Cambridge Quantum

PRESS RELEASE

Cambridge, United Kingdom
Tuesday, August 10 2021

IDB Lab, Cambridge Quantum and Tec de Monterrey develop blockchain resistant to quantum computing

IDB LAB, CAMBRIDGE QUANTUM AND TEC DE MONTERREY develop blockchain resistant to quantum computing

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, August 10 2021

The Inter-American Development Bank and its innovation laboratory, IDB Lab, together with Cambridge Quantum (CQ) and Tecnológico de Monterrey have identified and resolved potential threats to blockchain networks posed by the advent of quantum computer development. In response to these threats, the project team developed a cryptographic layer that allows blockchain networks to protect themselves from this new generation of computing technologies.

Four potential threat areas for blockchain networks have been identified, including communication between network nodes and the integrity of digitally signed transactions. Each threat area relies on cryptography and keys which are vulnerable to attacks by quantum computers and needs to be improved to ensure the security and integrity of blockchain networks.

To address these threats, a post-quantum cryptography layer that protects networks and offers resistance to quantum computer attacks was developed on the LACChain Besu blockchain network, based on Ethereum technology. Transactions and communications were protected with quantum-proof keys from CQ's Ironbridge platform, which uses quantum computers to generate certified entropy.

"While certain quantum algorithms allow for breaches of digital security protocols, luckily we also have others we can use to strengthen our data protection capabilities,"

said Salvador E. Venegas-Andraca Professor-Researcher and Director of the Quantum Information Processing Group of Tecnológico de Monterrey.

THE PROJECT TEAM DEVELOPED A CRYPTOGRAPHIC LAYER THAT allows blockchain networks to protect themselves

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, August 10 2021

Duncan Jones, Head of Quantum Cybersecurity at CQ, emphasized that "LACChain blockchain was an ideal target for keys generated by our IronBridge platform. Only keys generated from certified quantum entropy can be resistant to the threat of quantum computing."

Irene Arias Hofman, CEO of IDB Lab, said that "in the digital age in which we find ourselves we have at our disposal different emerging technologies with the capacity to solve social problems, and to the extent that we are able to combine them we will achieve an exponential impact. In this case, the knowledge of the IDB team, together with CQ and TEC, in both quantum and blockchain technologies, has made it possible to achieve a fundamental milestone to guarantee the future integrity of LACChain, a blockchain platform created by the IDB Lab which more than 50 entities in the region are using already."

For more information, see the technical note documenting this milestone here.

ABOUT IDB LAB

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, August 10 2021

IDB Lab is the innovation laboratory of the IDB Group, the main source of financing and knowledge for development focused on improving lives in Latin America and the Caribbean. The purpose of IDB Lab is to promote innovation for inclusion in the region, mobilizing financing, knowledge and connections to test private sector solutions at an early stage with the potential to transform the lives of vulnerable populations by economic, social and environmental conditions. Since 1993, IDB Lab has approved more than US$2 billion in projects deployed in 26 countries in Latin America and the Caribbean.

FOR MORE INFORMATION

LinkedIn
GitHub
Bidlab.org

ABOUT CAMBRIDGE QUANTUM

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, August 10 2021

We set out our vision to positively transform the world using the power of quantum computing back in 2014. Today, we are recognised as one of the foremost quantum computing companies, delivering science-led, enterprise-driven solutions to tackle hard problems across a diverse range of industries.

Cambridge Quantum designs, engineers and deploys algorithms and enterprise application libraries, translating cutting-edge research into industry leading technologies through a product-centric focus. Tket, our hardware-agnostic software development platform, and other technologies are currently utilised by an expansive and ever-growing user base.

The team at Cambridge Quantum has been developing the theoretical foundations of quantum computing for over 25 years, forging ahead with breakthroughs in the fields of quantum chemistry, quantum artificial intelligence, quantum cybersecurity and quantum algorithms.

At present, we have the deepest roster of researchers, developers and engineers, working to democratise quantum computation and realise the benefits for the greatest possible number of people.

FOR MORE INFORMATION

CambridgeQuantum.com
LinkedIn
Access the Tket Python module on GitHub

Tecnológico de Monterrey

ABOUT TEC DE MONTERREY

PRESS RELEASE
Cambridge, United Kingdom
Tuesday, August 10 2021

Tecnológico de Monterrey was founded in 1943 thanks to the vision of Don Eugenio Garza Sada and a group of entrepreneurs who formed a non-profit association called Enseñanza e Investigación Superior, A. C. Tecnológico de Monterrey is a private, non-profit, independent institution with no political and religious affiliations. The work of Tecnológico de Monterrey and all its campuses is supported by civil associations made up of a numerous group of outstanding leaders from all over the country who are committed to quality in higher education.

FOR MORE INFORMATION

LinkedIn
GitHub
Tec.mx