THE BUSINESS TIMES

BT businesstimes.com.sg

Saturday, April 16, 2022

Is blockchain just a transition technology?

Amid rapid tech advancements, all blockchain applications will soon likely be rendered unsafe and useless

"WHAT happens when quantum computers become reality?" One of my favourite moments at a cryptocurrency seminar last year was when someone asked that question. The response was dead silence. After a long pause, the speaker said something to the tune of, "We will figure that out when we get there".

Let me explain. The entire premise of blockchain technology and the cryptocurrencies, non-fungible tokens (NFTs), and smart contracts that are built on it is that distributed ledgers are immensely secure and cannot be hacked with modern computers.

I am oversimplifying a bit, but in order for a transaction to be accepted by the blockchain, more than 50 per cent of the computers on the network that share the blockchain need to agree that the computer that claims to be the new owner of a crypto asset is indeed the legitimate owner. And the network only accepts claims that have a proof of work (PoW), which is essentially a massive multiplication exercise of several very large numbers. Again, I am oversimplifying here.

Once such a PoW has been submitted to the blockchain network and more than 50 per cent of the computers accept it, a new block is added to the chain and the longer blockchain is considered the true blockchain. Submitting a PoW for a new cryptocurrency is what creates a new token or coin.

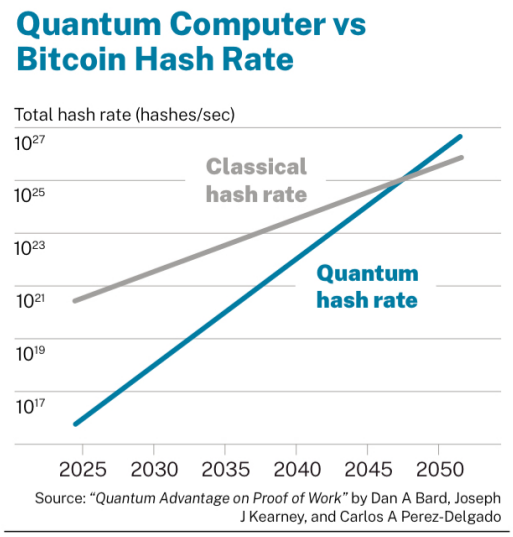
Similarly, submitting a PoW creates a contract that proves ownership of certain assets without relying on centralised databases or potentially corrupt government officials.

Now imagine you can churn out these PoWs faster than all the computers in a network can check the veracity of the PoW.

Then you could constantly outrun the verification process and generate new blocks in the blockchain before the rest of the network could check them. And since all blockchain technology assumes the longest blockchain is the legitimate one, you could effectively "hack" the system. All the other computers would simply accept your blockchain as the one against which to compare any new PoW.

Exponential advantage

With modern computing power, it is simply impossible to create such a so-called '51 per cent hack'. But quantum computers will be so much faster that at some point, they will easily outpace any network of traditional computers. In fact, speed won't be their only advantage.



Source: *"Quantum Advantage on Proof of Work"* by Dan A Bard, Joseph J Kearney, and Carlos A Perez-Delgado

... if you extrapolate current advances in the speed of computing power into the future based on Moore's Law, a single quantum computer will be able to hack the bitcoin blockchain by about 2045.

Conventional computers are based on transistors that differentiate between 2 binary states – called "bits" – 0 and 1.

But quantum computers can take on both 0 and 1 at the same time and superimpose these "Qbits". If that sounds weird, think of a typical old-fashioned computer that encodes letters or numbers as a series of 8 bits.

There are 256 different characters or numbers that can be coded with these 8 bits and at any given time, a transistor in a standard computer will be in one of those 256 possible states.

But a quantum computer with 8 Qbits could take all 256 states at the same time and use them for computations simultaneously. So, the advantage of quantum computers grows exponentially as they include more Qbits.

This means that algorithms in quantum computers have to be completely redesigned in order to leverage these computational capabilities. But it also means quantum computers will be so much more powerful.

They will easily crack problems that traditional computers could not solve within the remaining lifetime of the universe.

So, assume you are the first person or company to build a fully functioning quantum computer: Since all the world's networks are based on conventional computers, you could take over every blockchain on earth within a matter of seconds. Only once the majority of computers in a network also become quantum computers will the blockchain be safe again. But by then it may be too late.

This benefit of quantum computers holds even when they have not really achieved what is called a true quantum advantage, or when they can solve problems that no traditional computer can. Once the problem-solving capacity of standard computers is outpaced enough by their quantum counterparts, all the blockchains in the world will become hackable by anyone with a quantum computer.

So, when quantum computers become reality, blockchain technology will have to be completely recreated from scratch or lose all its decentralisation and security advantages.

Not just science fiction

But quantum computers are still just science fiction, aren't they? Yes, they are. But they are being developed right now. And if you extrapolate current advances in the speed of computing power into the future based on Moore's Law, a single quantum computer will be able to hack the bitcoin blockchain by about 2045.

And that estimate is based on 2 assumptions: First, that quantum computing advances at the same rate as traditional computing. We know, however, that new technologies tend to progress much faster than well-established ones.

Second, the 2045 date applies to the bitcoin blockchain, which is by far the most complex and computationally intensive one. (This is why bitcoin cannot compete as a payment system with the PayPals and credit-card networks of the world).

Other blockchains such as Ether or those underlying commercial applications employ much smaller networks. And, according to a new study on quantum computing advantages, quantum computers could hack such blockchains as early as 2023.

Personally, I do not think 2023 is realistic. But the more I read about advances in quantum computing, the more I believe it could be sometime this decade. And what happens then?

Unless all blockchain applications have been fundamentally redesigned ahead of time, they will likely be rendered unsafe and useless.

Joachim Klement, CFA, is a trustee of the CFA Institute Research Foundation