Why Google's "quantum supremacy" means the end of encryption security for cryptocurrency, military, finance and personal communications

By Mike Adams, Natural News, 23 September 2019

Over the last 24 hours, Natural News and NewsWars have spearheaded the reporting on the implications of Google's "quantum supremacy" announcement from Friday. What's astonishing is how few independent media publishers and mainstream media outlets are covering this story, considering it's the biggest computing milestone in the history of humanity, with game-changing implications for the future of the human race.

It seems apparent that many people simply don't want to believe those implications, so they choose to ignore what just happened. On the indy media side, one of the implications that seems to bother many publishers is the fact that **quantum computing makes cryptocurrency obsolete**. So quantum computing stories get ignored because the implications are too scary for the crypto crowd, which doesn't feel comfortable considering the implications of what happens when the "crypto" portion of cryptocurrency no longer offers any real security at all.

The "crypto" in "cryptocurrency," of course, stands for "cryptography." It is cryptography that allows cryptocurrency transactions to be securely communicated over non-secure networks (such as the open internet) while verifying the authenticity of the party sending cryptocurrency funds. Quantum computing makes classical cryptography obsolete for mathematical reasons explained below.

Cryptography relies on cryptographic asymmetry, which is rendered obsolete by quantum computing

To back up for a minute, cryptography relies on what's called *asymmetry* in computational difficulty in terms of encrypting something versus breaking that encryption. For example, it might take your desktop PC 10 seconds to encrypt a file, but breaking that encryption on another desktop PC might take 10 billion years (depending on the number of encryption bits and other factors).

However, quantum computing makes this roughly *symmetrical*, meaning the difficulty of encrypting a file is roughly symmetrical to the difficulty of breaking the encryption using quantum computing (qubits).

What this means is that even if Bitcoin doubled the number of bits used in its encryption algorithms to 512, quantum computers simply need to increase their qubits to 512 to be able to break all the Bitcoin encryption in about the same amount of time the encryption required (which is almost no time at all).

So you might say why not just make all Bitcoin encryption 1024 bits, or 2048 bits, or 4096? The answer should be obvious. Thanks to quantum computing, you no longer have an asymmetrical computing advantage, meaning that you are adding just as much computing burden to the encryption side as you are to the "breaking encryption" side of the equation. And if you thought Bitcoin was slow and bloated today, just imagine how slow it would become if you start doubling or quadrupling the number of bits needed for every secure communication.

Meanwhile, quantum computing is leaping forward at orders of magnitude that make your head spin. Honestly stated, **most people just don't follow the math** and can't comprehend the reality of how much faster quantum computers are at breaking encryption codes compared to classical computers.

, published in January of 2016, tested the speed of a quantum computer solving a 945-variable equation, using quantum tunneling computational principles. The result? According to the study:

For instances with 945 variables, this results in a time-to-99%-success-probability that is ?10^8 times faster than SA running on a single processor core. We also compared physical QA with Quantum Monte Carlo (QMC), an algorithm that emulates quantum tunneling on classical processors. We observe a substantial constant overhead against physical QA: D-Wave 2X again runs up to ?10^8 times faster than an optimized implementation of QMC on a single core.

Ten to the power of 8 (i.e. 10^8) is of course 100 million times faster than a classical computational core such as the one powering your computer. And this was over 3 years ago, by the way, before the "quantum supremacy" announcement by Google last Friday.

If you do the math on this, what it means is that this quantum computing system can solve a problem in one second that would take your desktop PC over three years to solve.

Quantum computers are "stargates" that send complex problems to a multidimensional, hyper-computational realm which computes the correct answer

But it's not just speed that matters. Quantum computers aren't necessarily good at rendering 3D graphics, for example, or crunching databases. They are very narrow-use computational devices, and their No. 1 best application is breaking encryption (they're also good at generating truly random numbers, which has many applications in cryptography). They do it almost by magic, invoking multidimensional mathematics that some say involve sending the encryption problem out to 2^n dimensions, where n is the number of bits used in the encryption. These 2^n dimensions each express one possible solution to the encryption problem. Yet the quantum computer is able to pick the "right" answer out of those multitude of dimensions and bring it back into our dimension, expressed as a readable state of qubits, which is then translated into regular binary.

Quantum computers, in other words, **use the mathematics inherent in the fabric of the cosmos to "solve" problems without having to compute the solutions**. You might say there really isn't any "computation" taking place, but rather a diverting of the encryption problem to the fabric of the cosmos which does the computing for you. You could even call it a "computational wormhole" or "stargate" that seems to cheat the laws of reality.

If this makes no sense, you're not alone. It's difficult for humans to grasp the fact that the very nature of the cosmos is pure mathematics, from which the emergent property of physics springs forward. I recently spoke at the *True Legends* event in Branson, Missouri, and there I met Hugo de Garis, an Artificial Intelligence expert who proposes that the entire universe may in fact be the creation of a hyper-advanced AI intellect that created the cosmos out of pure mathematics. He is proposing, in other words, that "God" is an AI intellect, which means he believes in Deism (a God creator) but not necessarily Theism (the Christian, loving God as creator).

According to de Garis and others who are proficient in AI system and high-level mathematics, the fabric of the cosmos is nothing more than the expression of mathematics. This means the cosmos is *computational* by its nature. In other words, the cosmos computes things all the time, inherently. This includes the orbital cloud waves of electrons, by the way, and the actions and properties of atoms and subatomic particles. The construction of quantum computers means that humans have built a way to send mathematical problems to the cosmos, using the computational power inherent in the cosmos, and retrieve the answers back in our "real" world (which is course isn't real at all, but lets pretend it is so we can get on with this explanation).

The fabric of reality is a hyper-dimensional, hyper-computational system

The very fabric of reality, in other words, is a hyper-dimensional supercomputer. If you can tap into it, you can ask it to solve incredibly complex mathematical problems for you. That's what quantum computers really are: **a sort of "stargate" into the mathematical hyperdimensional computational fabric of reality** that solves problems for you at essential zero cost, since it's part of the very structure of the universe itself.

A research paper published in 2014 confirms this, finding that quantum computers don't run any *faster* than classical computers. There's no "quantum speedup" of the CPU, in other words. The quantum "computer" isn't actually doing the computing at all. As CNET reported in 2014:

A research team at the Swiss Federal Institute of Technology in Zurich reports that there is still a lack of definitive evidence that the D-Wave Two can perform functions any faster than traditional machines. The results of the test were published in the journal Science Thursday…

By the way, if you think this is interesting stuff, listen to my recent podcast on the distortions of spacetime by Faster-Than-Light (FTL) warp drive systems and how they allow ships to travel at multiples of the speed of light without violating the laws of the universe, which limit relative speed to C. This podcast is highly technical, but incredibly fascinating, and it explains the movement of the non-Earth ships recently captured on video by Air Force jet fighter pilots, which has now been verified as authentic by the U.S. Air Force itself.

(You can watch more of my lectures on FTL travel, warp drives, spacetime distortions, antimatter fuel systems and cosmic economics at OblivionAgenda.com. Many more lecture videos are on the way, by the way, covering these topics and much more.)

Quantum computers solve highly complex computational problems by delegating the computational load to the multidimensional, hyper-computational nature of the cosmos

In summary (so far), quantum computers are not really computational devices at all. They are portals to the computational nature of reality. Quantum computers don't "compute" anything, simply stated. They dispatch highly complex problems to multiple dimensions which then return the "correct" answers to our reality. From there, scientists use classical circuits to read the state of the qubits and translate the answers into classical bit representations which are then of course easily translated into hexadecimal (base 16) expressions of values.

If you're not yet convinced that the nature of reality is computational, realize that classic logic gates such as "OR" and "AND" functions have already been achieved and demonstrated at the Femto level, which is 1/1,000,000th the scale of nanotech. (Metric units, to review, go in this order, with 10^3 scale between each: milli, micro, nano, pico, femto, atto, zepto, yocto.)

The computational nature of the cosmos goes even far beyond this. The very structure of what might be called "the grid" is both quantized and highly computational. Just ask Planck. (By the way, the quantization of the fabric of the cosmos is very nearly proof all by itself that the underlying nature of reality is mathematical. This does not disprove the existence of God, by the way. It just means God expresses creation through mathematics, which are also found across all living systems such as plants, microbes, etc.)

Atomic physics, you might say, is an emergent property of the mathematical and computational undercurrent that penetrates and pervades the construct of "reality." That's why there are no electrons until you observe them, collapsing mathematical probability wave functions into a momentary expression of "reality" in order to complete the illusion for the conscious observer.

Quantum computing makes all known classical encryption obsolete: Cryptocurrency, military comms, banking and finance, etc.

Now that we've covered a bit about how quantum "computing" harnesses the hyper-computational, multidimensional fabric of the cosmos to rapidly find answers to a very

narrow set of highly complex mathematical problems, we have to look more closely at the applications of this tech.

Here comes some more math. Be warned.

If you are encrypting files right now using a 256-bit encryption algorithm, and then you decide to switch to 512-bit encryption, in a classical computing model, you have just increased the difficulty of breaking the encryption by 2^256, which is a very large number. But with quantum computing applied to the problem, the difficulty of the original 256-bit encryption is merely *doubled* when it shifts to 512-bit encryption. In other words, quantum computing allows code breakers to tackle increasingly complex problems with a *linear* relationship to increased complexity rather than a *logarithmic* relationship. Explained again, even if Bitcoin (for example) were to quadruple the number of bits used in its encryption from 256 to 1024, a quantum computer that breaks the 256-bit code in 1 second would only need 4 seconds to break the 1024-bit encryption (this is oversimplified, but roughly correct). The implications of this linear code breaking relationship are not realized by most people. In fact, **almost no one seems to grasp what this means for our society**.

I remain stunned by the fact that very few people can see what I find to be immediately obvious. For whatever reason, I've been truly blessed with the ability to almost instantly realize the long-term implications of present-day trends. This is what allowed me to predict over two years ago that quantum computing would break cryptocurrency. It's also part of what got be permanently banned from YouTube, since the most dangerous thing in modern society is to be intelligent and a good communicator. (That's when I started building Brighteon.com, the YouTube alternative for free speech.)

IBM, Google, Microsoft, Nokia, D-Wave, Alibaba and others are relentlessly pursuing quantum computing breakthroughs

Today, many organizations are spearheading quantum computers, including D-Wave which offers a commercially-available quantum computing system that you can purchase and put on your desk. (It's only $15 million, but who's counting?) According to media reports, Google "is using D-Wave as its primary product" for quantum computing research.

Other companies involved in quantum computing research include IBM, Microsoft, Nokia and even China's Alibaba. The NSA, by the way, is heavily involved in some of this research for obvious reasons. Whoever breaks the most codes first will dominate the world. In fact, the race for high-qubit quantum computing earns an even higher priority than the race to develop the world's first hyper-intelligent AI system.

What happens when you combine AI with quantum computing? You create an omniscient God-like computational intellect that would know everything (in human civilization, anyway) and could control everything. Hence the concerns about Google being involved in all this research, since **Google is the most evil corporation in the world**… and it has become strongly allied with communist China.

Whoever achieves high-qubit quantum computing first will be able to achieve all the following:

- Spoofing all cryptocurrency transactions and effectively draining all crypto wallets, worldwide.
- Decoding all military communications. This is "Enigma" on steroids.
- Monitoring and spoofing nearly all banking and finance transactions. Full control over international wires.
- Reading all encrypted communications involving civilians, government and military. There will be no such thing as privacy, not even Pretty Good Privacy.
- Reading all encrypted hard drives, container files and other storage media, including those of the NSA and world governments. Too many secrets. **Setec Atronomy**.

The fact that so many powerful corporations and governments are pursuing quantum computing means **it's only a matter of time before present-day cryptocurrency becomes obsolete** and completely compromised. Perhaps some crypto systems can advance to an enhanced form of encryption, but this is just conjecture.

It is probably because of this that most independent media outlets are avoiding discussing this issue, since many are promoters of cryptocurrency, a technology that will cease to be secure in less than three years, if Google's scientists are correct in their predictions about quantum computing.

But guess what? **Quantum computers can't steal your gold**, because they can't teleport matter away from your home vault. So gold is still the best store of value, even in a world where digital secrets are all cracked. Quantum computers cannot alter the laws of atomic elements, and since gold is an element, its existence is guaranteed by the very nature of the universe. (Gold is gold, and you can't alter it into anything other than gold unless you control a working nuclear fusion device, in which case gold is the least of your problems.)

One possible solution to maintaining secrets is to use **quantum cryptography**, a form of cryptography that relies on the phenomenon of **quantum entanglement** to secure digital files in ways that may put them out of reach of quantum computing. A leading edge organization named Crown Sterling claims to have produced "Time AI," a so-called quantum computing solution that claims to securely encrypts data on computers and mobile devices. I'm skeptical of this claim, since your mobile phone doesn't have any capability whatsoever to read the spin state of entangled atomic particles. As a general word of caution, I would urge consumer to be wary of "quantum encryption" claims, given that anyone can assign such labels to almost any technology at all. True quantum encryption requires a lab full of advanced physics equipment, by the way.

In any case, it seems obvious that any cryptocurrency that wishes to survive the rise of quantum computing will need to adopt something far more advanced than RSA or AES encryption, or it will be rendered obsolete.

And whatever nation or corporation that develops 1024-bit quantum computing first will rule the world and become more powerful than anyone can currently imagine. Whoever can decode all the secrets will rule the world.

God help us if that turns out to be Google.

The era of secrets is about to come to an end. Consider the implications on government surveillance and intrusion into the lives of citizens. Then ask yourself why almost no one else is covering this topic, given that it's the biggest science story in human history. Has humanity become blind to the mechanisms of its own destruction?

Sadly, it seems the answer is yes.

Watch more science and "cosmic" video lectures of my work at OblivionAgenda.com.

Sources for this story include:

What is the Computational Value of Finite Range Tunneling? (Cornell University)

Google and NASA Say Their Quantum Computer Finally Works (Popular Mechanics)

Confirmed, finally: D-Wave quantum computer is sometimes sluggish (CNET)