Capgemini
RESEARCH INSTITUTE

breathe in(novation)

UNCOVER INNOVATIONS THAT MATTER

Quarterly review
N°5 — 2022

Conversations FOR TOMORROW

Conversations
FOR TOMORROW

From the Desk of

Silvio Micali
Founder of Algorand &
Ford Professor of
Engineering at MIT

BUILDING A SUSTAINABLE AND SCALABLE BLOCKCHAIN

Algorand

Silvio Micali is the recipient of the Turing Award in Computer Science (Editor's note: colloquially known as the Nobel Prize in Computing), the Gödel Prize in Theoretical Computer Science and the RSA Conference Award for Excellence in Mathematics (for his pioneering work in cryptography).

He is a member of the National Academy of Sciences, the National Academy of Engineering, the American Academy of Arts and Sciences, and the Accademia dei Lincei. Silvio received his Laurea in Mathematics from the University of Rome, and his PhD in Computer Science from the University of California at Berkeley. In 2017, Silvio founded Algorand, a fully decentralized, secure, and scalable blockchain cryptocurrency protocol that provides a common platform for building products and services for a borderless economy.

Meet the blockchain

The blockchain is a shared database that is not centrally organized. It is a shared database in which everybody can write, everybody can read, and nobody can alter what has been written. Here, trust in people or entities is replaced with algorithmic trust. What does this mean for large organizations or the economy itself?

1. The current lack of trust implies that, if two entities or individuals need to transact at distance, they must rely on an intermediary, who will extract 6% of the value of a transaction. Six percent of global GDP is a lot of money. It is also a lot of time; traditional intermediary settlement takes T+2 days. In 24 hours, a lot can change in the world. On the blockchain, this happens in a few seconds. Such speed lowers counterparty risk.

2. Blockchain helps drive democratization of finance. Intermediaries do not care about the poor as they cannot extract value from them. Blockchain can step in there. .

3. Blockchain brings an important ability to tokenize assets for everyone. It is much easier to sell a small share of an office building than to sell the entire office building. It can help make illiquid markets liquid, at speed.

BLOCKCHAIN CAN HELP MAKE ILLIQUID MARKETS LIQUID, AT SPEED

The smart contract is the secret sauce

A smart contract executes automatically when certain conditions are met. Smart contracts make blockchains programmable, increasing security and reducing the need for user involvement in transactions by establishing a clearly defined procedure for transferring assets. Decentralization makes blockchain a much more secure platform; whenever you have a single point of failure or endpoint of failure, it's much easier to subvert.

Take the case of selling a large building. With the blockchain, it is possible to tokenize the building and conduct a large-scale Dutch auction. The transparent nature of the blockchain allows participants to see all bids worldwide and to know who has won what and at what price. The winner receives shares of the building and payment is debited automatically.

To summarize, smart contracts bring forth several advantages:

- **Security:** Unlike credit- or debit-card purchases, transactions on the blockchain don't require the purchaser to entrust a third party with sensitive information, greatly reducing risk of data theft, fraud, and financial loss. Transactions are final and irreversible, so there is no risk of chargebacks or cancellations, another common route for fraud.
- **Transparency:** Transactions made by smart contracts can take place on public blockchains, meaning that anyone can verify each transaction.
- **Autonomy:** Because smart contracts are autonomous, they eliminate the risk of manipulation by third parties and intermediaries.
- **Cost savings:** Smart contracts eliminate the need for multiple intermediaries to process complex payments, saving money on service fees.
- **Accuracy:** Calculations are made automatically, eliminating human error.
- **Speed:** The automation of calculation, verification, and approvals can save hours of manual labor, freeing workers up for strategic tasks.

What are some use cases for smart contracts?

Improved security and increased efficiency through automation are the most obvious areas where companies can benefit from implementing smart contracts. However, the combination of security, trust, and transparency can enable a variety of services:

Escrow services
Large transactions, such as real-estate purchases or trade deals, currently require escrow: that is, a trusted third party holds the fee while a sale takes place. A smart contract can be programmed to hold the money and automatically release it to the seller once the legal requirements are fulfilled.

Global payments
Smart contracts can be used to execute multi-layered global payments based on predetermined criteria between two or more parties across borders, at minimal cost, with near-instant settlement speeds.

Payroll
The structure of work is changing and, with it, the structure of payroll systems. Smart contracts can automate payroll for thousands of employees. Hourly contracts, monthly salaries, bonuses, and commissions can all be integrated into smart contracts and processed instantly.

Dividends
Many publicly traded companies pay out dividends to shareholders on an annual or quarterly basis. Smart contracts can automate this process, updating details automatically if the stock changes hands. This also has the potential to lower dramatically barriers to issuing stock to investors.

Treasury management
Blockchain-based treasury management offers a number of benefits, especially for large organizations. Corporate treasury managers, for example, can view the disposition of accounts of different entities worldwide, in real time. This can enhance decision-making processes via improved cashflow forecasts and capitalizing on time-sensitive investment opportunities.

Blockchain challenges

Many blockchains waste tremendous amounts of energy. Another key challenge is decentralization. If you go to a centralized blockchain, you're essentially leaving yourself at the mercy of a few agents, who then decide whether you can transact or not. If you want an institutional-grade blockchain, it should be decentralized.

Another challenge is uptime. Uptime does not matter when the blockchain is used for speculation, but it becomes a major issue with real-time applications. Another big issue is the lack of universal definitions, so it’s very hard to compare blockchain to blockchain.

Why blockchain sustainability is important

We have a moral obligation to the planet, and that includes creating a blockchain that brings advantages without wasting energy. Global, borderless, open-source technologies must consider their impact on the environment. Providing inclusive access to new Internet-native financial products and services cannot come at the expense of the environment. Rather, the industry needs to ensure that new blockchain-powered solutions not only benefit businesses and consumers but the environment as well; or, at the very least, not harm it in the way that many legacy technologies have done. To achieve a sustainable blockchain industry, businesses and open-source projects should focus not only on deploying carbon-neutral technology but also supporting use cases that drive eco-friendly initiatives. In this context, evolvability is a key component of sustainability, because nothing lives or remains relevant for very long unless it has the ability to adapt.

> **"To achieve a sustainable blockchain industry, businesses and open-source projects should focus not only on deploying carbon-neutral technology but also supporting use cases that drive eco-friendly initiatives."**

The rise of the sustainable blockchain and Algorand

In the crypto world, it has been defined as the famous blockchain trilemma: the impossibility for a blockchain to be simultaneously secure, decentralized, and scalable. That did not sit well with me, wearing my cryptographer's hat. I admired the ethos and the idea of Bitcoin but I believe the way they implemented the achievement of this goal was not exactly as beautiful as the idea itself. So, I wanted to design something that retained the ethos and the goals of Bitcoin but in a technologically sound way.

Algorand takes a proactive approach to blockchain sustainability by deploying an environment-friendly consensus protocol and focusing on providing green blockchain solutions. Pure proof of stake (PPoS) is a protocol that enables Algorand to address the blockchain trilemma, ensuring that none of the three key elements of an ideal blockchain – scalability, security, and decentralization – is compromised.

> **“Algorand takes a proactive approach to blockchain sustainability by deploying an environment-friendly consensus protocol and focusing on providing green blockchain solutions."**

The PPoS enables Algorand to build a sustainable and scalable blockchain ecosystem that sets the standard for the future of finance. This makes it ideal for a variety of use cases for future finance (FutureFi), such as DeFi (decentralized finance), tokenization, NFT (non-fungible token) creation, stablecoins, payments, and more. By virtue of its network structure, Algorand is theoretically able to scale up to billions of users, while maintaining low costs and high levels of security and performance.

Embrace the blockchain

If you are the CXO of a large organization, there are some things you need to understand about blockchain:

1. It is here to stay. It is not a fad and it is not going away.
2. Not all blockchains are alike. Ask the questions that matter so you understand the tech:
   a. Is the blockchain green?
   b. Is it decentralized?
   c. Does it have the ability to evolve consensually?
3. Being an informed early adopter is key to success. Latecomers may not benefit.

Once you have done this, you should embrace blockchain. It's a wonderful technology, and can transform your industry, your nation, and the world at large.

> "Smart contracts eliminate the need for multiple intermediaries to process complex payments, saving money on service fees."

www.capgemini.com