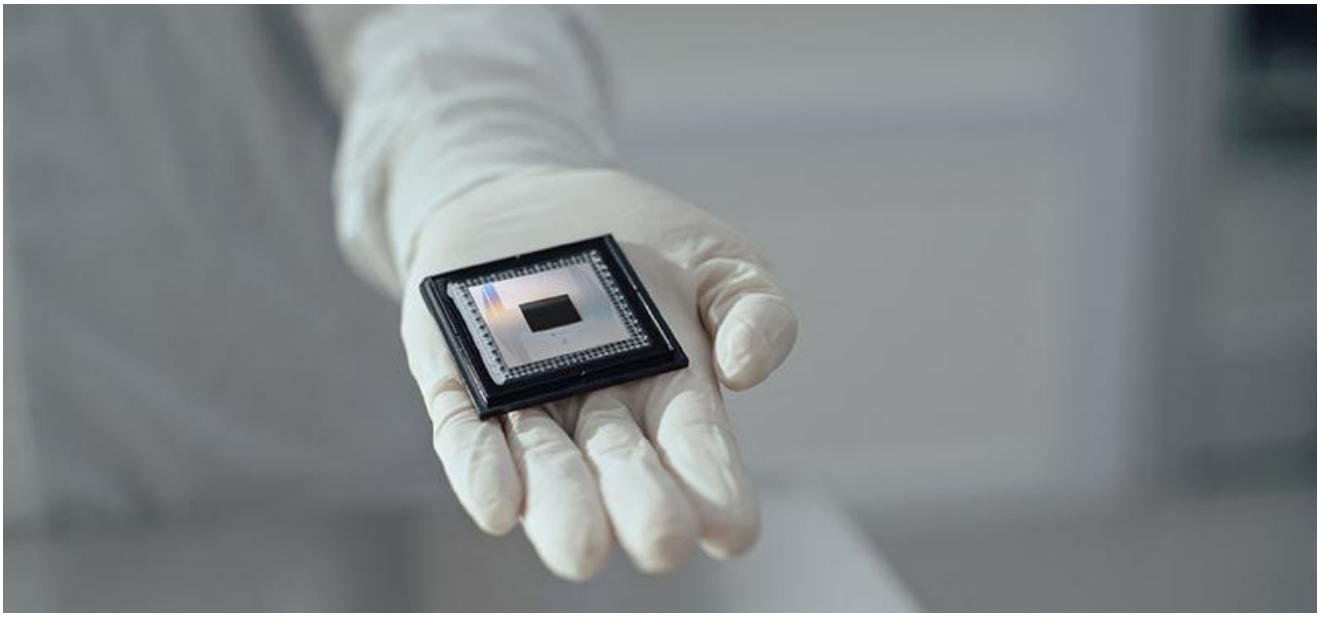
SANJANA B BENGALURU

Google unveils state-of-the-art Willow quantum chip, but can it break the Bitcoin?



distant dream? Experts believe Willow's 105 qubits fall

far short of the 13 million qubits required to decrypt Bitcoin ▪

Google unveiled its Willow quantum computing chip, which some speculate could "crack" the Bitcoin. However, cryptocurrency experts argue that decrypting a Bitcoin typically requires around 13 million qubits, far exceeding Willow's 105 qubits.

On Monday, Alphabet and Google CEO Sundar Pichai announced on social media platform X the development of Willow.

He said the quantum computing chip can reduce errors exponentially as Google scales up using more qubits, cracking a 30-year challenge in the field. In benchmark tests, Willow solved a standard computation in less than five minutes unlike a supercomputer that requires indefinite time.

A qubit, or a quantum bit, is the basic unit of information in quantum computing. Unlike a classical bit or a binary of 0 or 1, a qubit can represent both 0 and 1, allowing quantum computers to process many combinations simultaneously.

Existential threat?

X user Monetary Commentary pointed out that this development is potentially alarming for Bitcoin and other cryptos that rely on public-key cryptography.

The user explained that Bitcoin's security is supported by elliptic curve cryptography (ECC), a system designed to be computationally impossible for traditional computers to break within a reasonable time frame. However, quantum computers like Willow, with exponentially reduced error rates and vast computational power, pose a direct threat to ECC.

Quantum algorithms can factorise large integers and compute discrete logarithms — either of which can break ECC. A machine like Willow that can perform computations in minutes that would take supercomputers infinitely longer represents an existential risk to Bitcoin's security model.

"The idea of quantum computers cracking Bitcoin is still far off. Google's Willow chip, with 105 qubits, is impressive but light years away from the millions needed to challenge Bitcoin's security... Even if Willow's qubits are ground-breaking and hold promise for addressing challenges like climate modelling and drug discovery, that's not enough to break Bitcoin's encryption," observed Himanshu Maradiya, Chairman and Founder of CIFDAQ.

Obstacles like scaling and error correction remain. However, while the crypto world is building quantum-resistant solutions with the evolution of quantum technology, industries from finance to cybersecurity will need to adapt, ensuring that they are future-ready, he said.

Utkarsh Tiwari, Chief Strategy Officer, KoinBX, reiterated this, saying that while some discussions link quantum advancements to the potential for "cracking" it, Bitcoin is based on cryptographic algorithms like SHA-256, which would require more than a million qubits to pose a genuine threat.

'No immediate risk'

"Willow's capabilities, while impressive, do not yet pose an immediate risk to the cryptographic foundations. The estimated computational power required to compromise Bitcoin's encryption methods is still far beyond what Willow can achieve," said Balaji Srihari, Vice-President, CoinSwitch.

Quantum computing can theoretically solve cryptographic puzzles faster than classical systems. However, the timeline to achieve such capabilities remains uncertain, said Sathvik

Vishwanath, Co-founder and CEO of Unocoin. Willow's demonstration focuses on specific benchmarks rather than direct cryptographic attacks.

However, Mohammed Roshan Aslam, Co-founder and CEO of GoSats, said new cryptography practices and encryption methodology will have to be developed to address any potential challenge posed by Google's Willow. Its 105 qubits fall far short of the necessary 13 million qubits to complete Bitcoin's decryption, he pointed out.

"If subsequent R&D in Google Willow manages to integrate such computational power, cryptography and encryption developments may align to address this challenge. Additional software upgrades like hard fork in blockchain may be implemented to address this issue but that may not be the ideal solution. For now, we have only limited understanding of Google Willow, and crypto and tech stakeholders will have to work in tandem to find an amicable solution for this," he said.

The Willow development serves as both a breakthrough and a call to action, with quantum computing potentially reshaping financial systems, including Bitcoin, in the future.