

Blockchain and cryptocurrencies: welcome to the new digital paradigm

Technological change will change the payment system as we know it, and blockchain technology will probably play a very important role in this process by facilitating the emergence of digital currencies. What are the key aspects of the technologies that will enable this transformation? Which cryptocurrencies are most likely to succeed?

Blockchain technology

Advances in cryptography, combined with the potential for data transmission and storage, have enabled the emergence of so-called distributed ledger technologies (DLTs). These are databases of which there are multiple identical copies distributed among participants on the network and which are updated in a synchronised and consensual manner. The great attraction of DLTs is that they allow data to be securely managed and shared, as well as saved, without the possibility for the information to be altered. The most well-known type of DLT is a blockchain, which organises information into blocks and regularly compares it with a ledger that cannot be deleted.

Blockchain technology is based on three key ingredients:

- Thanks to cryptography, each block of information is uniquely identified.
- Participants on the network must approve and validate all the information entering the network.
- The register is tamper-proof and immutable, making it extremely difficult to hack or modify.

Blockchain technology facilitates the emergence of cryptocurrencies, because by creating a shared register of all the transactions and establishing a decentralised method of validation, money can be digitally exchanged between users, directly (traditional payment infrastructures have a central intermediary, such as the central bank, a digital payment processing company, a mobile platform, etc.). The best-known application for blockchain technology in the financial world is payment settlements (in cross-border transfers, cryptocurrencies can play a valuable role as a bridge currency), as illustrated in the first flowchart.

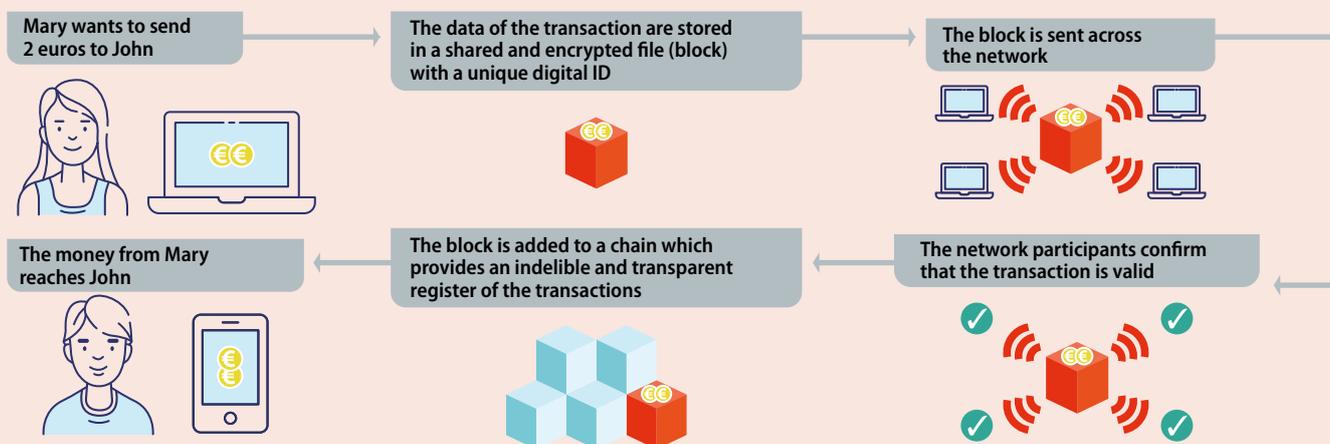
Blockchain, a rapidly-evolving technology that could facilitate the development of applications for mass use

One of the areas that is being worked on the most is in improving the scalability of blockchain payment systems, one of their key ingredients. The first initiatives that emerged were fully decentralised and public networks. In these cases, since all participants must validate the transactions, the number of transactions that can be processed is greatly limited (a prime example is that of Bitcoin, which processes 7 transactions per second compared to Visa's 65,000) and the energy costs are very high. One of the solutions being explored is the use of permissioned networks, in which an administrator controls the network and decides who can participate in it. The advantage of such networks is that they are more scalable and allow transactions to be validated much quicker, although they are more vulnerable to attacks aimed at altering the ledger.

Beyond blockchain

It is important to clarify that technological advances in the financial sector go far beyond cryptocurrencies and DLTs, and they have enabled improvements in the speed and operation of payment systems. A good example of this is the spectacular advances made in mobile payments. Besides, as we have seen, blockchain technology has a lot of potential, although it would be possible to issue a digital currency without having to resort to using it. In fact, an authority with process centralisation powers, such as a central bank, could do so by developing an infrastructure based on the payment systems that are already in operation today.

How blockchain technology works



Source: CaixaBank Research.

The main areas in which the use of cryptocurrencies can prove beneficial are:

- **International financial transactions.** Although blockchain technology is not the only alternative being explored in this area, it is a clear candidate for improving the efficiency of cross-border payments by **reducing the costs involved and increasing the speed of transactions compared to highly-centralised systems.**
- **Reducing the underground economy.** Despite one of the main properties of cryptocurrencies being the anonymity of the transactions, mechanisms could be designed to facilitate the identification of illegal activities. For instance, they could be designed so that payments in certain areas or of a certain amount would not be anonymous.
- They can promote **financial inclusion** in underdeveloped or emerging countries, where a significant portion of the population is unbanked (but could store cryptocurrencies in a digital wallet linked to their mobile phone).

Not all cryptocurrencies are made equal

According to the definition by the BIS,¹ cryptocurrencies stand out because **they are digital** and because **they allow exchanges to be carried out peer-to-peer.** However, there are many types of cryptocurrencies. The so-called «money flower» helps us to classify different currencies, including cryptocurrencies, based on their properties in the most important areas: the type of issuer of the currency (central bank or not), its accessibility (widely accessible or restricted), its form (digital or physical) and its transfer mechanism (peer-to-peer or centralised). For example, depending on the issuer, there are three major classes of cryptocurrencies:

- **Private cryptocurrencies:** issued by an individual or private entity.
- **Central bank cryptocurrencies.**
- **Hybrid solutions (synthetic cryptocurrencies):** the central bank is the issuer, but a set of private entities would be in charge of customer interaction and innovation (in advanced economies, the natural candidate would be commercial banks).

Central bank cryptocurrencies and private cryptocurrencies: pros and cons

A priori, if a central bank ends up issuing a **cryptocurrency**, and it has a well-defined regulatory framework and there are no doubts over its security, **it is highly likely to be accepted as a widespread form of payment.** Being backed by a public institution that cannot fail, the mere fact that a fraction of savings and transactions switch to being carried out with the «crypto» version of the currency should not affect its value. For private cryptocurrencies, in contrast, it is harder for them to maintain a stable value since it depends on their degree of acceptance and adoption. Given that this can change suddenly, their value tends to be more volatile.

In any case, proposals are emerging that attempt to overcome this disadvantage. So-called stablecoins seek to solve this pitfall by setting what is effectively a fixed exchange rate between the cryptocurrency and an asset with a stable value (such as the currency of an advanced country). Libra, the cryptocurrency proposed by Facebook, falls under this family of cryptocurrencies.²

Arguments are often made in favour of developing cryptocurrencies backed by a central bank that could complement traditional monetary policy tools. As an example, setting an interest rate on the digital currency would broaden the range of instruments available to the central bank.³

However, the introduction of cryptocurrencies issued by central banks would also present risks given that they could contribute, at least in part, to reducing intermediation in financial activities:

- If a portion of household and business bank deposits were converted into cryptocurrencies not managed by financial intermediaries, the supply of funds available for lending would diminish. This would tend to increase the cost of credit, as well as giving central banks greater prominence as structural suppliers of liquidity to the system.
- The existence of such central bank cryptocurrencies would increase the volatility of flows between bank deposits and cryptocurrencies in times of uncertainty or when doubts arise over the solvency of a financial institution, thus posing a risk to financial stability.
- The degree of financial disintermediation is critically dependent on who holds custody of the digital wallets for the cryptocurrencies. If it is the central bank, individuals could hold accounts directly in the central bank, which would aggravate the risk of disintermediation and financial instability. It would also be possible for financial institutions unrelated to commercial banks to perform this role; this would not eliminate financial intermediation but it would pose major challenges: how would such entities be regulated? Would the wallets be protected by a deposit guarantee?...

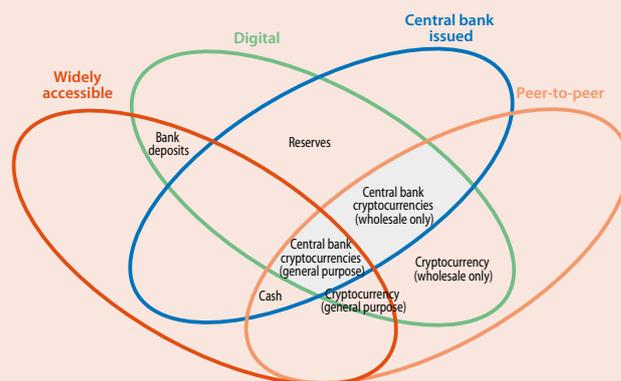
Javier Garcia-Arenas

1. See Committee on Payments and Market Infrastructures (2015). «Digital currencies». BIS.

2. See the article «[Libra, the cryptocurrency of Facebook](#)» in this same Dossier.

3. For more details, see the article «[The e-monetary policy of the new digital economy](#)» in this same Dossier.

The money flower: a taxonomy



Source: CaixaBank Research, based on the diagram by the BIS.