QUANTUM COMPUTING - PREPARING FOR THE MOST COMPLEX UPGRADE EVER: IT'S ABOUT TIME!

In January 2024 Abu Dhabi Global Market Academy (ADGMA) Research Centre (in partnership with ADIA Lab, Imperial College London and Nanyang Technological University) hosted a three-day conference, Quantum Computing for Finance, gathering nearly 300 leading experts from the financial sector, quantum technology firms and academia from around the world.

The intersection of quantum computing and finance holds promise for solving complex problems, optimising processes, and advancing computational capabilities. The outcomes of such collaborative efforts have the potential to reshape the landscape of financial technologies, bringing about innovative solutions and advancements in the field.

While there are many expected positives from quantum computing, there are also several challenges. One of the conference speakers, Dimitri van Esch, Chair & Founder of Quantum Gateway Foundation and former Quantum Lead at ABN Amro, believes that a move to quantum computing will be the most complex upgrade ever undertaken. And time is of the essence.

The ADGMA Research Centre sat down to discuss this with Dimitri.

ADGMA RESEARCH CENTRE: YOU'VE LONG BEEN A PROPONENT OF SECURITY RISKS AS A RESULT OF QUANTUM COMPUTING. WHY DOES QUANTUM PRESENT A RISK?

> ***Dimitri****: We live in a digital world, with most financial transactions taking place over the internet or through phone apps or by some electronic method. But we are not necessarily using the latest technology.*
>
> *Let me give a little history of the Internet. The Internet has grown from a few computers connected to each other with low-speed dialup phone lines in the 1960s to a global network of billions of people connected through medium and high-speed links that are reaching up to gigabits. Most of us can't imagine living our life without the Internet.*

Some of the technologies at the core of the Internet, however, were created in the 70's. TCP/IP started in 1974 and in 1975 SMTP was introduced, and both are still used today (with additional 'workarounds' and 'layers' built on top to meet evolving requirements privacy and security).

As the Internet has increased in importance, we've needed to add new and improved layers of technology. Layer after layer was added, updates from security protocols were created, until we reached the point that developing an application required significantly more focus on non-core functionality, resulting in shortcuts in security functions.

Today we're facing an Internet landscape consisting of more than one billion websites, almost nine million apps, 200 million API backends, over 700 programming languages, more than 350,000 software libraries and 100+ cipher suites to choose from.

Additionally, there is a significant use of COBOL, one of the early programming languages, still used by more than 90% of Fortune 500 companies (there are estimates of more than 30,000 organizations globally still using it). The real challenge is nobody speaks COBOL anymore. If you need to upgrade such an application, how are you going to do it?

This relates to quantum because in 1994 Peter Shor (Professor of Applied Mathematics in the Department of Mathematics at MIT), developed what's known as Shor's Algorithm, which constitutes a method for quantum computers to find the prime factors of a figure, offering an exponential speedup compared to classical computing. This 'hard' problem for classical computing is the foundation for most of our existing asymmetric security protocols, but it's 'easy' with quantum computing. These protocols are used in approximately 90% of all internet applications worldwide, and almost 100% of mobile phone applications.

ADGMA RESEARCH CENTRE: SO THE FUNDAMENTAL BENEFIT OF QUANTUM COMPUTING ALSO PRESENTS A SECURITY RISK. WHAT ARE WE TALKING ABOUT? HOW BIG IS THE RISK?

***Dimitri**: The risk is global, and could become a societal problem due to two factors:*

- *The way our cyber security governance works.*
- *The way we consume news and information.*

Let me give you a worst-case scenario. It's 2035 and someone is able to run Shor's Algorithm on a medium sized (4,000 logical qubits) quantum computer and can break an RSA2048 keypair in a couple of hours (and they can do this twice to demonstrate repeatability). When this happens, and they publish their results, current asymmetric security protocols will be labelled as insecure. This will likely lead to new regulations stating that regulated organisations must use security protocols that are either labelled 'secure' or 'recommended'. Hence there will be an immediate need to upgrade all existing security applications.

But that's not the worst part. When such a publication is made, news agencies and social media will elaborate and spread the news. I can picture headlines such as 'The Internet is broken'.

This could lead to a panic and a run on the banks. If Internet and mobile banking no longer work, it would have significant and far-reaching consequences. There would be a surge in the demand for physical cash, which banks will find challenging to meet. This would lead to delays in bill payments. Transactions that are normally instantaneous will take longer, impacting both individuals and businesses. This would result in an overall economic impact on stock markets, online trading etc. And the problem would not be localised. We live in an interconnected world, so the impact would be global.

ADGMA RESEARCH CENTRE: YOU MENTIONED 2035. WHY THEN?

***Dimitri**: According to a survey conducted by Dr. Michele Mosca (Institute for Quantum Computing, University of Waterloo) there's a 50% chance that a quantum computer could break our existing security algorithms in 2035. If you look at the current developments of quantum computers, this might well come true. It could also happen a few years later. Depending on who you ask, you'll get answers ranging from 2030 up to 2045. There are some, however, who say this will never happen.*

ADGMA RESEARCH CENTRE: IF WE ARE TALKING ABOUT SOMETHING THAT IS STILL SEVERAL YEARS AWAY (IF EVER), WHY DO WE NEED TO ACT NOW?

***Dimitri**: There are solutions being worked on to prevent this worst-case scenario ever taking place. We have developed new protocols called Post Quantum Cryptography (PQC), which are security protocols that are resistant to this quantum threat, and we are developing communication technologies protected by quantum technology to make online communication even more secure.*

The challenge is that to implement these new technologies we need time and resources.

Security protocol upgrades for large organisations have in the past taken more than 10 years to complete. And those are simple drop-in replacements of existing protocols (e.g. replacing one component with another one without any other code or configuration changes being required).

There is an additional factor that organisations must consider in terms of allocating resources to an upgrade. Many financial institutions have legacy systems that might be operating on 32-bit architecture. The 32-bit time counter will 'end' on 19th January 2038. This is similar to the Y2K issue in 2000. In this context it is based on the limitations of a 32-bit figure representing time. So we need to ensure all our applications are upgraded to 64bit. This has nothing to do with the quantum threat, but it will require a huge number of resources as we've previously seen with Y2K.

Quantum computers are still in the early stages of development, and practical, widely accessible quantum computers are still some years away. Quantum computing is, however, a rapidly advancing field, and progress continues to be made by researchers and companies every day.

Whether quantum computers become widely available before or after 2035 is not necessarily relevant. The reality is that when they do become available, they will have a significant impact on the global financial sector. It's just a matter of time. But it is also a reality that any kind of systems upgrade takes time and effort and comes at a cost.

ADGMA RESEARCH CENTRE: WE NEED TO BE READY TO TAKE ADVANTAGE OF THE BENEFITS PROMISED THROUGH QUANTUM COMPUTING WHILE AT THE SAME TIME MITIGATING THE RISKS. THIS IS A DIFFICULT TASK BASED ON A TECHNOLOGY THAT IS STILL IN DEVELOPMENT. WHAT CAN FINANCIAL ORGANISATIONS DO TODAY TO PREPARE FOR THIS?

> *Dimitri: Financial institutions have numerous interconnected and standalone systems across their organisations, with a variety of cryptographic protocols protecting them. But it's unlikely that they have a comprehensive inventory of those systems and protocols. As a first step institutions should create a comprehensive inventory. This is the only way in which they can be sure, when they time comes, that they upgrade all of their cryptographic protocols to be quantum ready.*

By outlining the short, medium, and long-term prospects of this new tool for the finance industry, the Quantum Computing for Finance conference focussed on clarifying the current state of quantum computing through discussions on machine learning, algorithms, portfolio optimisation, forecasting, and communications. The conference gathered global and local leading experts from finance, academia and quantum technology firms including the Technology Innovation Institute, Zayed University, UC Santa Barbara, National University of Singapore, NASA Ames, IBM, IonQ and JPMorgan Chase & Co. who tackled the central question – the impact of quantum computing in finance.

While still in its early stages of development, quantum computing has the potential to fundamentally reshape the financial industry. On the negative side quantum computers have the potential to break many of the encryption algorithms widely used in banking and finance for transactions and customer information. This means that traditional security measures may become inadequate in the face of quantum computing, posing significant risks to data privacy and financial security.

On the plus side, several success stories have shown that some computations can only be performed using quantum computers, as their classical counterparts quickly run out of memory. Banks that are early adopters of quantum computing technology may gain a competitive edge over their rivals. Quantum computing has the potential to revolutionize various aspects of banking operations, from risk assessment and portfolio optimisation to fraud detection and algorithmic trading.

Banks need to start preparing for this future now by investing in research and development, building internal expertise, and exploring potential use cases for quantum computing in banking and finance. Not only will they be quantum ready, but also seen as industry leaders and innovators.

It's TIME!

ADGM Academy
Research Centre

FOLLOW / CONTACT US:

- https://www.adgmacademy.com/
- research@adgm.com
- LinkedIn