LIFEBOATS ON THE TITANIC

BY GIDEON SAMID
gideon@bitmint.com

Call me a sore loser, if you will, having just lost the prestigious G20 BIS 2022 CBDC contest to a payment company from the Philippines, Dragonpay. I arm myself with excuses. Perhaps. Dragon is a fine, accomplished outfit. The thoughtful judges saw more merit there than they identified in BitMint.

But the reason I bring this story to the readers of my column is that BitMint's slogan was "Quantum Safe Technology," which was a cry in the wilderness. Only one other competitor, Idemia, addressed the quantum threat. None of the other shortlisted finalists in this competition (Mastercard included) claimed priority on account of their resilience to the pending quantum attack.

Moreover, when I asked the judges about the weight of quantum resilience in their considerations, the answer was unanimous: not a priority, nothing imminent, and anyway, the U.S. National Institute of Science and Technology (NIST) has already published several quantum-resistant algorithms, so all is well.

The prize-awarding international event brought together global financial executives of the highest order. They talked about what they know: cross-border, settlements, privacy, money laundering, escrow—policy, policy, policy. The fact that cyber finance (legacy and digital) relies on an obscure mathematical construct called an elliptic curve was not brought up. The fact that financial cybersecurity is hinged on the assumption that its attacker is armed with no more than Turing machines was not mentioned. The reality that every serious crypto shop in the world is busy advancing quantum computing—and most of them are doing so in stealth—was not an issue.

As to NIST, they are worried indeed. They launched a global campaign to develop quantum-resistant algorithms to meet the threat that bankers stubbornly ignore, and they are in a hurry. Unlike climate change, where we have credible models for when the coming threat will arrive and how damaging it will be, with quantum we have no credible estimate as to when the blow will fall and how powerful it will be. What is easy to conclude is that, if quantum hits before we are ready, global cyber payments will collapse. Only coins and banknotes will do.

Cryptographically speaking, we have a brute-force quantum defense, ready to fend off any attack, quantum included. I have personal knowledge that high-value cyber targets integrate this "pattern-devoid cryptography" in their cyber-defense posture. But talking about it is not good for business. It highlights the vulnerability of the ciphers the industry is promoting as flawless.

The Titanic was billed as the ship that could not sink, packed with the latest in high tech. It was a lonely voice that argued in favor of lifeboats, "just in case." That is how I see us, the few and far between who ask, while NIST is developing quantum-resistant high tech—none of which has been field-tested—why not deploy what we do have, which does not need testing because it comes with a "good-to-go" stamp from the most reliable source humanity has: mathematics. We have the lifeboats just in case. We hope we will never have to use them.

I am way out of my comfort zone here. Perhaps some readers of mine are ready to help out, knock on doors, do something creative. Oh yes, I did something quite unusual. Being a closet writer, I play with a literary pen. I've used it for matters of the heart, but now have turned it to a nail-biting cyber thriller: *The Cipher Who Came in from the Cold*. The psychologist Steve Harvith says that my style is similar to that of Ernest Hemingway. Do you agree? DT