पोस्ट-क्वांटम एन्क्रप्शन क्रप्टिोग्राफी

[स्रोत: हदुिस्तान टाइम्स]

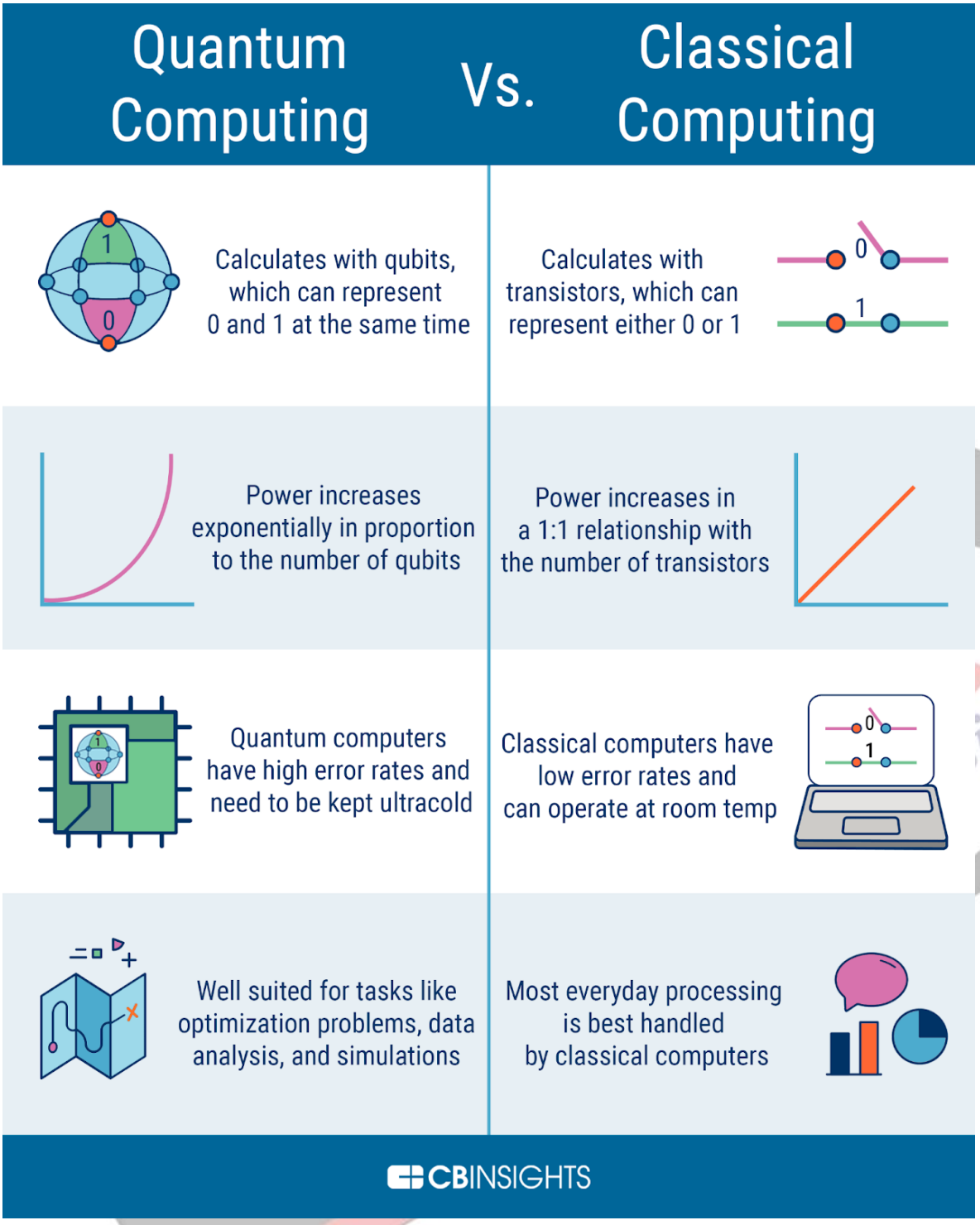
[वर्चुअल प्राइवेट नेटवर्क (VPN)] कंपनयिाँ [पोस्ट-क्वांटम क्रप्टिोग्राफी (PQC)] के कार्यान्वयन के माध्यम से [क्वांटम कंप्यूटगि] द्वारा उत्पन्न **संभावति खतरों** के अनुकूल बन रही हैं।

- [क्वांटम कंप्यूटगि] अत्यंत तीव्र गति से गणना करने की अपनी क्षमता के कारण **वर्तमान एन्क्रप्शन वधियिों के लयि कई खतरे** उत्पन्न करती है।
  - **असममति एन्क्रप्शन का सरलीकरण:** क्वांटम कंप्यूटर जटलि गणतीय समस्याओं जैसे **बड़ी संख्याओं का गुणनखंडन** और असतत लघुगणक को हल कर सकते हैं।
    - इससे [रविस्ट-शमीर-एडलमैन (RSA)] और [एलप्टिकि कर्व क्रप्टिोग्राफी (ECC)] जैसी एन्क्रप्शन वधियिों पर असर पड़ सकता है , जनिका व्यापक रूप से सुरक्षति संचार के लयि उपयोग कयिा जाता है।
  - **स्टोर नाउ, डक्रिप्टि लेटर (SNDL) अटैक:** साइबर अपराधी **एन्क्रप्टिेड डेटा को तुरंत संग्रहीत कर सकते हैं** और बाद में जब क्वांटम कंप्यूटर पर्याप्त शक्तशिाली हो जाते हैं, तो **उसे डक्रिप्टि कर सकते हैं,** जसिसे संवेदनशील जानकारी खतरे में पड़ सकती है।
  - **उद्योग-व्यापी डेटा सुरक्षा जोखमि:** यदि क्वांटम कंप्यूटर एन्क्रप्शन मानकों का उल्लंघन करते हैं, तो **वत्ति, स्वास्थ्य सेवा और सरकारी संचार** जैसे क्षेत्रों को डेटा उल्लंघन और वत्तिीय नुकसान का खतरा हो सकता है।

पोस्ट-क्वांटम एन्क्रप्शन/क्रप्टिोग्राफी (PQC):

- [PQC] उन **क्रप्टिोग्राफकि वधियिों** को संदर्भति करता है जो [क्वांटम कंप्यूटरों] द्वारा आसानी से हल कयि जा सकने वाले **गणतीय समस्याओं पर नरि्भर नहीं** होते हैं।
- इसे **क्वांटम-रेजस्टिेंस, क्वांटम-सेफ** या **क्वांटम-प्रूफ क्रप्टिोग्राफी** के रूप में भी जाना जाता है।
- इन वधियिों को **क्लासकिल और क्वांटम कंप्यूटगि सस्टिम** दोनों के **हमलों के खलिाफ सुरक्षति रहने** के लयि डज़िाइन कयिा गया है।
- [VPN] तकनीक **डेटा को एन्क्रप्टि** करती है और **उपयोगकर्त्ता के [IP एड्रेस] को गुप्त** रखती है, ताकि **डेटा की गोपनीयता और सुरक्षा** के लयि **उपकरणों के बीच सुरक्षति संचार सुनश्चिति** कयिा जा सके।

//



और पढ़ें: पोस्ट-क्वांटम क्रिप्टोग्राफी, वर्चुअल प्राइवेट नेटवर्क।