Global Challenges Foundation

Quantum computing

Reviewed by

Nicklas Berild Lundblad
PhD informatics, Global Head of Technology Policy at Stripe

While great progress has been made in quantum computing research, we are at least 5 to 10 years away from any real world applications of quantum computing. We can, however, already now sketch out the risks that will be associated with such real world applications. Technological risks can be divided into risks that have to do with access to these technologies, use of them and any unintended effects they may carry.

De Wolf (2017) has suggested that quantum computing is likely to impact three different areas - cryptography, optimization and simulation. If we look at these three we can construct a set of risks that need to be addressed as quantum computing improves.

First, access to quantum computation will allow an actor to break today's cryptographic systems and optimize far better. The simulation of quantum systems matter less in this category, but the two first present real risks. The reason for this may not be immediately obvious, but has to do with the possible technological asymmetry that arises if one actor has access to the technology and others don't. Today's quantum computing research is concentrated to the US, and to a few companies that also hold the majority of the patents.

There is a real chance that the US will achieve a sustainable technological advantage here. Such an advantage could trigger a pre-emptive attack from other countries that fear that with this technological advantage, the US will also achieve military advantages that present an unacceptable threat to these other countries. Asymmetric access to technologies that shift the power balance by an order of magnitude creates incentives for preventive moves.

Secondly, if we look at the use of the technology, the most obvious risk is that our cryptographic systems are built around problems that are easy to construct but hard to solve, such as factoring problems. Quantum computing could, theoretically, make such problems easy to solve and the mere existence of such technologies would undermine trust in the security systems that have been deployed in the last several decades. We should not overstate this risk, however,

since the technology would not immediately make it easier to mass-decrypt communications - the challenge is rather that we would know which transactions we could trust and which transactions that could have been corrupted.

In optimization the ability of some actors to optimize faster and better than others could drive inequality through network effects and scale advantages.
If a few companies manage to optimize far better than others, their ability to free up resources, learn and then use those improvements to create an accelerating improvement spiral would place them beyond competition.