

July 20th, 2019

ALGORAND

The Distributed Ledger for the Borderless Economy

Silvio Micali
MIT, USA

Abstract

A *distributed ledger* is a tamperproof sequence of data that can be read and augmented by everyone. Distributed ledgers stand to revolutionize the way democratic societies and traditional economies operate. They secure all kinds of traditional transactions –such as payments, asset transfers, titling– in the exact order in which they occur; and enable totally new transactions –such as cryptocurrencies and smart contracts. They can remove intermediaries and usher in a new paradigm for trust. As currently implemented, however, distributed ledgers cannot achieve their enormous potential. The global participation and trust necessary to realize an inclusive and borderless economy require substantially better technology.

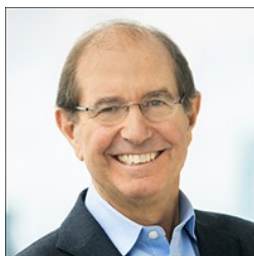


Algorand is an alternative, democratic, and efficient distributed ledger.

Unlike prior ledgers based on ‘proof of work’, it dispenses with ‘miners’. Indeed, Algorand requires only a negligible amount of computation. Moreover, its transaction history does not ‘fork’ with overwhelming probability: i.e., Algorand guarantees the finality of all transactions.

In addition, Algorand guarantees *flexible self-governance*. A successful society and economy must be able to evolve. A cryptocurrency cannot be an ocean liner on autopilot. By using its hallmark propose-and-agree process, Algorand can consensually correct its course, as necessary or desirable, without any ‘hard forks’, to meet the current and future needs of the community

Short bio



Silvio Micali has been on the faculty at MIT, Electrical Engineering and Computer Science Department, since 1983. Silvio’s research interests are cryptography, zero knowledge, pseudorandom generation, secure protocols, and mechanism design.

In 2017, Silvio founded Algorand, a fully decentralized, secure, and scalable blockchain which provides a common platform for building products and services for a decentralized economy. At Algorand, Silvio oversees all research, including theory, security and crypto finance.

Silvio is the recipient of the Turing Award (in computer science), of the Goedel Prize (in theoretical computer science) and the RSA prize (in cryptography). He is a member of the National Academy of Sciences, the National Academy of Engineering, and the American Academy of Arts and Sciences and of the Academia dei Lincei.

Silvio has received his Laurea in Mathematics from the University of Rome, and his PhD in Computer Science from the University of California at Berkeley.