Cryptography pioneer Silvio Micali on where crypto is headed

May 4 2022, by Laurence Darmiento

Credit: CC0 Public Domain

Some 40 years ago, Silvio Micali and his colleague Shafi Goldwasser wanted to figure out how to play poker together on their phones. They needed a way to ensure neither could know the other player's hands.

The two computer science graduate students at the University of California-Berkeley drew up what Micali calls "the first secure encryption scheme the world has ever seen." For their invention, which proved vital to the modern internet, they were awarded the A.M. Turing Award, considered computing's equivalent of the Nobel Prize.

Today, Micali, 67, is focused on another application of encryption: the blockchain, which is the foundation of bitcoin and other cryptocurrencies. At the Milken Institute Global Conference this week, the MIT professor promoted Algorand, a blockchain he developed that he says is greener, faster and more secure than other protocols.

Blockchains are typically described as public ledgers where transactions are recorded on an open network. Validating a set of transactions to add to the ledger is one of the biggest security challenges. Algorand says it uses a novel approach involving the random selection of its users to ensure blocks of transactions are more resistant to hacks, which cost cryptocurrency holders a record $14 billion last year by one tally.

Algorand is one of a swarm of new blockchains that aim to transform finance and the modern world by serving as the platforms for so-called decentralized smart contacts that can be conducted person to person and across borders without government intermediaries.

An announcement at the Milken conference that Algorand will partner with FIFA, the governing body of world soccer, drove up prices of its ALGO coin, making it the 30th-largest cryptocurrency on Coinbase on Tuesday, with a $4.5-billion market cap. (Bitcoin's market cap is $725 billion.)

Q: Your contribution to modern encryption won you the Turing Award. What applications does it have today?

A: It is used to secure a lot of things that go over the internet. When you send a message to Citicorp, one of the practical side products of our work is that your browser knows that it is talking truly to Citicorp and not to a middleman who is intercepting the messages and pretending to be Citicorp.

Q: Bitcoin has been around since 2009. What was your first impression of it?

A: I bought into the main idea. The idea is beautiful, but somehow the solution is not exactly elegant. We all aspire to beauty and elegance in what we do.

Q: One of the criticisms of bitcoin is the energy needed to validate transactions and mine new coins. There is a bill in the New York State Assembly that would impose a moratorium on bitcoin mining. Can you describe the energy efficiency of Algorand in terms I can understand?

A: Bitcoin absorbs as much electricity as a small country, and we are going to consume as much electricity as roughly 10 homes. [Algorand uses a so-called pure proof-of-stake method for validating blocks of transactions, versus bitcoin's far more energy-intensive proof-of-work system.]

Q: Where are we on the adoption curve with blockchain technology?

A: We are in a very divided world. We have blockchain 1.0, 2.0, 3.0, 4.0—which I believe Algorand is—coexisting during the same time. So that is very unique. If you look at the Industrial Revolution ... you have more and more sophisticated [technologies], so usually not all these things coexist. We are at a very unique moment in which there are extremely sophisticated blockchains like ours and when there are very early generation blockchains who continue to be there simultaneously. It's like you have Neanderthal man and Homo sapiens living together.

Q: What do you see 10 years down the road?

A: The moment the blockchain starts to be used for transactions, the few blockchains that are really capable of transacting at a very low cost, they're going to emerge, in my opinion. When traditional finance starts getting on the blockchain, you're going to see the blockchains that are really used in a massive and transactional way are going to accelerate. And a few store of values [like bitcoin] will maybe stay.

Q: New blockchains such as Algorand are being created to serve as platforms for diverse decentralized applications such as digital currencies, carbon offset trading and personal identification. Yet many people are more interested in buying the coins as a speculative investment.

A: First of all, we cannot stop people from speculating. But what we want to give is a technology to enable people to use our platform for a variety of transactions and really sophisticated transactions too.

Q: Can you give an example?

A: So if you look at stocks, right, stocks have a settlement time of T plus 2. T is the time when you buy a stock and two is the number of days after which this transaction settles. That is two days of waiting for a transaction to settle. We settle our [blockchain] transactions in 4.4 seconds today, at the end of Q2 in 4 seconds and at the end of Q3 in 2.5 seconds. That's an enormous difference.

Q: That future is hard to predict and any person signing on to a Coinbase account for the first time would be bewildered by all the investable cryptocurrencies. What single piece of advice would you give a newbie?

A: I really believe that you have to invest in what you understand. But nobody can say you have to understand the technology, no more than you have to understand how a plane flight works to take a plane. But you have to ask some very basic questions.

Q: What are those?

A: To invest in cryptocurrency the most basic tool is consensus [verification of the blockchain]. One question I would ask if you want to join a blockchain is, "Can I join the consensus process of this blockchain?" That's a very fair question. And if the answer is, "Sure, buy a couple of supercomputers and join us." And you say, "I don't have a bunch of supercomputers nor do I have the money to buy them." So, I'd say be careful.

Q: Any other bad answers?

A: If the answer is, "You could but we already have a club. Sorry, you are not one of the club." So then I have to say you have to be concerned.

Q: Is there a good answer?

A: If the answer is not only you are allowed to join, but you have the technical means to join because a laptop is enough or something very basic, so then I have to say that means that blockchain is really decentralized. And I believe that decentralization is really the ultimate source of security.

Q: Last question. You are a brilliant Turing Award-winning MIT computer scientist. Have you been lying to us? Could you be Satoshi Nakamoto, the legendary anonymous creator of bitcoin?

A: (Big laugh.) No, but I cannot prove it.

Citation: Cryptography pioneer Silvio Micali on where crypto is headed (2022, May 4) retrieved 27 April 2024 from
https://techxplore.com/news/2022-05-cryptography-silvio-micali-crypto.html