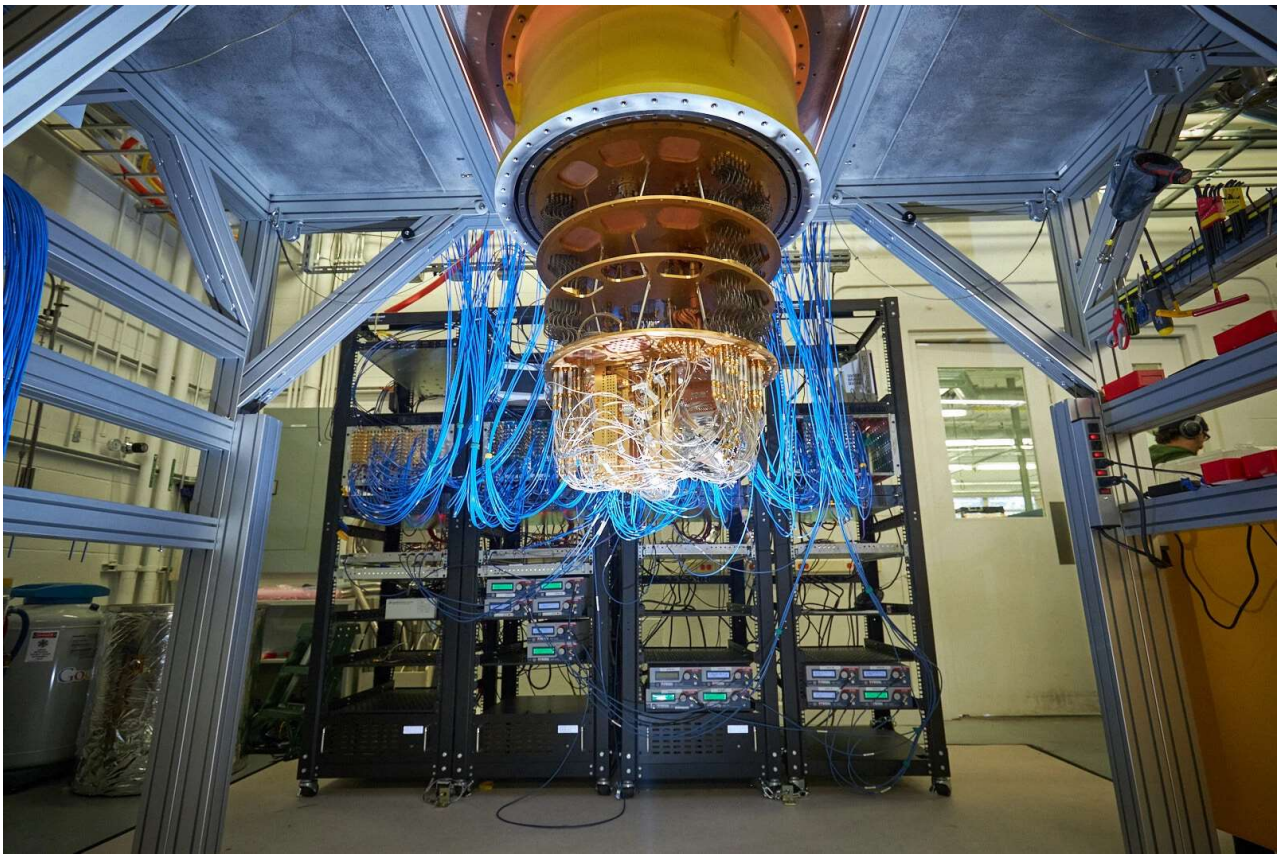
Ένας κβαντικός υπολογιστής μπορεί να αποκρυπτογραφήσει bitcoins;

secnews.gr/388747/kvantikos-upologistis-apokriptografisi-bitcoins/

February 1, 2022



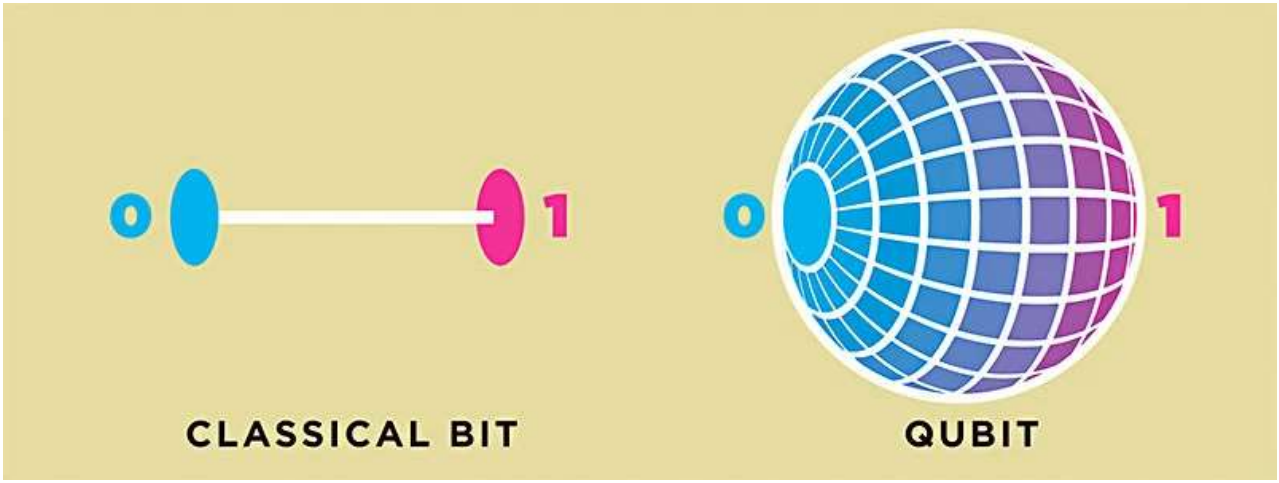
Επιστήμη & Τεχνολογία

By SecNews
1 February 2022, 16:00

Ένας εξελιγμένος κβαντικός υπολογιστής θα μπορούσε να εξυπηρετήσει την βιομηχανία με πολλούς τρόπους. Αυτήν την στιγμή ερευνάται η επίλυση δύο προβλημάτων: **Η αποκρυπτογράφηση bitcoins και η προσομοίωση του μορίου που είναι υπεύθυνο για την βιολογική δέσμευση του αζώτου.**

Ένας κβαντικός υπολογιστής θα χρησιμοποιούσε υπεραγώγιμες συσκευές για να λειτουργήσει, όπως αυτές που χρησιμοποιούν η IBM και η Google. Το υλικό μεταχείρισης του υπολογιστή θα διαφέρει ανάλογα με τον ρυθμό των υπολογισμών και την ποιότητα ελέγχου στα κβαντικά bit. Σε πολλές περιπτώσεις χρήσης αυτού του υπολογιστή

απαιτείται διόρθωση σφαλμάτων, η οποία επιτρέπει την εκτέλεση μεγαλύτερων αλγορίθμων αντισταθμίζοντας τα εγγενή σφάλματα που δημιουργούνται στον υπολογιστή. Ωστόσο η διόρθωση σφαλμάτων έχει μεγαλύτερο κόστος φυσικών κβαντικών bit.



Ένας κβαντικός υπολογιστής μπορεί να αποκρυπτογραφήσει bitcoins: Φωτογραφία από κανονικά bits σε σχέση με κβαντικά bits

Δείτε επίσης: Bitcoin bug έμεινε κρυφό για δύο χρόνια για να μην χρησιμοποιηθεί από hackers

Οι ερευνητές προσπαθώντας να δημιουργήσουν έναν τέτοιων προδιαγραφών κβαντικό υπολογιστή, αυτοματοποίησαν την διόρθωση σφαλμάτων και πρόσθεσαν περισσότερα κβαντικά bits για να γίνονται πιο γρήγορα οι υπολογισμοί. Επιπρόσθετα, εκμεταλλεύτηκαν κάποια σχέδια ιόντων για να μπορέσουν να μειώσουν τον αριθμό των κβαντικών bit, άρα και το τελικό μέγεθος του υπολογιστή.

Στις μέρες μας, χρησιμοποιείται η κρυπτογράφηση RSA και η κρυπτογράφηση των bitcoins, την οποία κανένας υπολογιστής δεν μπορεί να “σπάσει”. Ο κβαντικός υπολογιστής που θα κατάφερνε να πετύχει την αποκρυπτογράφηση bitcoins θα χρειαζόταν να έχει **30-300 εκατομμύρια αναγκαία κβαντικά bits,** σύμφωνα με τους ερευνητές. **Στην εποχή μας υπάρχουν κβαντικοί υπολογιστές μέχρι και 100 κβαντικά bits.**

Αποκρυπτογράφηση bitcoins και κβαντικός υπολογιστής

Να σημειώσουμε ότι 4 χρόνια πριν, μια συσκευή παγιδευμένων ιόντων, θα απαιτούσε ένα δισεκατομμύριο κβαντικών bits για να πραγματοποιήσει αποκρυπτογράφηση του RSA, πράγμα που αναγκάζει την συσκευή να έχει μέγεθος 100 επί 100 τετραγωνικών μέτρων. Μετά την τεχνολογική εξέλιξη των τελευταίων χρόνων όμως, το εκτιμώμενο μέγεθος είναι 2,5 επί 2,5 τετραγωνικά μέτρα.

Δείτε επίσης: Κβαντική συσκευή εκτελεί υπολογισμό 2,6 δισεκατομμυρίων ετών σε 4 λεπτά

Εν κατακλείδι, ένας τόσο μεγάλος κβαντικός υπολογιστής που χρησιμοποιεί την διόρθωση σφαλμάτων θα βοηθούσε στην εξέλιξη πολλών τομέων στην ανθρώπινη παραγωγή και στην ποιότητα ζωής.Η προσομοίωση των μορίων θα εφαρμοζόταν σε καλύτερες μπαταρίες και καταλύτες, καινούρια υλικά και φάρμακα. **Επίσης, θα μπορούσε να χρησιμοποιηθεί στην οικονομία, στην ανάλυση δεδομένων και στην αποδοτικότερη λειτουργία των αεροπλάνων.**

Με πληροφορίες από scitechdaily.com