. So stronger and more capable computers are also an important drivers of investment decisions, but more so for corporations, than for governments. For corporations, it all comes down to profits, and higher performance technology means better problem solving, and eventually, higher profits.

Competitiveness: Lastly, a culmination of all the other reason, being competitive, both economically, and in terms of national security. For most governments, it would be catastrophic if they lacked quantum capabilities possessed by other nations. This need is especially enhanced for countries with ongoing rivalries with each other. Just as nations develop nuclear weapons as a bargaining chip, having quantum capabilities can also serve a similar purpose, not only protecting own information from foreign attacks, but also having the leverage of attacking. Essentially, the appearance of having these capabilities can be just as important as actually using using them.

I think that the most convincing reason is having security assurances. Of course, the financial incentives, and the enhancements that quantum computers will provide are important bonuses, but not as important as being protected. It would be surprising if any of the countries investing in quantum computing and quantum research care more about simply the supremacy of these computers in solving everyday problems, than they do about their national security status, because that is the one incentive, the absence of which can have the most devastating ramifications for the investing countries.

The article quotes IBM vice president Dario Gil saying, "The power of quantum computing is rediscovering all the problems that computers cannot solve, and having a path to solving them." Discuss three ways "quantum software" addresses this idea, and argue whether one should believe Dr. Gil's statement (or not).

The three fundamental properties of quantum systems that differentiate them from the classical are **superposition**, **entanglement** and **probability amplitudes**.

Superposition The idea of a superposition is that unlike classical bits, where they are either a 1 or a 0, qubits are in an indeterminate state, posing as both a 0 and a 1, until the qubit is measured, in which case it collapses to either a 0 or a 1. This adds a new layer to bits as we know them, where 1 qubit can be used to present much more information than 1 classical bit. As an example of the kind of power the property of superposition brings into the game, "To describe all the states of a 50-bit standard computer requires 50 bits of digital memory; a description of a 50-qubit computer would require a quadrillion."

Entanglement Entanglement introduces another difference. While in classical computation, it is essential to keep one bit separate from the effect of another for error free computing, quantum computers rely on the exact opposite, the entanglement of the computer's qubits. According to the article, the more qubits that are intangled in a quantum system, the better, and performing an operation on one qubit, implicitly performs operations of varying degrees on all the other qubits that it is entangled with.

Probability Amplitudes As opposed to anything we're used to in classical probability theory, probability amplitudes can take on negative values in the quantum world. The modulus square of a probability amplitude shows the probability of a qubit collapsing to the given state once it is measured. These amplitudes can interfere with each other, ultimately lowering the probability of getting wrong answers, and enhancing the probability of correct answers, which is the other power of quantum algorithms, the ability to essentialy filter out wrong answers and end up on the correct one.

The problem with Dario Gil's statement is, it's not that classical computers *cannot* solve these problems, but that it isn't efficient for them to do so, or that it is more efficient for quantum computers to solve those problems.

The article states "subjects that used to be mere footnotes to physics will rule, and engineers (and perhaps even consumers) will have to learn to speak quantum." How is this point presented in the article (cite corporate and government examples), and can you give examples from your own experience?

Take the example of the atomic clocks, which did utilize properties of quantum mechanics, but weren't really thought as being a product of quantum technology, and people weren't really sure how to put the properties of quantum mechanics such as superposition and entanglement to uses in creating powerful technology. This shows the importance of having computer engineers who understand the fundamentals of quantum mechanics, in order to be able to fully harness its powers and apply those powers in the creation of useful quantum computers. According to the article, while huge resources are being spent in the creation of quantum hardware, it is not proportional to what's being done in the quantum software field, meaning that it is way ahead, and much more needs to be done in developing quantum software in order to meet the needs of utilizing the quantum hardware. As Tim Polk, of the White House Office of Science and Technology Policy said, "it doesn't help to have a quantum computer if no one knows how to program it." Think of classical computers, if we didn't have engineers who understood how to program them, they would not be the powerful tools that they are today. This logic is simple, and it applies to quantum computers as well, in stressing the need for engineers who know how to "speak quantum."

Freeke Heijman, one of the leaders the Quantum-Technology Institute of the Netherlands, warns of the dangers of spending all this money on developing these quantum technologies, and then making them commercially available for regular consumers, specifically the ones developed for national security/defense applications. This is contrasted with the creation of the Global Positioning System, or the GPS, where the U.S. government spent large amounts of resources to develop this technology behind the scenes, made for consumption only by the military, later becoming commercially available to all, eventually becoming something almost everyone uses. This contradicts with the notion that even consumers will "have to learn to speak quantum." Some examples of the importance of learning to program quantum computers, or learning to "speak quantum" in general are presented in the article.

1. In order to combat the deficit of programs which interact with these quantum machines, many companies have set off to create such languages, one example being IBM, who released a commercially available program to use for programming general purpose quantum computers.
2. Another example is Microsoft, who is developing LIQUi$|\rangle$ (liquid), targeting to create everything from UI to machine language, planned on being compatible with the machines being developed by Microsoft, and not only.
3. Even in the business world, companies such as QxBranch are looking for companies whose product or business could benefit from utilizing quantum technology, showing the importance of businesses who are not necessarily in the tech industry being able to understand quantum in order to optimize their business model using quantum technology.
4. Governments necessity to "speak quantum" is perhaps the most important, being exemplified by the NSA stating that they would be updating all of their encryptions to make it safe from quantum computers, and this could apply to all government agencies, across the world, not just specifically national security agencies.