The economic stakes of blockchains

Patrick Waelbroeck,
professor, Télécom ParisTech-Institut Mines-Télécom

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
Blockchain technology extends far beyond time stamps, bitcoins and the security of financial transactions. The Internet of things, a system of smart, connected devices, is not likely to develop without a form of this technology. Blockchains open the way toward a "liquidification" of the physical world, an economics of real-time microtransactions and the smart sharing of data bases. However it is important to distinguish between types of blockchains, in particular private and public (open) ones, since they have quite different economic properties. The problems related to the governance of open blockchains suggest that this technology cannot, by itself, create trust.

Blockchain technology uses a decentralized, secure electronic register (or ledger).[1] When a node in the blockchain network wants to make an entry in the ledger, all the other nodes have a part in acknowledging the new entry as an indelible block added to the ledger. Each such block bears the stamp of the preceding block, whence the formation of a chain of data. A new entry in the ledger cannot, therefore, be falsified or backdated, because the blockchain is copied to all nodes in the network.

A blockchain is not just a tool for breeding trust thanks to its safe storage of validated data. Banks are taking a keen interest in this technology since it can serve as a ledger for entering a transaction at a cost of a few cents (compared with a few euros with current methods). A blockchain irrefutably authenticates a transaction's date and time: it is a generalized time-stamp system. Such a register can also be used for data on intellectual property rights or as a land registry. Some blockchains, such as Ethereum, allow for executing code, called "smart contracts", on elements in the chain. This opens new prospects for the Internet of things (henceforth IoT).

The difference between the two major types of blockchains — open (or "public") and private — has to do with the authorizations granted to the nodes in the network. In an open blockchain, all nodes have read and write permissions to the ledger, whereas a private blockchain grants permission to write in the ledger to a few nodes only. Consequently, the rules for validating new entries in the chain are different too. In the open Bitcoin blockchain, two methods provide incentives for validating entries in the ledger: a fixed amount of bitcoins (BTC) paid for "mining" each block and a variable amount for the transaction costs. In a private blockchain, the incentives tend to be linked to the governance of the chain. These different types of blockchains will be analyzed from an economic viewpoint.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

For what other reasons should economists be interested in blockchain technology? There are at least three.

First of all, blockchains open new perspectives on economic security, by creating a decentralized organization of incentives for making an information system secure.

Secondly, blockchains and smart contracts, by bringing economic agents together in a decentralized system, alter our ideas about firms and the nature of work. They also have an impact on the organization of industry, since agents share computational resources over a network. This could lower the fixed costs of market entry in sectors where heavy investments have to be made in servers and computers. Blockchains are a countervailing force to the centrifugal tendencies of multisided platforms, where certain players on the Internet have managed to concentrate power.

Thirdly, blockchains represent a technological innovation that will spread rapidly throughout the economy. Opinions about this diffusion will be presented in the attempt to gauge whether this technology is disruptive enough for a very fast diffusion or, on the contrary, whether it is a "foundational" innovation that will spread throughout the economy over a period spanning several decades.

These three points and their ramifications will be discussed hereafter. Bitcoin will be used as an example, in particular to help us understand this cryptocurrency in terms of supply and demand. A point to be dwelled on is the governance of the Bitcoin network, a major issue for other blockchains too. After analyzing the economic value of bitcoins, the disruptive aspects of this technology and its economic prospects will come into focus in the conclusion.

What is disruptive in blockchain technology?

Blockchains can be used for digital or easily digitized products. However this technology extends far beyond its use as a mere electronic ledger for time-stamping entries. Three technical aspects deserve our attention: tokens, smart contracts and liquidification.

Tokens

A blockchain remunerates the work of securing entries and the ledger by issuing tokens. These tokens might be a cryptocurrency, or might be similar to voting shares. Their value increases with the number of eventual uses. To take the case of Bitcoin, positive network effects, direct as well as indirect, exist between the agents who own bitcoins and those who accept them. These tokens might also be used to authenticate voting rights in a general assembly or elections.

Smart contracts

Smart contracts — code to be executed by the blockchain — could validate the tasks accomplished and remuneration for them. Let us take as example *Ubik*. In Philip Dick's science fiction novel (1969), Joe Chip, a specialist who tracks people with telepathic powers, is expecting a visit and wants to have his rented apartment cleaned. He calls the building's cleaning service to have a few robots sent. The service is fully automated: the robot (or "chatbot", we might now say) tells him that he has to settle his debt before asking for the housecleaning robots. Since he is penniless, he asks for a real-time microcredit; but the robot replies that the loan company has lowered his credit score and is blocking any new loan request. Chip puts a dime in the coffee machine, but needs a nickle to open the door of his apartment for his guests (who will end up paying to open the door). He offers them coffee, but the refrigerator, also automated, needs a dime to open its door and a nickel for cream.

This economic system is based on real-time micro-payments and -transactions. Jason Lanier (2013) has seen in such a system an alternative to copyrights for paying creators. By the way, connected doors are now being developed by Slock.it, a website for a "universal sharing network" that is devising a procedure for opening locks (subject to a payment condition).

Liquidification

A blockchain can be used to track and authenticate physical products and persons via techniques for digital identification, hashes and sensors. It can, for example, track a serial number, a physical object's "passport" on the assembly line. Everledger; a blockchain in the diamond trade, traces transactions by using a digital "passport" assigned to each diamond. A diamond's metadata (size, diameter, weight, etc.) are recorded in the blockchain.

This technology makes the physical world and digital realm converge, by improving the traceability of products and services. It makes the economy more "liquid".

Let us take the example of a DAEMON, a computer program that, running as a background process in memory, performs certain tasks upon the occurrence of given events. A daemon is the prototype of a smart contract but without any micro-payment. In Daniel Suarez's novel *Daemon* (2006), Matthew Sobol, a genius in programming computer games, codes connected devices for automatic execution after his death: a house with booby-traps, an electrified door, a self-driving killer vehicle, etc. A daemon has less to do with artificial intelligence than with the distributed, automatic, conditional execution of a program. It executes tasks thanks to physical sensors for detecting real events or by following the news on Internet to validate the sequence of events.

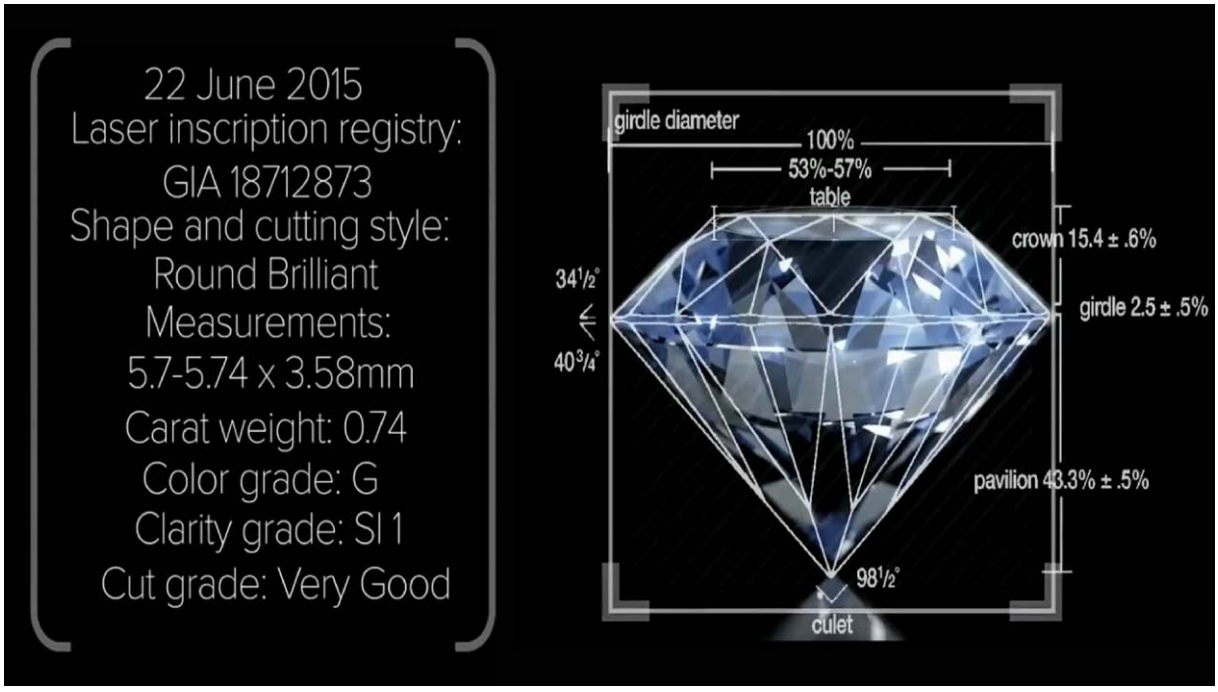

Figure 1: Quantitative and qualitative specifications of the cut and shape of a diamond listed in the Everledger blockchain.
Source: https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods
[consulted 25/12/17]

The economic properties of blockchains

Let us now analyze blockchains as a function of their economic characteristics.

Read/write permissions

An important distinction between blockchains is whether or not users need permission to read entries in the ledger or to enter data there. Table 1 presents the four possible combinations of these permissions. Discussions usually center on the two configurations in the gray cells.

Table 1: Types of blockchains by read/write permissions

	Reading permission required	*No permission required for reading*
Writing permission required	Private blockchains	Government blockchains
No permission required for writing	Monitoring/insurance	Open ("public") blockchains

PRIVATE BLOCKCHAINS require permissions for both reading stored data and writing new data to the ledger. They are growing fast, since governance is easy and the confidentiality of the data is ensured. In effect, only a limited number of users have access to the ledger. This limitation makes it easy to determine responsibilities when a problem crops up. A private blockchain is normally assigned a specific use, as in the case of Everledger.

In contrast, OPEN BLOCKCHAINS are open to everyone, whence problems of governance and responsibility. Examples of open (or "public") blockchains are the first cryptocurrencies, bitcoins and ethers. Although the use of pseudonyms guarantees the confidentiality of data, all transactions corresponding to a given pseudonym are visible by all users, and can be explored using search tools (such as Blockchain.info).

Though less widespread, blockchains using the other two configurations are in the pipeline. An example requiring writing permission but not reading permission is government blockchains such as real estate registers. The state of Delaware is developing, along with the start-up Symbiont.io, plans for using to smart contracts to automate procedures for initial public offerings (IPO). An example of blockchains requiring reading permission but not writing permission, we think of the blockchains used for insurance policies that monitor events via connected devices and use smart contracts to automatically trigger reimbursements when preset conditions are met.

Rivalry and excludability

Economic goods are generally said to have two characteristics: rivalry and excludability. If the consumption of a good by one person keeps others from consuming it, the good is "rivalrous". If a person who has not paid for a good can be kept from having access to it, the good is "excludable". The data stored on a blockchain are not rivalrous. However the governance of the blockchain may deprive some users of read or write permissions under certain circumstances. This means the data are "club goods" (nonrivalrous but excludable) or "public goods" (nonrivalrous and nonexcludable).

What about the tokens generated by a blockchain? They are rival goods, since a given token can only be used by a single person. When some persons can be kept from having tokens (a private blockchain), the token is a private good. When anyone has access to this resource, as in open blockchains, the token is a common good.

The direct externalities of investments in "mining"

The blockchains that require "mining" for validating new blocks have two types of direct network externalities, the one positive the other negative.

The positive network externalities have to do with making the blockchain secure. They occur when the value of a product (or service) increases with the number of users. For example, a software program's value increases with the number of its users, since this makes it easier to transfer files among friends, colleagues and other persons. In a blockchain, each additional node reinforces the chain's security, by making it harder to launch so-called "51% attacks" or to guess who will be the winning miner (*cf*. denial-of-service attacks below).

But there is also a negative externality: each miner, when investing in new material, increases both his marginal income and his overall mining costs, since the difficulty of mining increases as a function of the number of miners and of their computing power ("hash-power"). In the Bitcoin network, the difficulty of the cryptographic problem to be solved is validated by a proof-of-work consensus that increases the network's global hash-power. The risk looms of overinvesting in mining capacity, since individual miners do not take account of this negative effect on the scale of the whole network.

Increasing the difficulty of mining reduces the incentives for mining while increasing the time needed for validation and, therefore, the blockchain's efficiency. This brings to mind the tragedy of the commons, as shared resources (hash-power) wane and their upkeep falls on fewer "mining pools". This voids the very principle underlying an open blockchain, which is supposed to be decentralized. The capacity for mining risks being concentrated in a few agents' hands, thus nullifying the blockchain's foundational principle.

Private blockchains address the negative externalities of mining but at the risk of causing a "tragedy of the anticommons", when resources are no longer held in common but are privatized, protected by private property rights.

Indirect network externalities

A blockchain brings several groups of economic agents together. Cryptocurrencies match sellers and buyers; and certain platforms match lenders and borrowers. Everledger, for instance, matches the buyers and sellers of diamonds. These markets have the same characteristics as the multisided markets where two or more groups of economic agents come in contact. Such markets have indirect network externalities, often positive: the value of the service being offered by the platform to the one group increases with the number of agents in the group on the other side of the market. In the digital economy, these markets are highly concentrated. We need but mention platforms such as YouTube, Google, Facebook or eBay.

Differences between private and open blockchains

How do the advantages and disadvantages of private and public blockchains compare? For many users, a public (open) blockchain offers a decentralized solution to the problem of trust. Counter to the libertarian dream about open blockchains, private blockchains can be completely centralized in a few players' hands. The important distinction between these two types of blockchains must be borne in mind: open blockchains are not centralized; they are, quite to the contrary, very decentralized. However these sorts of blockchains also differ in many other ways.

A major difference between the two concerns the confidentiality of transactions, of data and of smart contracts. As already pointed out, ensuring the privacy of the data stored on a private blockchain is rather easy, since only a limited number of users have access. This accounts for the fast growth of this type of blockchain. In contrast, the data stored on an open blockchain are accessible to anyone, since the purpose is to keep a decentralized public ledger.

Nonetheless, it is possible to attain a degree of confidentiality on open blockchains, such as Bitcoin, where users have pseudonyms. Furthermore, technical procedures have been devised for protecting sensitive data on open blockchains. On MIT's Opal/Enigma project for a blockchain of health data for example, a node cannot access all the data when using the Secure Multiplatform Computation. The data are distributed over various nodes and cannot be disclosed in full during a query. Other procedures are based on a zero-knowledge protocol, which checks the validity of transactions containing encrypted metadata.

Scalability is a major problem for open blockchains where consensus is achieved via a proof-of-work system (*e.g.*, Bitcoin). This system requires not only an increase in hash power as the network grows but also several validations (which can take an hour) before a new block is added. Other types of consensus systems are under study, such as proof-of-stake on Ethereum. In contrast, private blockchains use consensus procedures that allow for writing a very large number of bytes of information per minute (as in delegated proof-of-stake systems).

An especially important difference is governance. On an open blockchain, all nodes in the network must agree on any major change to be made to the protocol for validating blocks, a very important point to be discussed hereafter. In a private blockchain, a very small number of nodes are the decision-makers.

Finally, there is the hanging question of responsibility and liability. According to blockchain specialists in France, it is much easier to establish liability in private blockchains (at least when contracts fall under the law of a single nation). Jurists are working on this question with regard to open, international blockchains.

Table 2: **A comparison of private and open blockchains**		
	Private blockchains	*Open ("public") blockchains*
Governance	+	-
Indirect externalities: multisided platforms	0/+	+
Externalities of security	0	+
Negative externalities of mining	0	-
Efficiency of the system of proof	+	-
Responsibility/liability	+	-
Openness and interoperability	-	+
Confidentiality	+	0
Monetization	+	0

Blockchains and the economics of security

Let us now turn to the factors that weigh on corporate decisions about the security of information systems. After showing that economic forces push firms to underinvest in security, we shall analyze how blockchains address the economic issues related to security.

Let us start with the example of a customer data base. First of all, the negative externalities associated with inadequate data protection are not offset by market mechanisms. Customer data are at risk of being leaked, stolen or fraudulently used. Secondly, firms develop strategies for rapidly reaching a critical mass of business, strategies to the detriment of their information system's infrastructure. Thirdly, owing to an asymmetry of information, firms share their customers' personal data with third parties who do not necessarily have any incentives for protecting them.

Public goods and network externalities

Since public goods are nonrival and nonexcludable, a single agent is unable to capture all the surplus that he/she creates for the public. As a consequence, the private sector will underinvest in such goods. Besides, in an environment where firms share data, individual companies benefit from the efforts of others in the network who are trying to safeguard the system. As a whole, this system will, therefore, be weakly protected.

Moore and Anderson (2012) have studied the effect of network externalities on the level of security adopted by software manufacturers. For a firm to dominate a market thanks to strong, positive network externalities, it must attain a critical mass very fast. Because of this, there are few incentives for devoting time and effort to making personal data secure. On the contrary, it is more profitable to leave to others the discovery of bugs and holes in security, and then propose updates and patches for the software.

Business models and data-sharing

When their sales strategies rely on advertising, firms bring in income by selling their customers' data to third parties. So, they have an interest in drafting very general terms of service in order to be able to use and reuse, exhaustively, their customers' data. When a customer's personal data are communicated to a third party, he/she hardly knows how they are going to be used, stored or protected. Real-time auctions of data on "ad exchange" platfoms make these problems worse. The personal data available from cookies are transmitted, mixed and matched by other platforms or companies.

Blockchain solutions and their limitations

By offering outright incentives for securing data, blockchains provide a solution to the problems arising from the economics of security. In the proof-of-work Bitcoin network, the incentives are monetary, namely its cryptocurrency. In proof-of-stake systems, tightening security is a way to gain voting shares and thus more actively participate in the blockchain's governance. The governance of a blockchain can also allow nodes in the network to coordinate actions so as to fend off attacks (BÖHME *et al*. 2015).

Despite the objectives backed by incentives, Bitcoin is based on a secure hash algorithm (SHA-256) that risks becoming obsolete.

As for smart contracts, they are, despite the name, nothing but bits of code that can, like other software programs, vehicle bugs. Because of a bug in the DAO smart contract on Ethereum, a group of hackers made off with $50 million.

A last point: if the private key for protecting data is lost, the user can no longer access his data; and if it is extorted, the security of these data is compromised.

Blockchains, firms and industry

Besides its effects on the economics of security, blockchain technology raises questions about the nature of firms and of work, and about the organization of the digital industry. Each sector of e-commerce is now dominated by a single firm holding a quasi monopoly. This situation has resulted from two main economic forces. First of all, the investments made by this dominant firm in the digital infrastructure generate fixed costs for production and for market entry related to a change of scale. Secondly, the positive network externalities, direct and indirect, of multisided platforms create a snowball effect. Blockchains deter these two forces.

Smart contracts and decentralized autonomous organizations

Blockchain technology, since it allows for a decentralized voting system, might menace hierarchies where the decisions of workers at the bottom are transferred to a higher-up, and so on… all the way up to the CEO. Thanks to the voting system allowed by blockchain technology, all workers may, in principle, make strategic decisions. Taking this argument to the extreme, the CEO could be eliminated.

In line with R. Coase (1937), a firm's size is often said to be determined by the costs of performing a task in house or outside. Blockchains could extend contractual relations to suppliers and workers at a lower cost. Pushing this argument farther, we can say that blockchains have two consequences for firms and on the work done by wage-earners. First of all, the very concept of the firm as such is menaced: an industry could be organized around a blockchain and the smart contracts concluded between various, relatively small units. Secondly, wage labor could be replaced with free-lance work. This trend is already visible on centralized platforms such as Uber; decentralized methods such as blockchains do not counter it.

Market entry, contestability and decentralization

Although the fixed costs linked to the information infrastructure discourages newcomers from entering the market, blockchain technology enables independent agents to pool resources for the purpose of executing automated tasks. Markets become, once again, "contestable"; and newcomers could challenge dominant firms, even those holding a quasi monopoly.

Given its decentralization of tasks and work, blockchain technology runs counter to platforms such as Uber or Airbnb. Returning to the example borrowed from *Ubik*, the door with a "smart lock" could be used to automate rentals, safely rack guns or manage safety-deposit boxes or vaults. Some pundits argue that blockchain technology might end up "uberizing" Uber; but nothing should be taken for granted, since Uber can develop its own blockchain to automate its contracts with drivers. Likewise, Airbnb could develop a blockchain for automating rental payments and caretaker services.

Bitcoins, an emblematic case

Bitcoin was the first open blockchain network on a mass scale. By May 2017, it had nearly seven thousand nodes. A node corresponds to several pools of shared resources and to farms with thousands of application-specific integrated circuits (ASIC) for mining blocks. The major pools and farms are located in China.

The proof-of-work consensus system is based on the difficulty of solving a cryptographic problem (identifying a block by calculating its hash). The difficulty increases as a function of the network's global hash-power, whence questions about: the cost of this open blockchain; its governance; and the economic value of bitcoins (BTC).

The costs of Bitcoin

Electricity accounts for most of the costs of a mining farm: from 90% to 95%. According to the calculation by Böhme *et al* (2015), the Bitcoin network's electricity consumption amounted to more than 173 megawatts nonstop in 2015 — equivalent to about 20% of the electricity generated by a nuclear power station and to a cost of $178 million per year (based on residential electricity rates in the United States). This might seem considerable; but according to Pierre Noizat,[2] it is not more than the annual cost of electricity for a fleet of automated teller machines (ATMs) for cash withdrawals worldwide, which has been estimated at 400 megawatts.

[2] http://e-ducat.fr/2015-11-28-cop21-et-blockchain/

Governance

The issue of governance is crucial for gauging the prospects of cryptocurrencies. When there is disagreement about how to develop a communications protocol, the network risks splitting into "hard forks" with incompatible currencies. The major issue is how to choose the rules of consensus for validating new blocks. A consensus must be reached on the consensus system, something the technology seems unable to do by itself.

The distribution of mining pools is clear evidence that hash power is concentrated. Approximately a dozen pools wield power over the decision-making process for changes in the protocol. A protocol is the equivalent of a grammar in a spoken language. Rules may be added or deleted but at the risk that users will no longer understand each other. In the Bitcoin network, "soft" and "hard forks" refer to changes in the rules.

Several Bitcoin protocols have been implemented — Bitcoin Core, Libbitcoin, Bitcoin XT, Bitcoin Classic — all under the oversight of their core-developers. For instance, the governance of Bitcoin Core involves a meritocratic process of peer evaluation via the Bitcoin Improvement Proposal moderated by Wladimir Van Der Laan, who coded much of the Bitcoin protocol.

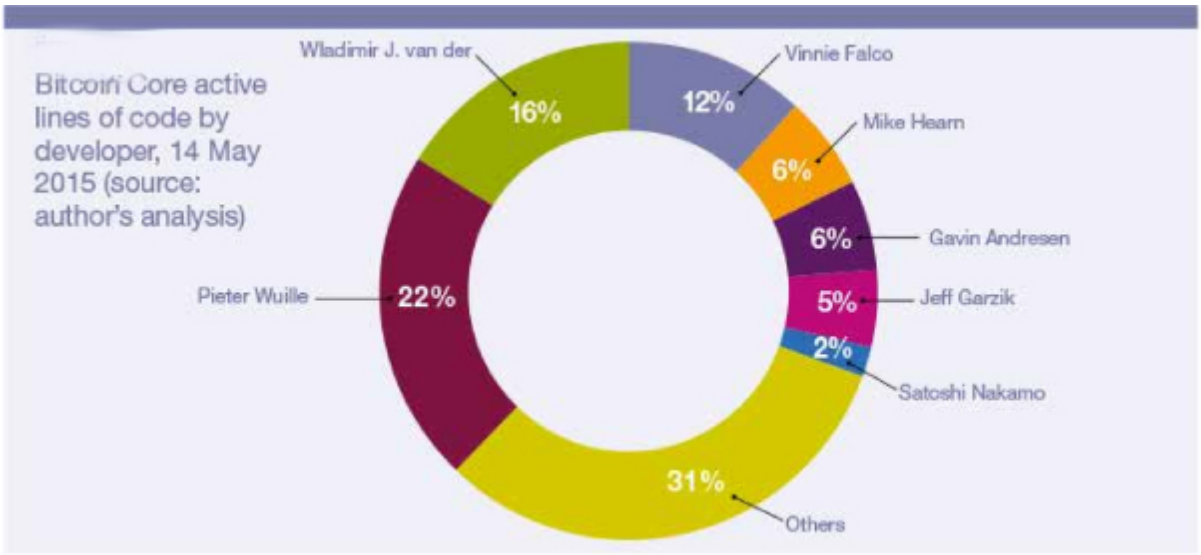

Figure 2: Lines of code by developer at Bitcoin Core (May 2015).
Source: WALPORT (2016).

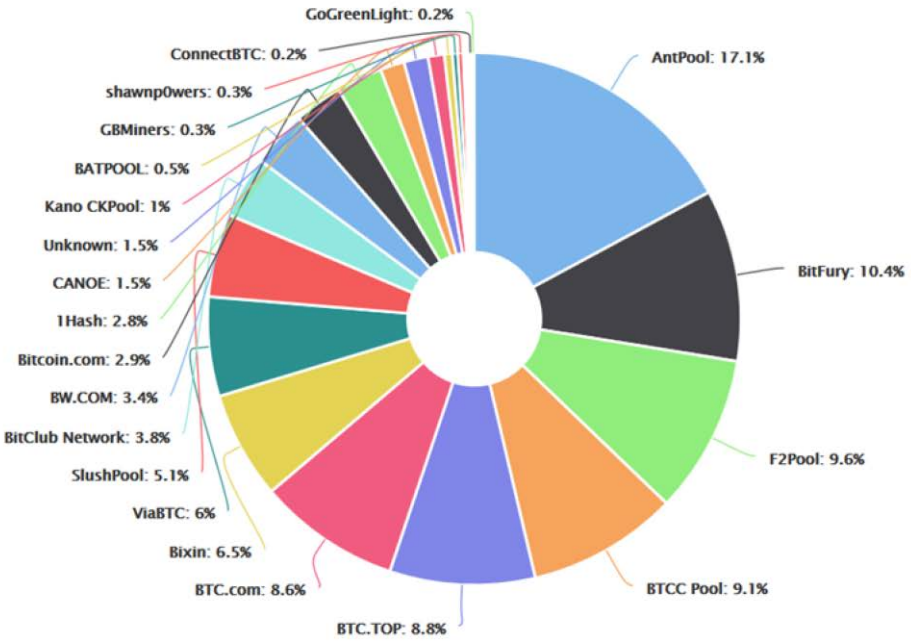

Figure 3: Bitcoin's blockchain partners.
Source: https://blockchain.info [consulted 22/5/2017].

Governance of the Bitcoin protocol is up to the nodes who choose whether or not to implement changes. Changes in the protocol can impact the four layers of the network: the consensus system, the peer-to-peer layer, the application programming interface (API), and the applications themselves. For brevity's sake, I shall discuss only the first of these four.

A majority corresponding to 95% of the hash power is needed to add a soft fork rule. The old blocks become invalid; and the nodes that do not upgrade suffer a loss of security and efficiency (hash power). To force miners to upgrade, a soft fork might use a new mining algorithm so as to make mining equipment obsolete. To delete a rule in a hard fork, all nodes must adopt the change lest the Bitcoin network split into two incompatible networks.

To conclude, technology alone cannot provide governance. This situation is paradoxical insofar as blockchain technology allows for decentralized validation procedures and automatically executed code; but it cannot ensure governance.

The BTC's value

A cryptocurrency has a value only if all participants in the monetary system accept it as a currency. It should, therefore, be scarce — it should not be easy to copy it (an act like making counterfeit fiat money). Blockchain technology, which prohibits double spending, meets this requirement. Bitcoins take on value not only through acceptance but also via economic mechanisms that, not exclusively monetary, will be discussed in relation to supply and demand. But let us first examine network externalities and then, after discussing the BTC's value, conclude with a comment on the function of alternative currencies in a monetary system.

Positive network externalities related to security and the means of payment

The level of security increases with the number of nodes in the Bitcoin network, since more computing power will be needed to breach the system (via a 51% attack, double spending or denial of service). In fact, a denial-of-service attack is all the harder to make insofar as it is hard to guess who will be the beneficiary. There are, therefore, positive network externalities: the BTC value increases with the number of nodes in the network.

Bitcoins are a means of payment, like cash or debit/credit cards tied to a banking account, like Visa, Mastercard or American Express. The theory of multisided markets describes situations wherein two sets of economic agents benefit from crossed externalities. The satisfaction of a consumer with a means of payment depends on merchants accepting it for settling transactions. In turn, a merchant is motivated to offer a payment service in proportion to the number of customers using it. The momentum on a multisided market tends to set off a virtuous cycle. Although the first phase might start out slowly, it is followed by a phase of quick deployment. If bitcoins follow this pattern, their value should enter a phase of acceleration.

By the way, the fees paid by consumers or merchants are not, in the Bitcoin network, controlled by the platform serving as a go-between but by the miners (a point to which I shall return).

On the supply side: The BTC's value on the primary market

The number of bitcoins created is halved every 210,000 blocks, the goal being to place 21 million BTC in circulation (some of which will have been lost). This is a rule under the Bitcoin protocol, which the consortium Bitcoin Foundation may modify. A modification might be made, for example, in response to market fluctuations but… at the risk of creating a hard fork. If demand is constant, reducing the issue of new bitcoins will automatically appreciate the BTC's value. Eventually, when the supply becomes inelastic, this price (setting aside the question of speculation) will mainly be set by demand.

On the demand side: Motivations, risks and secondary markets

The demand for a cryptocurrency stems from several motives, such as financial privacy, and is affected by uncertainty about how long the currency will be valid.

To fight against money laundering and black markets, governments are tightening measures on the use of cash. Cash is the only fully anonymous means of payment. Bitcoins and other cryptocurrencies rank second. The pseudonyms in the Bitcoin protocol enable the parties to a transaction to hide their identities. Some cryptocurrencies (Zcash for instance) even hide a transaction's metadata.

Why an anonymous means of payment? There are several reasons. First of all, financial privacy. Such a payment leaves no traces that officials, employers or firms (in particular banks and insurance companies) can track for surveillance purposes. For example, some firms and banks have strategies based on price discrimination that disadvantage certain consumers. Such a firm might use the traces left by a payment to reinforce its efforts for attracting customers and targeting advertisements, which some customers perceive as a nuisance. Finally, paying anonymously limits supervision "from below" (*i.e.*, by persons who are close or family), as in the case of a payment made from a joint banking account. Anonymity thus limits the externalities stemming from the traces left during a purchase. It has, therefore, economic value. Owing to pseudonyms, bitcoins generate value.

Furthermore, the blockchain Bitcoin keeps working during a crisis; and it can be used by economic agents to avoid controls over capital movements. Bitcoins came into being right after the financial meltdown in 2008. During this period, governments and central banks showed their might to control cash withdrawals and the capital in circulation. There are not many ways to dodge these two institutions. Bitcoins is one. Even if withdrawals in cash were to be prohibited, bitcoin bearers could still make payments with their private keys.

The risks related to controls and regulations stand out among the factors that limit the demand for bitcoins. For one thing, governments might start requiring that gains from the sale and purchase of bitcoins be declared to tax authorities. For another, bitcoins, if used in industries under regulatory oversight (such as insurance or banking), will come under control by regulatory authorities. Nor should we overlook the possibility that, for reasons of security, governments might start requiring access to private keys.

Another constant risk is that the data on the hard drive where the user's private key is stored are lost along with the bitcoins linked to the key.

Bitcoins can be bought and sold on the platforms that allow for such transactions. In this case, a bitcoin is similar to a financial security, an investment made in expectation of earnings. Factors thus come into play that can drive up the BTC's value.

Bitcoins, a restraint on governments

Bitcoins (like other cryptocurrencies) can be seen as an alternative form of money, one that is not under a central bank's control. For economists like F. Hayek, alternative moneys, by competing with official currencies, will discipline governments that are tempted to fund their debt by inflation. In this case, consumers and investors would turn away from the official currency to buy the alternative, whence a deflationary pressure on the official currency.

Economic prospects: A foundational or disruptive innovation?

Blockchain technology is inevitable, since developing the Internet of things depends on it. Specialists are, however, debating how fast this change will happen. Two points of view are at odds: the one foresees that this technology will take decades to be diffused and transform industry, whereas the other predicts a disruption. Specialists at IBM see blockchain technology as disrupting many current applications in fields ranging from logistics to financial transactions. In contrast, Lansiti and Lakhnani (2017) have suggested a parallel between the diffusion of a disruptive technology, such as the TCP/IP protocol, and of blockchains, a diffusion in four phases that might take decades till the final transformation phase.

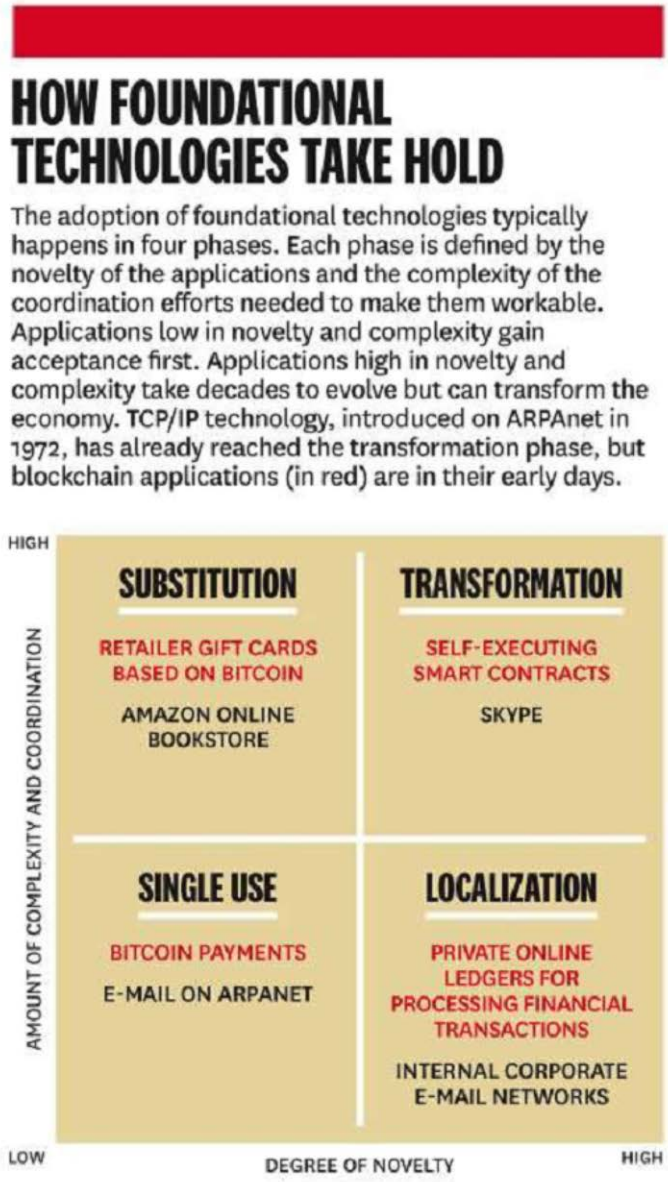

Figure 4: How foundation technologies take hold.
Source: LANSITI & LAKHANI (2017).

At first sight, the TCP/IP protocol is both similar to, and different from, blockchains. It is an open protocol like blockchains. However it was, from the start, a matter for specialists only, whereas thousands of users soon adopted bitcoins and the second generation of blockchain technology. All things said, blockchains tend to be a disruptive technology that will be adopted massively rather than a slowly diffusing technology. But hurdles have to be leapt…

Vectors of disruption	Liquification of the physical world
Unlock excess capacity of physical assets	Instantly search, use and pay for available physical assets
Create liquid, transparent marketplaces	Real-time matching of supply and demand for physical goods and services
Enable radical re-pricing of credit and risk	Digitally manage risk and assess credit, virtually repossess and reduce moral hazard
Improve operational efficiency	Allow unsupervised usage of systems and devices, reduce transaction and marketing costs
Digitally integrate value chains	Enable business partners to optimize in real-time, crowdsource and collaborate

Figure 5: Five vectors of disruption
Source: BRODY & PURESWARAN (2014).

Conclusion

In conclusion, blockchain technology is revolutionary. It is not limited to bitcoins alone. The development of an Internet of connected devices probably depends on blockchains of one sort or another. This technology opens the door toward the liquidification of the physical word, an economy of real-time microtransactions and a “smart sharing” of data bases. However the hurdles on the path toward this transformation must be taken down. First of all, liability must be clearly established, as well as the law code to be applied to open blockchains. Secondly, the EU must see to it that the regulations (General Data Protection Regulation, GDPR) on protecting personal data are applied. Thirdly, the fiscal and legal status of cryptocurrencies must be clarified. Finally, it is necessary to devote thought to articulating the smart data from blockchains with the principle of Internet neutrality in Europe.

References

BÖHME R., CHRISTIN N., EDELMAN B. & MOORE T., "Bitcoin: Economics, technology, and governance", *Journal of Economic Perspectives*, 29(2), pp. 213-238, 2015.

BRODY P. & PURESWARAN V.(2014), "Device democracy: Saving the future of the Internet of things", 28p. (IBM Institute for Business Value), September 2014. Available at https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/global-business-services-global-business-services-gb-executive-brief-gbe03620usen-20171002.pdf

COASE R.H., "The nature of the firm", *Economica*, 4(16), pp. 386-405, 1937.

DICK P.K., *Ubik* (NY: Houghton Mifflin Harcourt) 1969. French translation *Ubik* by Alain Domérieux (Paris: Robert Lafont) 1970.

LANIER J., *Who Owns the Future*? (New York: Simon & Schuster, 2013).

LANSITI M. & LAKHANI K.R., "The truth about blockchain", *Harvard Business Review*, 95(1), pp. 119-127, 2017.

MOORE T. & ANDERSON R., *Internet security: The Oxford Handbook of the Digital Economy* (Oxford: Oxford University Press) 2012.

SUAREZ D., *Daemon* (Pasadena, CA: Verdugo Press) 2006. French translation by Leslie Boitelle: *Daemon* (Paris: Éditions Pocket) 2011.

WALPORT M. (2016), "Distributed ledger technology: Beyond block chain", 88p., a report by the UK Government Chief Scientific Adviser (London: UK Government Office for Science) 2016. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf