BLOCKCHAIN IN THE AGRI-FOOD CHAIN: EVOLUTION, REVOLUTION OR HYPE?[1]

Blockchain technology, which appeared in 2009 as the technological support for the virtual currency Bitcoin, has been described in recent years as the great revolution that will change the economy and many businesses. In 2014, Marc Andreessen, co-founder of Netscape and inventor of the first web browser, referred to Bitcoin (and its underlying technology, blockchain) as the most important technological invention since the creation of the Internet in 1993. The Economist defined blockchain as "*the great chain of being sure about things,*[2]" and stated that *"the technology behind Bitcoin lets people who do not know or trust each other build a dependable ledger, and this has implications far beyond the cryptocurrency.*"

WHY DO WE NEED A TECHNOLOGY LIKE BLOCKCHAIN? [3]

According to the original document that described it[4], "*Bitcoin is a peer-to-peer electronic cash system (…) that allows for online payments to be sent directly from one party to another without going through a financial institution.*" In other words, Bitcoin makes digital economic transactions possible without a "trusted intermediary." Blockchain technology was invented to support this electronic currency. Why was this necessary?

---

[1] This is a case of the Research Division of San Telmo Business School, Spain. It has been written by Professor Jose Antonio Boccherini Bogert of San Telmo Business School and is intended as a basis for class discussion only and not to illustrate any judgement on the effective or ineffective management of a specific situation.

[2] "The great chain of being sure about things." The Economist, October 31st, 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things (accessed on February 10th, 2019).

[3] This section is an adaptation of the explanation included in the document "What is blockchain technology?" CB Insights, September 11th 2018. The document can be downloaded following this link: https://www.cbinsights.com/research/what-is-blockchain-technology/

[4] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," October 31st 2008, https://bitcoin.org/bitcoin.pdf, accessed on February 11th 2018. Satoshi Nakamoto is a pseudonym. A programmer or group of programmers published the document in a mailing list that operated under that pseudonym, remaining anonymous thus far.

Let's imagine that Mario wants to pay Julia one euro in the world of physical money. Mario hands over the coin to Julia, and the transaction is complete, safely. After the transaction, the coin is no longer in Mario's possession, and now Julia has the coin. Mario and Julia do not need an intermediary to verify the transaction. Mario cannot give Laura that coin to make another payment because he no longer has it. It is not possible to make two payments with the same coin, and the conditions that grant value to the currency are guaranteed: property can be certified and remains a scarce asset.

What would happen, though, if that coin were not physical but digital? Mario could send the digital currency to Julia by email (for example) to make his payment. Then Julia should have that digital coin, and Mario should no longer have it. But what if Mario keeps a copy of that digital coin before sending it to Julia and then uses it to pay someone else? After all, a digital coin is just a string of ones and zeros and can, therefore, be easily reproduced. If this problem remained unsolved, virtual currencies would be of no value or use.

If Mario and Julia own the same string of ones and zeros, how can we know who is the legitimate owner of the coin? One possible answer would be to use a digital record (i.e., a ledger) to track transactions and attest who is the legitimate owner of the coin. In that way, if Mario made a payment to Julia, it would be recorded that the coin now belongs to Julia and no longer to Mario.

But who will manage the ledger? It cannot be Mario because he could erase the transaction and claim that he still owns the coin. For similar reasons, it cannot be Julia, either. One solution could be to use an intermediary, a third party (let's call him Leonardo), trusted by both Mario and Julia. Leonardo would hold the ledger and keep it up-to-date.

In a way, this is the case nowadays with most payments made by bank transfer. Money is an accounting entry (and, therefore, it is digital). A transfer is a mere electronic transaction that subtracts an amount from the payer's account and adds it to the account of the person receiving the payment. The transaction is made by a trusted third party (the bank) who attests that the balance in both accounts is correct. Today, most people in countries with developed banking systems trust banks.

However, Leonardo (Mario and Julia's trusted intermediary) could decide to charge a fee for this work that neither Julia nor Mario are willing to pay; or Mario could bribe Leonardo to erase the transaction, thus recovering his digital currency; or Leonardo might not be so trustworthy after all and want to steal the coin, adding a false transaction to the ledger and claiming that Mario gave him the coin.

That is, what if Mario and Julia do not want to pay the intermediary a fee or do not trust the intermediary? One possible solution would be to distribute copies of the ledger to all their friends, decentralizing trust. Because the ledger is digital, all copies of the ledger should sync together, and any new transaction should be updated in all of them simultaneously. If a simple majority of participants agree that the transaction is valid (that is, confirm that Mario is the legitimate owner of the coin he wants to use to pay Julia), it is approved and added to the ledger.

This is known as a distributed ledger. If Mario or Julia wanted to forge a transaction, they would need to bribe the majority of participants or modify most copies of the ledger, which is even harder to do. Leonardo only has one copy of the ledger; if he altered it to try to steal the coin, it would no longer be the same as the other copies, and the forgery would be spotted.

The more “trusted parties” that keep a copy of the ledger, the more secure and reliable it becomes. The system, therefore, builds trust between parties that do not necessarily know each other and who are not necessarily reliable as individuals. If more than half of the participants are honest and trustworthy, security is absolute. But even if they were not, it would be difficult for everyone to be interested in forging the ledger in the same way for most copies to be consistent and considered valid.

In the previous example, the two participants who kept a copy of the ledger were "friends" and, therefore, relatively reliable. When it comes to Bitcoin, however, the ledger is entirely public, and anyone can participate and keep a copy. This means there is a higher risk of malicious participants and false transactions.

Bitcoin’s solution to this problem is to reward honest participants and punish malicious ones. Some participants in the Bitcoin network (called "miners") receive incentives to do the "dirty work" of ensuring the integrity of the ledger. When a new transaction is added, miners compete to fit the transaction into the structure of the ledger by solving a deliberately complex mathematical puzzle that requires enormous computational effort. The first one to solve the problem receives, after verification of at least 51% of the remaining miners, a reward in Bitcoins. Considering the price Bitcoin has reached, this is no small incentive. In this way, hackers are also discouraged because a false transaction would require a tremendous amount of computing power, electricity, and, hence, a lot of money (way more than could be hacked). Moreover, even if it were assumable to hack the Bitcoin network, the most significant disincentive would be the very result of the operation: the value of the currency would plummet, and any potential gains would vanish.

WHAT IS BLOCKCHAIN TECHNOLOGY?

Blockchain, the technology that underlies Bitcoin, has potentially many applications besides cryptocurrency. It offers a way to create a digital record of information (transactions, events, contracts, etc.) that is distributed and decentralized, secure and immutable, all without the need of an intermediary or a central authority to certify that the information recorded is reliable:

- **What can be recorded using blockchain?** Although it can be used to record any information, it is specially designed for transactions between two or more parties (for example, payments between individuals), contracts (such as the sale of a house, for instance), events (like the dispatch of a truck loaded with specific merchandise from a warehouse), and other similar information. Each piece of information (transaction, event, etc.) is recorded in a so-called block.