Blockchain 4.0

Silvio Micali

MIT, Algorand, and Algorand Labs

There is a real difference between digital platforms, especially 'closed' ones, which tend to create legal systems, and blockchains, which are ontologically open, as their business model requires wide use of the chain. This will be discussed by others at this conference. In this speech, I would like to limit myself to some preliminary aspects of blockchain technology that can be decisive when addressing the issue of blockchain regulation, in which the States and the regulatory and supervisory authorities must participate.

My speech consists of two inter-related parts: *On Technology* and *On Regulation*.

ON TECHNOLOGY

The media (except for the most professional media) are stuck in an old narrative. It is thus imperative to correct immediately outdated perceptions.

What are the most frequent misconceptions in most of the Media? Well:

1. All blockchains are the same
2. All blockchains are bad for the environment
3. Blockchains are a solution looking for a problem
4. Blockchains vanify all forms of control

These statements have one thing in common: they are ALL FALSE.

Then, what is the TRUTH?

TRUTH # 1: There exist DIFFERENT types of blockchains.

> *Earlier* blockchains could NOT simultaneously be secure, scalable and decentralized. This was unfortunate, because each of these three properties is crucial.
>
> **Blockchains 4.0**, by contrast, ARE secure, scalable and decentralized *at the same time*. As so they should be in order to be useful to the world.

TRUTH # 2: There exist GREEN Blockchains.

> While some *earlier* blockchains, which still operate today, consume as much electricity as a small country, **Blockchains 4.0** consume IN TOTAL the energy equivalent of 10 homes. Ten well-lit homes, perhaps. But only ten homes, nonetheless.
>
> This is important to understand. The idea that blockchain progress necessarily comes at a cost for the environment is just the *dystopia of the uninformed*.

TRUTH # 3: **Blockchains 4.0** offer powerful SOLUTIONS TO REAL PROBLEMS**.**

> *Earlier* blockchains could just offer an immutable archive of *static data*. Thus, at best they could only provide “digital gold”. At worst, only speculation: the false promise of high returns on small investments.
>
> BY CONTRAST, **Blockchains 4.0** offer way more than an immutable and transparent database. They also secure all kinds of *transactions*. For instance, they enable two parties to exchange assets *directly. Without having to rely on costly intermediaries.* In a SINGLE,

INDIVISIBLE transaction. In just a few seconds. With total security. And at the cost of *a fraction of a cent*.

Such security and such time and cost efficiencies are crucial to small and medium enterprises and wherever economic development is needed. Because *traditional mediators are too costly and do not have the time or the financial incentives to enroll ordinary people and help them in their ordinary transactions.*

TRUTH # 4: **Blockchains 4.0** guarantee *a priori* compliance with clearly established rules.

Traditionally, regulators could rely only ex post inspection to verify that the rules of the game have been followed.

BY CONTRAST, in **Blockchains 4.0**, super efficient smart contracts can *automatically* guarantee that agreed rules are indeed followed without any supervision. This may actually vastly simplify the role of regulators. For instance, Blockchains 4.0 may algorithmically prevent that securities end up in the hands of non-accredited investors.

More holistically, the truth is that **Blockchains 4.0** are an instrument of *real* progress.

For the first time in Finance, bilateral exchanges can be truly simultaneous, secure, and *unmediated*. Mediators that add value to the transaction will always be welcome, but when the only function of a mediator is to enable the transaction itself, then what is welcome is a secure and efficient technology that *replaces* that mediator!
To be sure, some countries are lucky enough to have already in place payment systems that are electronic and extremely fast. Yet such payments are still *unilateral*. Even when they are used to purchase digital goods and services, *expensive* and *slow* architectures must be relied upon to guarantee that you will get what you are paying for. *Payment vs. Delivery* continues to be a major problem. Also when payments are super-fast. Only **Blockchains 4.0** have finally solved this vexing and century-old problem. But not only that.

Blockchains 4.0 provide a sustainable, incorruptible platform on which air and water quality can be monitored by a multitude of independent actors, and thus with no cheating.

They provide a platform that is so efficient and so decentralized to really achieve financial inclusion.

They may enable regulators to participate in setting new, more articulated, and more currently relevant standards, and automatically guarantee that they will be followed.

They provide a technology enabling the Public Administration to become a "*transparent house",*
All of this is possible TODAY, not in some mythical future. Cost, performance, and sustainability are no longer barriers to mass adoption. We must correct outdated narratives. And all of us, businesses, regulators, and researchers, must seek and be open to new information that is aligned with current reality**.** *The welcome reality of* **Blockchain 4.0.**

ON REGULATION

It is urgent for regulators to intervene in blockchain matters *and* to do so *correctly*. To begin with, we must acknowledge that this is *not* an easy task. Correctly regulating the blockchain requires grappling with two major issues.

FIRST ISSUE: *Some blockchains out there **are bad***. They promise financial inclusion, but they either fail to deliver on their promise or, worse, harm those who trusted them. This is a problem, because *bad blockchains cannot be punished.* Whereas the crypto wallets of individual criminals can be traced through forensic work, bad blockchains do *not* have a physical address. They do *not* have a phone number. They are everywhere and nowhere. There are no offices to seal shut. The platforms themselves cannot be shut down. If bad blockchains were to dominate the market of digital ledger technology, *it would be a collective nightmare*.

SECOND ISSUE: *Blockchain technology is already EXTREMELY popular and is here to stay.* The demand for this technology, in so many domains, cannot be suppressed. In the world there is a natural demand for transactions that do not need costly intermediation. For inclusive finance. For speedy, reliable, and transparent administration. With this kind of demand, the blockchain cannot be ruled out of existence. Nature abhors a vacuum. And in the absence of correct regulation, the risk is that *bad blockchains* will rush in to fill this vacuum and provide ineffective or harmful solutions to the ever-greater demand for this powerful technology.

Then, how to act?

Because punishing bad blockchains is impossible and because the appeal of blockchain technology is irresistible, let me suggest that what the regulators should and can do is to allow *good blockchain projects* to fulfill the world's demand. And to do so *as quickly as possible*. With regulatory uncertainty, good blockchain projects will, by and large, refrain from entering the arena, and with outdated regulation, good blockchains will compete at a disadvantage with bad blockchains that simply ignore all rules. Thus, the danger is that this crucial and needed space will be filled by *bad blockchains,* which cannot be dislodged.

So: Can we distinguish which blockchains are good and which are bad? Which foster financial inclusion, and which do not? I think we can. Let me suggest seven *simple* tests that go a long way in this direction.

FIRST TEST: *Scalability.* Financial inclusion, by definition, needs scalability. So, a simple but very useful question is: *How many transactions per second are possible in this blockchain?* If the answer is, say, 16 transactions per second, then there CANNOT be any financial inclusion. There are billions of us and with this transaction rate you are lucky if you transact once a year. Such a blockchain can only support *speculation* and does NOT pass this test!

SECOND TEST: *The Cost of Basic Smart Contracts.* The quintessential basic smart contract is a *bilateral exchange*: I have an asset that you want, you have another asset (e.g., money) that I want, and we wish to swap them. Thus, *What is the cost of a bilateral exchange of assets in this blockchain?* If the answer is *"50 cents or more"*, then this blockchain cannot deliver financial inclusion! Because exchanging assets is the most fundamental form of trade –indeed the heart of commerce itself– and because 50 cents is an *exorbitant* amount when your salary is 50 Euros per month, or when the assets to be exchanged are worth only 10 Euros.

THIRD TEST: *Environmental Sustainability.* Blockchains, like any other product, require energy to be produced and energy to operate. So, *How much power does this blockchain consume?* If the answer is *"a LOT of energy,"* then there is no hope for financial inclusion. And worse. Because the less privileged are the first to suffer from the degradation of the environment. A blockchain that is **bad** for the environment is a **bad** blockchain. Period.

FOURTH TEST: *Consensus.* Consensus is the fundamental process by which new blocks of transactions are chosen and added to the chain. So, let's ask: *Can anyone participate in the consensus protocol of this blockchain?* If the answer is: *"sure, as long as they buy a couple of supercomputers,"* then there cannot be any financial inclusion either. Because most of us cannot afford buying super computers. If the answer is *"Sorry: we already have a club of, say, 10, 20, or 100 agents who are in charge of choosing future blocks on behalf of all of us,"* then, again, there is no guarantee of financial inclusion. In fact, such an elitist club has the full power to *exclude* whomever they want from transacting.

FIFTH TEST: *Continuity of Service*. Let's put it simply: *How often is this blockchain 'down'?* If the answer is "for a few hours every month", then the chain is inappropriate for financial inclusion. Truly decentralized services do not frequently stop working. Speculation can easily skip a day, but essential financial services must operate without interruption.

SIXTH TEST: *Upgradability*. *Can this blockchain be upgraded? Has it ever been updated?* If the answer is "No, never. We are proud that the chain will continue to operate in the same way it has always operated," then, walk away. When new and safe technology becomes available, a blockchain must be able to incorporate it seamlessly, without interruption of service and in an automatic, decentralized manner. Only so can a blockchain continue to satisfy the needs of its community, today and tomorrow.

SEVENTH TEST: *Decentralized Interoperability*. We should never trust any blockchain, or any infrastructure for that matter, which would not allow us, when necessary, to transfer our assets and our information elsewhere. So: *Can this blockchain easily transfer assets and information to another blockchain? Can it do so in a decentralized fashion?* Unfortunately, most approaches to blockchain interoperability today are centralized, naïve, and dangerous. They envisage a few 'trustees' who would tell with absolutely authority, and hopefully with absolutely honesty, what is transferred from one blockchain to another. Introducing such centralization is very dangerous, because corrupting or hacking a few trustees is very easy. Moreover, imposing a proportionate fine upon a trustee who, maliciously or not, has made a mistake would be an *empty threat*. The value transacted across blockchains would be enormous, and no trustee would have the ability to pay fines commensurate to the damage done. Decentralization is the real source of security. Interoperability between two blockchains should be achieved directly by the two blockchains involved, without the intervention of anyone else. It is only a question of technology, and such technology is already mature. Let's not settle for anything less.

In conclusion: *What specific steps should regulators, in particular, and more generally governments, businesses, technologists, and citizens at large, take?* In my opinion, two steps: *education* and *experimentation*.

STEP 1: EDUCATION, because we should understand and clarify to the general public which *technical properties* blockchains should have in order to be truly useful to civil society. This step goes a long way towards preventing that individuals, businesses, institutions, and governments, honestly intending to participate in Decentralized Finance, Transparent Administration, etc., find themselves stuck in an inferior blockchain whose technology can only deliver centralization, if not risky speculation.

STEP 2: EXPERIMENTATION. Because experimentation is essential to allow the regulator to understand first-hand not only the potential, but also the limits of blockchain technology. Joint experimentation is the best way to enable the regulator to keep pace with a new technology that keeps evolving at super speed, but also to jointly set its deirection. *The blockchain cannot be regulated with the rules of the last two decades, let alone those of the last century.*

Only through education and experimentation can we achieve **CORRECT** REGULATION; *permitting* responsible blockchain technologies to help all of us move forward in a safe way; and fostering *true* financial inclusion and *true* international collaboration.