DC^3 Conference

From cryptocurrencies to CBDCs

25 – 27 January 2022

https://itu.int/go/dc3c

An event of the Digital Currency Global Initiative

Organized jointly:

FDCI | Future of Digital Currency Initiative

ITU

What is the quantum computing threat to classic cryptography?

The importance of classic cryptography

- Various cryptographic primitives are foundational to DC Systems:
  - digital signature
  - public key encryption
  - key exchange / key agreement

- Pre-quantum crypto algorithms depend on a very small number of hard problems for their security:
  - integer factorization
  - discrete log in a finite field
  - discrete log on an elliptic curve

- We have called them hard problems, because we as mathematicians and computer scientists have not been able to construct algorithms for classical computers that can efficiently solve these problems in acceptable time frames

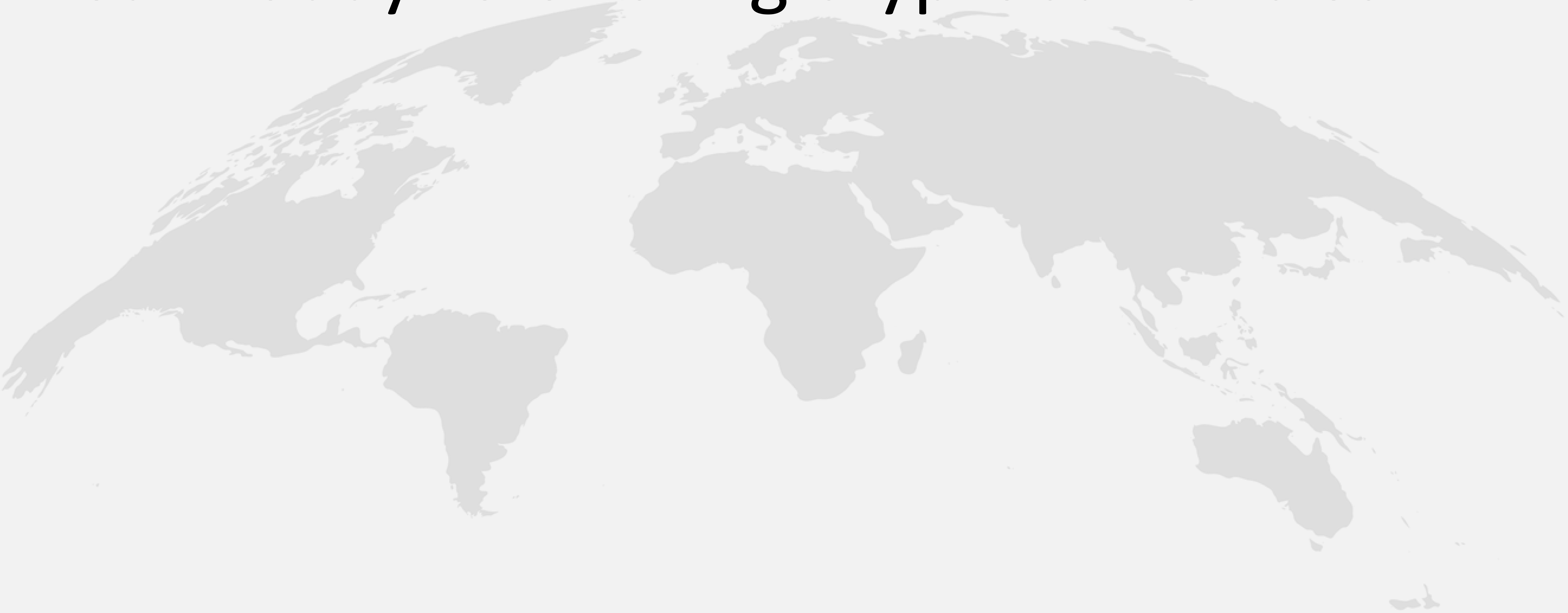
The threat of quantum computers

- Algorithms have already been designed that demonstrate that these problems are not hard for quantum computers
  - Quantum computers will break some of the classic cryptographic algorithms on which cryptocurrencies have been built

- Quantum computing makes attacks against symmetric ciphers and hash functions easier

- We must prepare now for a post-quantum world

What would a viable quantum computer mean today to existing cryptocurrencies?



High level perspective

- Any cryptocurrency based on traditional cryptographic primitives that rely on classically hard problems would be at some level of serious risk

- Ranking them would require an exhaustive technical deep dive, but there are things worth highlighting to help understand how nuanced the situation can be and how important it is that we prepare now

Digital signatures based on elliptic curves

- ECC-based digital signatures are pervasive in today's cryptocurrencies

- An attacker today with a viable quantum computer could forge digital signatures given a public key.

- Cryptocurrencies that expose public keys would face issues such as forging the signatures that authorize spending one's digital currency
  - Simply put: a catastrophic situation

- Cryptocurrencies that do not expose public keys – for example via a one-way hash of the public key – have a much different exposure
  - But risk is generally still there somewhere, as there are still situations in which the actual public key must be exposed and used
  - Cycling key pairs after use can be used as a way to limit exposure of public keys

Proof-of-work based on hash function

- Anyone with access to viable quantum computers has an immediate advantage over those who do not

- Cryptocurrencies that are mined based on proof-of-work would face certain parties having a significant advantage over others

- The worst case would be a successful 51% attack that gains control of the cryptocurrency's blockchain

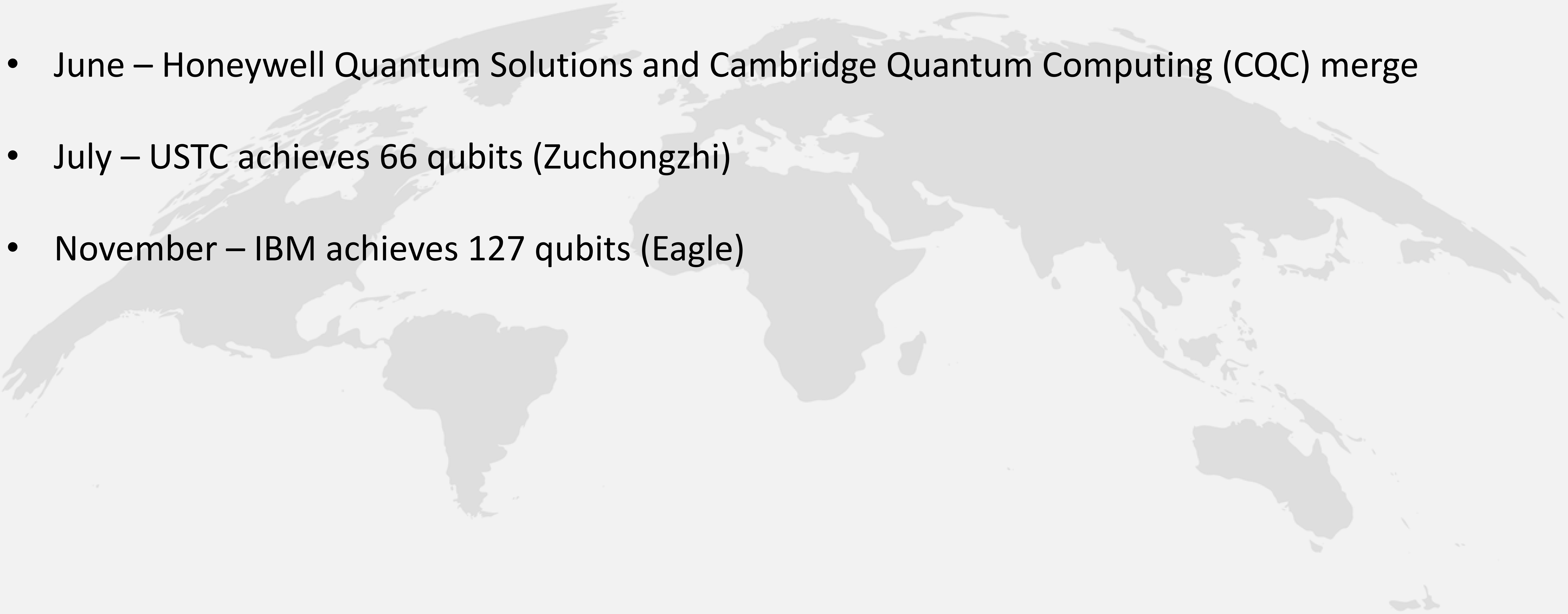
What’s the message?

- We don’t need to panic
- We need to plan. Now

How far away are viable quantum computers?

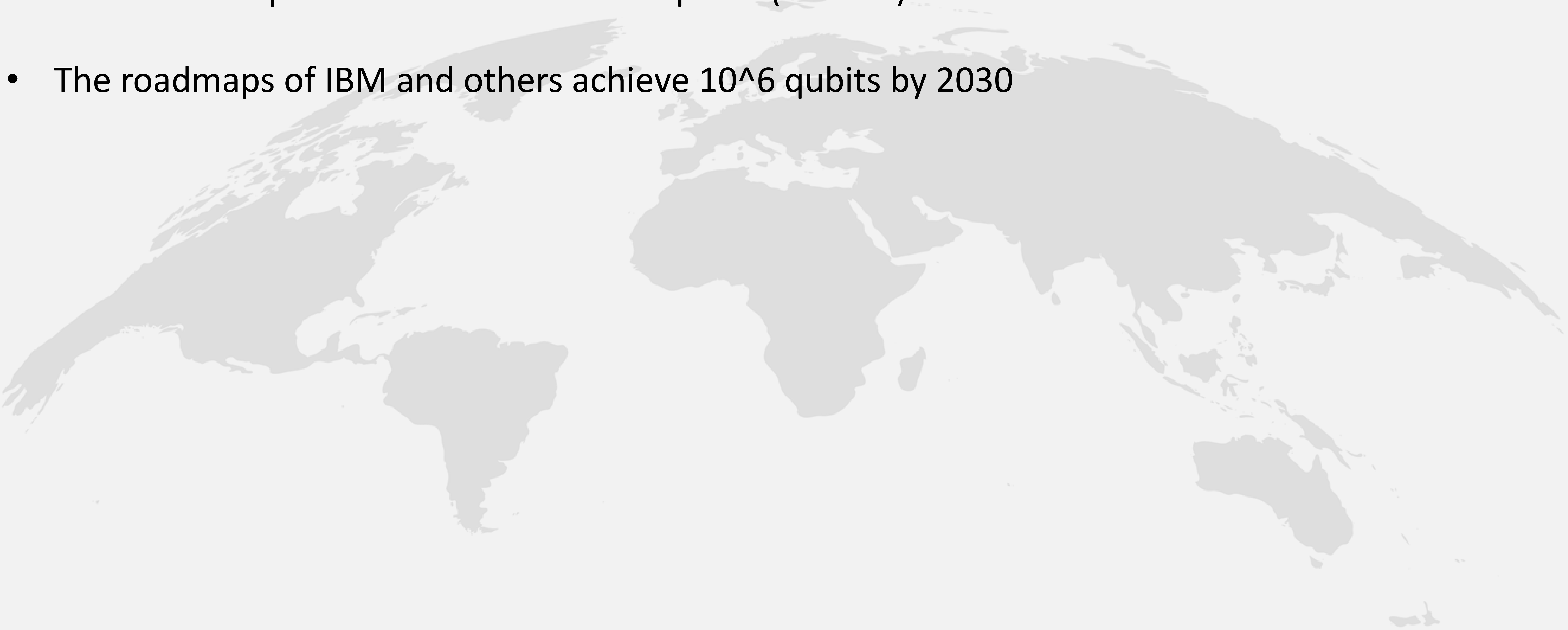
Let’s look back at 2021

- February – IBM’s publishes five year road map
- April – DARPA announces quantum benchmarking program
- June – Honeywell Quantum Solutions and Cambridge Quantum Computing (CQC) merge
- July – USTC achieves 66 qubits (Zuchongzhi)
- November – IBM achieves 127 qubits (Eagle)



What do these tell us about the future?

- IBM’s roadmap for 2022 achieves 433 qubits (Osprey)
- IBM’s roadmap for 2023 achieves 1121 qubits (Condor)
- The roadmaps of IBM and others achieve 10^6 qubits by 2030



What’s the message?

- For our purposes of protecting digital currencies, exact dates are less important than accepting that viable quantum computers will likely be here within the next decade

- The fact that it likely will happen and will happen before or in the same time frame as broad adoption of things like CBDCs is enough to influence our thinking

- We need to plan. Now