Chapter 5
Design and Dissemination of Blockchain Technologies: The Challenge of Privacy

Cécile Caron

Abstract Presented as trust technologies, blockchains, by allowing immediate secure peer-to-peer exchanges without a trusted third party, have strong disruptive potential, but raise privacy issues. We illustrate some challenges that this antagonism raises and the sociotechnical compromises made to overcome them, by analysing the design of a mobility service by a consortium of some fifteen operators, and its experimentation with the employees of these operators. The service seeks to respond to the new needs linked to the electrification of company fleets, by tracking the recharging of (personal) electric vehicles at work or (professional) vehicles at home with a view to reimbursing employees' professional expenses by relying on a blockchain. Privacy management is a skill, based on emerging expertise, distributed across a range of professions and users, which requires compromises between different conceptions of technology and data to be guaranteed. For blockchain designers, these compromises have limited the disruptive potential of blockchain technology by recentralising data management and losing the open nature of blockchain. However, in the eyes of other designers and users, they have allowed unexpected uses and benefits to emerge, such as reinforcing the choice of blockchain technology as a "*privacy solution*".

Keywords Blockchain · Privacy

Blockchain is a technology for storing and sharing information, based on the recording of data in the form of blocks linked to each other in the chronological order of their validation, making it possible to certify with certainty the date of the transaction. These blocks are processed in a decentralised manner and are protected by cryptographic methods. Each piece of data deposited in the blockchain is verified by intermediaries (the "miners") according to a precise protocol. The infrastructure is thus distributed within a network ("distributed ledger technology"), which makes it possible to do without a trusted third party when a transaction is carried out. In the

C. Caron (✉)
EDF Lab, Paris, France
e-mail: cecile.caron@edf.fr

J.-C. Le Coze and S. Antonsen (eds.), *Safety in the Digital Age*,
SpringerBriefs in Safety Management,
https://doi.org/10.1007/978-3-031-32633-2_5

context of the energy transition, FinTech blockchain technologies are seen as likely to be disruptive innovations for the energy sector. By allowing secure, immediate and almost free of charge peer-to-peer exchanges without the intermediary of a trusted third party, blockchains have strong disruptive potential [29] for tracking and transferring assets or for executing *smart contracts* (autonomous programs that automatically execute the terms and conditions of a contract, without human intervention).

However, they are controversial, especially in terms of privacy [17]. Indeed, if blockchains offer sufficient guarantees that no external attack can access personal information [20] and allow "*respect for privacy through the proactive use of cryptography"* [27], they raise questions of compliance with the European General Data Protection Regulation (GDPR) around the adequate processing of personal data [11], but also in terms of responsibility and explicability. The GDPR requirement to specify a data controller when processing personal data is incompatible with the decentralised operation of the blockchain. The right granted to users to delete and modify their personal data conflicts with the immutability of the registry, while the requirement of explicability is difficult to apply to the implementation of complex cryptographic algorithms.

Blockchains and the GDPR constitute two relatively antagonistic proposals for trust models. The principles of blockchain were conceived in the context of a crisis of confidence in institutions, particularly banks [2]. Gathered in the Bitcoin white paper [25], they combine a series of technical and social properties (trust and distributed consensus, infallibility and auditability of the register) which are similar to a proposal for trust in an "expert system" characteristic of modernity [16]: trust is no longer placed in a person, but in a system. For Giddens, our modern, anonymous, highly complex and functionally differentiated society has led to a radical transformation of the status of trust: social order is no longer based solely on familiarity and personal trust but also on trust in abstract systems. In contrast (see Table 5.1), the GDPR reflects a conception of trust as the "empire of the third party" [21], with primary social relations coming under the aegis of the instituted third party (as authority in a third-party position and as internalisation of the condition of a legal subject).

These issues of regulatory compliance are accentuated by the emergence of a growing concern among users about the protection of their privacy [24]. "In the vein of "surveillance studies" [5], a body of work argues that the increase in technological capabilities [has] broken down the boundaries that protect us from an Orwellian world" [8]. The technologisation of surveillance is said to be a constant threat to individual freedoms and privacy. Other approaches link the end of privacy to the very extension of the norms of authenticity and the public sphere that are derived from it, which reduces the possibilities of preserving one's freedom behind social roles that deliver the self to the "tyrannies of intimacy" [31]. While departing from this hypothesis of the "end of privacy", recent work associated with the emergence of surveillance capitalism [30] or with the analysis of social and digital practices attests to profound changes both in societies' perception of privacy and in the articulations between its different components [4, 9, 23]. The work on privacy reflects the plurality of dimensions that it incorporates. It is a right, notably to tranquillity [28], a commodity that although contested can be commensurable and exchangeable [6];

Table 5.1 Summary of the principles underlying trust in blockchains and in systems concerned by the GDPR

Principles of blockchains			Principles of GDPR	
Principles	Expression		Principles	Expression
Decentralization	Public (without third parties), private (with a central entity) or semi-private (consortium) blockchains	versus	Accountability of processing	Appointment of a Data Protection Officer and maintenance of a register of processing operations and purpose limitation
Transparency	Unforgeable history of all transactions and anonymity	versus	Protection on of personal data	Collection of consent if no legal basis, minimisation of data and their retention, exercise of rights (to information, to erasure, to correction)
Security	Cryptographic algorithms and secure transmission protocols	versus	Explicability	Transparency of algorithms
Trust in "expert systems" [16]		versus	Trust in "the empire of the third-party" [21]	

a state that allows personal spaces to be preserved from the intrusion of others by reserving access to limited groups of people [32], a capacity to manage social capital in a negotiated form [10] and a capacity for control [4]. All of these dimensions are affected by major technological, regulatory and societal developments that interact and generate vulnerability for individuals, but also for organisations, in terms of privacy management [24, 4, 33).

In a context where privacy issues, from a regulatory and societal point of view, impact the design and use of emerging technologies such as blockchain, this chapter analyses the way in which the actors involved in the design and experimentation of a service deal with these tensions between blockchain and privacy.

To do this, we will study a use case, the design and experimentation of a mobility service based on a blockchain. The service seeks to respond to new needs linked to the electrification of corporate fleets, by tracking the recharging of (personal) electric vehicles at work or (professional) vehicles at home with a view to reimbursing employees' expenses. Indeed, the electrification of business fleets implies a change in the business model. Whereas the management of a combustion car fleet is based on a "just-in-time" model (employees have a petrol card or are reimbursed for mileage allowances), the management of an electric fleet is based on an "anticipatory" model which requires that the cars be sufficiently charged at the time of departure to make the journey. Recharging takes place either at the workplace or at the employee's home, and the cost of recharging is passed on to the energy bill at the workplace or at home. It is difficult to distinguish the cost of recharging on bills that aggregate a range of uses and therefore for employers to reimburse or charge for the cost of recharging.

This service combines several technologies to meet this new need for tracing and certifying electric car recharges:

- a blockchain that allows validated charges to be written and information to be stored in a secure and reliable manner;
- communicating objects (IoT) installed in the vehicles;
- a mobile application for employees allowing them to declare the start and end of the vehicle's charge and authorise the cross-referencing of this information with electricity consumption data from the Linky meter (which certifies to the employer the existence of the home charging);
- a web application that allows company managers to monitor recharging.

We will mobilise the results of a survey carried out between November 2020 and January 2021 in the Nantes region of France, concerning the design of this mobility service by a consortium of some 15 operators from three main activity sectors: transport, energy and new technologies, and its experimentation with the employees of these operators.

The survey was carried out in two phases:

- interviews with a dozen designers of the service belonging to the various companies in the consortium (from the world of new technologies, mainly blockchain specialists; from the world of energy, electricity suppliers and distributors; from the world of mobility, transport companies);
- interviews with a dozen or so experimenters of the service (employees of the consortium companies testing the service).

This hybrid collective coalescing around new technologies will be confronted with the issue of privacy. How have the designers dealt with the blockchain's compliance with regulations protecting privacy? Have privacy issues undermined the ways in which trust in the service is built? More generally, has the trajectory of diffusion of blockchain technology been affected by the options chosen?

We will show that the issue of privacy protection gives rise to a series of "tests" in the sense of the sociotechnical approach to innovation [1] which will punctuate the "trajectory" [26] of the service's design and experimentation. These tests give rise to confrontations between actors (on the way they envisage privacy and the use of technologies),but also, to negotiations and new alliances that enable the tensions between privacy and blockchains to be resolved. Here we can observe the social dynamics and normative mediations that run through the trajectories of innovations [3], but these contribute to shaping sociotechnical compromises that are able to articulate the regulatory and acceptability requirements of privacy protection with the particularities of the technology. These compromises are made at the cost of reducing the initial promises associated with the blockchain technology studied here, but allow the emergence of solutions that are the subject of consensus within the consortium of actors. In a first part we will study the way in which the actors, here the developers, manage to define a governance mechanism that meets the GDPR obligations concerning responsibility. Then, in a second part, we will study the solutions found around the management of personal data. Finally, in the last part, we will discuss the challenges that security and explicability represent for this group of actors.

5.1 A First Privacy Test: Defining Governance

Among the general obligations of the GDPR, as soon as the presence of personal data is identified, is the identification of a data controller. This obligation is not self-evident, especially when it comes to blockchain technology. Indeed, blockchain mobilises a series of actors around the data. For example, the "miners" (who validate transactions and create blocks by applying the rules of the blockchain), especially on public blockchains (where anyone can carry out a transaction, participate in the block validation process or obtain a copy of the blockchain) could, in a completely decentralised system, be qualified as a data controller. Nevertheless, the recommendations of the French data protection agency CNIL (2018) on how to define the data controller on the blockchain indicate that "participants, who have a right to write on the chain and decide to submit data to be validated by miners can be considered as data controllers". Despite this indication, the question of how to define a controller has challenged the consortium.

5.1.1 The Appointment of a Controller, a "Test" for the Consortium

This first test concerns above all the world of service design; this world of designers is shared between designers from the digital, electrical and mobility sectors who have joined forces to design this service for tracking the recharging of electric vehicles based on a blockchain. These designers include a range of blockchain specialists from start-ups and large companies who have joined forces in a consortium.

The consortium members initially had a technical reading of the problem of processing responsibility, imagining that start-ups specialising in blockchain technology would take on this role in data governance. The "privacy" deliverable entrusted to one of the consortium's start-ups specialising in blockchain was thought to be a way of delegating the management of the issue to someone specialising in the technology.

> What organisation do we want in terms of GDPR? Who is the controller?" And there, no one raised their hand, whereas we thought it was going to be the start-ups or the software developers. (Designer, electricity sector)

Nevertheless, the lawyers of the large companies participating in the consortium will, in accordance with the recommendations of the CNIL, redirect the responsibility for the processing to the companies that designed the service, rather than to the start-ups, which occupy a position of “subcontractor” within the consortium. The definition of governance puts the consortium to the test, on the one hand because it forces a hierarchy of roles among the members of the consortium who could previously think of themselves as equal partners, and on the other hand because it requires one of the members of the consortium to take responsibility for the processing of the data and run the risk of a penalty (which could potentially be as high as 20 million euros or 4% of the annual worldwide turnover).

> And sometimes this is not necessarily obvious. When there are projects where the stakeholders are somewhat intertwined, to determine who is really responsible for processing, who is a subcontractor, to see if there are potentially cases of joint responsibility, i.e., the parties determine together the purposes and means of processing. And this, all this governance of the GDPR, is not necessarily very simple to apply to a technology such as blockchain either. (Lawyer, electricity sector)

5.1.2 A Form of Recentralisation Contrary to the Imagination of Blockchain Designers

The definition of a data controller thus introduces a form of recentralisation of the consortium’s operations by attributing responsibility for processing to one of its members. Responsibility is no longer shared equally among all the members of the consortium, which clashes with the sociotechnical conception [13] associated with the technology by the blockchain designers [7]. Its inventors “*trace or dream of a network and a community operating without intermediaries, claiming a desire for anonymity and total security of transactions*” [15]. The blockchain designers we interviewed testify to this shared ethic with libertarian roots. They see blockchain as a technology that can enable unmediated exchange within a horizontal society and thus forms of democratic administration independent of unrepresentative or failing centralised institutions.

This attachment to decentralised forms of organisation leads them to prefer public blockchains to consortium or private blockchains, which restrict the use of the technology to a small, closed community and hinder its wide dissemination. They regret the choice of creating a consortium blockchain, preferred to a public blockchain by designers from the electricity and mobility sectors, unfamiliar with blockchain and worried about the negative images associated with the technology (particularly with regard to bitcoin in terms of money laundering and energy sobriety) and anxious to keep control of the service being designed.

> For me, when I came into this subject, I said to myself, and I think I’m not the only one who said it to myself, we tried to put blockchain where it wasn’t necessarily needed. For me, the pure blockchain use case would be the one that could not be replaced by a centralised system. (Blockchain designer, IT department, Energy World)

The choice of relying on blockchain was not made by the service designers solely on the basis of the technology’s properties, but because this technology, which is perceived as having value, attracts public funding (in this case, a call for projects financed by future innovation programmes), which supports innovation on a territorial scale. Blockchain designers believe that the use case does not necessarily lend itself to the use of a blockchain; while other designers are unfamiliar with the properties and promises of the technology.

5.1.3 The Compromise of Choosing the Consortium Blockchain

The designation of a data controller within the consortium, in compliance with the requirements of the GDPR, reinforces in the eyes of blockchain designers the compromise that the choice to create a consortium blockchain represented. It contributes to foregoing the disruptive promise of a perfectly decentralised technology. Nevertheless, the experimentation will displace these representations of the technology to validate its contributions in the eyes of the service designers. On the one hand, blockchain is less costly than managing a centralised platform, mobilising teleoperators who supervise the management of information, which lends credibility to the economic model of the service (which is of little value, since it concerns small transactions, the cost of an electric recharge being low). On the other hand, consortium blockchain appears to be a way of securing data storage and guaranteeing trust within a consortium of various partners.

While the blockchain designers keep the public and decentralised blockchain as their horizon, the other service designers rally around the technology on the basis of its restricted nature, limited to the consortium, and on the classic governance modalities that are associated with data management. The blockchain, backed by the requirements, appears to all the designers of the service as a technique allowing interoperability and guaranteeing compliance.

5.2 Second Privacy Test: Management of Personal Data

The governance and responsibility for processing aims to ensure that personal data is properly handled. Around this service, a large amount of data can be qualified as personal data.

> Personal data is anything that can be linked, directly or indirectly, to a natural person. In the context of the service, this can be, for example, a number plate, an IP (Internet Protocol) address, a telephone number, an e-mail address, a surname, a first name, an identification number, I don’t know, a contract number, for example, for someone who has an electricity contract, that sort of thing. So, this goes very far, i.e., in practice, there is an enormous amount of information that can be qualified as personal data. For example, the load curve of someone, of a customer, of an individual, is personal data, i.e., it is an imprint of his electricity consumption. It is linked to a natural person. (Lawyer, energy sector)

The GDPR aims to guarantee the right to information, deletion, correction and portability of data to those whose data are collected and processed. As we have already mentioned, these rights are difficult to apply on a blockchain because of the immutable nature of the register and the impossibility of deleting what is written on the blockchain.

The designers have resolved this intrinsic contradiction in two ways. On the one hand, by setting up an off-chain storage system, i.e., a data management system independent of the blockchain, and on the other hand by seeking to "minimise" the data that will be registered on the blockchain so that it can no longer be qualified as personal data.

5.2.1 Setting up an Off-Chain System to Store the Data

The implementation of an "off-chain" management system emerged as a compromise solution that was the subject of a form of consensus among the designers of the service. They agree on the practice of not recording personal data on the blockchain, which allows GDPR compliance. This obligation leads to the use of servers, in addition to the blockchain, to manage off-chain personal data.

Designers from the energy and mobility sectors saw this as an opportunity to adhere to a strict legal framework and to curb challenges associated with energy data [12] or geolocation data that informs on user behaviour.

> We must not forget that we are under the spotlight and that although it is an experiment, we are never safe. We know that Linky is a really sensitive subject for the media. And today, the CNIL is not very favourable. It finds that everything that is blockchain is not necessarily protective of personal data. So we have been very vigilant in trying to be as protective as possible. (Designer, energy sector).

But this solution is also valued by blockchain designers because it allows the open nature of the blockchain to be preserved in part and its potential transfer, at a later stage (when the service is industrialised), to a public blockchain. Blockchain designers are distinguished by a very specific conception of the processing of personal data in line with the libertarian ethics that guide their representation of "privacy". They want to allow people to keep control of their data. They anchor this vision in a conception of private property as a property of the self [14] which, when extended to data, and in particular personal data, proclaims the right of each person to dispose of it for themselves. In line with this reading, blockchain technology should make it possible, via the establishment of exchanges between peers, to avoid the constitution of economic monopolies and the capture of the value of data by digital companies. For them, surveillance capitalism [30] is the antimodel that blockchain technology should make it possible to thwart.

Nevertheless, this solution, which articulates blockchain with a classical off-chain data management system, is not optimal in their eyes. They also recommend algorithmic solutions to preserve confidentiality, such as Zero Knowledge Proof methods, referring to their belief in the neutrality of the technology. The algorithmic authority and automation of processes contained in the technology are perceived as guarantees of objectivity. The representations of blockchain actors are therefore part of a form of technical solutionism; they intend to solve the problems of trust in a market through technical solutions. Thus, blockchain designers demonstrate a professional culture that aggregates values, representations and practices specific to the worlds of design [18]. These also shape their reading of privacy.

5.2.2 Data Minimisation

The second direction chosen to manage personal data was to strongly minimise the data recorded on the blockchain. In particular, the charging curves (which, when cross-referenced with the user's charging declaration, certify the existence of a charge) are stored in an off-chain system to comply with the GDPR. Only the duration of the recharge has been recorded in the blockchain, as the duration is not considered as personal data, given that a person cannot be identified from this information alone.

This desire to minimise the data retained for legal reasons allowed the conditions of acceptability by the final users to be considered. Thus, the employees involved in the experiment did not wish to show their employers their recharging hours or to be geolocated (two options that were retained at the start of the experiment). Indeed, this data could inform their employer about their presence at home or their travels; but they see no problem in transmitting the charging times via the service. The blockchain set-up provides "privacy by design" in accordance with the users' reading of it; however, it does not meet the ambition of the blockchain designers to keep the data as close to its owner as possible. The experimentation has made it possible to articulate compliance and acceptability by considering the notion of privacy that users have.

5.3 Third Privacy Test: A User Pathway Tested for Explicability and Security

5.3.1 Three Requests for Consent

The demands of compliance with privacy legislation gave the lawyers a major role in the design of the experiment. The latter argued for a strict, even extensive application of the GDPR by requiring multiple consent requests: via the signature of an experimentation agreement, via the customer management applications authorising access to Linky meter data and via the mobile application during each recharge declaration by the employee.

> "In the end, all that was put in was very classic GDPR. Basically, nothing was created or invented." There, for example, on the application, we told them that they had to tick "I accept"; but inevitably we're also going to make them sign a little paper in which they actually also agree to communicate their load curves." Take a belt and braces approach! (Lawyer, mobility Sector)

For their part, the experimenters believe that the consents collected as part of the experiment to authorise access to and processing of their data do not constitute a guarantee for the user, but rather a guarantee for the institutions that collect and process the data. Transparency, security and data minimisation constitute the triptych of trust with regard to privacy issues as expressed by the experimenters.

> In fact, what goes through my head when I read this kind of thing is: "what information am I disclosing, and to whom?" (User of pilot system, male, mobility sector).

This multiplication of consents, as well as the intertwining of technologies, has contributed to shaping a complex customer journey that is unrealistic for a service that is to be developed industrially.

5.3.2 An Opaque Security Key System

Faced with this complex user journey and their representation of blockchain as a technology that is difficult to explain and controversial, the designers have chosen to make the technology invisible to experimenters.

However, this choice is, in fact, relatively questionable. Users have expressed a series of fears and misunderstandings about the blockchain's key system (each participant has a public key and a corresponding private key: the public key is similar to an identifier, an address; the private key allows the user to sign a transaction. This provides security in the exchange but also privacy by anonymising the identity of the participants in the exchange).

> The only information I have is my profile, public key and all that. I don't have much. I didn't understand what it was for. (User of pilot system, female, mobility sector)

The requirements of the GDPR were thus apprehended through the collection of numerous consents, rather than through the requirement of explicability.

5.4 Conclusion

Confronted with three dilemmas that the designers had to decide upon according to the objectives of the project and the constraints attached to it, the protection of privacy on a blockchain requires the implementation of sociotechnical compromises between designers and experimenters with different representations. The first is decentralisation versus responsibility, which arises around the designation of a data controller.

The second is that of anonymity and identification, which arises around the off-chain storage of personal data. The third is transparency versus confidentiality.

As we have seen from this experiment, managing privacy protection is a skill, based on emerging expertise, distributed across a range of professions and users, which requires collaboration to be implemented.

Privacy is a distributed issue in innovation ecosystems, generating sociotechnical compromises. The service designers from the mobility and energy worlds do not defend a purist vision of technology as absolutely guaranteeing transparency and decentralisation based on an open protocol. Rather, they defend a vision of the technology as a tool for interoperability (making data available in a secure and technically simple way to multiple stakeholders), corresponding to the use case of the experiment, which mobilises data from a variety of sources (meters, production facilities, vehicles, data centres, etc.) operated by multiple players (individuals, SMEs, major accounts, public services, local authorities, etc.). Consortium blockchain has emerged as a technical compromise between these two visions. In the eyes of blockchain designers, these compromises have limited the disruptive potential of blockchain technology, by recentralising data management and losing the open nature of blockchain. However, they have allowed other designers to see unexpected uses and benefits of the technology, such as appearing as a privacy "solution".

> We don't necessarily do without intermediaries, but at least the intermediaries between them have a protocol to trust each other. (Designer, mobility sector)

Ethics Statement Informed consent was obtained from the people interviewed for this study, and their identity has been anonymised. The study protocol was approved by a manager in EDF's research division. Ethics board approval is not required for this type of study in France.

References

1. M. Akrich, M. Callon, B. Latour, *Sociologie de la traduction.* (Presses de l'Ecole des Mines, Paris, 2006)
2. Y. Algan, P. Cahuc, *La société de défiance: comment le modèle social français s'auto-détruit* (PSE Ecole d'Economie de Paris, 2007)
3. N. Alter, *L'innovation ordinaire* (PUF, Paris, 2000)
4. D. Antony, C. Campos-Castillo, C. Horne, Toward a sociology of privacy. Ann. Rev. Sociol. (2017)
5. K.S. Ball, K.D. Haggerty, D. Lyon, *The Routledge Handbook of Surveillance Studies* (Routledge, New York, 2012), pp.1–11
6. L. Barraud De Lagerie, E. Kessous, La mise en marché des données personnelles. In: Steiner P, Trespeuch M (dir.) *Marchés contestés. Quand le marché rencontre la morale* (Presses Universitaires du Mirail, Paris, 2014)

7. J. Bohr, M. Bashir, Who uses bitcoin? An exploration of the bitcoin community. In: 2014 Twelfth Annual International Conference on Privacy, Security and Trust, pp. 94–101. IEEE (2014)
8. F. Castagnino, Critique des *surveillances studies*. Éléments pour une sociologie de la surveillance. Déviance et Société **42**, 9–40 (2018)
9. A. Casilli, Contre l'hypothèse de la fin de la vie privée. La négociation de la *privacy* dans les médias sociaux. Revue française des sciences de l'information et de la communication **3** (2013)
10. A. Casilli, P. Tubaro, Y. Sarabi, (en) *Against the Hypothesis of the End of Privacy : An Agent-Based Modelling Approach to Social Media* (Cham, Springer, 2014), 57 p
11. F. Chafiol, A. Barber-Massin, La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données. Dalloz IP/IT **2017**, 637 (2017)
12. A. Danieli, La "mise en société" du compteur communicant. Innovations, controverses et usages dans les mondes sociaux du compteur d'électricité Linky en France. Sociologie. Université Paris Est Marne-la-vallée (2018)
13. P. Flichy, *L'innovation technique. Récents développements en sciences sociales. Vers une nouvelle théorie de l'innovation* (Paris, La Découverte, 2003)
14. J. Gharbi, C. Sambuc, Propriété de soi et justice sociale chez les libertariens. Cahiers d'économie Politique **62**, 187–222 (2012)
15. C. Gasull, Des racines libertariennes à la bienveillance du monde économique: aperçu des idéologies dans le développement des blockchains. In: Toledano J. (dir.), *Les enjeux des blockchains* (France Stratégie, juin 2018)
16. A. Giddens, *Les conséquences de la modernité* (L'Harmattan, Paris, 1994)
17. O. Lasmoles, La difficile appréhension des *blockchains* par le droit. Revue internationale de droit économique **t. xxxii**(4), 453–469 (2018)
18. S. Levy, L'éthique des *hackers*. Globe (2013)
19. A. Manas, Y. Bosc-Haddad, La (ou les) *blockchain*(s), une réponse technologique à la crise de confiance. Annales des Mines - Réalités industrielles **3**, 102–105 (2017)
20. S. Moatti, Technologies de la confiance. L'Économie politique **75**(3), 5–7 (2017)
21. F. Ost, *Le droit ou l'empire du tiers* (Dalloz, Paris, 2021)
22. R. Sennet, *Les tyrannies de l'intimité* (Seuil, Paris, 1974)
23. D.J. Solove, I've got nothing to hide and other misunderstandings of privacy. San Diego Law Review **44**, 745–772 (2007)
24. B. Rey, *La vie privée à l'ère du numérique*. Lavoisier, coll. Traitement de l'information (2012) 297 p
25. N. Satoshi, Bitcoin: a peer-to-peer electronic cash system. www.bitcoin.org
26. A. Strauss, Hospital and his negotiated order, traduction (1992). Baszanger, I., *La trame de la négociation. Sociologie qualitative et interactionnisme*, Paris L'Harmattan.
27. J. Toledano (sous dir.), *Les enjeux des Blockchains* (France Stratégie, juin 2018)
28. S.D. Warren, D.L. Brandeis, The right to privacy. Harv. Law Rev. **4**(5), 193–220 (1890)
29. C. Zolynski, *Blockchain* et *smart contracts*: premiers regards sur une technologie disruptive, RD banc. fin. 2017. Dossier 4 (2017)
30. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, January 2019)
31. R. Sennett, The fall of public man. (New York, Norton, 1974)
32. A.F. Westin, Social and Political Dimensions of Privacy. J. Soc. Iss. **59**, 431–453 (2003). https://doi.org/10.1111/1540-4560.00072
33. A.F. Westin, Privacy and freedom. (New York, Atheneum, 1967)