New white paper maps the very real risks that quantum attacks will pose for Bitcoin

November 2 2017

Credit: Macquarie University

Combining expertise in quantum technologies and cryptography, researchers have been projecting future dates that quantum computers

could jeopardise the security of current cryptocurrencies, a market now worth over USD $150 billion, and assessing countermeasures to such attacks.

Macquarie University physicist Associate Professor Gavin Brennen, together with Australian entrepreneur Dorjee Sun and researchers in Singapore and Sydney, has announced a collaboration with blockchain company Hyperchain on providing quantum security to digital currency. The team named Quantum Resistant Coin (QRC), includes researchers A/Prof. Brennen at Macquarie U., Prof. Miklos Santha at CNRS Université Paris Diderot and Centre for Quantum Technologies (CQT), A/Prof. Troy Lee at Nanyang Technological University and CQT, and Senior Lecturer Dr. Marco Tomamichel at UTS.

They have just released a whitepaper which finds that Bitcoin and other cryptocurrencies will be vulnerable to attacks by quantum computers in as little as 10 years. Such attacks could have a disastrous effect on cryptocurrencies as thieves equipped with quantum computers could easily steal funds without detection, thus leading to a quick erosion of trust in the markets. They also assess the risk of quantum dominated mining in so called Proof of Work protocols which are the basis for verifying transactions in Bitcoin and many other cryptocurrencies.

Leading edge blockchain company Hyperchain, which provides technical services to Hcash (CoinMarketCap.com Hshare with a market capitalisation of over USD $300 million), has now enlisted QRC as technical advisors. They will work with Hcash, Hshare and Hyperchain to make sure that their cryptocurrency is resistant against quantum attacks.

"I've been working on the theory of quantum computers for well over a decade and the exciting thing is that now very simple quantum machines, like the Google device, are a reality," says co-author Brennen, who is

director of the Macquarie Quantum Science and Technology Centre (QSciTech) where researchers work on quantum science theory and experiment.

"Understandably, there is a lot of nervousness in cryptocurrency communities about whether their digital assets will resist future attacks by very fast quantum computers. Our service is providing advice and algorithmic protocols to digital currencies and blockchains like Hcash who want to certify their product will be quantum safe. HCash has put emphasis on quantum security from the start so this collaboration will be a benefit to both teams"

Brennen, comments further, "I'm excited to be part of this team joining excellent people working in pure physics and computer science at UTS, CQT, and NTU with Dorjee Sun who is a social entrepreneur. The open environment at Macquarie was key in getting this going, in fact the whole enterprise started with a conversation with Dorjee over coffee and lots of scribbled notes at the Macquarie Hub this Winter."

More information: Quantum attacks on Bitcoin, and how to protect against them. arXiv:1710.10377 [quant-ph] arxiv.org/abs/1710.10377v1

Provided by Macquarie University

Citation: New white paper maps the very real risks that quantum attacks will pose for Bitcoin (2017, November 2) retrieved 29 April 2024 from https://phys.org/news/2017-11-white-paper-real-quantum-pose.html