

Berita Harian, Page 4, Section: BERITA

Friday 18 July 2025

498 words, 483cm<sup>2</sup> in size

28,500 circulation

# OCBC, universiti tempatan jalin kerjasama dalam bidang pengkomputeran kuantum

Bank OCBC memeterai perjanjian kerjasama dengan tiga universiti tempatan bagi memanfaatkan kuasa pengiraan komputer kuantum yang dipertingkat bagi mengukuhkan pengesanan penipuan dalam masa nyata dan memastikan data lebih selamat terhadap ancaman baru.

Perjanjian kerjasama penyelidikan selama 12 bulan antara bank itu dengan Universiti Nasional Singapura (NUS), Universiti Teknologi Nanyang (NTU) dengan Universiti Pengurusan Singapura (SMU), diumumkan dalam satu taklimat media pada 17 Julai.

Di bawah perjanjian itu, OCBC akan memanfaatkan algoritma kuantum bagi melaksanakan penentuan harga derivatif, proses menentukan nilai produk derivatif ekuiti seperti opsyen, perdagangan hadapan dan swap, lapor *The Straits Times* (ST).

Ketua Penasihat Kuantum, Kementerian Penerangan dan Pembangunan Digital (MDDI), Encik David Koh, berkata kerjasama itu adalah langkah ke landasan yang betul kerana kuantum kini adalah sesuatu yang nyata. .

Ini memandangkan teknologi itu akan dapat menyelesaikan masalah yang dianggap mustahil oleh sistem pengkomputeran biasa.

Beliau, yang juga Ketua Eksekutif, Agensi Keselamatan Siber (CSA), berkata:

“Bagi OCBC, ia boleh mengoptimumkan instrumen kewangan.”

Bagi institusi perbankan lain pula, ia boleh antara lain menyelesaikan masalah logistik yang kompleks, mempercepat penemuan dadah dan meningkatkan keselamatan terhadap peningkatan ancaman siber, tambahan.

“Jika kami boleh melakukan hal ini dengan baik, kami akan ada ekosistem kuantum yang menawarkan perniagaan kami kelebihan daya saing sangat dalam hab digital bagi generasi akan datang,” kata beliau.

Singapura telah membelanjakan \$700 juta bagi penyelidikan dan pembangunan teknologi kuantum sejak 2022.

Pada 2024, OCBC mula melatih pekerja dalam pengkomputeran kuantum, termasuk kecekapan dalam aplikasi kuantum, pengaturcaraan dan langkah keselamatan.

Sebahagian daripada 50 kakitangan OCBC yang te-



Sesi pemerataian perjanjian kerjasama bagi penyelidikan dihadiri (dari kiri) Pengarah Pusat Strategik Penyelidikan dalam Teknologi dan Sistem Pemeliharaan Privasi, Universiti Teknologi Nanyang (NTU), Profesor Wang Huaxiong; Ketua Operasi Kumpulan dan Teknologi OCBC, Encik Praveen Raina; Ketua Penasihat Kuantum, Kementerian Penerangan dan Pembangunan Digital (MDDI), Encik David Koh; Timbalan Pengarah Pusat Teknologi Kuantum, Universiti Nasional Singapura (NUS), Profesor Valerio Scarani; dan Dekan Bersekutu, Sekolah Pengkomputeran dan Sistem Maklumat Universiti Pengurusan Singapura (SMU), Profesor Madya Zhu Feida, pada 17 Julai. – Foto OCBC

lah dilatih setakat ini akan terlibat dalam kerjasama penyelidikan dengan ketiga-tiga universiti tersebut.

Penyelidikan itu melibatkan kerjasama dengan Pusat Teknologi Kuantum (CQT) NUS bagi mempercepat simulasi *Monte Carlo*, teknik yang digunakan secara meluas dalam penentuan harga derivatif kewangan.

Derivatif ialah kontrak antara dua pihak, dengan nilai bergantung kepada pelbagai keadaan pasaran, ujar Penolong Profesor NUS Patrick Rebentrost.

Untuk mendapatkan nilai saksama, bank perlu mendapatkan purata menyusuli simulasi pelbagai keadaan pasaran.

Beliau berkata: “Komputer tradisional perlu melaksanakan simulasi jutaan senario berbeza manakala komputer kuantum hanya perlu melaksanakan simula-

si ribuan senario bagi mendapatkan hasil yang sama.”

Bagi mempercepat pengesanan penipuan secara tepat, OCBC akan bekerjasama dengan SMU untuk menggunakan teknik pembelajaran mesin kuantum.

Ini dilakukan untuk memproses data kompleks dan tidak berstruktur bagi mengenal pasti corak dan anomalai yang menunjukkan kegiatan penipuan.

Sementara itu, Pengarah Pusat Strategik Penyelidikan dalam Teknologi dan Sistem Pemeliharaan Privasi di NTU, Profesor Wang Huaxiong, berkata kerjasama OCBC dengan NTU dijangka mengukuhkan teknik kriptografi bagi memanfaatkan kepakaran universiti tersebut dalam “membangunkan penyelesaian yang mampu bertahan dengan serangan siber generasi seterusnya”.