EDITORS' PICK

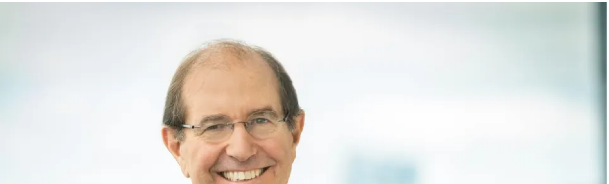
Algorand Founder Silvio Micali Breaks Down How To Construct A Fast And Secure Blockchain In A World Full Of Adversaries

Steven Ehrlich Forbes Staff
Director of FDA; Editor, Forbes CryptoAsset & Blockchain Advisor.

Nina Bambysheva Forbes Staff
Senior Reporter, Digital Assets

0

Jul 12, 2021, 08:27am EDT



Algorand Founder Silvio Micali ALGORAND

Algorand founder Silvio Micali is one of the most preeminent mathematicians and computer scientists of the last 50 years. Father to many of the key components of any functioning blockchain, his research interests include cryptography, zero knowledge technologies, pseudorandom generation, secure protocols, and economic mechanism designs. He is a recipient of the Turing Award in computer science, often referred to as the Nobel Prize of computing, in addition to numerous other accolades such as the Gödel Prize (in theoretical computer science) and the RSA prize (in cryptography).

At Algorand, Silvio oversees all research, including theory, security and crypto finance related to the decentralized blockchain. Aside from being an MIT faculty member since 1983, he is a member of the National Academy of Sciences, the National Academy of Engineering, the American Academy of Arts and Sciences and Accademia dei Lincei. Silvio received his Laurea in mathematics from the University of Rome, and his Ph.D. in computer science from the University of California at Berkeley.

In this discussion I spoke with Silvio, as well as Algorand CEO Steve Kokinos, about how blockchain technology, and Alogrand in particular, combine encryption with economic models to create efficient and secure blockchain systems. We also discuss how Algorand solves for the notorious "blockchain trilemma" and get an update on Algorand's latest progress.

This interview was first published in ***Forbes CryptoAsset and Blockchain Advisor*****.**

Forbes: Silvio, you are one of the most influential computer scientists in the industry. In fact, you fathered many of the key foundational pieces for blockchains. I'd love you to briefly summarize your career and tell us how that led you to crypto.

Silvio Micali: I'll be brief. I started in Rome, in mathematics, logic and calculus. But when I discovered algorithms, which are some of the newcomers still in the grand scheme of things in mathematics, I fell in love with them. So I decided to pursue theoretical computer science at UC Berkeley. And there I took a course in computational number theory. The last few lectures of the course were devoted to cryptography, which I then fell in love with as well.

When I started being a cryptographer, my first Ph.D., which I'm afraid to admit was in 1985, was on the subject of Byzantine agreement, which was one of the foundations for distributed computation. Then after a few decades in cryptography, I got bored and decided to start working on economic mechanisms, designing a new type of auction, and then suddenly I heard about Bitcoin. It was a perfect storm, because I consider blockchain to be the intersection of cryptography, distributed computations and economic mechanisms. I felt it was too good to let it go and decided to throw my hat into the arena and get working on it.

Forbes: Many people have heard of algorithms, but most cannot define them. From your perspective, what is an algorithm in its most basic form? What are your definitions for terms like determinism and cryptography?

Micali: An algorithm is a very, very precise procedure, so precise that a computer can follow it without asking any questions to anybody. The output is uniquely determined by the input and a deterministic algorithm is a recipe so detailed that a computer can execute it from beginning to end. And that was really how mathematics became constructed. Because rather than saying a solution exists, an algorithm actually allows you to compute the solution—this is a very big deal in computing efficiently. In my opinion, it was really as momentous an invention as the control of fire.

Forbes: I want to give an analogy to my readers to understand the term. Is it sort of like, if you're following the scientific method to do a basic experiment, and you set it up the same way and use the same input you will get the same output?

Micali: Absolutely. Every single time. Regarding cryptography, the name means secret writing, because originally, the only cryptography in existence was a way to encrypt messages from the prying eyes of an adversary who may see the message. If I send a message to you, whether it is on horseback or a computer network, an adversary can intercept and try to decipher it. We want to make his life miserable, but I still want the intended recipient to understand very clearly what we are saying to each other.

We then started using the same mechanism and algorithm for other uses, such as generating pseudo random numbers, which was a precursor to the digital signature scheme (a key element to users authenticating themselves on a blockchain). Here, I want to make sure not only that the message is correct and secret, but also that the sender is real and not an imposter. So slowly, cryptography morphed into a general science of interaction in the presence of an adversary. In some sense, it is a very powerful tool because you don't need to be a cryptographer to believe that adversaries are everywhere. An adversary could decipher your message, pretend to be the sender of a message and try to predict your random numbers or your future moves.

Forbes: How else does cryptography fit into blockchain technology? How do you use it in Algorand?

Micali: The traditional application of cryptography to blockchain is to prevent an adversary from altering the content of a block or the order of blocks. But in Algorand we use it for doing what we call a cryptographic sortition: we select an unpredictable committee (to add blocks to the network) whose members are not known until they show up with a proof that they belong to the committee. That is really the secret sauce of Algorand, which allows us to be very scalable and very distributed. In some sense, this is a use of cryptography because even though I am running my own lottery (forming the committee members), I cannot cheat. I cannot alter the probability of winning. And if I win, I can prove to you that I'm a legitimate winner of my own lottery.

It is really a new application for cryptography that allows us to unpredictably convene a committee. You cannot somehow control the committee members or know in advance who they are going to be. As you may know, many blockchains propose the blocks by way of a round-robin: participants take turns, and an adversary knows in advance who is going to generate the next block and could perhaps attack. But if the generation of a new block is entrusted to a few committee members, say a few hundred or a thousand, and nobody knows who they are because they are the winners of secret individual lotteries, an adversary cannot go after them in advance. Once these people show up and say, "I won the lottery," you can believe they are the real winners because nobody can alter the probability of winning or pretend to have won when they have actually lost.

Forbes: Talk a little bit about how Algorand is able to scale faster than other blockchains.

Micali: Here's the way we operate differently from other blockchains: First, we agree on one block before producing or starting the generation of the next block. But our agreement on the block is so fast – essentially a few seconds – say in 4.5 seconds we already have produced the block, circulated it and agreed on it. Then we start working on the next block or transaction. So, the good part of this is by agreeing on the block, our blockchain never forks (splits into various variations) and that is really a big advantage over other chains. Because not only do you want to add the blocks quickly, but you also want to add them with finality.

If in a typical blockchain you see a payment made to you in the latest block, you should not necessarily ship the goods because if there is a fork, the blockchain will go in another direction and the block with your payment may actually end up on the short fork, which will disappear.

Forbes: Are you talking about how it is good practice to wait for six block confirmations before considering a bitcoin transaction final?

Micali: Exactly, Bitcoin and other blockchains as well. But if you are paid in ALGO (Algorand's native currency), you can ship the goods right away because any block we produce is going to stay on the chain forever. Say, there is a two thirds majority, all the participants know what the block is, and there is not going to be another alternative block where two thirds of majority think about something else. There is an honest majority that can only agree on one block and this is a very big property of Algorand.

Forbes: I want to ask a bit more about a few key terms in computer science that relate to crypto and blockchain. Our investors would want to get a little bit into the details and understand why blockchains work the way they do and the differences between them. For instance, I know that you were one of the co-inventors of zero-knowledge proofs. Can you briefly talk about that explaining how they work? Does Algorand include zero-knowledge proofs?

Micali: To tell you the truth, right now we don't need them, but we have plans for using them in the future. So first of all, let me tell your readers about zero-knowledge proof. A proof is a way to convince somebody that something is true. Now, if you are skeptical, I cannot just claim the following statement is true, I must prove it to you. But by the time I prove it, I must reveal a lot more information in order to convince you that the statement that's been claimed is indeed true. And a zero-knowledge proof does something very unorthodox: it proves the statement directly, so you know that the statement is true, but you have no idea why, and you don't gain any additional information, except the statement or whatever I want to prove.

Then people say "Gee, a little bit more information never hurt anybody. So, what's the point?" Remember, adversaries are everywhere. So, in a distributed system, when you need to prove to others what is true – for instance, if we are in different processors, and I do a part of the computation and you do your own part, I want to give you my part together with a proof that what I've done is correct. So, you can keep on going, knowing that you are starting to work on something that is true and correct. Very often, when you have a distributed system, not knowing who an adversary is and who is not, zero-knowledge proofs guarantee the integrity of a joint computation.

That said, we are not using them right now. Regulators are still thinking about how to deal with blockchains, and they want to foster innovation but also make sure no bad actors can be given a free ride. The notion of zero-knowledge proofs is perhaps so complex that I think we want to establish first how blockchain works, make sure that the regulators and everybody else understands, and add that later.

Forbes: Probably the most prominent blockchain that incorporates zero-knowledge proofs is Zcash. But the vast majority of Zcash users actually don't use shielded addresses or shielded transactions, probably also because they're computationally heavy. Do you have any insight on that, and is there a way to incorporate zero-knowledge proofs in a way that's a bit more lightweight so that it doesn't weigh down a network?

Micali: Absolutely. I think when we are going to introduce zero-knowledge proofs according to our schedule, as you say they're going to be very light (computationally). By the way, I very much like Zcash. I think it is a great idea, and, in fact, one of my best students was a co-founder and co-inventor of its algorithm. They do indeed leverage zero-knowledge proofs. And sometimes people use zero-knowledge proofs not only for secrecy, but certain forms, called snarks or CS proofs, can be used to shrink large amounts of information in an efficient way. However, because we are already so efficient, we will zero-knowledge proofs mostly for privacy at the right time.

Thank you for that background. Before we wrap up, I want to get an update on Algorand. What's its latest status?

Micali: We launched in June 2019, and we produce blocks in less than five seconds every single time. We've never had an outage or a stopping; we never had to call back anything. We are just minting new blocks with greater resiliency and progress. At the same time, one thing we've wanted from the very beginning of Algorand is to bake into our very code the ability to change our mechanism in a consensual way. This has enabled us to add to our chain a lot of good features. We've upgraded our system several times already. One time we added a Layer 1 smart contract, another time – another thing. I don't buy this mantra that we often hear in the blockchain world that "law is code, the code is law," that whatever you see is going to be the same forever. In my opinion, being static is the opposite of being alive. I think that our life is about intelligent adaptation to changing circumstances. So, we wanted to be able to fulfill the needs of our customers, members of our community of not only today, but also our community of tomorrow. If we want to do this, we need to upgrade in a consensual way, and that's what we do in Algorand. Every few months, we have essentially a special type of boat in which 80% of the people agree on upgrading the algorithm. So, we are able to incorporate and we'll continue to incorporate new tricks.

Forbes: Okay. And Steve?

Steve Kokinos: One of the things that we are excited to see is adoption in the ecosystem, people using the technology, projects building on top of Algorand and supporting it. Today, there's a little more than 11 million users across over 500 projects that are building on top of Algorand, generating an average of around 750,000 transactions a day, and that cuts across a lot of different areas. One of the things we've been most excited about is the way new projects and DeFi applications are starting to interact with more traditional businesses coming on-chain. To give an example in the creator economy, the Italian music rights system deployed about 4.5 million NFTs onto Algorand – that represents the music rights for more than 100,000 artists, and there's about a billion dollars a year in royalties represented by those creative assets. What we're seeing in response is platforms like Opulous, which is a DeFi application allowing for fractional sales, borrowing and lending of music assets as well. It's a sort of community growth that we think is really exciting.

A couple of other interesting examples that we're seeing: we are powering the first blockchain-based Covid-19 passport for Colombia. And the country's vaccine passport program is running on Algorand. We're seeing applications like central bank digital currencies (CBDCs): the Marshall Islands is using Algorand for its national currency, and we see a lot of activity in those areas – kind of overarching all these interesting decentralized financial applications and people coming and joining in with more traditional businesses that can take advantage of those.

We've been very focused on climate. We announced recently on Earth Day that we're the first carbon-negative chain. We have smart contracts that look at how much carbon is being consumed by the actual nodes supporting the network and make sure that offsets are automatically purchased in response to that. And that's thanks to partners like ClimateTrade that are using the blockchain for novel applications. They have only UN-approved sources of certified climate credits, and the fact that they're transacting those in a blockchain-based marketplace is really exciting.

Another good example is PlanetWatch, which is deploying air quality sensors around the world to make it both the case that people can understand what air quality looks like near them but also in cases where countries need to adhere to air quality standards or pay carbon taxes. In the cases that they're not [adhering to those standards], now they can be held accountable and there’s transparent data associated with that.

So, I think what we're seeing is a very broad array of decentralized applications that really span the gamut from novel financial applications to digital art and music. We are really excited to see more and more uses of the technology and this path from not just the 11 million users we have on-chain today across those application but seeing hundreds of millions of people starting to take advantage of applications that really help them transact in new ways and help them get access to different types of products than they would have in the past.

Forbes: Can you talk about the ASA token standard (which lets designers mint tokens on Algorand in the same way that ERC-20 enables tokens to run on top of Ethereum) and what type of adoption it has created?

Kokinos: Sure, well, the idea behind the ASA standard and, I think, a broader idea in Algorand is that for many things that are represented by smart contracts on other blockchains really ought to be part of the protocol itself. And so, in Algorand, the ASA standard is actually in Layer 1. The smart contract does not require people to create a new asset. They can be used for tokens, security tokens, which we have many on-chain, non-fungible tokens – it really kind of spans the gamut. We've seen great responses to that. As I mentioned, we've got more than 4.5 million non-fungible tokens on the platform. There are several hundred fungible tokens including some of the largest stablecoins in the blockchain space: USD Coin (USDC), which is a project between Circle and Coinbase, Tether (USDT) and over a dozen stablecoins in all including the Canadian dollar, Brazilian Real, Digital Euro, and many others. We're really excited to see the take up that has been happening there. What's even more interesting is that there's a combination of regulated securities with things like the Republic Note and several others. Exodus wallet did a Reg A+ $75 million round on Algorand as a security token. So, I think we're starting to see more assets come on-chain and more applications that enable transactions or transact-ability of those assets on-chain as well.

Forbes: Let’s talk about your competitors. For one, Ethereum is transitioning to proof-of-stake; they also have a bunch of Layer 2 solutions. Silvio, what's your outlook on Ethereum? Do you think this transition will be successful and if so, what does it mean for Algorand from a competitive point of view? Additionally, how do you compare and contrast Algorand with Cardano? I interviewed Charles Hoskinson a few weeks ago and he was very deferential to you and Algorand. Obviously, there are differences, so I'd love to get your perspective.

Micali: First, let me make sure your readers understand one thing. Blockchain is a big arena of change for humanity. We've already gone through the communication revolution; we can send information to millions of people very easily. Now, the blockchain is making sure, in a nutshell, to guarantee common knowledge. It is a very big opportunity and a very big challenge.

So yes, they are competitors but, in my view, they are also collaborators. This is a very big enterprise. And Charles is a good friend, a fellow mathematician. He also believes in improvements and rigor in blockchain. I wish him good luck because the opportunity is so big; no blockchain wins it all. I think there are going to be a few foundational blockchains and I believe that Algorand will be one of them.

Speaking of change, with Algorand we've baked in the ability to change in a consensual way without hard forks or soft forks. That is really the advantage because if you don't have that, then you must be very cautious any time you introduce a chain. You cannot at every change split the community in half and then in another half. There are so many splits you can do to the community, right? So, I wish everybody success in their changes and transitions. But I really want to stress the importance of enabling change, by design, in a consensual way because nothing lives for too long if it's not capable of adapting or changing.

Forbes: One of the big metrics that everyone looks at to gauge the health of a blockchain is developer activity. Steve, you are probably the right person to contextualize the level of developer activity on Algorand right now and shed a little insight on how you market to developers. In particular, how do you get them to build on Algorand as opposed to other Turing-complete blockchains?

Kokinos: The number of developers building on Algorand has grown by an order of magnitude over the past year. We've had more than 20,000 downloads of our developer tools. The number of users coming to develop on Algorand.org, which is one of our key sites, has continued to increase. One of the other things we've tracked is what testnet activity looks like. If you look at that, it’s a good harbinger of applications getting ready to deploy, and we're seeing literally thousands of assets and applications deployed there and then transitioned into mainnet applications. We look at both a combination of developer activity growth and new applications, but we're also interested in what the resulting user growth is and transactional volume growth. We think about all three of those things together and we're pretty excited about all of them.

When you look at the proof of being in the pudding, the fact that we've gone from tens of thousands to 11 million users across a variety of different applications over the past 18 months or so is a really good sign. The fact that this growth is accelerating, not declining, as new applications deploy, is a really positive sign. If you think about what we're creating as the internet of money, Algorand is sort of that Layer 1 bandwidth and transactional capacity that people need, and other ecosystem players are providing things like wallets, custody services, borrowing and lending applications, and decentralized exchanges. Those are all the building blocks of the next generation of applications. It’s great to see so many launches and so many new people joining the community.

Forbes: Thank you.