[Vint's comments regarding my post where I suggested that there is considerable hype surrounding the announcement of a U.S. "Quantum Internet" project. Shared publicly with Vint's permission. - Lauren]

Date: Fri, 24 Jul 2020 10:52:55 -0400
From: (Vinton Cerf)
Subject: Re: [The hype is strong with this one!] "U.S. hatches plan to build a quantum Internet that might be unhackable" [Washington Post]
To: (Lauren Weinstein)

It is not clear whether it will be useful and there is really no argument I can think of that justifies the "unhackable" label. This is blockchain on steroids. First of all, transferring entangled photons so as to transfer quantum states from one quantum computer to another will be super hard. State deteriorates with time so a partial computation that transfers an entangled photon to another quantum machine has to solve the problem of maintaining the fragile quantum state through an entangling repeater (which has not been invented yet) and then continue the computation by entangling the arriving photon with quantum dots (or other quantum-preserving mechanism) so as to continue the computation.

This whole thing is a kind of fantasy, trying to combine two largely incommensurate ideas: the internet and quantum computation. Better to build larger scale local quantum computers than to try to link them over distances. Also, keep in mind that once the state of two distant machines become entangled, further progress on the computation involves the manipulation of the quantum state of two (or more) machines. Einsteinian distance means that clock sync is absolutely crucial because the quantum state manipulation now has to be coordinated. That's so because the manipulations affect both machines instantaneously as nearly as we can tell. The transfer of entangled photons, however, take time (speed of light latency). So how does the donor quantum computer "know" when the recipient quantum computer has taken onboard the arriving entangled photon? Any handshake takes time. Once again, to preserve the now-entangled machine states is a challenge because it may take between three and five transit times to confirm state. Putting at risk the maintenance of quantum entanglement.

Probably TMI, but I am not very enthusiastic because I think it would be more fruitful to build larger local quantum computers. Now, as to exchange of cryptography keys, the "big deal" is that it would be hard to capture information during the generation of a shared secret. Interference to detect the state of an entangled photon affects the state and would, theoretically, affect the measurement of the quantum state of the transferred photon. While the interception of the quantum key would be defeated, so would the generation of the key in the first place, effectively executing a denial of service attack. It's a bit like interfering with GPS. The signals are so weak, it is easy to wreck the GPS computation.

Color me skeptical.