Quantum-Safe Cryptocurrency: Challenges for the Future

Health/Science

Posted by:

Posted on : 2018/3/25 17:18:08

“In the 2020s, we will have quantum computers that are significantly better than super computers today, but they most likely won’t be in mass use by governments and companies until the 2030s.”

By Eric Eissler for CCN, Mar 25, 2018: The future of computing is starting to arrive with the race to build the first stable quantum computer that would be able to far exceed classical computers’ ability to perform operations. For example, a 50 quad-bit computer equals 1.125 quadrillion classical bits. Quantum computing is the next level of computers and they carry with them the power to totally supplant work that classical computers do, namely crack uncrackable encryption within seconds, and compromise Bitcoin address and API keys. For a quantum computer, this will be a small feat. Currently, the chances of someone being able to hack a private key to a bitcoin wallet that might contain a substantial amount of currency is very small: 0.024% chance with a classical computer. To put that in perspective, that percentage of a successful hack is equal to winning the lottery multiple times in a row. Practically impossible, but not improbable. While quantum computing is not there yet, companies such as Google and IBM are working on projects and state that we are only 5 years away from so-called “quantum supremacy,” where quantum computers surpass what a classical computer could ever imagine being able to do. Referencing the 50-quadbit computer mentioned previously, IBM is currently working on one of this size. […] https://www.ccn.com/quantum-safe-crypt ... hallenges-for-the-future/