

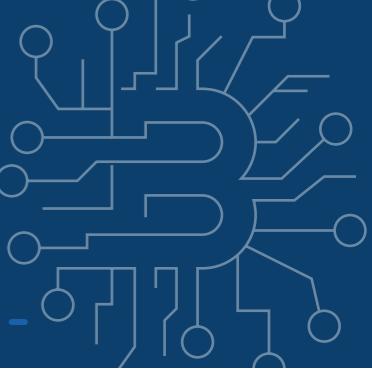
TOULOUSE SCHOOL OF ECONOMICS AND CRYPTOCURRENCIES

JUNE 2018

Analysis by Bruno Biais, senior TSE faculty
and CNRS Research Director in finance,
on the technological and socio-political aspects
of cryptocurrencies.



INTRODUCTION



Satoshi Nakamoto aimed to create and circulate a currency with no intervention from central banks and financial institutions. To do so, he created the blockchain protocol and the cryptocurrency, bitcoin. As Nakamoto wrote in the abstract of his article in 2008,

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network."

A bitcoin was worth only 50 cents in 2010. Today it is worth nearly \$10,000. A fine performance! Yet bitcoin has received its fair share of doubts and even severe criticism. In 2018, at the University of Frankfurt, the General Manager of the Bank for International Settlements said (see speech here: <https://www.bis.org/speeches/sp180206.htm>)

"Money is an indispensable social convention backed by an accountable institution within the State that enjoys public trust. Experience has also shown that to be credible, money requires institutional backup, which is best provided by a central bank. Private digital tokens posing as currencies, such as bitcoin and other crypto-assets that have mushroomed of late, must not endanger this trust in the fundamental value and nature of money."

Serious warnings have also been issued by the most prominent economists including Joseph Stiglitz and Jean Tirole, who published an warning op-ed about bitcoin in the Financial Times on 30 November 2017.

"We should be cautious of this trend: investors must be protected and regulated banks, insurance companies and pension funds should be prevented from building exposures to these instruments. [...] Governments that still give sympathetic consideration to bitcoin and ICOs would be well-advised to protect their citizens and their financial institutions against risky and socially harmful developments."

There are two opposing views on the matter. On the one side is the libertarian and technological view, which sees bitcoin as a peer-to-peer currency based on an IT protocol with no external intervention. On the other side is the institutional and political view which considers the currency can only be trusted if it is issued and managed by a reliable public institution such as an independent central bank.

Cryptocurrencies have developed against the backdrop of two major social trends: the questioning of the establishment and our institutions, and the thriving influence of new information technology. Instead of a central power that intervenes as a last resort to manage the allocation and value of the currency, partisans of cryptocurrencies defend the idea of a direct democracy among internet users via a blockchain that is public, open and transparent¹.

What position should we hold on these two contradictory views? Should we support the libertarian or the institutional view? Will blockchains and cryptocurrencies revolutionise society and the economy, or are they only dangerous illusions?

To shed light on these issues, Bruno Biais, senior TSE faculty and CNRS Research Director in finance, uses economic theory to analyse how blockchains operate in the first section of this document, and the value of cryptocurrencies in the second section.



B R U N O B I A I S



Professor at TSE, B. Biais is also a senior researcher at Centre for Research in Management (CNRS). His work has been published in *Econometrica*, the *JPE*, the *AER*, the *Review of Economic Studies*, the *Journal of Finance* and the *RFS*. He has taught at HEC, CMU, LBS, Oxford and LSE. He has been a scientific adviser to Euronext and the NYSE. He received the CNRS bronze medal and is a fellow of the Econometric Society. He has been editor of the *Review of Economic Studies* and is co-editor of the *Journal of Finance*.

RESEARCH INTERESTS

- Market microstructure
- Corporate finance
- Financial contracting
- Political economy
- Psychology and economics
- Experimental economics

¹/ Financial institutions, central banks and companies are currently developing private blockchains. These initiatives are interesting, but radically different from public blockchains, which are decentralised, transparent and open to all, whereas private blockchains are managed by a central authority that decides who has access to the chain, who can intervene, and how. Here we are going to deal only with public blockchains.



How do blockchains work?

In the abstract of the paper (2008) mentioned above, Nakamoto goes on to say that,

"The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone."

This is not easy to understand at first, what with mysterious terms like 'proof of work', 'hash' and 'the longest chain'. To try to clarify this, first I will explain the objective and mechanism behind blockchains. Secondly, I will present the predictions of economic theory on how the chain works.

Nakamoto's vision (2008)

Let us first recall the three basic characteristics of blockchains:

1) It is a ledger that indicates to which IT identification the objects or assets - in our case, bitcoins - belong. All of the blocks in the chain describe the changes to the ledger.

2) It is a distributed ledger because it is accessible to all those who have access to the network and can consult and modify it. The blockchain is therefore known as distributed ledger technology.

3) In the distributed ledger, decisions are made by internet users who are members of the network. The blockchain protocol holds a kind of IT vote by the members of the network. The aim is to prevent an individual from controlling the blockchain a central authority. Rather than an actual vote, the blockchain protocol organises a type of random draw among the members of the network. For each block, i.e. for each change in the blockchain, a member of the network is chosen at random to decide whether or not to approve the change.

The first blockchain and the largest one so far is the ledger indicating who each bitcoin belongs to. When a bitcoin owner exchanges it for goods or services, or another currency, the owner informs the network. The network's job is to validate the transaction, include it in a block with other transactions, and attach the block to a previous block. The new chain including the additional block results in a new ledger status.

The members of the network who approve the transactions and link the blocks together are referred to as miners. Nakamoto (2008) describes how he suggests the miners work (see Figure 1):

- I) The miner receives messages via the network with the transactions.
- II) The miner groups the messages together to form a block.
- III) The messages are approved (for instance checking that someone transferring a bitcoin actually owned it). This step is very fast.
- IV) The miner then works on a complicated numerical problem, devoid of interest in itself, and unrelated to the number of type of transactions in the block.

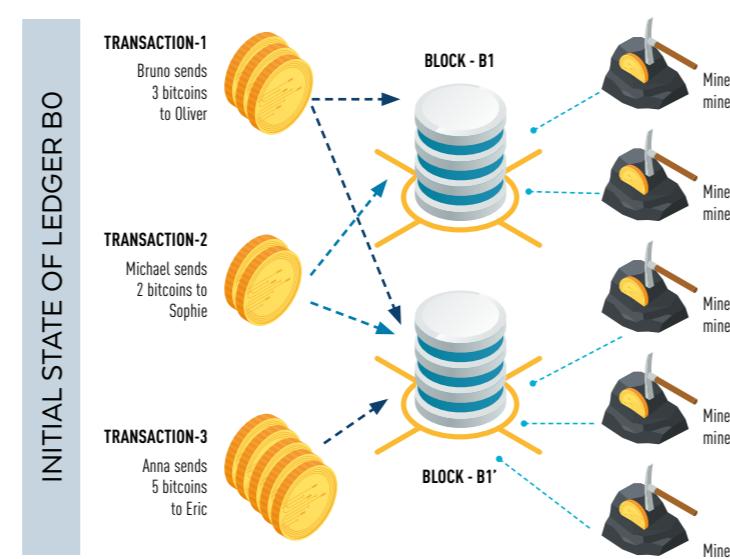


Figure 1A: Miners, transactions & blocks



When the miner has solved the problem, the network is informed that a block has been solved and to which previous block it is chained. The other miners receive that information. They can choose to ignore it and keep looking for a solution to the problem of their block. However, Nakamoto (2008) recommends that miners give up working on their block and start mining another block chained to newly solved block. By following that recommendation, the miners follow the "longest chain rule", mining the chain with the larger number of blocks.

Suppose that the miners follow the longest chain rule. After a block has been solved by one miner it is checked by the others. By checking the solution, the network members obtain proof that the miner has done the job (i.e. 'proof of work'). After obtaining this proof of work, the miners decide whether or not to accept the new block. If they do, they link chain their next block to it.

Why would miner follow the longest chain rule and give up mining on a block to focus on the new one created by another miner? The first part of the answer lies in the process of solving blocks. To solve the numerical problem, the miner draws answers at random and checks each randomly drawn answer to see whether it is the right solution. To do this, the miner uses computers. The bigger the CPU power of these computers, the more solutions the miner can draw per second (ie the larger the hash rate), and the faster the miner can solve the problem. However, for the same CPU power and problem solving difficulty, time the miner needs to find the solution is random. An important property of this random variable is that the remaining time before the problem is solved is independent of the time already spent on solving the problem. You get an idea of how this property works by imagining that the miner draws balls out of an urn, with replacement. One of the balls has the solution to the

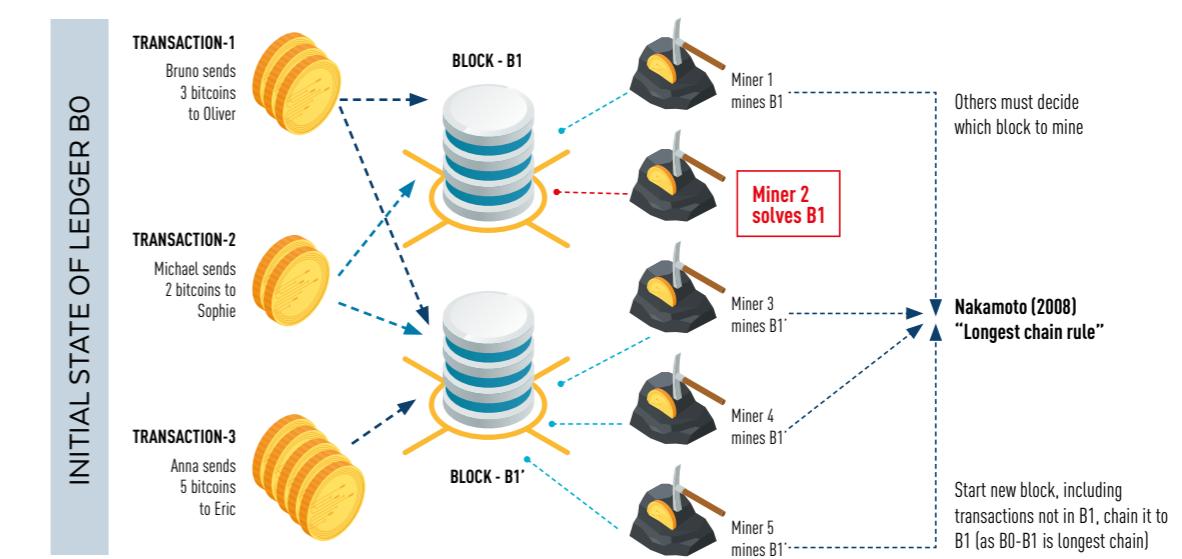


Figure 1B: Rule of the longest chain

problem while the others contain no information whatsoever. A miner who has worked for one second on the problem has the same chance of solving it as another miner who has already worked for 15 minutes on it. From this point of view, there is no more incentive for the miner to continue trying to solve the same problem than there is in attempting a new problem.

But why do miners devote their time, CPU power and electricity to solving problems? Because for each block they solve, the miners are given a reward. In the bitcoin protocol, miners who solve blocks receive a certain number of bitcoins - currently 12.5. Practically speaking, the miner registers a transaction within the block that allocates bitcoins to the miner. If the other miners agree with the block that has been mined, by attaching their blocks to it, they thereby show their approval of the reward. These 12.5 bitcoins are created out of nothing. This monetary creation is predetermined by the bitcoin protocol and gradually decreases. It was worth 50 bitcoins initially, and is halved every four years. In 2020, the reward will be 6.25 bitcoins. By 2140, 21 million bitcoins will have been mined, by which time the bitcoin monetary creation will cease.



How will the miners be paid when the creation of bitcoin ceases? In addition to creating currency, the miners are paid commissions by economic agents who make transactions. If I transfer 1 bitcoin to one of my children and want the transaction mined quickly, I can promise a high commission, say 0.01 bitcoins, to the miner who solves the block including my transaction. When there is no more currency creation, the miners will be paid only by commissions.

In Nakamoto's view (2008), the protocol described above and the longest chain rule will allow for the creation of a unique and transparent chain open to all, with a ledger that has a reliable and sustainable consensus. Is his view realistic? What has been observed in reality? And what light does the theory shed on the past and future of the currency?

From vision to practice

The first observation is that the bitcoin currency is hugely successful. Many people buy and sell bitcoins, resulting in transactions that are approved by the miners. Accordingly, mining has also increased, using more and more CPU and power (10 terawatt-hours (TWh) one year ago, 44 TWh three months ago, and 62 TWh today. See <https://digiconomist.net/bitcoin-energy-consumption>). This consumption of power is equivalent to the amount used by Switzerland. Other cryptocurrencies also using CPU and electricity have enjoyed huge success, including ether, based on the Ethereum blockchain.

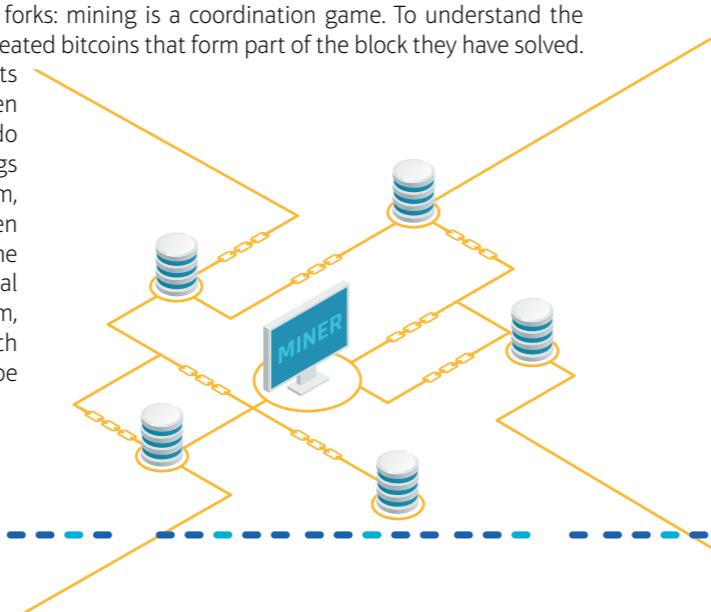
Many of the newly created cryptocurrencies result from forks. In summer 2016, Ethereum split into two different blockchains creating a rival currency, Ethereum Classic. In August 2017, Bitcoin also forked to create Bitcoin Cash, and in Autumn 2017, a new split occurred with the creation of Bitcoin Gold. In December 2017, as the value of bitcoin was soaring, more and more forks occurred, giving rise to Super Bitcoin, Bitcoin X, Oil Bitcoin, Bitcoin World, Lightning Bitcoin, etc.

While most of the recent forks will probably be short lived, some will survive and attract miners and investors. This is the case for Bitcoin Cash. The hash rate on the bitcoin network currently stands at 30 exahashes a second (30×10 to the power of 18). This is only eight times higher than the Bitcoin Cash hash rate. One bitcoin cash is currently worth 0.16 bitcoins. However, each fork is a deviation from Nakamoto's longest chain rule and from the consensus, and leads to different ledgers, which can undermine the value of cryptocurrencies.

Why are so many forks occurring? How is this even possible, when Nakamoto announced the creation of a single blockchain?

The forks mentioned above are caused by disagreements within the community of miners and developers. In the case of Ethereum Classic, ethers had been siphoned off from a fund (The DAO, or Decentralized Autonomous Organization). Members of the community suggested going back on the blockchain to cancel the embezzlement. At first it appeared the entire community agreed with the solution, but soon a minority opposed it and believed the blockchain should remain untouched. One and a half years later, the new currency is still around. One ether classic is worth around \$20, while one ether is worth around \$700. In the case of Bitcoin Cash, a disagreement occurred about how to change the protocol to increase the size of the blocks. For Bitcoin Gold the disagreement was about the use of ASIC, specific integrated circuits that can only be used for mining, the production of which is dominated by a powerful Chinese company.

These disagreements demonstrate the underlying reason for the forks: mining is a coordination game. To understand the phenomenon, you will recall that miners are rewarded with newly created bitcoins that form part of the block they have solved. These bitcoins are only recognised as valid by other economic agents if the block itself is recognised as valid. This is what happens when other miners link their blocks to the existing one. They will only do this if they believe there is a consensus on the chain the block belongs to. In this context, there exist multiple equilibria. In an equilibrium, the miners anticipate that chain A will achieve consensus. They then decide to attach their blocks to that chain and subsequently the chain attracts more blocks, achieving consensus in line with the initial anticipation, which is thus proved rational. But in another equilibrium, most of the miners believe that A is not valid and so decide to attach their blocks to other chains. A is abandoned and turns out not to be



valid, in line with the initial anticipation. In our joint research article with Christophe Bisière, Matthieu Bouvard and Catherine Casamatta (The blockchain folk theorem) we demonstrate the existence of multiple equilibria, and that forks can occur and persist in equilibrium (cf. https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2017/wp_tse_817.pdf)

To summarize this first section: that in line with Nakamoto's view, blockchains attract miners and serve as ledgers for cryptocurrencies valued by investors. However, in contradiction to his view, miners do not always follow the longest chain rule, there is no single chain that achieves complete consensus, but forks offering different versions of the ledger. The appearance and persistence of these forks is due to the fact that mining is a coordination game which allows for multiple equilibria.



What is the economic value of a cryptocurrency?

Given the promises and difficulties of blockchain technology, what is the economic value of cryptocurrencies? Could they one day rival currencies supervised by central banks? To shed light on this issue, we will begin by detailing the economic function of a currency, and then discuss the ability of cryptocurrencies to fulfil that function.

What is a currency, and how is its value determined?

A currency is something you accept as payment because you expect that it will be accepted as payment when you want to make a purchase with it in the future. Definition points to the key role of expectations. When it comes to currencies, it is all a question of beliefs.

To discuss the economic role of currencies, we can begin with a barter system, and analyse how the situation improves when you introduce money.

In a barter system, when only bilateral exchanges of goods and services prevail, the issue arises of the double coincidence of wants. Suppose that Alan has apricots, but he likes carrots, while Bernard likes apricots but has bananas; suppose also that fruits cannot be stored, except by their initial owner. When Alan meets Bernard, Bernard wants Alan's apricots, but Alan doesn't want



Bernard's bananas and Claire has carrots but likes bananas. Similarly, when Bernard meets Claire, he does not want her carrots in exchange for his bananas. There is no double coincidence of wants, so the exchange cannot take place.

To allow the exchange to happen, we need a more sophisticated relationship, as demonstrated by Wicksell's Triangle the eminent Swedish economist (1851-1926) (see Figure 2). Let retain the hypothesis that the transactions are bilateral

In order for each person to eat what they like, the following exchanges are needed

- Alan gives his apricots to Bernard.
- Bernard gives his bananas to Claire
- Claire gives her carrots to Alan.

How do we achieve this? All we need is a coin, created for instance by a central authority or bank, which agrees to lend it. In this situation, the exchanges can be performed as such:

- Bernard borrows a coin from the central bank and gives the coin to Alan in exchange for his apricots.
- Alan gives the coin to Claire in exchange for her carrots.
- Then, Claire gives the coin to Bernard in exchange for his bananas, and Bernard can give the coin back to the central bank.

In this model, while the coin has no intrinsic value, it allows the exchanges to take place, satisfying all of the economic agents. We can extend this type of currency model to include many more agents interacting over a longer period. This is known as the overlapping generations model devised by Maurice Allais in 1947 in his work "Économie et Intérêt" (economy and interest).



Figure 2A: Wicksell's triangle

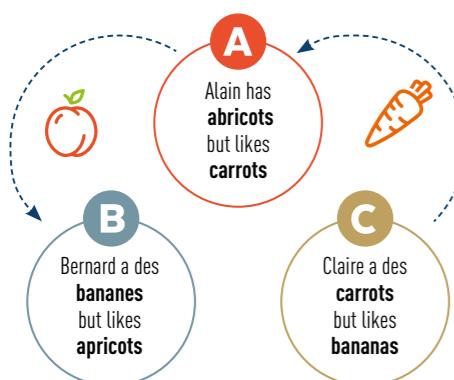


Figure 2B: Optimal exchanges

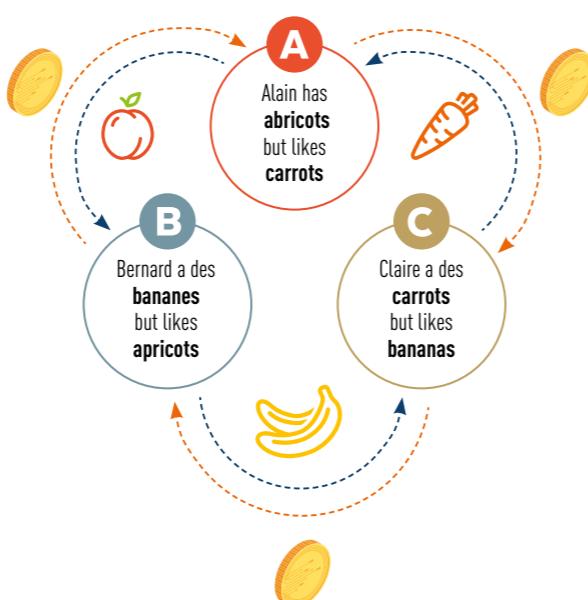


Figure 2C: Currency exchange

Wicksell's triangle illustrates the crucial role played by beliefs in monetary exchange: Alan accepts the coin given by Bernard in exchange for his apricots, because he assumes that Claire will accept the coin he plans to give her in exchange for her carrots. As for Claire, the reason she accepts the coin given to her by Alan is that she expects that Bernard will accept the coin she plans to give him in exchange for his bananas. It is a rational expectation equilibrium that everyone will accept the currency because they think it will be accepted. But this hierarchy of beliefs (beliefs, beliefs about other beliefs, etc.) is not the only possible one to achieve equilibrium. There is also an equilibrium of defiance: all of the agents believe the others will not accept the coin they have, and refuse to accept the one they are given. Defiance is also a rational expectation. Here again, we find the multiplicity of equilibria that we encountered in our blockchain analysis.

In the analysis above, all of the fruits were worth the same price: one coin. In a more complex environment, there are many prices: prices for different goods and services relative to the currency (the price of bread in euros, for instance), but also the price of different currencies compared to one another (e.g. the value of the euro compared to the dollar). What does economic theory teach us about these prices?

As Jean Tirole demonstrated in his article published in 1985 in Econometrica, "Asset bubbles and overlapping generations", currencies are a special type of asset, different from other assets like firms equity shows. The fundamental value of shares is the present value of the actual goods and services the firm will produce in the future. It is the future fundamental value that determines the price. In contrast, currencies do not create real goods but provide transactional services. They can be used in the future to purchase goods and services. The value of this transactional service increases with the price of the currency in the future. The higher the value of the euro in a month's time, the higher the transactional service provided by the euro you purchase today. So unlike shares, it is the future price which determines the fundamental value today. As such, the price today reflects the beliefs about the price of tomorrow.

And again, the importance of belief results in the existence of multiple rational expectation equilibria: some in which the value of the currency is low today because we expect it to be low in the future, and others in which it is high today because we expect the same tomorrow. What is more, beliefs can change over time, even if nothing changes in the actual economy, resulting in currency fluctuations and volatility.

How do we stabilise the value of money? By coordinating anticipation. This is the role of the central authority. It can do this if it is reliable, as for instance an independent central bank with clearly determined objectives. Another way to stabilise the value of money is to agree to accept it as payment, as countries do by agreeing to accept the national currency for the payment of taxes.

But while the intervention of a central authority can stabilise the currency value, by coordinating assumptions, it can also destabilise it. This is the case when the state acts in a predatory way. It can devalue monetary assets by creating inflation or preventing economic agents from using their assets, for instance by implementing capital controls. Distrust in the central authority or bank can result in pessimistic beliefs causing the value of the currency to fall.

Where do cryptocurrencies fit into this analysis?

Cryptocurrencies can prove useful when the political situation prevents agents from using the currency issued by the central bank and the banking system to meet their needs. The political collapse in Zimbabwe resulted in a complete lack of faith in the currency, and its banking system became extremely fragile and risky. To settle their transactions, economic agents turned to the bitcoin. Similarly, in Venezuela, escalating inflation and the political crisis almost destroyed the value and credibility of the national currency on top of using dollars. Economic agents there turned to cryptocurrencies, in particular bitcoin. Because electricity is cheap in Venezuela, economic agents even engaged in cryptocurrency mining. In China, the government controls banks and money transfers outside the country. To get around this, the Chinese increasingly began using cryptocurrencies. This explains the Chinese government's strong negative attitude about cryptocurrencies, and the regulations aiming to limit their use.

Even if the political situation of a country is relatively stable, its banking system may still be underdeveloped and inefficient, making payment difficult and costly. Settlement of transactions using cryptocurrencies on the internet can be a useful solution. Cryptocurrencies can also be useful for transferring international funds when traditional methods are ineffective or too expensive.

However cryptocurrencies also have drawbacks:

- a) As we mentioned above, the value of a currency at any given time depends on the anticipation of its future value. But

CONCLUSION



this anticipation can fluctuate widely, making the currency volatile, as it is the case for bitcoin. What's more, by definition, there is no central authority intervening to stabilise the value of the cryptocurrency. One of the effects of the volatility of cryptocurrencies is that they cannot fulfil one of the three essential functions of a currency, which is to serve as a unit of account.

b) The use of cryptocurrencies to pay for goods and services exposes the parties to a difficult risk. Either the seller will only agree to sell the goods after the blockchain has validated the currency transfer, in which case the purchaser is exposed to the risk that the seller will not deliver the goods, or the seller delivers the goods immediately, thereby exposing the seller to the risk that the transaction is not validated by the blockchain.

c) The boom in cryptocurrency exchanges (fuelled by speculation) has led to a congestion of blockchains. The bitcoin blockchain only validates a block every ten minutes, and each block has a maximum size of 1 MB. This slows down the validation of the transactions. To include a transaction more quickly in a block, and have it validated faster, the economic agents can promise the miners larger commissions (as explained above). The average commission for a bitcoin transaction is currently around \$30. Congestion and commissions make the validation of bitcoin transactions slow and costly, which reduces the currency's ability to fulfil another of its basic functions which is to serve as a means of payment.

d) Cryptocurrencies only play a minor role as a means of payment, when compared with currencies issued by banks and central banks. In order for them to play a bigger role, the number of transactions validated must be increased, and to do that, the size of the blocks must also be increased. But this has proven difficult

e) The proof of work protocol consumes a lot of electricity. For cryptocurrencies to be environmentally sustainable, alternative protocols must be developed. Proof of stake could be a promising alternative, but it is not operational yet.



At the beginning of our discussion, we mentioned that cryptocurrencies were developed against the backdrop of two major social trends. One is a technology trend - the increasing use of new information and communication technology. The other is both social and political - the questioning of the elite class and the desire to give power back to the people. What have these analyses of the prospects of cryptocurrencies taught us about these two technological and socio-political dimensions?

From a technological point of view, in order for cryptocurrencies to play a more significant role than the marginal one they currently do, miners need to be able to validate a greater number of transactions. One way of increasing the number of transactions would be to increase the number of cryptocurrencies and blockchains. This would hardly be a satisfactory solution because increasing the number of cryptocurrencies would diminish their reliability, whereas the increase of blockchains (using the proof of work concept) would overly increase the use of electricity. The other solution would be to increase the size of each block. But as we saw above, this is not so simple. Suppose that the community of developers and miners manage to develop and adopt a change of protocol to increase the size of the blocks. Would this approach increase the number of transactions validated without using up too much electricity? In a protocol based on proof of work, the higher the reward for validating blocks, the more miners will devote CPU to the task, using up more electricity as a result. To limit the amount of electricity used, we would need to limit the rewards for solving blocks.

As we saw above, the reward for solving a block tends to decrease. Currently it stands at 12.5 bitcoins, but will fall to 6.25 in 2020, and 3.125 in 2024. This trend is headed in the right direction, but in order to reduce the miners' rewards, the exchange rate of the bitcoin cannot be too high. It is possible and even likely this will occur, but we cannot be sure of it. Moreover, the overall value of the commissions offered by economic agents to validate transactions must remain low. However, if the number of transactions (included in the largest blocks) increases, it will push up the overall level of commissions. To tackle this phenomenon, the individual value of each commission must remain low. To achieve this, the network cannot be overly congested, but in overcapacity. This brings us back to the need to increase the block size, which is really the fundamental condition to developing blockchains and cryptocurrencies.

From a political and social point of view, one of the common themes of the discussion we have put forward is the difficulty coordinating assumptions and beliefs of various economic agents. Poorly coordinated and unstable beliefs can lead to massive fluctuations in value, and to fragile and volatile currencies. These same poorly coordinated beliefs can also result in a larger number of forks, preventing the blockchains from functioning properly. This is a considerable problem, which could put a strain on the future of public blockchains and cryptocurrencies. The libertarian inspiration of this technology prohibits the intervention of a central authority and requires coordination to come from the base, which is difficult to achieve in practice. From this point of view, cryptocurrencies differ greatly from conventional currencies, where central banks can help agents coordinate their beliefs, as demonstrated by Isabel Schnabel and Hyun Shin, in a recent document published by the Bank for International Settlements, "Money and Trust: Lessons from the 1620s for money in the digital age." (cf. <https://www.bis.org/publ/work698.htm>)

To conclude this discussion, let us recall an episode in monetary history that illustrates the dangers created by volatile and poorly coordinated beliefs. In 1707, John Law went to France. He suggested replacing the existing currency (coins made of precious metal) with paper notes based on the shares of the West India Company. This was not merely seen as an innovation but a breakthrough. In 1719, the value of the Company's shares rose from 500 pounds to 10,000 pounds. The currency created by John Law was a huge success. People jostled to get hold of it. Some even sold it for a profit. Nobles, clerics, servants and innkeepers alike soon amassed impressive savings. Then in 1720, the value collapsed, and the Mississippi notes were worthless, leaving many people completely ruined.

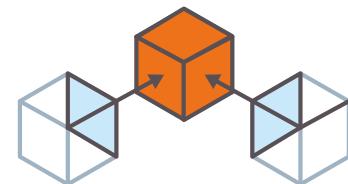


THE TSE WORK GROUP ON BLOCKCHAIN

In 2016 TSE launched a taskforce on blockchains:

Bruno Biasi, Christophe Bisière, Catherine Casamatta, Fany Declerck, Bertrand Gobillard et Alexandre Guembel.

The aim of the taskforce was to explain the impact of this technology on financial intermediation and payment systems.



Bruno
Biasi



Christophe
Bisière



Catherine
Casamatta



Fany
Declerck



Bertrand
Gobillard



Alexandre
Guembel

