

ARE YOU READY?

Quantum randomness made simple



July 11, 2019

Jeffrey Cohen, President, US Advanced Computing Infrastructure, Inc.

The word map of the first month of tweets from Chicago Quantum (note the business language)

On July 2, 2019, the founder blogged about the challenge of converting quantum computing into business language. He discussed our first beta client, a pizza chain, and how we were going to optimize pizza delivery. It was full of jargon and clever math terms like ‘quasi-Monte Carlo simulation,’ vectors, dimensions, and even ETL (extract, transform and load) the data. We could have discussed stochastic sampling if we liked.

This is not helpful in a most business or social contexts. People ask about the business and ‘hey, what’s quantum’ and expect an answer they can relate to.

Sean, an office colleague, asked about the business yesterday. We spoke about generalities (sales, revenue, hiring, marketing, collaboration, etc.) and then our current client challenge. Here is how I explained the work.

Do you gamble with cards? Games like poker or blackjack? “Sure”, he said. You know the computer games where you practice hands at home? If you win 400 out of 500 hands you feel ready to go to the casino and bet real money, but it usually does not work out that way when you go. That is because today’s computers and phones are not good at being random.

Quantum computers work super-fast with probabilities and lots of choices. They can also be very random, like the nature it is based on. He said, “So, when you measure it, it’s over, right? Like Schroedinger’s Cat?” Yes, when you ask for the answer, you get the best answer at that moment...a real number. To be sure, you can ask it to repeat the problem and take the most common answer. That answer is what you use.



Founder & CEO, Jeffrey Cohen during the start-up of the Chicago Quantum division.

“So, when you measure it, it’s over, right? Like Schroedinger’s Cat?”

SEAN (OFFICE COLLEAGUE)

So, you do the up-front calculations and preparation on a regular computer, then call the quantum computer, then go back to regular computers (or write a report) to use the answer.

Back to winning at cards. So, imagine we could deal truly random cards. If you won 400 out of 500 hands, you would be more confident heading to the casino (we believe is random). This made sense to him. Run an analysis many times, using truly random input, and take the

most common answer. For pizza delivery, we would also look at the distribution of answers to understand our confidence with the operational, mathematical model we built based on truly random samples of their data.

As an aside, post-quantum security requires large amounts of random numbers to create keys to encrypt communications. This is why we see firms pair up quantum key distribution (QKD) and quantum random number generators (QRNG).

Key take-aways:

- Quantum computers are truly random (based on nature), which gives more independent results.
- Quantum computers look at many probabilities and choices, then stop and give you an independent answer. Repeat often enough and you build confidence in the answer.
- We do all data preparation work on a classical computer (like a Linux server), then call the quantum computer for the computationally hard work.
- In casino gambling, once we know the best cards, draws, and bets to make in a truly random casino game, we then have to think whether our casino experience is random.

Hope you enjoyed this BLOG post.

Jeffrey Cohen

@Chicago_Quantum (Twitter)

<https://www.chicagoquantum.com>

+1.312.515.7333 (cell)