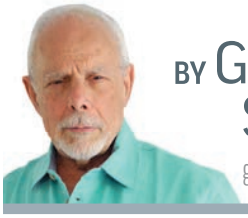
SHOULD YOU WORRY ABOUT QUANTUM?



BY GIDEON SAMID
gideon@bitmint.com

LAST MONTH, *The Wall Street Journal* reported that Visa and JPMorgan Chase are gearing up to face the threat of quantum. Indeed, the drumbeat is getting louder. A new class of computing machines is coming down the pike, and much as present-day computers upended the payment industry, so will the new ones.

Richard Feynman, a primary physicist, a Noble Laureate, once asserted that "no one understands quantum." This includes payment professionals. Indeed, while all modern electronics is based on quantum physics, it is not clear how reality behaves in microcosm. We observe this behavior and express it with math, but we don't understand what we observe.

I have had some success laying the quantum story out to colleagues, so let me try it here. Present-day computers are based on electronic circuitry that generates the same output for a given input, time and again. That premise holds true in the visible world, but, as was discovered early in the last century, the smaller elements of reality react to the same stimulus the way dice reacts to tossing then. When you roll the dice on the table, you don't know what they will show. You only have probabilities. If the dice are "fair," then every outcome is associated with a probability of 1/6. Elements of the microcosm are characterized by the probability of an outcome when engaged.

In addition, we have another mystery called entanglement. If two spinning coins are entangled, then their collapse into heads or tails appears coordinated, even though they may be very far apart. Again, no explanation, only observation. This combination of probability outcome and entanglement allows us to construct computing circuitry that far exceeds what non-quantum machines can do.

Very well, so we compute faster. Why worry? It turns out that payment today is based on a silent assumption that computers are sufficiently slow to prevent them from breaking the security of money transfer. Once this assumption collapses—as will happen with the emergence of quantum computers—then everything from small online purchases to large interbank wire transfers will no longer be secure. Unfortunately, cryptocurrencies will not save the day. They too hinge on this under-emphasized assumption that computers will remain not much faster than they are today.

The threat is real. Imagine that payment goes back to coins and banknotes only! So now the question is, how much time do we have to prepare for this calamity? Recent bold announcements by China, Google, IBM, and Microsoft suggest an imminent emergence of quantum machines. Moreover, powerful computers are national strategic assets, so most governments are feverishly—and silently—developing their own capabilities. They calm everyone with assurances that quantum is years ahead.

We at BitMint join a determined movement to use present-day computers to fend off the quantum assault. Our particular choice is to apply a "quantum vaccine" against the quantum attack. This "vaccine" is the new technology for quantum-grade randomness (see U.S. patent 10,467,522), which, if applied lavishly (patents 10,728,028 and 10,541,808), will defend digital payment against the most robust quantum attack. Preliminary deployment of our technology is very promising.

The flipside of the quantum threat is the quantum promise. Those probabilities of outcome I mentioned earlier are very delicate, which makes any "data touching" detectable. This is big. Digital data today can be stealthily compromised. But quantum-set data cannot be looked at without leaving fingerprints.

Quantum computers used for artificial intelligence will result in artificial personal CFOs—software in charge of our personal money management. Exciting times ahead! DT