Blockchains, a technological response to the crisis of confidence

Arnaud Manas,
engineer, PhD in Economics and History, associate researcher at Université de Paris I — Sorbonne (IDHES);
& **Yoram Bosc-Haddad**,
specialist on the governance of emerging initiatives and steerage of the economy

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

Abstract:
In its canonical form, a blockchain is the refusal to accept trusted third parties to transactions — an ideological stance tainted with populism. This refusal of established institutions can partly be set down to the crisis of confidence in modern societies. Technological "solutionism", which tries to establish "trust" through algorithms without any legal or social grounds, is an illusion. Taking account of the costs and risks, using blockchains without trusted third parties has little interest outside a few fields. In contrast, their use within an established sociolegal framework by the institutions that serve as trusted third parties holds promises. Active monitoring and oversight are an indispensable for benefitting fully from blockchains.

Creating a land registry in the former "very, very democratic republic" of Gondwana, after the departure of its founding president would probably not be an easy feat. Transposing a Western sort of administration into this (imaginary) country, notorious for its corruption, would likely be a sure formula for failure. Conventional land registries are expensive, neither very efficient nor corruption-proof; and their operation tends to be opaque. Besides, they have not undergone the post-Internet technological transition.[1]

Some pundits have no doubts but that the "blockchain revolution" could solve this problem. A transparent "wikiregistry" would be set up and certified by the worldwide "community" of information technologists. It would rely on a blockchain of a canonical form with its five specified ingredients (CASEAU & SOUDOPLATOFF 2016). Gondwana would thus have a modern land registry without a state administration and without a trusted third party — all this at a low price.

Such plans — stemming from a "technological solutionism" without any real connection to social reality — risks becoming "White Elephant 2.0". The acceptance and diffusion of blockchain technology depends on confidence. Confidence (and even more so trust) cannot be demeaned to an algorithm. A mix of conventional procedures and blockchain technology is necessary to overcome the crisis of confidence in modern societies and offer new technological opportunities.

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

The “crisis of confidence” and “technological solutionism”

A blockchain — this set of cleverly put together protocols and cryptographic primitives that leans on the Internet — seems to be an ideal modern solution for building confidence. The social solutions (public notices, depositories, central banks, etc.) worked out in the past have come under criticism for two reasons: their lack of efficiency and the loss of confidence in institutions.

Admitted: established institutions are often conservative and slow to profit from technological innovations. Also admitted: this loss of confidence is quite real. Suspicion is spreading in the West, especially in France (ALGAN & CAHUC 2007). The financial meltdown in 2008 and the Snowden affair in 2013 have widened the divide between citizens-consumers and institutions: “Trust no one.”

In the wake of Bitcoin, blockchains have popped up as an alternative to discredited institutions. Being “anti-system” or “anti-establishment” falls in line with the resurgence of a form of populism. The technological response to this “crisis of confidence”, which is undermining modern societies, rests on an anarchist/libertarian rationale and on the historical fantasy of individualistic miners during the 19th-century Gold Rush. At the junction of a refusal of the state by libertarians and of a “technophile communitarianism”, blockchain technology now embodies a vision whereby the conjunction of private interests — and even vices — will produce public virtues. This vision opposes not just governments and the idea of the state representing the general interest, but also conventional procedures for building trust and for regulation by the law.

It is worth noting the parallels between several initiatives for creating currencies during the 1930s and bitcoins (or blockchains) today. In particular, the idea of a currency with a planned depreciation rate (*monnaie fondante*: see the Swiss WIR and the Austrian experiment in Wörgl)[2] along with the stamping techniques used at the time inspired the writing of a considerable body of literature. These techniques were soon forgotten after the war.

Paradoxically, the suspicion directed at individuals and institutions is now paired with confidence in computer systems and blockchain algorithms. This confidence resembles what nearly amounts to a religious belief insofar as the protocols and economics of these networks demand a leap of… comprehension. Many a spirit has made a parallel between blockchains and Facebook. Both were born on the social media where “friends” on a “network” “like” a post, thus forming an “anonymous multitude of confidence”.

In its canonical form, a blockchain is, in behalf of the general interest, intended to replace the persons or institutions who serve as trusted third parties (vested with legal rights and obligations) with an immaterial community of individuals motivated uniquely by their own interests. This approach, skirting as it does around history, is risky.

A detour via money

Fiat money is probably the social institution most dependent on trust. A currency is a slow social construction that has been put to the proof during recessions. Though relying on techniques, this legal construction is mainly grounded on the law. The technology underlying fiat money is fallible. After all, counterfeiting exists; and no technique (whether related to typesetting, the paper for printing banknotes or something else) will stop counterfeiters. However forgery remains at a socially acceptable level because of the Penal Code, which sanctions it, and the police, who track forgers.

[2] Respectively:
http://www.alpesolidaires.org/le-cercle-de-cooperation-economique-wir-une-monnaie-suisse-depuis-1934
&
http://www.alterinfo.net/L-experience-de-monnaie-fondante-de-Worgl-a-pris-fin-il-y-a-75-ans-Une-solution-pour-des-temps-de-crise_a29371.html

In contrast, bitcoins have been devised outside the state; they are grounded on a professed and unlimited confidence in technology.[3] Blind faith in technology raises the problem of responsibility. If a hacker breaches a computer network, no one is responsible; and no one is in charge of cracking down on such acts (VAN WIRDUM 2016). At this point, the formula "*Code is law*" is misleading. The growth of the Bitcoin network has been spurred by a refusal of the "system", a *dégagisme* for draining the swamp of banks and institutions.

This upsurge in suspicion and mistrust, a clear trend over the past decades, might correspond to the descending phase in the Hirschman cycle of alternating shifts between a move toward public interventions and a retreat toward the private sphere (with an increase in suspicion) (HIRSCHMAN 1982). If so, the cycle will repeat itself, and institutions will be "reinvented", vested with trust.

A last point: it is of utmost importance to avoid the pitfall of "solutionism", which starts out from the assumption that it is natural to want to use new tools as much as possible independently of their marginal utility: "To a hammer, everything looks like a nail head." The interest aroused by blockchain technology might be evidence of a solutionism that retrenches every problem to the question of finding an algorithm, even whenever a combination of social, legal and technological approaches could provide a better response.

Technology, aspirations and institutional monopolies

The crisis due to a lack confidence in institutions is, suffice it to say, feeding on three sources. First of all, the Internet is sowed with the seeds of a libertarian vision that reflects its origins in the 1960s and its moorings in California. Secondly, the institutions holding a *de jure* or *de facto* monopoly are often, despite significant improvements and modernization (*e.g.*, electronic certification), trusted third parties that are deemed to be inefficient owing to the aspirations for immediacy, transparency and peer-to-peer contacts. Paradoxically, owing to the multiplication of transactions lacking the conventional intermediaries but passing through "platforms of confidence",[4] educating digital consumers are learning to take risks (when the perceived value seems to justify it and when the comments posted on the platform are generally favorable).

The crisis of confidence and the hope for high profits have sowed the seeds for a proliferation of companies, projects and investments that try to find blockchain solutions for customer-to-customer (C2C) transactions and even business-to-business (B2B) operations… and why not X2Y2Z? A situation like the 1990s dot.com bubble is probable. At the very least, 80% of start-ups in blockchain technology are going to burst.[5] In my opinion however, exaptations — in Darwinian theory: a trait that initially brought an advantage and continues to exist but for another purpose — is a more likely scenario than stillbirths or extinction.

[3] The *a priori* conception of social constructions is risky (HAYEK 1953).

[4] The archetypes of these platforms are BlaBlacar and Airbnb. Note, too, that Airbnb or eBay with their rating systems have done nothing less than resume and modernize the former technology for building trust (*i.e.*, letters of recommendation). Likewise, a parallel can be made between blockchains and the successive endorsements on a single financial instrument that transfer ownership and liability.

[5] See the remarks by W. Mougayar on:
http://www.ibtimes.co.uk/ethereums-william-mougayar-successful-ico-not-indicative-success-ico-1607859

Blockchain techniques and plausible prospects

Constraints — vulnerability, the computational power needed, the energy needed, the absence of governance and negative consequences on employment (TAPSCOTT 2016) — are, I think, going to limit the number of "real" blockchains to a very few cases, often on the borderline of legality. However I also think that the components of blockchain technology are eventually going to be used on a large scale to reconstruct the "infrastructure" for transactions and exchanges at a low cost but with a much higher performance in terms of: *a)* automation, *e.g.*, as a transfer agent for fund shares (SCHAFROTH 2017) or letters of credit; *b)* the latency time for recording a transaction, ranging from a few months nowadays for public notices of real estate transactions to a few milliseconds tomorrow thanks to automated contracts; and even more *c)* immediate, transparent access to certified information.

If we pay no heed to this creative business or, worse yet, try to stymie it, we run the risk of missing the high potential for innovation inherent in a blockchain's technological components. This is how I see, for example, Hyperledger (Linux Foundation) and Ethereum.

Between the historical trusted third parties (slow, opaque and inefficient) and the anonymous distributed contraptions on the dark web, there is room for "reinvented" trusted third parties. Consortiums will probably propose mixed solutions, similar to what happened in payment systems but, this time, without centralized operators (the problem of the trusted third party being approached from a different angle) but with open, transparent solutions (like Blablacar's or Airbnb's in the hotel and transportation businesses).

However the pace for developing viable business models still seems highly uncertain.

The outlook for established institutions, platforms and start-ups (that want to last)

Given this environment, extreme strategies carry high risks for all players:

- Wait-and-see means taking the risk of overlooking a real disruption or of making massive investments in an infrastructure that might suddenly collapse in value.
- Betting everything on blockchains means adding technological onto financial risks (except, of course, for the "lean start-ups" and their investors who intend to sell out fast to an institutional consortium).

Looking toward the future, we should be equipping ourselves for, on the one hand, actively monitoring this new technology in order to obtain an in-depth understanding of it and, on the other hand, learning through focused, reiterative experiments to cope with a real, changing world. For institutions, this means responding to the demand for transparency and speed by adopting hedging strategies for controlling (if possible) problems looming at weak points. For the start-ups that want to last, it is important to consolidate their core activity as suppliers of the bricks of technological know-how or as the designers/developers of new uses. And for everyone, it is essential to be supportive of the creation of consortiums, for conducting experiments and tests, and of vertical incubators, the crucibles for emulation and for improving know-how about the uses of blockchain technology.

Conclusion

To Jean-Paul Delahaye (2016:40) musings: *"Imagine […] a very big book that everyone can read freely and for free, where everyone can write but that cannot be modified or destroyed,"* we add: "Imagine the keepers of the book, the depositories of the general interest, who are responsible before the law and before society, who are in charge of interpreting rules." To sustain this new musing, I would like to point out that forgery in bookkeeping and notarial activities carries a sanction of ten years imprisonment, compared with three years for "ordinary" fakes. Believing that algorithms will regulate everything is an illusion: legal expertise and responsibility are necessary to the "depositories of confidence". Must we make the choice between an "old-fashioned" trusted party and the "new-fangled", computerized blockchains that rely on an immaterial, anonymous community? By combining the technology of the signed, transparent registry accessible for free with "confidence" in individuals or institutions, the best of the two worlds is possible.

Let us take leave of the starched cuffs, the jealously kept ledgers and, too, the ideological refusal of trusted third parties. Let us be ready to create concepts and forms of technology that combine social trust and algorithmic confidence for the realization, with electronic signatures, of horizontal, transparent distributed systems that are fully responsible and that operate at the speed of the Internet.

References

CASEAU Y. & SOUDOPLATOFF S., "La blockchain, ou la confiance distribuée", 52p. Fondapol.org, June 2016. Available at: www.fondapol.org/wp-content/uploads/2016/06/083-SOUDOPLATOF-2016-05-26-webDEF.pdf

ALGAN Y. & CAHUC P., *La société de défiance: comment le modèle social français s'autodétruit*, 103p. (Paris: Éditions Rue d'Ulm/Presses de l'ÉNS) 2007. Available at: www.cepremap.fr/depot/opus/OPUS09.pdf

DELAHAYE J.P., "Les blockchains, clé d'un nouveau monde", pp.40-48 in his book *Mathématiques et mystères* (Paris: Belin) 2016.

HAYEK F. von, *Scientisme et sciences sociales* (Paris: Plon) 1953. [Translated from *Scientism and the study of society*].

HIRSCHMAN A., *Bonheur privé, action publique* (Paris: Fayard), 1983 [Translation of *Shifting involvements: private interest and public action* (Princeton, N.J.: Princeton University Press) 1982].

SCHAFROTH E., "La blockchain s'invite dans la gestion d'actif", *Les Échos*, 4 April 2017.

TAPSCOTT, D. "How blockchains could change the world", May 2016. Consultable at: https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world

WIRDUM, A. van, "Rejecting today's hard fork, the Ethereum Classic Project continues on the original chain: Here's why", *Bitcoinmagazine* 20 July 2016. Consultable at: https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808/