LISTEDRESERVE

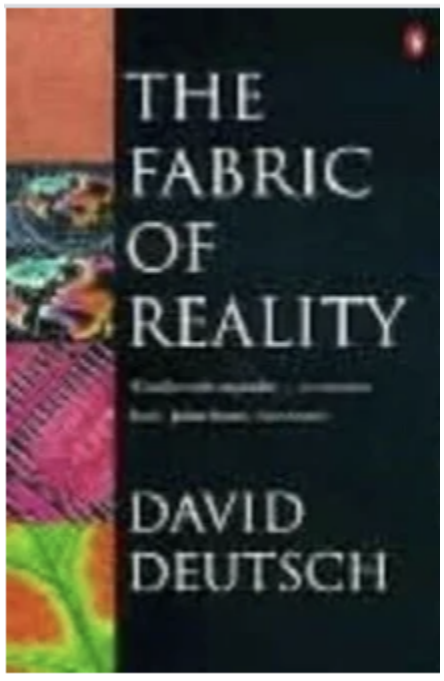
MoneyBits

The Quantum Edition

This week's edition is dedicated to the question of quantum computing. If you aren't interested you can come back next Friday when normal programming resumes.

Many Worlds beyond Copenhagen

People throw "quantum computing" around quite casually as though it is just another kind of computer chip. I was promised by an investment banker in 2017 that a practical version of a quantum computer was "months away". Yet, here we are today without a practical one. Why?



The inventor (or perhaps discoverer) of the quantum computer is David Deutsch of Oxford University. He proved that a quantum computer could do everything a classical computer could do, and importantly, certain things a classical machine could not. Specifically

"a universal quantum computer can, in principle, simulate any physical system and render any virtual reality (VR) that is not logically impossible"

You should pause for thought because that is quite a claim.

For some reason, he remains much less famous than he should be, perhaps because he is actually alive and more likely because the scientific community does not agree with his ideas. In his excellent book the Fabric of Reality he lays out how (in his view) a quantum computer actually works. His explanation is known as the MWI (many worlds interpretation) and it competes with the older explanation of quantum mechanics, known as the Copenhagen view.

What both attempt to explain is how it is possible that a computer can do such a large number of computations relative to a traditional machine.

Copenhagen goes a bit like this: the qubits of a quantum computer behave like a wave of various probabilities, that wave creates many variations through which the machine performs its computation. At the point of measurement, the wave collapses into a solution. Importantly, the waves of incorrect answers cancel each other out and correct answers are amplified by the orchestrator's algorithm that runs the calculation. When the wave collapses, voila! This is a disservice to the brilliance of that original discovery, whose equations do work, the theory just does not explain *how* they work.

Even so, it remains the prevailing explanation of quantum computing and it is the majority view taught in universities. In essence, a magic wave of possibilities collapses on the right answer.

David Deutsch does not accept this view because it's a magic hand wavey "it just happens". He points out that a quantum computer can perform a calculation of this size $2^{\wedge 300}$. This is a larger number than the atoms in the observable universe. If that is possible he asks, where does that computation happen? He goes on to say that Copenhagen is entirely inadequate in that regard because it denies the laws of physics which even quantum computers must obey. If there is a calculation, it *physically* must happen somewhere.

So, to Many Worlds (which Deutsch calls the multiverse). He asserts that there are in fact multiple universes and the quantum computer uses them, performing calculations across the multiverse. Google supported his view back in 2024 when they launched their Willow quantum machine.

The leader of Google's Quantum AI team explicitly linked Willow's success to the multiverse, suggesting that quantum computation's extraordinary power could be a direct result of interactions across parallel dimensions. This aligns with interpretations of quantum mechanics that posit the multiverse as essential for explaining such phenomena.

In Neven's words: "This mind-boggling number exceeds known timescales in physics and vastly exceeds the age of the universe. It lends credence to the notion that quantum computation occurs in many parallel universes, in line with the idea that we live in a multiverse, a prediction first made by David Deutsch."

Sounds ridiculous and warrants explanation. Before that though, it is worth repeating what is being thrown around with the casual 'quantum computer' talk. When someone mentions it, they are revealing they believe there is more than one universe, a possibly infinite number of them, in fact.

To the explanation then. In his book Deutsch uses the famous 'double slit' experiment to demonstrate what he believes is happening.

Double slit

In the experiment we shine a single beam of light at a piece of metal with two slits in it. It generates this pattern.

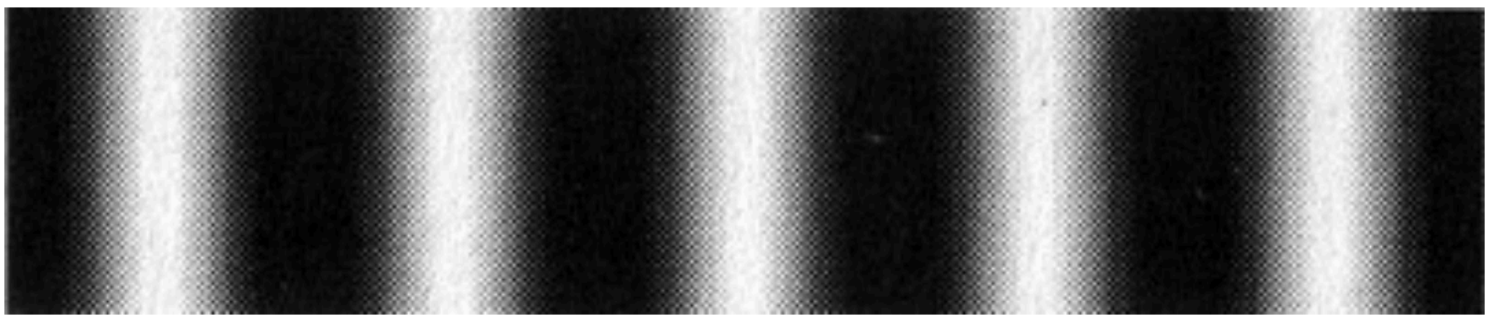


FIGURE 2.6 *The shadow cast by a barrier containing two straight, parallel slits.*

We now add two more slits. Our expectation is that we would see at least four and perhaps eight patches of light, but we do not. We now see darkness where we expected light.

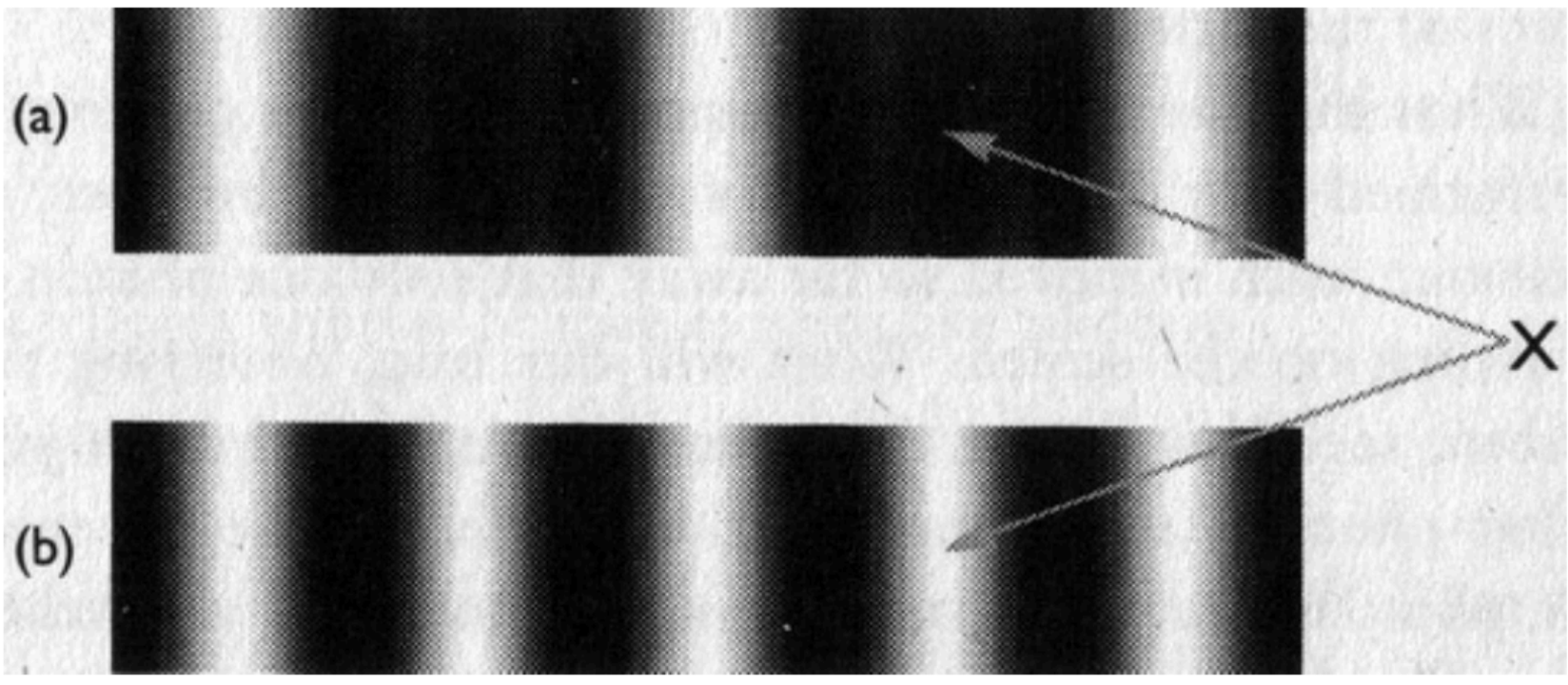


FIGURE 2.7 *The shadows cast by a barrier containing (a) four and (b) two straight, parallel slits.*

The 'obvious' explanation here is that the light waves are just cancelling each other out at X and so we see darkness. This was the explanation for about 100 years. However if we perform the experiment with a single photon, just one particle, that would eliminate the idea of cancelling, since it cannot cancel itself out. This was first done in 1909 with very dim light to simulate single photons; it took weeks to do because the light was so dim it took that long to capture the visible image. It was reperformed with much greater accuracy in 1986.

However you do it, it generates the *exact same pattern.* Dark patches from a single photon. It cannot have interfered with itself (although many disagree). There is no cancelling. So something else is happening.

Deutsch explains that the single particle is bumping into particles from other universes. Consequently, certain paths to the screen are blocked. It sounds fanciful but it is an actual explanation and a simple one. Something is in the way.

This is as opposed to the Copenhagen argument which says: The single, solid particle temporarily dissolves into a "wave of probabilities." This mathematical wave goes through all four slits simultaneously, perfectly interferes

with *itself*, and then snaps back into a solid dot when it hits the screen. It's just not physically satisfactory. If you were to ask a child, they would say "something blocked it". It is a simple and likely much better explanation.

The competing arguments are effectively:

1. Magic happens and boom, or

2. Something is in the way.

I have a preference for argument two, and as we saw earlier, so do Google's leading researchers.

This view is far from universal though, when I passed this article through GPT 5.4 Pro it was not pleased and is quite certain that a single photon can interfere with itself.

3. ❌ Double slit explanation (single photon section)

Severity: High

> "Single photon cannot interfere with itself"

This is **incorrect.**

- Standard QM result:
  - A single photon **does interfere with itself**
  - The wavefunction passes through both slits
  - Detection builds an interference pattern over time

✓ Your alternative:

> "It bumps into particles from other universes"

- This is Deutsch's interpretation, but:
  - **Not empirically distinguishable**
  - Not required to explain results

Even so, how does a quantum computer perform a calculation like 2^{300} ? Simply, according to Deutsch, there is more than one universe and so there is more physical compute ability than we currently can imagine.

This interview explores it with him and opens with the question "How can you believe such an extravagant claim?" Deutsch goes on to explain it rather well.

Relevance to cryptography

The specific relevance of all of this to us is that a quantum computer can break traditional cryptography. Including the type used in bitcoin. The discussion was accelerated a week ago by the release of a paper from Google that reduced the number of physical qubits required to do these computations. The paper is here. In essence the researchers believe that 500,000 physical qubits (and about 1,500 logical ones) would be able to resolve this cryptography in a few minutes.

There are several vectors here:

- First, physical qubits, we need 500,000. The current best is 6,100. We are a factor of 100x away from that
- We then need 1,500 logical qubits. The current best is 50. We are a factor of 30x away from that and the industry is targeting 100 by 2029.
- Finally, the most telling vector of all is the time windows these computers last. The current record is 1.68 milliseconds before the machine collapses. It will take minutes to resolve encryption. We are about 35,000 x away from that at the moment.

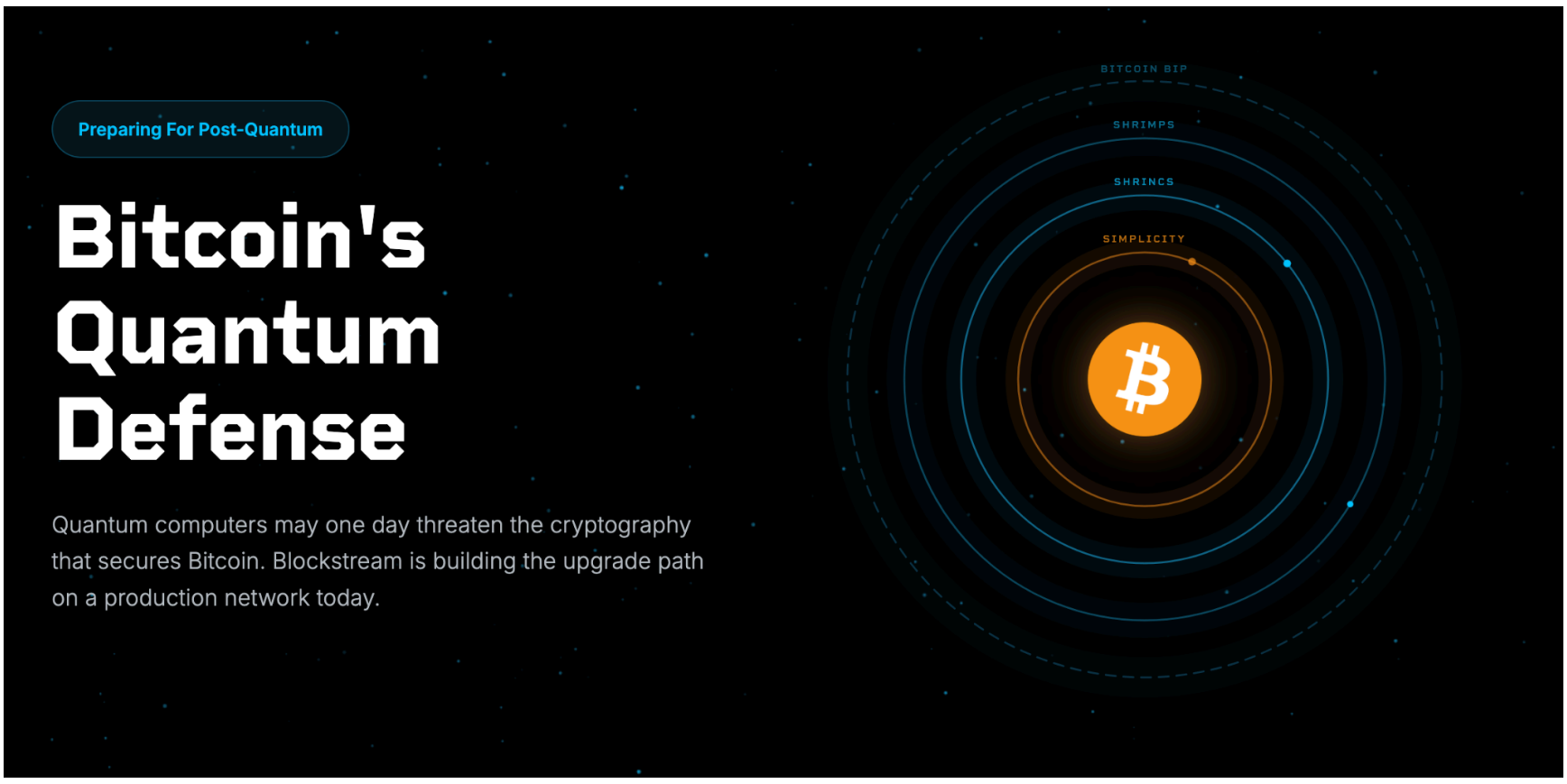
There are other technologies that produce longer coherence times, but they have lower gate speed (calculation speed), so there is a trade off. What's more, these machines are highly sensitive to the environment. They operate just above absolute zero, 180 times colder than outer space. It is a huge engineering challenge to maintain those conditions and any variation from it causes the machine to collapse.

Even so, all told it can be done. So it will be done but the reality is that it will be a long time before it happens. Worth noting too that as the quantum computer gets larger, maintaining its stability gets progressively harder, not easier.

Here is one of the world's leading cryptographers replying to the quantum threat (the man recently, and falsely, outed as Satoshi Nakamoto). Note the distinction between the theoretical possibility of quantum and the engineering hardware challenge.

What is bitcoin doing?

The actual upgrade path is well understood. Post quantum signatures already exist and integrating them into bitcoin is well understood. Indeed Blockstream has already performed the first post quantum transaction. Their quantum webpage is helpful as regards the issue and upgrade path.



An upgrade would look a little bit like this. A new signature scheme would be introduced. A user would then create a new quantum proof address and send their coins from the vulnerable address to the new one. Rather like transferring money from the NAB to CBA because you might believe one was safer than the other. That pretty much deals with all the coins, save for the 1.1 million Satoshi coins that have never moved. *They remain vulnerable.*

Satoshi Coins

Let us then imagine that Q day is here. The majority of users have migrated their coins to quantum proof addresses years ago but we all still know the Satoshi coins are vulnerable. They represent 5% of the total supply and dumped on the market at once would cause huge price ructions.

The only viable candidates for achieving this currently are Google, IBM and a few others. Consider that to ‘move’ the Satoshi coins is the equivalent of taking someone's password and stealing their assets. It would be unlawful in most of the world. Only a massively capitalised company or nation state can afford to design and then operate one of these machines, are they really then going to take Satoshi’s coins and dump them on the market? I would have to say almost certainly not. The most likely winner here currently is Google. Their paper covers responsible use of this technology, so if they ever manage to solve the engineering challenge I very much doubt their first action would be to steal assets and publicly dump them on the market.

The more likely outcome is that they are just left or pushed to a strategic reserve at the request of the USG to ensure that some other nation state doesn’t get their hands on them. At that point though, with a quantum computer working at that scale, the world would be a very different place in any event.

Estimates

Educated views differ on how long it will take to get a viable machine. Amongst those who actually know what they are talking about:

Adam Back (Hashcash inventor, cited in Bitcoin whitepaper) — 20-40 years

Jensen Huang (NVIDIA CEO) — 15-30 years for useful quantum computers

Scott Aaronson (UT Austin, leading quantum complexity theorist) — refuses to give a timeline; notes breaking RSA would require "someone investing $100 billion"

Craig Gidney (Google Quantum AI) — 10% chance by 2030; also notes he does NOT see another 10x improvement in qubit estimates under current assumptions — the optimization curve may be flattening

The reason the timelines to workable machines are so long is not just because of the engineering challenge. There is actually no consensus on what we are even dealing with. The founding father of quantum computing insists that the computing power must be drawn from many universes. Most physicists disagree, even though their explanations are more complex and rely on magic.

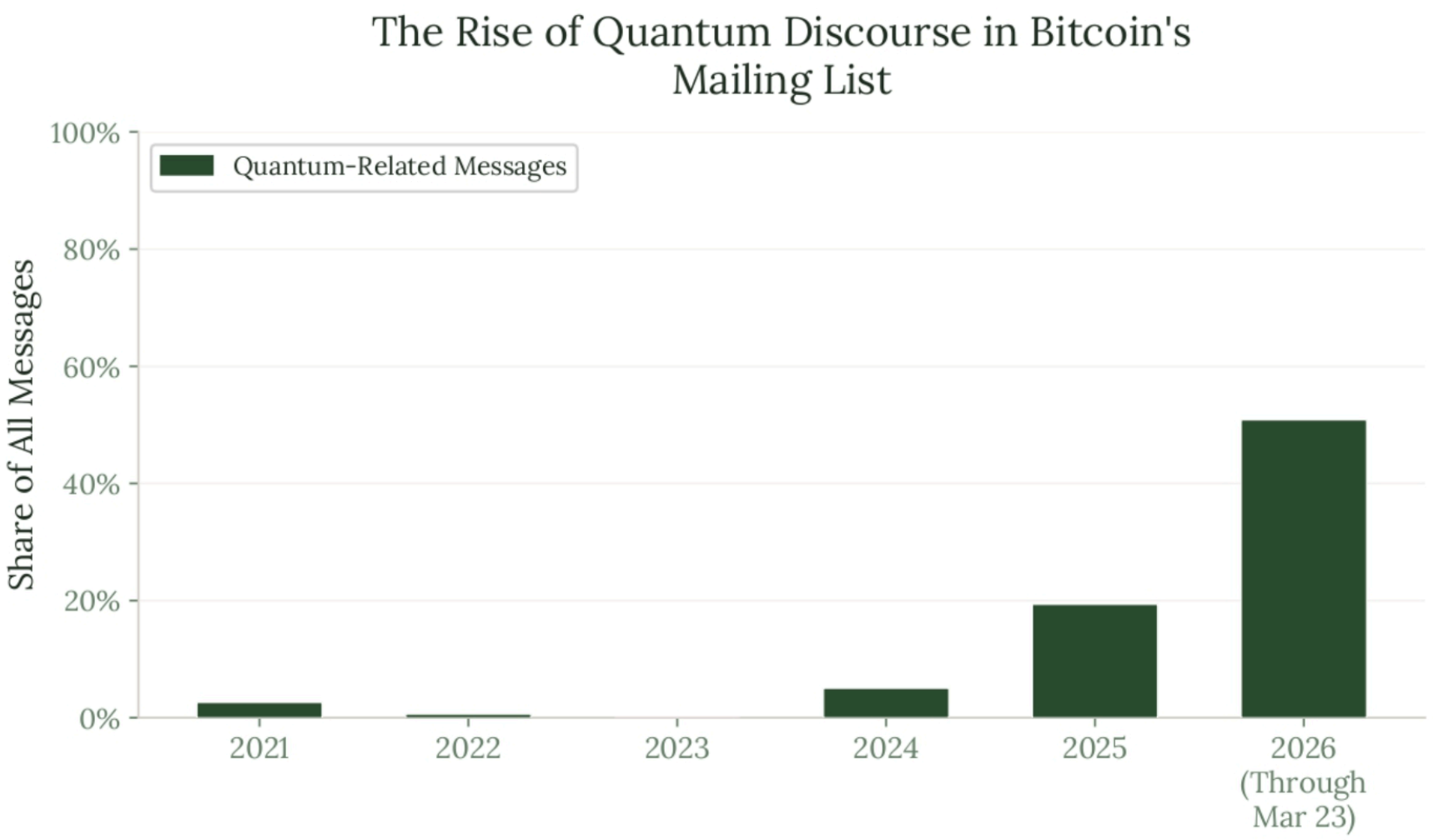
So when people challenge bitcoin on the grounds of quantum, I am inclined to wonder if they have even attempted to understand what they are suggesting. Which is, that we will hold in stasis multiple universes for minutes at a time while our desired computation works, all of that without any interference from our own universe. Those minutes are tens of thousands of times longer than we have currently managed with thousands of times more complexity thrown in.

It's an awful lot to ask and I am sure it will happen some day but I remain of the view that it will not be soon.

Preparation

Even so, bitcoin is an adversarial system. Imagine the worst and prepare for it. That is what is happening. The first technical proposal for transition, BIP360, is here. Further quantum analysis is here.

Signature testing has commenced and quantum proof transactions have already happened.



Bitcoin will migrate at some point to quantum proof signatures. The Satoshi coins will hang over us in the same way the Mt Gox coins hung over us for a decade but realistically the operators of a quantum computer are highly unlikely to be bad actors. The capital requirement is simply too great.

Cryptocurrency is not going to die because of quantum, but we will need upgraded signature schemes.

Final word then to Satoshi Nakamoto who was asked specifically about this in 2010. It's not a new story, or a new threat and his answer in 2010 is broadly what is now proposed.

Quote from: satoshi on June 14, 2010, 08:39:50 PM

If SHA-256 became completely broken, I think we could come to some agreement about what the honest block chain was before the trouble started, lock that in and continue from there with a new hash function.

If the hash breakdown came gradually, we could transition to a new hash in an orderly way. The software would be programmed to start using a new hash after a certain block number. Everyone would have to upgrade by that time. The software could save the new hash of all the old blocks to make sure a different block with the same old hash can't be used.