**Beyond Bitcoin: Smart contracts and transparency**

When in the year 2008 Satoshi Nakamoto presented his proposal for an electronic currency based on a nodal validation system (P2P), nobody imagined that the Bitcoin would become in the financial phenomenon of our time involving thousands of digital currencies and related products. Cryptocurrencies –from Greek “cryptos, “hide”; literally “hidden currency”– have become part of common talk, most people knowing the word even if the exact meaning remains vague. Many lament having missed the opportunity of getting in on the profits, nurtured by the idea of investments whose profits are estimated in the order of 1000%, but so too are the potential losses. In less than a decade the market value of Bitcoin went from a few cent up to $20,000 during its peak in December 2017. The euphoria raised by this revolution has created not only a toxic culture of speculation, but has also hidden the true value of a technological innovation that is only beginning to show its potential.

*Crisis and Innovation*

Nakamoto –a person or a collective, we cannot tell– declared when he presented his novel idea, that its objective was to “allow online payments to be sent directly from one party to another without going through a financial institution”. The appearance of Bitcoin during the boom of the 2008 crisis took advantage of the increasing uncertainty in the financial markets to offer an alternative to a system whose reliability was at stake. Many investors trepedatiously adopted the new currencies. What Bitcoin offered using the technology of blockchain was nothing short of the Holy Grail of liberal monetarism, that is, a currency functioning without a central bank, not subject to the whims of a government but dependent on the cold consistency of an algorithm.

Why, then, its volatility? The unprecedented inflation of Bitcoin’s value in a couple of months (from July to December 2017) has made many to doubt about if it is really an alternative to physical money. To answer this riddle, one must distinguish between the *intrinsic value* of any good, depending on material properties as durability and divisibility of metals, or technical properties such as the no-modifiability of a blockchain; there is, on the other side, a *subjective value*, that we may more accurately call *speculative value*, which is not dependent on the properties of the good, but the result of herd behavior of millions of investors following the same signals but not necessarily with the same information. The history of humanity is full of cases when goods of the most distinct nature, from tulips to mortgages, have been the focus of rampant speculation.

Volatility, against its critics, is not a property of the cryptocurrency blockchain, but of financial markets. It is not a defect in the algorithm but a result of the speculation that moves money from one market to another looking for big and fast profits and, furthermore, it is the product of a *parteogenic feedback*: goods have value because they are valuable. In a sense, it is possible to say that the technological properties of Bitcoin make it attractive to speculative attacks –if it were worthless nobody concern themselves with it–, with the result that it has not been able to function as a currency and it behaves more as a financial good or gold itself. Who would be willing to pay for a pizza with a currency that could buy 20 or 2000 pizzas tomorrow? When two or more currencies coexist in an economy, the good coin is hoarded following the dictatum of the Gresham’s law.

The Bitcoin protocol based on *proof of work* for the construction of *public blockchains* offers an alternative to a central authority whose job is to corroborate the validity of transactions, particularly by preventing double-spending. To achieve this aim without the need for a third party guaranteeing trust in the currency –that is, without a central bank– each transaction is announced publicly and the register of each remains visible to all participants. In other words, the history of transactions is *transparent*. This is, in short, what the blockchain technology implies: a public accounting book built over the effort of thousands of nodes –currency users; virtually anyone with a computer and internet– none of them being able to alter the record of transactions unilaterally and whose incentive to participate is given by a fraction of each cryptocurrency “mined”[[1]](#footnote-1). Trust in a bank is replaced by the rigor of a cryptographic equation, removing the human partiality of government whims. It is, additionally, a systems that can be labelled as “democratic” in its construction. In the words of Nakamoto “Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it”. It is not only another alternative to money, but a technology with strong mathematical basis that solves, at least in theory, the principal problems of current monetary systems, but it is not limited to it.

*All that Glitters is not Gold: Smart Contracts*

The potential uses of blockchain technology depends basically on human imagination. It also means that we must expect further innovation in the future development of cryptocurrencies. Blockchain technology is applicable, for example, to the creation of a unique register of names, such as the DNS, detailed population records, and even a reliable voter registration system. It is also possible, given the appropriate modifications, to create records of property or more secure methods of guaranteeing patent rights which would not require a notary nor a central authority to validate exchanges. Some steps in this direction have been taken by Sweden, Ukraine and Georgia. It could also speed up the exchange of *virtual assets* through the automatization of trading following predetermined algorithms. All this is possible thanks to to the application of *smart contracts*, which are blockchain protocols that regulate exchanges between peers. These do not necessarily imply currencies, and work without an intermediary or further legal contracts and, hence, can reduce the costs of transactions while at the same time guaranteeing *transparency, traceability* and *security* of the operations.

An example of this application is given by the function administration of *Digital Assets* (DA). DA’s are digital resources that can be owned by someone, or a digital representation of content that can be owned and used by someone and, therefore, represent a right of use. Following the analysis of BitFury Group, digital assets must fulfill three requirements: security of users, be impossible to falsify and it must be possible to audit them. Blockchain technology satisfies all three. Current examples include financial titles, Smart Property, coupon, vouchers, patents, etc. In its “pure” form, DAs are the good itself for which a purchasers is paying –i.e. Cryptocurrencies–, and not a representation of something else.

Another notable application of Smart Contracts is in the field of production and distribution of energy. New technologies in the production and storage of energy to a “micro-scale” in the form of smart contract present a possible solution to the ecological problems caused by the stablished fossil fuel energy industry. As a result we are approaching an historical moment when renewable energies can supply the needs of a household, and even produce a “surplus” that could be sold to another household without the need of an intermediary. The exact means through which this direct energy market would work are still in development, but it is important to recognize that beyond technical burdens, which are overcome every day at an outstanding pace. Nonetheless, there are other barriers which would be harder to overcome.

*Towards a Transparent Public Currency*

Whether Bitcoin will become a commonly used currency once it has reached its “natural” value, that is, once harsh speculation ceases, is undoubtedly an interesting question. But limiting blockchain to its Bitcoin application is equivalent to be blinding due to its gold-like-brilliance. One of the most attractive features of blockchain technology is its transparency, which is not the same as lack of privacy. A public blockchain does not imply the publicity of private “keys”. Only the information concerning the public transaction is visible to all the participants, while personal information it is not. You can know the sin but not the sinner. This confusion has led some critics to blame cryptocurrencies for enabling modern-day money laundering, which can be true in some cases, but it is not less true or more harmful than the current banking system which, protected under the statute of bank secrecy, hides the identity of its costumers on dubious tax havens. Corruption is a defect of people, not of their currencies.

On the other hand, the possibility of keeping identities private is so clear cut: not mandatory but a possibility. An individual could make their identity public with no further risk than that which its own activities imply. Evidently on a personal level privacy is a valuable feature which few will be willing to give up even when there is nothing to hide. But what happens in the public domain? One of most important topics in contemporary political debates concerns the *transparency* on the use of public resources. The overwhelming amounts of money flowing through public administration means that public audits became an expensive, dark and sadly inconsequential process. Just referring to the fiscal exercise of 2012-2016, the Superior Audit Agency of the Federation[[2]](#footnote-2) of Mexico detected “alleged” diversion of resources up to 6 thousand 876 million pesos, which implies not only a crime but also the lack of attention to the most important social problems, such as poverty, because it was precisely in this area where most resources were diverted. In the same vein, recently the civil movement “Nosotrxs” made public 47 official papers which confirmed that public officers approved 14 thousand 684 million pesos for the reconstruction following last September’s earthquake, out of which more than 5 million pesos “were diverted to the purchase of tablets and gifts” allegedly used during the presidential campaigns. The numbers are alarming, but little has been done to sanction these diversions and nothing to prevent further crimes. The fact that the audit was made by the government itself explains a lot.

The 2017 *Corruption Perception Index*, published by the non-governmental organization Transparency International (TI), ranks Mexico in 135th position next to countries such as Honduras or Russia. In its fourth recommendation to Mexico to fight corruption, TI remarked on the need to create interoperable and automatized systems of information with open format, which could help to make public operations more transparent. From this perspective, there is a possibility to apply blokchain technologies to the control of public expenditure, a space of transaction where privacy is not a problem and, conversely, transparency is a legitimate demand. The application of blockcahin technology would make it impossible to modify public books to hide diversions of resources.

What is the difference with the current audit system? Firstly, the cost of transactions could be reduced, something always valuable when we talk about public money and bureaucracy. Secondly, transaction costs are also reduced in the process of audit since the audit itself “disappears” as a separate process, substituted by a nodal web of users functioning as a real time audit which, additionally, creates a real time accounting book which would be in the public domain. Auditing would become, for so speak, democratic. Each node of the web –potentially any citizen with a computer, or a web internal to the institution but public in its functioning– would become a public auditor validating the expenditures and helping to create the accounting book of public resources[[3]](#footnote-3). At the same time, the flow of each operation in a public office is made *traceable*, not through *ex post* scrutiny, but in real time. Every movement would be registered in the chain easing the detection of resource diversions, current or past, since the “public book” would be unmodifiable.

This is definitely a great advance towards a “cleaner” and faster public audit system, but could it in some way solve the real problem that, despite the scandalous revelation of illegal diversions of fund in current audits, that this information remains inconsequential? Technically, yes. Diversions could be made impossible trough the implementation of *smart contracts* that would limit the use of public money to ends *a priori* defined, and whose payments are subject to the accomplishment of the conditions of the contract. The system works, in this case, as a logical protocol following the principle of “if this happens, proceed to that”. When all the conditions are satisfied, a block is added to the chain, guaranteeing not only the end of the contract –i.e. the supply of the product– but also that it is done under the already specified conditions of quality and efficiency –i.e. the validity of prices, the legal recognition of the supplier, etc.

*The Walls to be Overcome*

Perhaps the main limitation to innovation is fear of change. There is still some caution against digital commerce, but every day more people are willing to enter in this market –there is, doubtless, a distributive justice problem that closes the doors of technology to millions and that must be solved as soon as possible–. Resistance of consolidated entrepreneurs to “creative destruction” is even stronger, making the pat of new ideas a hard one.

Regarding the *transparency* of public spending, the walls that rise in front of us are huge. Public administration has been bureaucratized to an extent where public offices work less following the criteria of efficiency that following an inertia in practices which make difficult any attempt to change it. This is a serious problem but not an excuse to avoid the much needed amendments. Even more problematic seems the quest for the public will to submit the use of public resources to an effective public scrutiny, but again the adversity is not an excuse but an incentive to reach the much needed *transparency* and accountability reclaimed by a true democracy.

1. It is understood by mining the process of validation through the solving of the algorithm using a system of proof of work. Computers “lend” their processing power to build the blockchain in exchange for a fraction of the “block” created during the process. Currently there are hundreds of “mining farms” with a huge processing power, which means a huge spending in electricity and also a barrier for new competition. [↑](#footnote-ref-1)
2. Auditoria Superior de la Federación [↑](#footnote-ref-2)
3. . In the case of a public chain, this can be done in exchange of a fraction of a public currency which could be use, for example, in the payment of taxes. [↑](#footnote-ref-3)