

Il potenziale impatto dei computer quantistici sul panorama della crittografia e delle criptomonete – Cyber Security Virtual Conference 2020



Il calcolo quantistico permetterà notevoli progressi scientifici, ma quali sono i rischi per la sicurezza?

Durante la tavola rotonda tenutasi su www.ictsecuritymagazine.com, è stato analizzato “*Il potenziale impatto dei computer quantistici sul panorama della crittografia e delle criptomonete*”. Lo scorso 8 luglio, gli esperti hanno condotto un’accurata e specialistica analisi sulle possibili modalità in cui i progressi nel campo del Quantum Computing avranno una serie di conseguenze sulle attuali misure di sicurezza informatica, in particolar modo su quelle usate nell’ambito della crittografia e delle criptomonete. Che cosa sono gli elaboratori quantistici? Al giorno d’oggi, esistono già dei computer in grado di compiere operazioni logiche secondo le leggi della meccanica quantistica? In realtà, nonostante i primi prototipi siano stati realizzati, l’avvento di una simile tecnologia – sulla quale colossi come Google stanno investendo ingenti capitali – non sembra essere così prossimo. Vi sono numerose ragioni che spingono a stimare un arco di tempo indeterminato, quasi sicuramente di gran lunga superiore ai dieci anni ipotizzati dai più ottimisti, per la concretizzazione di elaboratori quantistici con una capacità di calcolo utile. Ovvero, si dovrebbe raggiungere la capacità da 2000 Qubit, contro i 50

Qubit odierni. Le difficoltà sono molto elevate, a causa dell'instabilità degli attuali modelli, dovuta in gran parte alla difficile gestione delle particelle elementari, all'ipersensibilità alle minime variazioni ed alle peculiari condizioni ambientali in cui i computer quantistici possono operare.

In ogni caso, sono allo studio strategie efficaci per aumentare il livello di sicurezza – qualora il Quantum Computing compia balzi avanti –, sia nel campo della crittografia per la protezione dei dati che per quanto concerne le criptovalute, ad iniziare da Bitcoin. Negli ultimi anni, la crittografia simmetrica ha compiuto notevoli progressi che hanno del tutto rivoluzionato le tecniche di protezione dei dati strutturati, spostandosi sulle soluzioni dato-centriche – ossia, applicando chiavi di cifratura sul dato, proteggendolo indipendentemente dal contesto in cui verrà archiviato e rendendone inutile il furto. Invece, il problema si porrebbe sulla crittografia asimmetrica, poiché un computer quantistico sarebbe in grado di risalire in brevissimo tempo alla chiave privata, la quale è legata al possesso della criptovaluta. Come tenere al sicuro i propri Bitcoin? Quando diventerà concreto il rischio derivato dal calcolo quantistico?

Con **Paolo Dal Checco** – Consulente Informatico Forense, esperto di crittografia – nel ruolo di moderatore, intervengono: **Andrea Pasquinucci**, Consulente in Sicurezza Informatica, PhD in Certified Information Systems Auditor (CISA) e Certified Information Systems Security Professional (CISSP);

Federico Tenga, imprenditore in ambito Bitcoin, consulente strategico del Ministero dello Sviluppo Economico per l'industria Blockchain, Co-fondatore di BlockchainEdu e C00 di Chainside; **Vito Volpini**, Senior Security Solution Architect per Micro Focus ed Hewlett Packard Enterprise, ora Microfocus Security.

Sono attualmente disponibili i replay della Cyber Security Virtual Conference 2020, vi invitiamo ad accedere o effettuare la registrazione per visualizzare il contenuto integrale della conferenza, al seguente indirizzo web: 'Il potenziale impatto dei computer quantistici sul panorama della crittografia e delle criptomonete'.

<https://www.ictsecuritymagazine.com/notizie/il-potenziale-impatto-dei-computer-quantistici-sul-panorama-della-crittografia-e-delle-criptomonete-cyber-security-virtual-conference-2020/>