Digital technology, confidence and trust

Henri Isaac,
Paris-Dauphine University, PSL

Abstract:
The digital universe has developed so rapidly that the issues of confidence and trust might seem secondary. As uses diversify however, behaviors (fraud, identity theft, cyberstalking) are eroding confidence in this space. Questions also crop up owing to the massive collection of personal data by digital services, while cybercrime and state surveillance are hampering trust and confidence on line. How to produce and sustain trust and confidence in cyberspace? The initial means used imitate traditional trust mechanisms, but the digital universe has gradually produced its own mechanisms for generating and managing trust that are based on its characteristics, network organization and data processing. Consequently, the trusted third party, whatever its architectural modality, has come under question, whence the idea of a network architecture that, by design, generates trust in transactions.

The digital realm has grown at such a speed and intensity that questions about confidence or trust might seem out of place. As early as 2004 however, France transposed the EU directive on e-commerce into its national law under the name "*law for confidence in the digital economy*" (the LCEN Act), thus pointing to issues related to trust in the digital realm. Beyond the question of commercial transactions, such issues also arise in relation to the proliferation of contents posted by users and, along with them, of fake news. Users' behaviors lessen confidence on line: scams, identity theft, harassment…. In addition, the massive collection of personal data by so many online services raises questions, while various risks — cybercriminality, government surveillance of communications — deter the development of confidence on line.[1]

For these reasons, serious questions about confidence, about how to produce and sustain it, have cropped up in cyberspace. At its start, the Internet, a universe of pure confidence, had to set up several means and arrangements for creating confidence and facilitating uses. Although these arrangements imitated the classical procedures worked out in the physical world, the digital ream would gradually produce its own means for generating and managing confidence, means grounded in its very nature: data processing and its network architecture.

The classical solution of a trusted third party, in whatever form, has become problematic, whence the idea that the network architecture, by design, in and of itself, can generate confidence in transactions.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in June 2021.

The many aspects of confidence and trust during the digital age

The problem of confidence in technology is not new (TADDEO 2009). Confidence in robots, for example, has been widely studied (COECKELBERGH 2010). However confidence during the digital age is not restricted to our relations with machines. It extends to the confidence in devices and arrangements that mix technological solutions and human behaviors, as made possible by distributed technological infrastructures on a worldwide scale.

The digital realm is a space of both information and commercial transactions, a place where players with criminal intent engage in attacks and acts of piracy, and where governments pursue strategies of surveillance (as highlighted by disclosures during the Snowden affair). To build confidence on line, several issues must, therefore, be addressed.

● Confidence in transactions: With the development of online commerce, questions have arisen about the security of dematerialized transactions. Professional circles, such as the networks that use Electronic Data Interchange (EDI),[2] have devoted serious thought to this question. Nonetheless, turning the Web into a marketplace soon raised the question of how much confidence users would place in websites and the transactions occurring on them. Given the impossibility of deploying solutions based on electronic certificates among the general public, the number of fraudulent actions in online transactions shot up. This led many potential customers to refrain from e-commerce for several years. Over the past decade however, the rate of fraud in online payments has steadily decreased. For French banking cards, it was 0.167% in 2019 (OSME 2020). Nowadays, 62% of the French make purchases on line (CREDO 2019). The issue of security still hampers the development of online transactions however.

● Confidence in online contents: The proliferation of social media platforms has been conducive to the production and circulation of false "information". Governments have used these platforms to undertake disinformation campaigns. This situation has led users worldwide to have less confidence in online news than traditional news services. In a survey by the Reuters Institute in 2020, 56% of persons were concerned about the veracity of the information published on social networks — up to 84% in Brazil and 67% in the United States. Furthermore, only 26% placed confidence in the social media for news in comparison with 59% for the traditional media. The exposure to toxic contents (hate speech, terrorism, pedopornography, prostitution) has lessened users' confidence in the services provided by the social networks.

● Confidence in how data are collected and used: Digital services rely heavily on the processing of data, in particular personal data. Although the legal framework for processing personal data has been bolstered in Europe, some online services still massively collect personal data, we are forced to admit, for purposes that are not transparent or are unknown to users. A typical example is the third-party cookies collected on websites for advertising purposes; this sort of data collection arouses suspicion about its finality. Questions about the purpose of collecting data are very much on the minds of French users of the Internet: 76% of them in 2019 (ODOXA 2019). Furthermore, this massive collecting of data exposes users to the risk that their data will be leaked owing to insufficient protection and security measures when the data are stored. Leaks are a real concern to all categories of the population (RAHAL 2019), and the tendency is for them to occur more frequently.

[2] Exchange of structured information via automatic messages between two entities, machine-to-machine (https://fr.wikipedia.org/wiki/Échange_de_données_informatisé).

- SURVEILLANCE, CYBERSECURITY AND CONFIDENCE ON LINE: Given the gradual, constant migration of interactions, whether commercial or not, toward Internet platforms, the latter are exercising, in the opinions of many experts, a *de facto* surveillance of our comportment and actions. They can manipulate our choices of contents as well as individual decisions and behaviors (ZUBOFF 2019). This vision of the organization of digital society has led some users to shun websites lest they be tracked or traced by these platforms, by devices such as the cameras installed in computers, smartphones or voice command devices (CLAUSER 2019). Besides, the surveillance of cyberspace is not being done just to analyze patterns of purchases or consumption. It is also done by governments and their intelligence services. Snowden's (2019) revelations have let us glimpse the scope of state surveillance of electronic communications, and fostered a widespread suspicion that has lowered confidence in cyberspace.

In a "post-Snowden" world, cyberspace has become a place of geopolitical clashes, as attacks with increasing sophistication escalate against economic interests for the purpose of extorting funds as well as against public institutions, such as hospitals and election systems. In a world that fully shifted to digital technology during the pandemic, these attacks are ordeals for security systems, testing how resilient or robust they are. They also gauge the degree of confidence that we can place in these systems.

Confidence-building on line: From trusted third parties to the network as an infrastructure of confidence

To build up confidence in online services, several arrangements have been borrowed from classical methods for doing so. The idea of a trusted third party was soon introduced; but as the Web has grown, this idea has been reworked to take account of procedures specific to virtual transactions. The emergence of blockchain protocols has pushed the rationale of a network architecture even farther: the network itself becomes the trusted third party.

The usual methods of confidence-building

In a world of physical transactions, confidence hinges on several institutional arrangements, *e.g.*, labels, brand names and reputation (TADELIS 2015). These arrangements have been adopted in cyberspace. Online commerce had to develop such arrangements in order to reassure cybernauts who had been hesitant for a long time about making purchases on line (RATNASINGHAM 1998). Several "labels" have been created (TrustedShop, Fevad, etc.), including for payments (VeriSign, Trusted). Brand names also serve as an indicator of confidence. While the brand name is undeniably a factor in confidence for passing an order on line, the name is not, by itself, a warranty. After all, the quality of execution of the order and the supply chain are crucial factors in the confidence that will be placed in an e-business website. Some businesses have clearly understood how important this is to confidence-building. Nevertheless, these usual arrangements are not safeguards for online transactions.

Adapting the trusted third party to the digital age

Given the absence of digital identification, the idea of a trusted third party — a classical institutional method that vouches for the identities of the parties to a transaction and their integrity — has been introduced in cyberspace in the form of the electronic certificates delivered by a third party to the parties to a transaction. This procedure has been rolled out for business-to-business transactions (B2B), but has failed to develop for business-to-customer (B2C) or customer-to-customer (C2C) transactions because it is too technically complicated for nonprofessionals.

Consequently, several methods have been invented for boosting the confidence of end users in online transactions. One is customer reviews of products or services. Once organized, structured and highlighted, evaluations by the "crowd" and "likes" by customers are a powerful tool for building confidence. Business models have been built around customer reviews (*e.g.*, Tripadvisor in travel services or La Fourchette for restaurants). Since these arrangements for shoring up online confidence (UTZ *et al*. 2012) might be malevolently hijacked however,[3] regulatory authorities have set specific conditions for customer reviews.

For the services of what has been called the "sharing economy", it is necessary to have confidence in, for example, an unknown driver from a ride-sharing service (MAZZELA *et al*. 2016, MÖHLMANN 2016) or an unknown who is renting out his house (HAWLITSCHEK *et al*. 2016). In this case, the platform has the role of the trusted third party. It provides the infrastructure for transactions. Through its listing/delisting operations, it selects who will be interacting, verifies their identities, organizes customer reviews and thus, builds up confidence (ISAAC 2021). Regardless of its efficiency, such a centralized system encounters several limits. Customer reviews can be skewed; and fake opinions, posted. However tight controls might be, fraud is always lurking around these "sharing" platforms.

For this reason, it is necessary to move beyond the system of confidence centralized in a platform. Alternatives have emerged.

Blockchains: The network as a warranty of confidence

In the case of a blockchain, the trusted third party is the system itself (WERBACH 2018). Each distributed element on a blockchain contains what is needed to guarantee (via a cryptographic algorithm) the integrity of the data exchanged. A blockchain is a distributed database that stores and transmits information sent by users. Links within this database are verified and grouped at regular intervals into blocks, which form a chain. A chain of blocks thus corresponds to a list of records protected (by the storage nodes) against falsification or modification. In this regard, a blockchain is a secure, distributed ledger of all the transactions made since its launching. By becoming the trusted third party, this system trims the costs of transactions conducted on the blockchain. Unlike contracts, blockchains are not grounded on a legal system for upholding agreements; and unlike norms in human relations, they do not require confidence or direct relations between the parties involved (LUMINEAU *et al*. 2020).

[3] https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/faux-avis-consommateurs-sur-internet

An architecture of this sort responds, in part, to the issue of confidence in digital transactions. It provides a robust infrastructure for transactions, a complete traceability of transactions and full transparency for those involved. Consequently, this sort of system is often seen as a response to the many limitations on confidence in cyberspace. While we see the interest of this arrangement for commercial transactions, an infrastructure of this sort does not at all increase confidence in other sorts of digital contents (in particular fake news). It is incapable of confirming or denying the veracity of a piece of information. Nor does it address questions about government surveillance of online activities.

Cyberspace is still a place where confidence-building is an ongoing challenge. Technology by itself seldom provides adequate responses for building a robust framework for confidence.

References

CLAUSER G. (2019) "Amazon's Alexa never stops listening to you. Should you worry?", *New York Times*, 8 August, available at https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/.

COECKELBERGH M. (2010) "Humans, animals, and robots: A phenomenological approach to human-robot relations", *International Journal of Social Robotics*, 3(2), pp. 197-204.

CREDOC (2019) *Baromètre du numérique 2019. Enquête sur la diffusion des technologies de l'information et de la communication dans la société française* (Paris: CREDOC), 256p., available via https://www.arcep.fr/uploads/tx_gspublication/rapport-barometre-num-2019.pdf.

HAWLITSCHEK F., TEUBNER T. & WEINHARDT C. (2016) "Trust in the sharing economy", *Die Unternehmung – Swiss Journal of Business Research and Practice*, 70(1), pp. 26-44.

ISAAC H. (2021) *Les business models de plateforme* (Paris: Vuibert).

LUMINEAU F., WANG W. & SCHILKE O. (2020) "Blockchain governance – A new way of organizing collaborations?", *Organization Science*, 9 October, available at https://doi.org/10.1287/orsc.2020.1379.

MAZZELLA F., SUNDARARAJAN A., D'ESPOUS V. & MÖHLMANN M. (2016) "How digital trust powers the sharing economy", *IESE Insight*, 30, pp. 24-30.

MÖHLMANN M. (2016) "Sharing economy: Building trust in P2P online marketplaces", paper presented at the *New York Computer Science and Economics Day*, available at https://www.researchgate.net/publication/308631709_Sharing_Economy_Building_Trust_in_P2P_Online_Marketplaces.

ODOXA (2019) "Données personnelles. Les Français se disent préoccupés par leur utilisation mais ne se prémunissent pas toujours", public opinion survey, available at http://www.odoxa.fr/sondage/donnees-personnelles-francais-se-disent-preoccupes-utilisation-ne-se-premunissent-toujours/.

OSMP [Observatoire de la Sécurité des Moyens de Paiement] (2020) *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2019* (Paris: Banque de France) 82p, available via https://www.banque-france.fr/sites/default/files/medias/documents/820124_osmp2019_web_vf.pdf.

RAHAL A. (2019) "Five data breaches to understand the importance of data security", *Cisomag*, 29 May, available at https://cisomag.eccouncil.org/5-data-breaches-to-understand-the-importance-of-data-security/

RATNASINGHAM P. (1998) "The importance of trust in electronic commerce", *Internet Research*, 8(4), pp. 313-321.

SNOWDEN E. (2019) *Permanent Record* (New York: Metropolitan Books); French translation by É. Menanteau & A. Blanchard (2019) *Mémoires vives* (Paris: Le Seuil).

TADELIS S. (2015) "The economics of reputation and feedback systems in e-commerce marketplaces", *IEEE Internet Computing*, 20(1), DOI: 10.1109/MIC.2015.140, available via http://faculty.haas.berkeley.edu/stadelis/Annual_Review_Tadelis.pdf.

TADDEO M. (2009) "Defining trust and e-trust: Old theories and new problems", *International Journal of Technology and Human Interaction*, 5(2), pp. 23-35.

UTZ S., KERKHOF P. & VAN DEN BOS J. (2012) "Consumers rule: How consumer reviews influence perceived trustworthiness of online stores", *Electronic Commerce Research and Applications*, 11, pp. 49-58.

WERBACH K.D. (2018) "Trust but verify: Why the blockchain needs the law", *Berkeley Technology Law Journal*, 489, 64p., available at https://ssrn.com/abstract=2844409.

ZUBOFF S. (2019) *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs).