FONDATION POUR
L'INNOVATION
POLITIQUE
fondapol.org

www.fondapol.org

THE BLOCKCHAIN, OR DISTRIBUTED TRUST

Yves CASEAU
Serge SOUDOPLATOFF

FONDATION POUR
L'INNOVATION
POLITIQUE
fondapol.org

The Fondation pour l'innovation politique
is a French think tank for European integration and free economy.

Chair: Nicolas Bazire
Vice-chair: Grégoire Chertok
Executive Director: Dominique Reynié
Chair of Scientific and Evaluation Board: Laurence Parisot

The Fondation pour l'innovation politique is publishing this paper
as part of its work on *digital*.

FONDATION POUR L'INNOVATION POLITIQUE

A French think tank for European integration and free economy

The Fondation pour l'innovation politique provides an independent forum for expertise, opinion and exchange aimed at producing and disseminating ideas and proposals. It contributes to pluralism of thought and the renewal of public discussion from a free market, forward-thinking and European perspective. Four main priorities guide the Foundation's work: economic growth, the environment, values and digital technology.

The website **www.fondapol.org** provides public access to all the Foundation's work. Anyone can access and use all the data gathered for the various surveys via the platform «Data.fondapol» and data relating to international surveys is available in several languages.

In addition, our blog "Trop Libre" (Too Free) casts a critical eye over the news and the world of ideas. "Trop Libre" also provides extensive monitoring of the effects of the digital revolution on political, economic and social practices in its "Renaissance numérique" (Digital Renaissance) section (formerly "Politique 2.0").

The Fondation pour l'innovation politique is a state-recognized organization. It is independent and receives no financial contribution from any political party. Its funding comes from both public and private sources. Backing from business and individuals is essential for it to develop its work.

DEFINITION OF THE BLOCKCHAIN

The blockchain is an innovative technology that enables users to execute transactions, of a financial nature or otherwise, that are guaranteed and can be audited by everyone without the need for a trusted third party.
After each transaction, a new line is added to the block, forming an indestructible chain: the blockchain. This is Accounting 2.0, with the history of each transaction indexed in a decentralised ledger and redistributed to all users. The complexity of the algorithms involved makes these transactions impossible to falsify.

SUMMARY

The greatest innovations result from new technological advances coinciding with a favourable sociological context that can transform these technologies into uses. In this sense, the blockchain is the product of, on the one hand, the convergence of asymmetric cryptography and distributed systems and, on the other hand, an opportune sociological climate. The latter is itself the result of a crisis of confidence from internet users towards their institutions, which has led them to seek out new forms of governance.

The rise of the internet has demonstrated how effective a worldwide communication system, free from the constraint of one unique, overarching telecommunications operator, can be. All around the world, it is now possible to connect to any given WiFi network in a matter of seconds. Similarly, the blockchain is at the forefront of a revolution affecting the way we carry out transactions. It enables individuals to carry out operations among themselves, particularly those of a financial nature, which are guaranteed without the involvement of a trusted third party. This speeds up such interactions, and reduces their cost. Therefore, the existence of the blockchain is seriously challenging the role of institutions, banks and notorial studies, and having a profound effect on the way we approach administration.

The first experiments, which are by no means limited to bitcoin, such as decentralised autonomous organisations, demonstrate the radically disruptive nature of the blockchain.

THE BLOCKCHAIN, OR DISTRIBUTED TRUST

Yves CASEAU
Member of National Academy of Technologies of France (NATF)

Serge SOUDOPLATOFF
Internet expert, co-founder of Sooyoos and Scanderia

Please note: As often where digital matters are concerned, the subject of blockchains can get very technical. It is difficult to address this issue without providing certain technological insights, which can be found in the middle section of this document. Readers should not be afraid, for they will be perfectly able to negotiate these more challenging passages and reach the end of the document without losing their way.

Not a day goes by without the subject of "blockchains" cropping up in one form or another. They revolutionised money with bitcoin, and now they are poised to disrupt not just our banks, but our notaries, lawyers, estate agents, as well as the energy, healthcare, cultural and administration sectors. In brief, one would be hard-pressed to find an area of transactional human activity that will not be affected by blockchains. In the financial sector alone, banks have been experimenting with blockchains since July 2015, including institutions such as BNP Paribas, Société Générale, Citi, Deutsche Bank, Westpac, ANZ, Santander, ABE, DBS, Commonwealth Bank, UBS, Barclays, ING, Fidor and even the American Federal Reserve. The Caisse des Dépôts recently brought together sixteen separate institutions (four banks, four insurance companies, five manufacturers and three scientific partners) in a bid to better accommodate blockchains in France.[1] The British government has published its own report;[2] the Honduran government is trialling the use of the blockchain for its land

1. 'La Caisse des dépôts lance officiellement l'initiative de place Blockchain', caissedesdepots.fr, 31 March 2016 (www.caissedesdepots.fr/la-caisse-des-depots-lance-officiellement-linitiative-de-place-blockchain).

2. Government Office for Science, 'Distributed Ledger Technology: beyond block chain', 2016 (www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf).

registry, as part of the fight against corruption;[3] the Estonian government is using it for notarial services for its e-residents;[4] and the French Minister for the Economy, Industry and Digital Affairs intends to "develop regulations in order to test out the blockchain".[5]

This is no longer about untested, futuristic projects. bitcoin was created in 1998, and its blockchain has not stopped growing ever since.[6] Bitcoin cryptocurrency is based on an operational system that has fully proved its value, and whose construction required a lot less effort than other large financial transaction systems, some of which failed to become operational despite their enormous expense.

Although, to begin with, the blockchain was nothing more than the technology that underpinned bitcoin, it quickly became evident that it could be used for a whole lot more than just cryptocurrencies. To sum up, everything that is transactional in nature, be it financial or otherwise, can be put on a blockchain with the same guiding principle: to guarantee trust and better efficiency by, on the one hand, offering improved fluidity and a higher transaction rate and, on the other, by significantly reducing costs, via the simple elimination of the operational bottleneck known as the "trusted third party". These changes are significant enough to be referred to as "disruptive". Graphic 1 succinctly illustrates the diversity of what blockchains are currently used for.

We may legitimately wonder where the blockchain is currently positioned on Gartner's famous "hype cycle",[7] and speculate that we are currently reaching the Peak of Inflated Expectations and that we will soon be diving headfirst towards the Trough of Disillusionment. Without falling into the trap of those consultancy firms that predict the future rather than shape it, what we can say for certain is that the blockchain story is only just beginning, that the twin mechanisms of percolation and exaptation that characterise the expansion of the digital world[8] are going to set to work, and that the blockchain's uses will ultimately prove to be much more varied and very different from those that we may imagine today.

3. 'A Humble Update on the Honduras Title Project', factom.com, n.d. (www.factom.com/a-humble-update-on-the-honduras-title-project/).

4. Giulio Prisco, 'Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents', 30 November 2015 (bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243).

5. Enguérand Renault and Benjamin Ferran, 'Macron aménage la loi pour tester la "blockchain" sur la finance', *Le Figaro*, 24 March 2016.

6. Visitors to blockchain.info/ can monitor the development of the bitcoin chain in real time.

7. See the Wikipedia entry entitled 'Hype cycle' (en.wikipedia.org/wiki/Hype_cycle).

8. Exaptation is the capacity of nature to create certain traits to resolve a specific problem, but which then serve another purpose entirely. See Serge Soudoplatoff, 'Internet, entre percolation et exaptation', in Martine Behar-Touchais, Nicolas Charbit, and Rafael Amaro (eds), *À quoi sert la concurrence ?*, Institut de droit de la concurrence, 2014, pp. 501-506.

Graphique 1 : Possible uses for the blockchain

Source:letstalkpayments.com/blockchain-use-cases-comprehensive-analysis-startups-invoved

However, we still need to pay a lot of attention to the blockchain today. The blockchain not only represents a genuine shift, in terms of architecture, from the world of financial transactions (whose paradigm has not significantly changed since the invention of money and double-entry accounting) and other transactional domains. Indeed, and above all, it finds itself in a climate that is conducive to its growth, namely the current crisis of trust in institutions. It is exactly this combination – a new, powerful technological possibility in a climate that is conducive to disruption – that lies behind all the greatest innovations.

THE CLIMATE: A CRISIS OF TRUST

We are at the dawn of a veritable Renaissance. On the one hand, enormous progress is being made in science and technology. We are discovering exoplanets, exploring our own planet in increasingly fine detail and building quantum computers, just as during the Renaissance we invented the parachute, the dry dock and perspective in painting. We now know our place in the universe and are able to map it out with ever-greater precision, just as during the Renaissance we explored a world that suddenly had no limits. The internet is to our era what the printing press was to the Renaissance. We have the tools to understand our brains in more depth, enabling groundbreaking progress in neuroscience. We are sequencing the genome to such an accuracy that it may be divisible in units of 30 million, empowering improved diagnosis of illnesses, just as, during the Renaissance, André Vésale revolutionised medicine by challenging ancient Roman texts and dissecting the body with a modern methodology, reducing the personnel required from three people to one. However, just like during the Renaissance, the establishment is battening down the hatches to protect its privileges, refusing to change and killing innovation by demonising it, all in the name of holding onto power at any price. We are also currently going through a phase of economic regression which, fuelled by fear, is leading to a period of repression.

All of this has left a murky cloud hanging over the fundamental issue of trust. Transformation cannot take place without trust. Fear is a tool used by those in power who reject all change, and it is incompatible with trust. Who do we trust in 2016? Not Google, nor Facebook, whom we are entrusting with fewer

and fewer of our secrets, nor Apple. We no longer trust brands, nor do we trust states. Even in France, one of the countries where levels of confidence in the State remain relatively high, this trust is ebbing away.[9] Genuine trust exists today in only two domains: the family and the community. If war broke out tomorrow across the country, it is uncertain whether young French soldiers would stand up in defence of their nation, but they would undoubtedly defend their family and friends.

Trust is an unstable equilibrium. When two people trust each other, it only takes one of them to have doubts for the other to also start doubting. The result is that the parties descend into a state of mutual mistrust, a sentiment that is much less precariously balanced. It therefore takes energy to retain trust; yet it takes information to facilitate this energy. One of our era's most violent breaks with established models concerns the source of this energy. France follows a model whereby energy is externalised: it is the nation's judges, teachers, managers, parents, and so on, who are responsible for driving this energy. In the Anglo-Saxon model, the energy comes from both parties (or from the community, when there are several people involved). When eBay was created, it was not the only online auction and shopping website, but it invented the concept of buyers and sellers rating each other, a scoring feature that can now be found on all community sites such as Airbnb, BlaBlaCar, and so. What eBay understood is that trust could only be created by the community itself and not by the presence of third parties, which in its case would have meant expert auctioneers.

We could discuss the relative merits of the community-based trust model and the externalised trust model until the cows come home, but what we can say for sure is that the externalised trust model is proving inadequate in a world where the sheer volume of interactions is multiplying at such a rate, and it is starting to struggle. It is therefore very tempting for the regulator, the trusted third party, to demand ever greater resources in order to deal with this increase in the number of transactions. Unfortunately, this method clashes with the law of diminishing returns: past a certain threshold, the greater the means are, the more dysfunctional the system becomes. The community-based trust model is much more scalable and able to handle this increase in the number of interactions. Indeed, this is its main strength.

9. See Cévipof and SciencesPo's 'Baromètre de la confiance politique, vague 6bis', published in February 2015 (www.cevipof.com/fr/le-barometre-de-la-confiance-politique-du-cevipof/resultats-1/vague6/vague6bis).

The blockchain model is even more powerful than the community-based trust model: it offers a model in which trust in transactions is reliable, can be audited by all and distributed thanks to its decentralised means of reaching a consensus.

Generally speaking, the construction of the internet was the product of a break from conventions. Whereas telephone operators were developing and maintaining a centralised network, the internet has shown the feasibility and, above all, the scalability of a totally decentralised network, without a centralised organisation and, therefore, without a single owner. Those same fundamental principles are there to be seen in its very construction: there has never been an "Internet project manager", for the simple reason that the Internet has never existed as a project. The internet was built by "a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies".[10] Whereas the old world thought only in terms of broadcasting, and above all mass broadcasting, the internet has shown that everyone can create and deliver content – and that it is an error to try to apply the television model to the internet. Whereas the old world was based on "supplier to customer" chains, the internet has shown the feasibility of large-scale peer-to-peer exchange models.

It was inevitable that, at some stage, these new principles would be applied to the transactional model: whereas the old world believed in the necessary presence of a trusted third party, and whereas Internet 2.0 still features organisms offering platforms for interaction, the blockchain model shows that we can do without either and create a pure "peer-to-peer" model (P2P). In this sense, the blockchain is the transactional version of peer-to-peer networks such as Bit Torrent, which reflected – it bears repeating – the fundamental principles of the internet as far back as 1968, well before the invention of the Web (1991). The approach of this purely P2P model differentiates it from the "content provider" model (Web 1.0) and the "interaction platform" model (Web 2.0).

10. Cited in Paul Hoffmann (ed.), *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*, www.ietf.org/tao.html, 2012.

THE BLOCKCHAIN

The blockchain consists of two separate elements: firstly, a technology and, secondly, a system that uses this technology.

Historically speaking, the blockchain is the technology that underpins bitcoin. The invention of bitcoin in 2008 aimed to prove the feasibility of a currency based on a system of shared trust. It is an encrypted currency, whose trust mechanism is based on a system where the ledger is shared between multiple nodes of the network. The encryption algorithms for the transactions are open source, which reinforces this element of trust in the currency.

Bitcoin was effectively the first time that the trusted third party, a bank in this case, was demonstrated to be obsolete. Traditionally, it is the bank that guarantees the reliability and security of our transactions, making it the stereotypical example of an externalised trusted third party. Bitcoins are exchanged without being overseen by a trusted third party, but they still guarantee the same level of security, auditability and reliability. However, the subject of this paper is not bitcoin,[11] but rather the technology on which bitcoin is based: the blockchain. The latter is itself based around three pillars: two are technological, asymmetric cryptography and distributed systems, and the third is sociological, the vision of a transaction model with a peer-to-peer structure, thereby enabling a distributed consensus to be reached without the need for a trusted third party.

The first pillar, cryptography, is based on the concept of a key. When symmetric, the key is held only by the two parties, and must therefore be secret; this has been known since ancient times. Asymmetric cryptography, which dates back to the 1970s, consists of combining a public key and a private key. The importance of this invention lies in the fact that it solves the problem of how to transmit a key without an intermediary. To illustrate how the mechanism works, we can use the example of a real estate property changing hands. Current conventions dictate that a notary holds the keys to the property, and oversees its transferral from one owner to another: this is a symmetric key. In an asymmetric transaction, the old owner places the key (along with any other possessions that are being transferred) in a trunk that can be secured by two padlocks. He sends it to the new owner having attached one padlock, to

11. On the specific subject of bitcoin, see en.bitcoin.it.

which he holds the key. The new owner receives the trunk and adds his own padlock, to which he holds the key. He sends the trunk back to the first owner, who removes his own lock and sends the trunk back once more to the new owner, who takes off the remaining lock, his own, and takes possession of the contents. On completion, all parties still have possession of their own locks, and nobody else has been able to open the trunk while it was being sent back and forth because there was always at least one padlock secured to it. There was therefore no need for a notary.

The second pillar is distribution. There is no finer demonstration of the feasibility of a distributed system than the Internet itself. Anyone, no matter where they may be in the world, can connect to the Internet, with no need for a unique, overarching telecommunications operator. It also bears repeating that the intelligence of the Internet is found at its extremities, and that the web itself is neutral. Nevertheless, the Internet is not "transactional" in nature; it is concerned with communication, and transactions are just one of its uses.

The third and final pillar of the blockchain – a distributed consensus – is an algorithm that offers us a solution to an amusing conundrum known as the Byzantine Generals' Problem. Let us consider an army, split into several battalions, that is surrounding an enemy city. All of the generals must attack at the same time in order to take the city because, were they to attack separately, the city would be too strong. They must therefore find a way of communicating certain crucial information, namely the date and time of the attack, among themselves. Unable to meet in person, they must therefore send messengers. However, among the generals, there are traitors who may send false messages. For example, one of them may say to half his fellow generals that they need to attack at a given time, and to the other half that they need to retreat. This would lead to a difference in strategies, and the siege would be bound to fail. Until the invention of the blockchain, it was generally accepted that a consensus could only be achieved with the help of a central authority to coordinate all the generals: a higher power or, in other words, a trusted third party. The groundbreaking quality of the blockchain's algorithm is to provide a way of reaching consensus without the need for this central authority.

The solution, discovered by the inventor of bitcoin, is as follows: each general can only send one order at a time, stamped with the time and date. But, most importantly, on receipt the orders are bound together and then encrypted, forming a chain of messages stored in a "register of transactions", which

is redistributed to all generals. In this way, if a traitor general receives the information "we attack tomorrow at 8 a.m." and decides to only pass the message on to only half of the other generals and to send an order to retreat to the other half, he will create two incoherent chains. The honest generals at the source of the information will therefore be able to detect that foul play is afoot.

As such, a blockchain is an encrypted ledger, distributed and replicated at all the nodes of the web, containing order chains that are capable of generating trust without an external institution, thanks to consensus.

When a new transaction takes place, the information – including the time and date of the transaction – is placed in blocks of data that are integrated into the chain, hence the name "blockchain". In order to be integrated, this chain is encrypted and must be validated. This validation work is carried out by the nodes in the network, computers capable of resolving the cryptographic problems required to validate any given transaction. This process of validation is known as "proof of work". The people (or institutions) who perform this work are called "miners". [12]

"Proof of work" is a cryptographic object that miners must present to prove they have spent a certain amount of time on the problem, which avoids simple cloning that would see a corrupt miner transformed into an army of clones. [13] As the blockchain relies on consensus, it is important to guarantee those involved in it are "genuine participants", thereby preventing any fraudulent retroactive manipulation of the blockchain. In fact, the mechanism is even more sophisticated than that: at regular time intervals, the level of difficulty increases. [14]

In order to encourage miners to validate transactions, they are set in competition against one another, with the first miner who manages to resolve the problem of a new block being rewarded (in bitcoins, at the start of this currency). In the early days of bitcoin, it was private individuals who carried out this work, through an innovative use of computer graphics cards, whose processing capacity is significantly greater than computer processors themselves. Computers then started appearing that were specifically designed

12. As in "data mining", the idea of digging deep to resolve a problem. For more information on this concept, see en.bitcoin.it/wiki/Mining.

13. This idea is down to Adam Back, the inventor of the Hashcash protocol, which is at the heart of the blockchain. It is also used to guard against spamming. See en.wikipedia.org/wiki/Hashcash.

14. To monitor the difficulty curve, see blockchain.info/charts/difficulty.

to carry out this blockchain mining work. But with the size of the chains increasing, the processing power required has become enormous, and nowadays there are institutions that carry out this work. In March 2016, there were 7,420 nodes processing bitcoin blockchain around the world.[15] New companies have started appearing on the market, offering mining services from their datacentres ("cloud mining"). However, the work is becoming less and less profitable for private miners.

The following photo shows a mining centre located in Boden, Sweden.[16]

Photography credits photo: KncMinerltc (2016). http://en.kncminerltc.org

It is important to note that, while it requires a lot of power to validate the blocks, checking an integrated block is simple and can be done by anyone. A distributed consensus is therefore easy to reach.

15. A list is available at bitnodes.21.co.

16. See Peter Sayer, 'Bitcoin miner KnC is planning another four-week datacenter build-out', networkworld.com, 11 December 2015 (www.networkworld.com/article/3014467/Bitcoin-miner-knc-is-planning-another-four-week-datacenter-build-out.html).

What the blockchain provides

The blockchain enables the construction of a vast ledger that is distributed as far and as wide as desired, visible to everyone, updated in accordance with a transactional principle similarly distributed and guaranteed by a community, without the need for a trusted third party as a central authority.

The blockchain makes five promises:

1. Distributed trust.
2. A system of transactions.
3. Guaranteed by an extended community.
4. No trusted third parties.
5. The capacity to operate complex protocols.

The blockchain is a genuine innovation: twenty years ago, it was by no means obvious that one day it would be possible for one technology to honour even the first four promises. Having said that, it is very much the combination of the five promises that defines the blockchain's scope of application. If we needed a solution capable of fulfilling only one or two of these promises, other cheaper and more efficient methods would exist (see below).

The fifth promise is crucial, as it lends the blockchain its capacity for disruption: the ability to handle complex protocols (money transfers, banking, validation, and so on) in an automated way, with much lower transaction costs compared with systems that require human input, above all in the form of a trusted third party. In other words, the blockchain not only transports information, but also algorithms, and it does so with the same guarantee of trust as applies to the information itself. Already, the reader can begin to imagine the consequences that this could have regarding the automation of a whole range of processes currently carried out by human beings – notarised certificates, to take just one example. We will expand on this point below.

The key ingredients

The magic recipe of the blockchain contains five ingredients:

1. Validated chains, that become almost impossible to falsify.
2. Public and private keys that identify, and must be signed by, the participants.
3. A peer-to-peer document distribution protocol (like BitTorrent).
4. A large community, resistant to manipulation.
5. A consensus validation protocol: the proof of work.

The understanding of this section requires an explanation of the role played by the "hash". A hash is an algorithm that transforms a chain of characters (which may be a file) into a key, generally of a fixed length and which is hopefully unique, or at least possessing a low "collision rate" (a collision is when two chains have the same key). The hash is irreversible: it is not possible to recover the original text from the key, without the aid of a special dictionary. [17]The hash is used to encrypt passwords: tests are carried out uniquely on the key and it is only the key that is stored on the database, which avoids the need to store passwords in clear.[18]

In the blockchain, the sequence of a fresh block and the key from the whole preceding chain is encrypted, providing a new key[19] that enables the integrity of the entire chain to be verified. Once the key is established, no one block can be substituted with another, because the key would no longer be the same.

Let us consider the example of a corrupt individual who wishes to falsify data by changing, deleting or modifying an existing transaction. To do so, this person would need to recreate a whole new chain of blocks, starting from the date of the corrupted transaction all the way up to the moment the falsification takes place. More than half the nodes in the network would need to be convinced that the new version of the chain is correct. Thanks to the difficulty of proof of work, to do so requires too much effort in a limited time, as well as requiring the corrupt individual to possess over half the nodes. This is what makes the chain so robust. As with a public key, the cryptography work is asymmetric: it is very difficult to retrieve the original

17. Lest we forget, this has proved to be the main problem with the MD5 password encryption protocol: dictionaries are available online that allow users to search for the original word and, in turn, to break the key.

18. But there are still too many websites that store passwords in plain language, thereby creating dangerous vulnerabilities (for example lesechos.fr).

19. Expert readers may be interested to know that it is the SHA-256 that is used (see fr.wikipedia.org/wiki/SHA-2).

message using the key, but easy to verify the validity of the key, which in turn is what makes the blockchain easily auditable. Finally, another important factor is that the blockchain is not anonymous but pseudonymous: the participants in transactions are identified, even if their identity remains unknown.

Point 4 is also crucial. In order to do away with the need for a trusted third party, the community must not be open to manipulation. Point 5 guarantees the presence of a genuine community, but Point 4 dictates that the latter must be sizable and independent, so that no corrupt individual or institution can take control over the community of miners. This is particularly important because it means that the blockchain only takes on its full meaning on a large scale. In the same way as if there were only three Byzantine generals, there would be no guarantee of consensus, a small blockchain is useless. On the other hand, if it were just a group of trusting friends, there would be no need for the five ingredients: the first three would be sufficient, and the group could find a cheaper and more efficient solution than the blockchain.

Point 5 is the most complex since, as the chain keeps growing, the quantity of calculations required also increases. It works because the algorithm dynamically alters the cryptographic workload, and also because the size of the blocks remains constant. There is an ongoing debate over whether the size of the bitcoin's blocks should be increased. As with all fundamental Internet decisions, this will be decided by consensus, with opinions currently being shared on a wiki.[20] The mining time allowed to guarantee the proof of work, set at 600 seconds per block, also remains constant. In practice, there appears to be a limit of 6.6 transactions per second.[21] The good news is that this works on a worldwide scale; the bad news is that, in order for it to work, a significant share of the world's processing power is being used up.

Wonderfully enough, in its early days the blockchain used processing power available on empty machines that were distributed throughout the community, which was doubly beneficial in terms of both CO^2 emissions and Point 4. At the same time, private individuals used graphics cards, which were more powerful than their computers' actual processors. There are also specific "blockchain mining" machines available for sale over the internet. But at the moment, 50% of all mining power is in the hands of a limited number of Chinese entities, who are using specialized hardware.

20. See en.bitcoin.it/wiki/bloc_size_limit_controversy.

21. For the full calculation, see en.bitcoin.it/wiki/Scalability_FAQ#What_is_this_Transactions_Per_Second_.28TPS.29_limit.3F.

What we can do without the need for the five promises

Fulfilling promises 4 and 5 comes at a price. Indeed, so long as the credibility of the trusted third party is assured, the same outcome will generally be possible at a fraction of the cost. For example, a trusted third party can offer to register and validate documents and information in a digital depot, set up in the form of two application programming interfaces (API).[22] The first API allows anyone to store information, and the second to validate a claim. Promises 1 and 2 are fulfilled by this transactional approach, and the capacity to distribute trust is carried out in the form of the verifiable certificates. Although we must accept that the depot itself is a black box, it is easy to make and a lot less expensive than a blockchain.

Promise 3 stipulates that the depot should be open and visible to a large community. Promises 1 to 3 can therefore be fulfilled with a blockchain that is shared with all but validated by just one (the trusted third party). In this eventuality, the structure of the distributed blockchain is of real interest: a chain is a way of incrementally guaranteeing integrity; furthermore, by using a peer-to-peer distribution mechanism, many participants are empowered to check the coherency of said chain. In terms of API, this means that the first step of the transaction is retained (insertion, followed by confirmation of receipt by the trusted third party), but that the verification API is no longer required as the chain is widely distributed and can be checked by anyone, as is the case with the blockchain. This solution satisfies promises 1 to 3, and such an approach is therefore armed with one of the disruptive powers of the blockchain ("trust as a service"), from the moment trust is placed in the third party.

Solutions do therefore exist that envisage the production of (much cheaper) alternative blockchains that can be applied to functional sub-domains. As such, the main interest is to reduce transaction costs by eliminating human work that can be carried out in greater security and at a lower cost by algorithms. For example, by using a blockchain, transferring money from one country to another would cost a tenth of the price and would take ten minutes to be validated, instead of several days. It is this promise that has suddenly caught the attention of the financial sector.

22. APIs are programming interfaces that allow an external information system to be opened. They can be considered as supply points that deliver specific services.

Let us remind ourselves one last time: the blockchain's claim to be resistant to fraud does not hold up when confronted by a declining community. In other words, a small community cannot protect itself against a hostile third party possessing very strong processing power. This is why the blockchain requires global interest that can attract a community of miners from all over the world. The questions that need to be checked carefully are whether it is possible, for every proposed use of the blockchain, to assemble a global community around the subject (without which Point 4 is not met and there is a risk of submersion) and whether the cost of the huge proof of work remains cheaper and more fluid than the services of a trusted third party.

From a political point of view, the response may be very different (here it is not cost which is at stake but liberty, and this is what motivates the majority of the crypto-blockchain community). But from an economic point of view, potential uses are still emerging. In the world of traditional finance, the idea of doing away with the trusted third party is unthinkable. Any initiatives currently emerging from among the financial institutions do not respect all of the blockchain's promises; if they did, the cautious and reserved signs of interest that banks are showing in the blockchain would surely be replaced by a wave of panic, since the blockchain fulfilling all of its potential would render their role of trusted third party obsolete. On the other hand, when transaction costs become too high, in terms of both time and money, the credibility of the trusted third party evaporates. Under these circumstances, the third party-free blockchain offers a more efficient alternative.

The situation somewhat differs when viewed from a social or political perspective. When citizens genuinely start challenging the efficiency of administration services, the latter should look into the blockchain. There are numerous examples of situations in which the blockchain can be of real political or societal benefit, and in which we could happily bypass our institutions, or even the State. As such, a new model is emerging known as Decentralised Autonomous Organisation (DAO), described in greater detail below.

Three key issues

The first important issue is that of latency. Due to the way the blockchain is constructed, two factors directly impact on its latency: firstly, the proof

of work requires time and, secondly, the validation of each transaction block depends on the requisite probability of it being secure. Therefore, a certain amount of validation time is needed, which fluctuates randomly like a queue (the validation time is at least 10 minutes per block for bitcoin). Any scalability problems essentially translate as slower response times. There are many financial services that will not tolerate such delays, above all at high frequency trading times.

"Scalability" is a more complex issue, and the subject of much debate. In order for the blockchain to continue to grow harmoniously, an ever-increasing level of processing power is required (measured in petahash per second),[23] but the "distribution" of the community must be preserved (i.e. a significant number of independent participants). Ingredient 4 effectively states that the community of miners has more resources at its disposal than a malicious attacker, and that the community is sufficiently vast and distributed so as to resist any attempts to take control of it. However, rapid growth and the need for scalability mean that the community is becoming increasingly concentrated. An interesting parallel can be made with the distributed architecture of Domain Name Systems,[24] which is also experiencing a de facto concentration.

The phenomenon of distributed trust also generates costs. In the early days, the processing power consisted of free cycling power provided by under-utilised machines. The competitive nature of the consensus process (the first users to reach consensus take a share of the reward) created a Darwinian environment. The energy cost of the proof of work process is not negligible, despite the progression towards specialist ASICs, a trend that, furthermore, goes somewhat against the preservation of an open community of developers. We are starting to hear complaints that the validation costs are becoming high in comparison with other more traditional methods. This is only going to get worse: the rules of Moore's law go in favour of those other methods (the costs of which will continue to fall as machines become more powerful at less expense), while the blockchain, by its very nature, will require more and more effort as computing technology advances. Alongside proof of work – in which, let us be reminded, everyone must solve the same puzzle – another means of

23. As a reminder, 1 peta = 1015, or 1,000 tera.

24. The DNS is the Internet's global directory. It is the DNS that decides that a given address (www.fondapol.org, for example) will direct users to its corresponding server. If it ceases to grow outwards the Internet will explode, as the same address would direct users to other servers depending on their location. This would signal the end of the web's worldwide nature.

reaching consensus has emerged: "proof of stake",[25] where the miners' effort is concentrated only on the subsets of the blockchain that they own. Bitcoin is based on proof of work, but other cryptocurrencies have tended to move towards proof of stake, such as Peercoin.

THE IMPACTS OF THE BLOCKCHAIN

Smart Contracts

Anyone who has ever read a contract will be able to attest to how complex they are. Lawyers seem delighted by the prospect of creating such complex documents, which nevertheless makes them difficult to execute and increases the risk that they contain contradictions. But it often feels like there is a whole series of hoops to jump through to establish even the simplest of contracts.

In 1993, the concept of the "smart contract" was invented to automate contractual relations, by eliminating human intervention. A bank loan, for example, is perfectly capable of being entirely automated, without any human input, since all of its conditions are impartial. But there will always be doubts over whether a contract is being correctly executed; in other words, over the auditability of the contract.

What makes blockchain technology unique is that it enables the storage of not just content, but also algorithms, thanks to the sections of code that it holds. As the blockchain enables everyone to audit these algorithms, trust can only be strengthened.

Let us consider a simple example: VAT. There are enormous sums to recover in unpaid VAT (€32 billion in 2013, in France alone)[26] and fraud, above all so-called "carousel fraud", is responsible for a large share of these missing payments. Now imagine that all VAT transactions were stored on a blockchain. All the parties involved could carry out their own audits in order to ensure that the rules were respected and that all transactions were entirely above board

25. For a description of *proof of stake*, see www.bitsharesfcx.com/bts2_11.php.

26. Philippe Ricard and Patrick Roger, 'TVA : 32 milliards d'euros perdus par la France chaque année', lemonde.fr, 18 September 2013 (www.lemonde.fr/politique/article/2013/09/18/tva-32-milliards-d-euros-perdus-par-la-france-chaque-annee_3479706_823448.html).

– that calculations were correct and that payments had been made. Fraud is therefore no longer possible.

The verification costs are a lot lower than if the checks were carried out by a human operator and it is, above all, a lot quicker. This remains true, provided the events that enable those involved to verify the execution of the contract can be automatically detected by the blockchain, like in the case of a bank loan and its repayments. But what if, for example, an action (such as a payment) were to be triggered by a physical event, like the delivery of goods? This is where the "smart" elements that make up the smart contract take on their full meaning. Imagine a world of electronic keys, where transferral of a real estate asset would be automatically triggered by the execution of a sales or rental contract present in the blockchain. The contract would be impartial and fully auditable, which would in turn make the property inviolable. The former owner would no longer have access to the property because the old electronic key would no longer work, and the new owner would only be granted access once the software had unblocked the new key.[27] Airbnb's recent decision to experiment with blockchain technology could well mark the start of a new trend of tenant-owner relations being governed by smart contracts.[28] Only now is it becoming clear how the professions of trusted third parties such as notaries, lawyers and clerks could be totally transformed by the blockchain.

Autonomous decentralised organisations

The world of business, just like the world of administration, is experiencing a fundamental crisis. The reasons are the same in both domains: silo business models, vertical structures and overbearing hierarchies; management based on mistrust; governance leaving little space for creativity and invention; and a differentiation between the "thinkers" and the "doers". In a world of interactions, where collective intelligence is the rule, these models are inefficient because they do not sufficiently circulate information and develop knowledge.[29]

27. The principal manifestation of this idea is nicely explained in a video entitled 'Rent, sell or share anything – without middlemen' (slock.it), produced by a start-up that enables its users to rent out or lend any personal belonging, thanks to a blockchain.

28. See 'Airbnb just acquired a team of bitcoin and blockchain experts' qs.com, 12 April 2016 (qz.com/657246/airbnb-just-acquired-a-team-of-bitcoin-and-blockchain-experts).

29. For more on the importance of a society based on knowledge, see Idriss J. Aberkane, *Économie de la connaissance*, Fondation pour l'innovation politique, 2015 (www.fondapol.org/etude/idriss-j-aberkane-economie-de-la-connaissance.

In 1937, the economist Ronald Coase showed that the concept of the firm was chiefly designed to reduce transaction costs by, among other methods, connecting information and logistics.[30] In this model, hierarchy is important because it reduces uncertainty and, in turn, transaction costs. But why is the world not, therefore, one big firm? Because a second cost must be added to the first: the cost of organisation. In other words, the law of diminishing returns dictates that the benefit is not always proportional to the amount invested. The peer-to-peer model enables the ongoing transmission of information while guaranteeing trust. This also applies to the transaction model.

Ronald Coase was also interested in social costs. He showed that the State does not have enough information to impose all taxes at the correct level, but that tax agents and taxpayers could come to an agreement – in a "peer-to-peer" mode, to use today's parlance – so long as the transaction costs were low.

There was just one missing link to make Coase's ideas workable, and it is blockchain technology that can serve to bridge that missing link. We can now see the extent to which the blockchain is seriously undermining the principal *raison d'être* of our institutions.

An organisation is made up of tangible assets, intangible assets and people. According to the traditional paradigm, certain people make the decisions (the board, management teams, the parliament, the government) and others execute them. The industrial revolution significantly reduced the number of "doers" and replaced them with robots. But white-collar workers will soon be going the same way: brainpower may have replaced manpower,[31] but it too can be automated and replaced by computers. The more a firm is governed by rules and processes, the more obvious it will become that they should be automated. If we return to the example of the bank, the presence of a "middle man" is by no means required to execute a money transfer. The latter slows down the process and contributes nothing, only becoming useful when it comes to bending the bank's rules. In order to make a valid transaction, a company's rules can be applied via software alone, as we have seen with smart contracts. This does not signal the end for the human being, of course, but rather marks the emergence of a business model that will no longer use our intelligence to carry out repetitive tasks that bring no added value. Instead, our intelligence

30. Ronald Coase, 'The Nature of the firm', *Economica*, vol 4, n° 16, November 1937, pp. 386-405 (onlinelibrary.wiley.com/doi/10.1111/j.1468-0335.1937.tb00002.x/epdf).

31. Jean-Pierre Corniou et al., *Le Choc numérique*, Nuvis, 2013 (see also www.lechocnumerique.fr).

will be used to create knowledge. All the conditions are now in place for us to create an entirely efficient business model, where all stakeholders can participate in decision-making, can audit the rules and can check that they are applied. The political equivalent of this phenomenon would be "government as a platform", as defined by Tim O'Reilly.[32] And the blockchain is the tool that enables the management of these organisations.

DAO is a theoretical model of governance whereby autonomous entities cooperate with each other in accordance with an unfalsifiable set of working rules. To achieve this, one method is to implement the rules by using open source software distributed onto the computers of all stakeholders. A sample set of encoded rules of governance can be found on the Ethereum website. [33]Seeing the rules in their code form may seem bizarre, but it makes them easier to understand and, therefore, easier to audit. One side effect of using a blockchain would be to verify the consistency of the rules of governance. The codes are sure to be full of contradictions, which become far easier to detect. Another interesting effect is the possibility, via the blockchain, of implementing liquid democracy, in which each person can choose a representative to vote in his/her place for certain decisions, within a limited time and space. For any readers interested in this model, a start-up named Boardroom offers DAO-specific management tools.[34]

Ethereum

In the world of the Internet, very often the first party to arrive takes all the spoils, providing it finds the right economic model, what is called "winner takes all". We saw it with Google and Amazon, then Airbnb, Uber and others. [35]With respect to the blockchain, only one company is currently emerging that offers a generic blockchain: Ethereum.

Ethereum consists of a foundation based in Toronto and a company based in Switzerland. It offers a blockchain that enables users to manage not just cryptocurrency but also smart contracts, via a Turing machine. Its code is

32. Tim O'Reilly, 'Government as a Platform', in Daniel Lathrop and Laurel Ruma (eds), *Open Government. Collaboration, Transparency, and Participation in Practice*, O'Reilly Media, February 2010, chapter 2 (chimera.labs.oreilly.com/books/1234000000774/ch02.html).

33. 'How to build a democracy on the blockchain', www.ethereum.org/dao.

34. See boardroom.to. Their white paper nicely sums up the workings of a DAO: Nick Dodson, *BoardRoom: A NextGeneration Decentralized Governance Apparatus*, n.d. (boardroom.to/BoardRoom_WhitePaper.pdf).

35. AltaVista existed before Google, but was unable to find the right economic model. When Digital was valued prior to its acquisition by Compaq, AltaVista was not even taken into account.

open source and its currency, which is called ether, was worth $900 million in April 2016. [36]

Ethereum works on several levels – simultaneously identifying what must be done to mine and what is possible to validate – as the ultimate aim is to have a complete validated Turing machine. There is a risk of amassing such a high level of complexity that other problems emerge, at a time when we are still a long way from having explored everything that it is possible to do with the blockchain. But we must keep faith in the capacity of the Americans to resolve any problems that may arise.

Microsoft has just started offering "blockchain as a service", based on the Ethereum technology. [37] It remains to be seen whether Ethereum will become the next quasi-universal service, or indeed whether Amazon will pursue its Amazon Elastic Compute Cloud (EC2) project and create its own blockchain.

SOME OF THE BLOCKCHAIN'S USES

The blockchain is already used in numerous different ways, and within varied domains. It is no longer possible to list them all here, but it is nevertheless possible to give some examples. In all likelihood, an overview of the uses in a year's time (in 2017) will look entirely different to how it does today. On the other hand, not all of these experiments truly fulfil all of the five promises. It is hard to imagine a trusted third party suddenly creating a blockchain that honours promises 1 to 5, without first considering how its new role will look in a world where the blockchain guarantees trust in all transactions, thus rendering the third party obsolete.

Finance

The first example of the blockchain in use was, of course, the bitcoin. This cryptocurrency, which respects all five of the blockchain's promises, was

36. Visitors to coinmarketcap.com/currencies/ethereum can monitor its development in real time.

37. Giulio Prisco, 'Microsoft Launches Ethereum Blockchain as a Service (EBaaS) at Devcon, Boosts Ethereum', 11 November 2015, bitcoinmagazine.com (Bitcoinmagazine.com/articles/microsoft-launches-ethereum-la blockchain-as-a-service-ebaas-at-devcon-boosts-ethereum-1447277647).

invented in 2007 by the mysterious Satoshi Nakamoto. It is limited in quantity (21 million) and is starting to be a prominent fixture in the landscape: in May 2016, over 7,600 destinations around the world accepted bitcoin as a method of payment,[38] and the US Securities and Exchange Commission (SEC) has even authorised donations to political parties made in bitcoins. Bitcoin has quickly been caught up by other cryptocurrencies: Wikipedia numbers them at over 600, including 9 with a value of over $10 million.[39]

Finance is a typical example of a model that finds any sort of change difficult. Not only is the cost of banking transactions enormous, but they are not at all fluid: we still have to wait several days to carry out an intra-European money transfer, in return for a service that is not of great quality. And above all, banks are very reluctant to open up; it took the introduction of PayPal for them to start opening their APIs. Any human intervention in a transaction slows it down, resulting in a lower overall processing capacity, and therefore a poorer quality of service. The cost of mistrust is immense. One of the blockchain's great assets is that it empowers the progression to a model based on trust.

For customers, the blockchain's great strength is that it speeds up transactions while preserving collective trust. For financial institutions, the blockchain represents an enormous reduction in costs and the possibility to offer a better service. But a blockchain that fulfils promises 1 to 5 essentially renders the institution obsolete. This is why banks are currently in the process of building blockchains that do not honour all five promises, with a view to reducing costs and making transactions more fluid. Right now, these traditional financial institutions are only at the start of their experiments. But Estonia, for example, decided, with the help of Nasdaq, to put the voting procedures for the shareholders of every company in the country on a blockchain.[40]

Healthcare

Our healthcare system dates back to ancient times.[41] There is barely any information transferred between the various stakeholders (town doctor, nurse, hospitals, and so on) and it is still the patient's job to take care of communication by bringing his/her own medical file to appointments. France's

38. See the updated world map at coinmap.org/#/world/47.57652571/6.67968750/4.
39. 'List of cryptocurrencies', Wikipedia (en.wikipedia.org/wiki/List_of_cryptocurrencies).
40. http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654.
41. See Jean-Michel Billaut's blog on e-healthcare: billaut.typepad.com/jm/e-sant%C3%A9/.

personal medical file project (known as the *dossier médical personnalisé*) has been a dismal failure, for purely political reasons. The result is an increased level of suspicion in healthcare institutions.

A blockchain would offer many benefits: first and foremost, there would be no more trusted third parties wasting the public's money on complex systems that do not work. The blockchain can help to create a healthcare system whose construction and running costs are lower, thus increasing the amount of money available for patient reimbursement. Furthermore, the ability to integrate smart contracts into the blockchain enables a much more personalised service, with expenditure and reimbursements calibrated in accordance with each individual profile. Ultimately, the community would be rewarded with a fully functioning service, rather than opaque administration.

This is not a utopia: Estonia, a country renowned for investing heavily in digital solutions, is currently creating a blockchain to store the medical files of all of its citizens.[42]

Politics

The complexity of French law and regulations is not a matter open to debate. Labour laws alone consist of somewhere between 2,000 and 15,000 pages of text, depending on what we consider to be core regulation and what to be jurisprudence. But even 2,000 pages is an awful lot, particularly when we also consider the branch agreements, special status regulations, European laws, and so on. And let us be quite clear about this: no politician will ever have the courage to reduce the French labour law. It would be a Herculean task. However, it would surely be beneficial to codify these texts into smart contracts – and in doing so iron out any contradictions held within them – and then to place these smart contracts in a blockchain, which would then be shared with all stakeholders: companies, administrations, employees, etc. All the calculations would be automatic and the financial gains for the state, and therefore for all involved, would be enormous in terms of control.

Generally speaking, all rules of governance, be it for a company, a charity or a country, can be put on a blockchain (as detailed during the section on DAOs).

42. 'Guardtime Secures Estonian Health Records', e-estonia.com, 8 March 2016 (e-estonia.com/guardtime-secures-estonian-health-records).

In politics, this would result in the concept of "liquid democracy". Debates are currently raging as to the limitations of this system, which could lead to the "tyranny of code".[43] Certain political parties, like the Pirate Party in the UK and Nous Citoyens in France, already use blockchains to manage their voting procedures.[44] One political party in Australia, The Flux Party, decided to build its governance on a blockchain. The principle is that the party's senators must apply the decisions chosen by the members' vote, which takes place via the blockchain.[45] The innovation is that members each have voting credits, which they can exchange on the blockchain in order to focus their votes on their own personal areas of interest. This is a genuine example of the principles of liquid democracy in action, with delegation on certain subjects and direct voting on others.[46]

The media

The music and cinema industries endure a love-hate relationship with the Internet. As an example, merely consider the impressive rage with which the Recording Industry Association of America (RIAA) has taken on the so-called "pirates". We will enter the debate only so far as to say that these are examples of material economies and that the famous law that "when we share a tangible good, it divides itself; when we share an intangible good, it multiplies" fully applies to music.

On the other hand, the problem of equitable distribution of rights is a genuine transactional problem, which is crying out for trust. But the e-reputation of the majors has suffered greatly due to the fierce battle they have waged against peer-to-peer platforms, above all among a geek population that accuses them of not giving enough back to creators and not offering a service worthy of the percentage that they take. There is therefore a great temptation to use a blockchain to redistribute money to everyone, and to cut out the trusted third party. The start-up Muse was created to explore this idea.[47] Its aim is to create a worldwide music blockchain, which shares out the rights between all stakeholders.

43. See Aaron Wright and Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, abstract, Social Science Research Network (SSRN), 10 March 2015 (papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664).

44. See, for the United Kingdom, 'The Democracy Interface: Time to Upgrade?', ppuk.org.uk, 10 July 2015 (www.ppuk.org.uk/tags/blockchain); for France, 'La blockchain au service de la politique ?', nouscitoyens.fr, 8 April 2016 (www.nouscitoyens.fr/blog/2016/04/08/frenchweb-la-blockchain-au-service-de-la-politique).

45. See voteflux.org.

46. Dominik Schiener, 'La démocratie liquide : une véritable démocratie pour le 21e siècle', n.d. (framablog.org/2015/12/09/democratie-liquide).

47. museblockchain.com.

Classified advertisements

OpenBazaar (still in beta) is a 100% peer-to-peer classified advertisements platform.[48] Instead of having to visit a website, users download software onto their computer, which they use to access what is on offer or to sell their own items, without any commission. It is a competitor of eBay and the French website, Le Bon Coin.

Transport

Collaborative transport also has its own blockchain. Lazooz coordinates a journey share service and, of course, all financial transactions on a blockchain.[49] Just like Open Bazaar, the main benefit is to reduce transaction costs. However, it still remains to be seen whether the presence of a trusted third party remains necessary for the success of a car sharing service, as it gives the user a partner to turn to and share the risks, thereby guaranteeing customer satisfaction.

THE FUTURE

There is a tension that pits the diversity of opportunities discussed above directly against the need for one unique, worldwide infrastructure that guarantees the community remains larger than any potential attackers (see Ingredient 4). We have seen that the idea of having "my own little blockchain, all to myself" is not compatible with the five promises. However, once a trusted third party is accepted, it is nevertheless easy to instantiate a whole subset of these technologies for individual cases. For example, for the certification of documents (land registry, damages, property, etc.) a simpler system, implementing promises 1 to 3, is sufficient, and does not entail the additional financial and energy cost related to proof of work.

Nevertheless, using the blockchain to create a *trust as a service* model makes a lot of sense. Essentially, the beauty of the blockchain approach is to enable a small unknown entity, for example a start-up, to offer the same guarantees of transparency, sustainability and other trust-related characteristics that

48. openbazaar.org.
49. www.lazooz.net.

are traditionally associated with established, institutional structures (this is the competitive advantage held by large financial institutions). Once it starts registering its transactions in the international blockchain, this start-up will offer a non-repudiation guarantee that is the equal of, or superior to, that offered by a State or a bank. It nevertheless remains unclear whether the current infrastructure is able to host the avalanche of requests and opportunities that we have briefly alluded to here.

Consequently, we are witnessing the emergence of a tree structure: a large central blockchain, available worldwide and validated by a vast community, with branches (blockchains or otherwise) operated on a simpler level by start-ups or small communities with an interest in them. The interest here is that the start-up can place the ledger of its own activities in the central blockchain, immediately making it trustworthy and transparent in the eyes of its customers. The ledger, meanwhile, can be managed with lighter techniques that require less of an investment in terms of time and money.

This approach has given rise to several technological developments, including sidechains. A sidechain is a chain of transactions managed by a sub-community, with similar encryption and authentication techniques as the blockchain, but with a simpler protocol facilitating improved performance levels. The distribution of control (the sidechain is controlled by a smaller group) lends it more agility, but the end of this sidechain (the *peg*) is integrated within the blockchain so that the former benefits from the increased security of the latter.[50]

This solution also extends the blockchain with the addition of richer protocols, meaning that the "blockchain/sidechain" blueprint is a better direction for the ecosystem to evolve in than the creation of new, autonomous blockchains.[51]

Can a true peer-to-peer mode survive without the presence of a large entity behind it? For Uber or Airbnb, the brand value is not in the platform but in the promise made to their customers. And it takes human resources to provide the service once the sale has been made. But on the other hand, the Internet itself functions without the presence of such an entity. Early internet detractors pointed towards the absence of an operator, which supposedly rendered it too

50. For more detailed information on the sidechains mechanism, see Adam Back *et al*., 'Enabling Blockchain Innovations with Pegged Sidechains', abstract, 22 October 2014 (blockstream.com/sidechains.pdf).

51. Read, for example, 'Drivechain – the simple two way peg' (www.truthcoin.info/blog/drivechain).

inaccessible for the uninitiated. This is true, but community help systems have worked perfectly, and have in time replaced and improved upon the much less efficient hotlines and call centres.

PROVISIONAL CONCLUSION

In the future, when the blockchain's influence becomes truly disconcerting for the established institutions, there will be a great temptation for those currently in charge to suppress it, by outlawing it or limiting its effects. The Internet was born in 1969, but did not become widely available to the public until 1991. It is only 25 years later that the majority of politicians are now trying to suppress the innovation that the Internet brings with it. [52]

But attempting to hold the Internet back is like trying to stop the rain. The decentralisation of the web, the fact that intelligence is found at its outer limits rather than inside the network, the longing of many citizens for another model where they are more engaged, and above all the growing complexity of the world, characterised by an increasing number of interactions, will encourage our progression towards distributed trust. Any human intervention in a transaction slows it down, resulting in a lower overall processing capacity, and therefore a poorer quality of service. The blockchain's great strength is that it speeds up transactions while preserving collective trust, all at a lower cost.

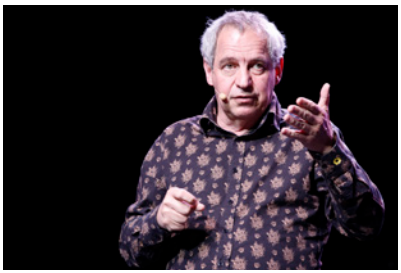
Thanks to the invention of the Internet technologies, the world of telecommunications has progressed from a centralised model with a prominent role for trusted third parties (the operators) that justified their role by the promise of "total quality", to a decentralised model where everyone can effortlessly connect to the internet from anywhere, and benefit from a universal array of low cost services. Thanks to the invention of the blockchain, it is increasingly likely that the world of transactions, and not just the world of finance, will experience the same disruption; one that will not prove any less painful for the operators.

52. For more information on Internet censorship, see https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country.

Find videos of the speeches made during the event organized by the *Fondation pour l'innovation politique* on our website

LE PROGRÈS, C'EST NOUS ! 24 HEURES NON-STOP

NOVEMBER 16, 2013 AT MAISON DE LA MUTUALITÉ IN PARIS



Serge Soudoplatoff
on «Digital technology and innovations»

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-serge-soudoplatoff-toile-a-tisser/

Élisabeth Grosdhomme-Lulin
on «Public service 2.0»

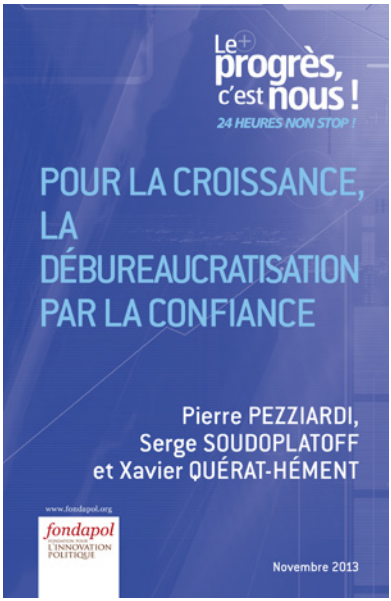
http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-elisabeth-grosdhomme-lulin-des-idees-pour-decider/

Idriss J. Aberkane
on «Economy of knowledge»

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-idriss-aberkane-toile-a-tisser/

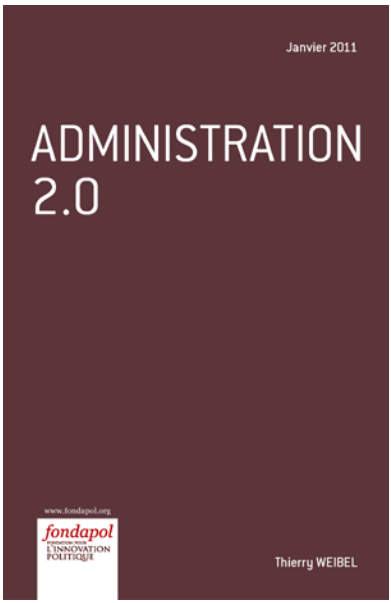
Pierre Pezziardi
on «Trust through digital technology»

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-pierre-pezziardi-toile-a-tisser/



Debureaucratisation through trust to promote growth
Pierre Pezziardi, Serge Soudoplatoff and Xavier Quérat-Hément, November 2013, 48 pages

Digital transformation
Jean-Pierre Corniou, June 2011, 52 pages



Public service 2.0
Thierry Weibel, January 2011, 48 pages

Internet, politics and citizen coproduction
Robin Berjon, September 2010, 32 pages

OUR PUBLICATIONS

The radical Left: links, places and struggles (2012-2017)
Sylvain Boulouque, May 2016, 56 pages

Governing to reform: elements of methodology
Erwan Le Noan and Matthieu Montjotin, May 2016, 64 pages

Occupiers of Zones-to-defend (2): the temptation of violence
Eddy Fougier, April 2016, 44 pages

Occupiers of Zones-to-defend (1): a new anticapitalist phenomemon
Eddy Fougier, April 2016, 44 pages

Regional elections (2): political parties are questioned but not challenged
Jérôme Fourquet and Sylvain Manternach, March 2016, 52 pages

Regional elections (1): far-right vote and terrorist attacks
Jérôme Fourquet and Sylvain Manternach, March 2016, 60 pages

Law serving innovation and growth
Sophie Vermeille, Mathieu Kohmann and Mathieu Luinaud, February 2016

Lobbying: a democratic tool, Anthony Escurat, February 2016
Values of Islam, Dominique Reynié, January 2016

Shiites and Sunnis – is peace impossible?
Mathieu Terrier, January 2016

*Companies governance and society needs**
Daniel Hurstel, December 2015

Mutuality: meeting insurance-sector challenges
Arnaud Chneiweiss and Stéphane Tisserand, November 2015

*Noopolitics: the power of knowledge**
Idriss J. Aberkane, November 2015

European public opinion in 2015
Dominique Reynié, November 2015

Political Innovation 2015
Fondation pour l'innovation politique, October 2015

Good COP21, Bad COP21 (2): beyond political correctness
Albert Bressand, October 2015

Good COP21, Bad COP21 (1): Europe's Kant meet China's Machiavel
Albert Bressand, October 2015

SMEs: new financing methods
Mohamed Abdesslam and Benjamin Le Pendeven, October 2015

Long live motoring (2): the case for road use
Mathieu Flonneau and Jean-Pierre Orfeuil, October 2015

Long live motoring (1): conditions for user-friendly mobility
Mathieu Flonneau and Jean-Pierre Orfeuil, October 2015

Crisis of the Arab/Muslim conscience
Malik Bezouh, September 2015

Département elections of March 2015 (3): second round
Jérôme Fourquet and Sylvain Manternach, August 2015

Département elections of March 2015 (2): first round
Jérôme Fourquet and Sylvain Manternach, August 2015

Département elections of March 2015 (1): background
Jérôme Fourquet and Sylvain Manternach, August 2015

Higher education: the limits of a Master qualification for all
Julien Gonzalez, July 2015

Economic policy: the Franco-German issue
Wolfgang Glomb and Henry d'Arcole, June 2015

Laws of primaries, past and future.
François Bazin, June 2015

*Economy of Knowledge**
Idriss J. Aberkane, May 2015

Fighting theft and burglary: an economic approach
Emmanuel Combe and Sébastien Daziano, May 2015

Uniting for action: a programme for growth
Alain Madelin, May 2015

A new vision of enterprise and human value
Francis Mer, April 2015

Transport and funding mobility
Yves Crozet, April 2015

Digital technology and mobility: impact and synergies
Jean Coldefy, April 2015

Islam and democracy: facing modernity
Mohamed Beddy Ebnou, March 2015

Islam and democracy: the foundations
Ahmad Al-Raysuni, March 2015

Women and Islam: a reformist vision
Asma Lamrabet, March 2015

Education and Islam
Mustapha Cherif, March 2015

What have parliamentary by-elections since 2012 told us?
Dominique Reynié, February 2015

Islam and the values of the Republic
Saad Khiari, February 2015

Islam and the social contract
Philippe Moulinet, February 2015

Sufism: spirituality and citizenship
Bariza Khiari – February 2015

Humanism and humanity in Islam
Ahmed Bouyerdene, February 2015

Eradicating hepatitis C in France: what public strategies should be adopted?
Nicolas Bouzou and Christophe Marques, January 2015

Keys to understanding the Koran
Tareq Oubrou, January 2015

Religious pluralism in Islam or the awareness of otherness
Éric Geoffroy, January 2015

*Future memories**
a survey conducted in partnership with the Fondation pour la Mémoire de la Shoah, Dominique Reynié, January 2015

A disintegrating American middle class
Julien Damon, December 2014

The case for supplemental education insurance: middle class schooling
Erwan Le Noan and Dominique Reynié – November 2014

*Anti-Semitism in French public opinion. New perspectives**
Dominique Reynié, November 2014

The competition policy: a plus for industry
Emmanuel Combe, November 2014

2014 European Elections (2): rise of the FN, decline of the UMP and the Breton vote
Jérôme Fourquet, October 2014

2014 European Elections (1): the left in pieces
Jérôme Fourquet, October 2014

Political Innovation 2014
Fondation pour l'innovation politique, October 2014

Energy/climate: the case for an effective policy
Albert Bressand, September 2014

Global urbanisation. An opportunity for France
Laurence Daziano, July 2014

What can we expect from monetary policy?
Pascal Salin, May 2014

Change is constant
Suzanne Baverez and Jean Sénié, May 2014

Too many emigrants? Perspectives on those who leave France
Julien Gonzalez, May 2014

European public opinion in 2014
Dominique Reynié, April 2014

Tax better to earn more
Robin Rivaton, April 2014

The innovative State (2): Diversifying the senior civil service
Kevin Brookes and Benjamin Le Pendeven, March 2014

The innovative State (1): Strengthening the role of think tanks
Kevin Brookes and Benjamin Le Pendeven, March 2014

The case for a new tax deal
Gianmarco Monsellato, March 2014

An end to begging with children
Julien Damon, March 2014

Low cost: an economic and democratic revolution
Emmanuel Combe, February 2014

Fair access to cancer therapies
Nicolas Bouzou – February 2014

Reforming teachers' status
Luc Chatel, January2014

Social impact bonds: a social finance tool
Yan de Kerorguen, December 2013

Debureaucratisation through trust to promote growth
Pierre Pezziardi, Serge Soudoplatoff and Xavier Quérat-Hément - November 2013

Les valeurs des Franciliens
Guénaëlle Gault, october 2013

Settling a student strike: case study in Quebec
Jean-Patrick Brady and Stéphane Paquin, October 2013

A single employment contract incorporating severance pay
Charles Beigbeder, September 2013

European Opinion in 2013
Dominique Reynié, September 2014

*The new emerging countries: the 'BENIVM countries**
Laurence Daziano, July 2013

Energy transition in Europe: good intentions and poor calculations
Albert Bressand, July 2013

Minimising travel: a different way of working and living
Julien Damon, June 2013

KAPITAL. Rebuilding Industry
Christian Saint-Étienne and Robin Rivaton, April 2013

A code of ethics for politics and public officials in France
Les Arvernes and the Fondation pour l'innovation politique, April 2013

The middle classes in emerging countries
Julien Damon, April 2013

Political Innovation 2013
Fondation pour l'innovation politique, March 2013

Reviving our industry through automation (2): issues
Robin Rivaton, December 2012

Reviving our industry through automation (1): strategies
Robin Rivaton, December 2012

Taxation a key issue for competitiveness
Aldo Cardoso, Michel Didier, Bertrand Jacquillat, Dominique Reynié and Grégoire Sentilhes, December 2012

An alternative monetary policy to resolve the crisis
Nicolas Goetzmann, December 2012

Has the new tax policy made the solidarity tax on wealth unconstitutional?
Aldo Cardoso, November 2012

Taxation: why and how a rich country is a poor country ...
Bertrand Jacquillat, October 2012

Youth and Sustainable Development
Fondapol, Nomadéis, United Nations, June 2012

Philanthropy. Entrepreneurs in solidarity
Francis Charhon, May/June 2012

Poverty statistics: a sense of proportion
Julien Damon, May 2012

Freeing up funding of the economy
Robin Rivaton, April 2012

Savings for social housing
Julie Merle, April 2012

European opinion in 2012
Dominique Reynié, March 2012

Shared values
Dominique Reynié, March 2012

The right in Europe
Dominique Reynié, February 2012

Political Innovation 2012
Fondation pour l'innovation politique, January 2012

Free schools: initiative, autonomy and responsibility
Charles Feuillerade, January 2012

French energy policy (2): strategies
Rémy Prud'homme, January 2012

French energy policy: issues (1)
Rémy Prud'homme, January 2012

Revolution of values and globalization
Luc Ferry, January 2012

The End of social democracy in Europe?
Sir Stuart Bell, December 2011

Industry regulation: accountability through non-governmental rules
Jean-Pierre Teyssier, December 2011

Hospitality
Emmanuel Hirsch, December 2011

12 ideas for 2012
Fondation pour l'innovation politique, December 2011

The middle class and housing
Julien Damon, December 2011

Three proposals to reform the healthcare system
Nicolas Bouzou, November 2011

The new parliament: the French law of 23 July 2008 revising the Constitution
Jean-Félix de Bujadoux, November 2011

Responsibility
Alain-Gérard Slama, November 2011

The middle class vote
Élisabeth Dupoirier, November 2011

From annuity to competition
Emmanuel Combe et Jean-Louis Mucchielli, October 2011

The middle class and savings
Nicolas Pécourt, October 2011

A profile of the middle class
Laure Bonneval, Jérôme Fourquet and Fabienne Gomant, October 2011

Morals, ethics and ethical conduct
Michel Maffesoli, October 2011

Forgetting Communism, changing era
Stéphane Courtois, October 2011

World youths
Dominique Reynié, September 2011

Increasing the purchasing power through competition
Emmanuel Combe, September 2011

Religious freedom
Henri Madelin, September 2011

The ways to a balanced budget
Jean-Marc Daniel, September 2011

Ecology, values and democracy
Corine Pelluchon, August 2011

Valoriser les monuments historiques : de nouvelles stratégies
Wladimir Mitrofanoff and Christiane Schmuckle-Mollard, July 2011

Opposing technosciences: their networks
Eddy Fougier, July 2011

Opposing technosciences: their reasons
Sylvain Boulouque, July 2011

Fraternity
Paul Thibaud, June 2011

Digital transformation
Jean-Pierre Corniou, June 2011

Commitment
Dominique Schnapper, May 2011

Liberty, Equality, Fraternity
André Glucksmann - May 2011

What future for our defense industry
Guillaume Lagane, May 2011

Corporate social responsibility
Aurélien Acquier, Jean-Pascal Gond et Jacques Igalens, May 2011

Islamic finance
Lila Guermas-Sayegh, May 2011

The state of the right Deutshcland
Patrick Moreau, April 2011

The state of the right Slovaquia
Étienne Boisserie, April 2011

Who owns the French public debt ?
Guillaume Leroy, April 2011

The precautionary principle in the word
Nicolas de Sadeleer, March 2011

Understanding the Tea Party
Henri Hude, March 2011

The state of the right Netherlands
Niek Pas, March 2011

Agricultural productivity and water quality
Gérard Morice, March 2011

Water: from volume to value
Jean-Louis Chaussade, March 2011

Water: how to treat micro-pollutants?
Philippe Hartemann, March 2011

Water: global challenges, French perspectives
Gérard Payen, March 2011

Irrigation for sustainable agriculture
Jean-Paul Renoux, March 2011

Water management: towards new models
Antoine Frérot, March 2011

The state of the right Austria
Patrick Moreau, Februay 2011

Employees' Interest sustaining purchasing power and employment
Jacques Perche and Antoine Pertinax, February 2011

The Franco-German tandem and the euro crisis
Wolfgang Glomb, February 2011

*2011, World Youths**
Fondation pour l'innovation politique, January 2011

The European opinion in 2011
Dominique Reynié, January 2011

Public service 2.0
Thierry Weibel, January 2011

*The state of the right: Bulgaria**
Antony Todorov, December 2010

The return of sortition in politics
Gil Delannoi, December 2010

The People's moral ability
Raymond Boudon, November 2010

Academia in the land of capital
Bernard Belloc and Pierre-François Mourier, November 2010

*Achieving a new Common Agricultural Policy**
Bernard Bachelier, November 2010

*Food Security: a global challenge**
Bernard Bachelier, November 2010

The unknown virtues of low cost carriers
Emmanuel Combe, November 2010

Political Innovation 2011
Fondation pour l'innovation politique, November 2010

Overcoming the Defense budget issue
Guillaume Lagane, October 2010

*The state of the right: Spain**
Joan Marcet, October 2010

The virtues of competition
David Sraer, September 2010

Internet, politics and citizen coproduction
Robin Berjon, September 2010

*The state of the right: Poland**
Dominika Tomaszewska-Mortimer, August 2010

*The state of the right: Sweden and Denmark**
Jacob Christensen, July 2010

What is the police up to?
Mathieu Zagrodzki, July 2010

*The state of the right: Italy**
Sofia Ventura, July 2010

Banking crisis, public debt: a German perspective
Wolfgang Glomb, July 2010

Public debt, public concerns
Jérôme Fourquet, June 2010

*Banking regulations for sustainable growth**
Nathalie Janson, June 2010

Four proposals to renew our agricultural model
Pascal Perri, May 2010

2010 regional elections: where have all the voters gone?
Pascal Perrineau, May 2010

The European opinion in 2010
Dominique Reynié, May 2010

*The Netherlands: the populist temptation**
Christophe de Voogd, May 2010

Four ideas to boost spending power
Pascal Perri, April 2010

*The state of the right: Great Britain**
David Hanley, April 2010

Reinforce the regions' economic role
Nicolas Bouzou, March 2010

Reforming the Constitution to rein in government debt
Jacques Delpla, February 2010

A strategy to reduce France's public debt
Nicolas Bouzou, February 2010

Catholic Church policy: liberty vs liberalism
Émile Perreau-Saussine, October 2009

*2009 European elections**
Corinne Deloy, Dominique Reynié and Pascal Perrineau, September 2009

The Nazi-Soviet alliance, 70 years on
Stéphane Courtois, July 2009

The administrative state and liberalism: a French story
Lucien Jaume, June 2009

*European development policy**
Jean-Michel Debrat, June 2009

Academics: defending their status, illustrating a status quo
David Bonneau and Bruno Bensasson, May 2009

Fighting age discrimination in the workplace
Elise Muir, June 2009

*Stemming the protectionist tide in Europe**
Nicolas Bouzou, March 2009

Civil service vs civil society
Dominique Reynié, March 2009

The European opinion in 2009
Dominique Reynié, March 2009

Working on Sundays: Sunday workers' perspectives
Dominique Reynié, January 2009

*The titles marked with an asterisk are available in English.

THE FONDATION POUR L'INNOVATION POLITIQUE NEEDS YOUR SUPPORT

To reinforce its independence and carry out its mission, the Fondation pour l'innovation politque, an independent organization, needs the support of private companies and individuals. Donors are invited to attend the annual general meeting that defines the Fondation orientations. The Fondation also invites them regularly to meet its staff and advisors, to talk about its publication before they are released, and to attend events it organizes.

As a government-approved organization, in accordance with the decree published on 14h April 2004, the Fondation pour l'innovation politique can accept donations and legacies from individuals and private companies.

Thank you for fostering critical analysis on the direction taken by France and helping us defend European integration and free economy.