Unlocking the potential of blockchain technology

June 18 2021, by Zach Winn

Algorand uses a unique blockchain architecture developed by MIT Professor Silvio Micali to offer a decentralized, secure, and scalable platform. Credit: Massachusetts Institute of Technology

The Republic of the Marshall Islands is a country of around 50,000

people spread across more than 1,000 islands in a remote part of the Pacific Ocean. The country relies heavily on cross-border finance and trade, and the complexities of that system can make it difficult for citizens to get certain goods and financial services efficiently.

Now the federal government is seeking to become the first to issue a national digital currency using blockchain technology. Officials hope the move helps citizens avoid high transaction fees, simplifies compliance with international partners, and protects against inflation (the currency will have a fixed supply rate).

The new currency will be based on blockchain technology developed by Silvio Micali, the Ford Professor of Engineering in MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), and commercialized by Micali's startup, Algorand.

There has been considerable hype around the potential for blockchain technology and associated cryptocurrencies to disrupt the way money and other assets move around the world. Skeptics of that vision say blockchain technologies are not sustainable or efficient enough for mass adoption.

Algorand believes it has solved those problems with a unique, scalable architecture that doesn't sacrifice traditional benefits of blockchain technology like decentralization and security.

An increasing number of people are using Algorand for a wide range of applications, from creating carbon credit marketplaces to expediting real estate transactions and, in the case of the Marshall Islands, creating new legal tender.

"The advent of blockchain technology has opened up a world of opportunity for small nations like ours," Marshall Islands Minister-in-

Assistance to the President David Paul said when the country announced its plans. "By issuing a currency that is not physically embodied in cash, that can travel the globe instantly, and that is tamper-proof and completely secure, the Marshall Islands will finally be connected to the global financial system on its own terms."

Starting from scratch

Micali has long been recognized for his work in cryptography and security. He's been a member of MIT's faculty since 1983, and in 2012 was awarded the Turing Award with his collaborator and fellow MIT professor, Shafi Goldwasser.

Working with others, Micali's achievements include a new way for distributed parties to agree on a value or strategy even if some of the parties are corrupt (reaching so-called byzantine agreement), and a method for parties to securely send information to each other in a way that can later be verified by the public (called verifiable random functions).

Much of Micali's work occurred long before the rise of modern cryptocurrencies and hype around blockchain. In the case of verifiable random functions, Micali says he knew they'd be useful somehow, but couldn't figure out the application.

Still, Micali put off learning about blockchains for years after the creation of the first blockchain-linked cryptocurrency, Bitcoin, in 2008. One day he finally walked into his lab and asked some of his graduate students to explain it to him.

"I had two main reactions," Micali remembers. "One was it's a beautiful idea. Two was it's a very inelegant solution."

Of particular interest to Micali was a problem put forth by the founder of another blockchain, Ethereum. The founder said blockchains can guarantee at most two of the following: decentralization, security, and scalability.

"The notion that something was impossible really attracted my attention, because in cryptography, and MIT more generally, our business is to prove the impossible possible," Micali says.

Micali also credits MIT's ecosystem with helping him start Algorand. Of his first 10 hires, eight were from MIT.

"It's not only the tech, it's also the entrepreneurial spirit at MIT and the fact that we don't shy away from challenges," Micali says. "But the most important source for me and Algorand is also the most important resource at MIT: the people."

In 2017 Micali started from scratch to build a better blockchain.

The term blockchain refers to records of information, stored in blocks, that users can add to, forming chains. Each block contains an abbreviated version of the previous block and time stamped information like transaction data. As more blocks are added, the previous blocks become harder to alter, providing a secure ledger of transactions and other information. Many public blockchains have associated cryptocurrencies, or digital assets, and information about cryptocurrency transactions is stored on the blockchain ledger.

"The challenge is who should be able to append the next block of transactions to the blockchain," Micali says. "Because if I have the ability to declare something common knowledge, I have a lot of power. Who should have that power?"

Some blockchains select users to add and validate the next block by having them devote computing power to solving cryptographic riddles. That approach has been criticized for being inefficient and energy intensive. Other blockchains give users holding the associated cryptocurrency power to validate new blocks on behalf of everyone else. That approach has been criticized for being too centralized, as relatively few people hold the majority of many cryptocurrencies.

Algorand also relies on an associated cryptocurrency to validate new blocks. The company calls the currency Algo coins. Rather than giving the power to validate new blocks to the people with the most coins, however, Algorand has owners of 1,000 tokens out of the 10 billion in circulation randomly select themselves to validate the next block.

The tokens are selected in a microsecond-long process that requires relatively little computing power. The random selection also makes the blockchain more secure by giving no clear target to hackers, helping Algorand solve the "trilemma" put forth by the Ethereum founder with a scalable, secure, and decentralized blockchain.

On top of that architecture, Algorand's community has developed additional features tailored to specific functions, like smart contracts, which can self-execute based on predefined conditions in their code, in some cases eliminating the need for central authorities and intermediaries like lawyers.

To allow smart contracts to execute on its blockchain more efficiently, Algorand created a programming language called Transaction Execution Approval Language (TEAL). TEAL returns a true or false value depending on if specified conditions are met, simplifying the process of creating and executing contracts on the blockchain.

The contracts have since been used to enable financial transactions, build

a marketplace for small purchases of gold, and collect small-scale investments in startups.

Unlocking the potential of blockchain

The Italian Society for Authors and Editors was founded in 1882 after artists organized to avoid exploitation. A lot has changed since its founding, with conglomerate streaming services coming to hold huge amounts of power over content like movies and music. The result is a complex copyright ecosystem where royalties for artists are reduced by publishers, lawyers, auditors, and other intermediaries.

But today more than 100,000 artists in the organization have their copyrights digitally represented and can trade or sell those rights at publicly listed market prices on Algorand's blockchain. The artists can give permission to use their songs in certain cases while retaining the copyrights.

"We enjoy artists, but we often don't give them what is due to them," Micali says.

The use case fulfills a central promise of blockchain, empowering people to exchange goods without centralized authorities taking up money and time. It also exemplifies what's been a huge source of business for Algorand so far: the tokenization of digital assets, also known as non-fungible tokens, or NFTs.

The application also hits home for Micali, who has been happy to see people in his home country of Italy benefiting from his solution.

"It shows how you can regain possession of your own information," Micali says. "That's a big trend, because very often to make information available you have to give the rights of your information to someone

else, who then owns your information. It's easy to say you shouldn't do that, but we need technology to get around it. The only way to go forward now is decentralization."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology