From: Miller, Carl A. (Fed)
To: Huergo, Jennifer L. (Fed)
Subject: Re: Messages with Impact Materials
Date: Tuesday, April 23, 2019 12:59:28 PM

Hi Jennifer –

Thanks so much for the "Messages with Impact" seminar today. I learned a lot – you've got some great examples, and tools that seem applicable in many different contexts.

I am gearing up to start writing grant proposals about my work. I don't know if you all have time, but if so I'd be very grateful to get any feedback about the draft that I wrote today (below).

The audience for this would be grant program officers who are interested in funding research in quantum technology. (This document could be something that I'd send before the writing of a full proposal.)

-Carl

We are in the midst of the "second quantum revolution." Investments in quantum technology have skyrocketed in the last 5 years. The National Academy of Sciences has released a report this year laying out the landscape of this new revolution. At a basic level: since ordinary technology is achieving diminishing returns, its resources are now moving into the quantum realm.

At its core, quantum technology works because it breaks barriers -- impossible things become possible. Quantum technology is a fast-moving train, and so: where is the train going to go next?

Here is something to consider. Every day companies make transactions, and these transactions can go wrong for any number of reasons. One party was late but doesn't think that they were late. One party copies something that they were not supposed to copy, and so forth. $XXXXXX is spent every year on litigation that is concerned only with interactions between corporations -- not with their customers.

Someone great once said, "capitalism is based on fair balances." We shouldn't mind losing or winning an exchange, as long as it's done fairly. But where does that fairness come from? We can put our trust in third parties. But as we know, that has problems of its own -- when a party doesn't get an outcome that they like, they then sue the intermediary! And we're in a similar mess.

So, the question is: in a digital world, where parties don't even meet face-to-face, how do we establish fair interaction?

There is a phenomenon that I'm going to call the **quantum lever**. You can imagine two parties at a distance from one another operating a lever in a see-saw position. Person A's job is to adjust his side of the lever so that it doesn't go above 50% height, and Person B's job is to make sure that his own side doesn't go above 50% height. If either of them persists in pushing

the lever too far, the other can say, "this guy is uncooperative -- I'm just going to walk away." Otherwise, a coin flip gets magically carried out, and the likelihood that Person A wins the flip is determined by Person B's lever-height, and vice versa. In this ideal scenario, each party can get a fair 50% shot at winning the exchange.

Remarkably, quantum technology can actually achieve this in principle --- even across huge distances. But, it's hard. In 2007, Carlos Mochon (the Bill Watterson of quantum cryptography) solved the quantum lever problem with a long and difficult proof, and shortly thereafter left academia. His approach since been deeply studied and simplified some, but it remains extremely inefficient. In "Quantum internet: the road ahead" by S. Wehner et al. (2018), the quantum lever was identified as one of the most difficult cryptographic tasks to realize in practice.

However, there's hope. The work that I've done in the past year strongly suggests that we can find more efficient ways to do the quantum lever. Mochon's original proof was -- like many early proofs in quantum -- like a giant lego castle. In the past we've been able to shrink castles like these into structures that are streamlined, accessible, and functional. There is hope that we do the same with the quantum lever.

The quantum lever is the cornerstone of a much larger project, which is to create a toolbox for two-party cryptography. We want procedures that allow two parties to carry out whatever they task they choose (with fairness and security). "Coin flipping" -- that's basically what the quantum lever achieves -- is one. There's also identity verification, electronic currency, and message commitment, among others. I am excited about the vast landscape that this opens up, and would be honored to have your support.