WHITEPAPER December 22th, 2023

Quest for Quantum Supremacy

Quantum computer cannot be built in 100 years: This view assumes that quantum technology is complex and may take time before reaching the level of performance and functionality that can pose a serious threat to traditional cryptography.

Quantum computer is just around the corner, due to breakthroughs in improving qubit quality and coherence. Therefore, it may take less than a decade before quantum computers can break encryption methods such as RSA or ECC.

Probably reality lies somewhere in between these two extremes.

The discourse surrounding the timeline for quantum computing development oscillates between two extreme perspectives. On one end, skeptics argue that the realization of a functional quantum computer within the next century remains highly improbable. Citing challenges in maintaining quantum coherence, error correction, and the technological complexities involved, proponents of this view emphasize the formidable obstacles hindering quantum computing's imminent arrival.

Conversely, optimists contend that rapid advancements in quantum computing technologies are on the verge of ushering in a new era. They point to breakthroughs in quantum error correction, improvements in qubit coherence times, and investments from major tech players as indicators of imminent success. Quantum computing is accelerating at an unprecedented pace, potentially leading to practical, scalable quantum computers in the near future.

In reality, large scale quantum computers' realization hinges on addressing complex technological issues that may take 15-20 years to resolve.

In "Quantum Computing since Democritus“, Scott Aaronson, a renowned theoretical computer scientist, explores the profound implications of quantum mechanics on computation. Scott offers a balanced perspective that considers both the skepticism surrounding the challenges and the optimism fueled by recent advancements.