The Frameworks of Trust and Trustlessness Around Algorithmic Control Technologies: A Lost Sense of Community

Balázs Bodó and Linda Weigl

Abstract Certain techno-political infrastructures, e.g. blockchains, aim to replace our existing social and institutional modes of producing trust as a social resource. Can they successfully do that, without the reliance on the very same institutions, which could safeguard and guarantee their trustworthiness in the first place? By now we have more than a decade of experience trying to build autonomous, code-driven, private ordering infrastructures, designed to complement, disrupt, or replace both private and public institutions. The revolution of these 'trustless' digital technologies is yet to happen, raising concerns about their promises to address the existing trust challenges of centralized institutions, their capacity to eliminate the societal reliance on trust, and the potential consequences thereof. Therefore, in this chapter, we pose the following questions: How does trustlessness through the elimination of more-or-less trusted middlemen impact our values and our sense of belonging? How does the decision to end trust maintenance through trustless technologies impact the cultivation of a sense of community within a society? This chapter addresses these questions by critically reviewing the claims surrounding the trustlessness of automated, code-as-law-based governance systems in the field of digital identity management—an area that continues to command the attention of various organizations and institutions.

1 Algorithmically Produced Trust and Trustlessness

When one party places trust in another, they rely on the trusted party's intentions and capabilities to act in their best interest, and thereby expose themselves to the possibility of harm, deception, or failure. This inherent vulnerability is what makes trust a social construct and human phenomenon. Algorithmic control systems, such as blockchain technologies are developed to automate tasks and thereby reduce human intervention (and errors) to a minimum. They optimize resources by

B. Bodó (✉) · L. Weigl
Institute for Information Law, University of Amsterdam, Amsterdam, Netherlands
e-mail: b.bodo@uva.nl; l.weigl@uva.nl

J. Goossens et al. (eds.), *Public Governance and Emerging Technologies*,
https://doi.org/10.1007/978-3-031-84748-6_16

reducing invested time, money, and effort, increase efficiency, and distribute decision-making and power away from traditional institutional entities. While some view them as progressive alternatives to the perceived failures and untrustworthiness of traditional legal systems and institutions, others perceive them as strategic means to disrupt the existing institutional order to further their narrow, self-interested economic, political, or ideological agenda. What unites both contrasting perspectives, regardless of their ability to automize, economize or decentralize activities, is their evaluation of the technology's capacity to reshuffle power dynamics in society by reconfiguring, remediating, and potentially replacing institutional and interpersonal trust relations.

This replacement of trust relations is achieved by two means. First, a trustless system is able to generate an immutable, consensus-driven, and publicly accessible ledger of transactions without the involvement of a centralized intermediary.[1] Second, its 'trustlessness' is embodied by rules written as self-enforcing code running on the blockchain base layer, enforcing the compliance of anonymous parties through automated, algorithmic means.

Both these specificities of blockchain-based systems stem from a particular vision on trust in individuals and institutions. On the one hand, individuals' trustworthiness is inscrutable because their identity is unknown, and no identification is needed to take part in blockchain-based transactions. If, however, the trustworthiness of the individual behind the transaction is not possible to establish, the system has to offer other safeguards and guarantees to ensure that transactions take place even though the counterparty is anonymous—hence the need for strong, self-enforcing code-based rules. Confidence (i.e.: the expectation that the system will work as expected) in algorithmic systems is derived from the predictability of the mathematical rigor of the hashing algorithm, in particular public-private key cryptography, as well as the economic incentive schemes for miners and consensus algorithms governing the network. Hence, when users decide to subject themselves to the authority of a technological system, they do so because they may have confidence in its predictable, mechanistic, 'objective' operation, where no trust is needed, because no possible (human or institutional) betrayal is possible. These confidence-enhancing features, techno-optimists argue, allow the technology to enhance decentralized decision-making, transparency, tamper-resistance, automation, impartiality, and objectivity. The goal is to eliminate human malintent and fallibility, corruptible institutions, arbitrary enforcement, and essentially remove human and institutional messiness from the system altogether.[2]

[1] We acknowledge that all decentralized systems rely to some extent on centralized components to function, such as miners, validators, developers, computing infrastructure providers, developers, etc. The trustworthiness of these actors is of course an important question, but not substantially different from the trustworthiness concerns of other centralized institutions.

[2] However, despite the high degree of confidence that algorithmic control technologies can qualify for, it can be argued that the requirement for trust *in* such systems persists, thereby challenging the system's allegedly trustless character. This is due to their socio-technical nature, as technology can never be entirely impartial, unbiased, or apolitical. For a more detailed elaboration see Bijker et al.

Public and permissionless blockchains, known as such 'trust-free' or 'trustless' systems, pledge to transform interactions among anonymous-by-design peers that typically rely on trust, often mediated by third-party providers.[3] As we discuss in more detail later, identity information, and the way it is produced, maintained, made available, or not, is a central question that defines interpersonal and impersonal trust relations, as well as the socio-technical and institutional modes of trust production. Second, the deep distrust towards traditional, rule-based, socially embedded intermediaries requires that some of the functions they originally fulfill—such as maintaining ledgers of all sorts—be provided through other approaches, such as reliance on algorithmically defined rules. This raises the question of *what happens to our social trust relations organized around the principles of anonymity and algorithmic control?*

The claim of algorithmic objectivity is not limited to the domain of blockchain-based technologies. Other automated systems, such as AI, and algorithmic decision-making systems also operate on the principle of quantified objectification: on the claim that once unbiased, comprehensive data is fed into objectively formulated, automatically followed transparent algorithmic rules-based systems, the resulting output would therefore be more trustworthy than those produced by institutional processes riddled with human error, judgement, and subjectivity.[4] If the algorithmic decision-making system uses people as its input, then individuals (their identity, history, values, decisions, social networks) also get transformed by measurement, and conversion into data points, and the complexity of their trustworthiness gets simplified into plain scores of creditworthiness, fraud risk indicators, or online reputation.

Blockchains, AI, and algorithmically governed platforms are just a few examples of techno-social systems that aim to produce trust in various social, economic, cultural, or interpersonal relations.[5] Here is why: irrespective of the actual trustworthiness or reliability of algorithmic trust-producing systems, their mere existence has an immediate impact: for better or worse they disrupt the trust in external actors, individuals, and traditional institutions. Blockchain-based systems, for example, don't simply try to eliminate the need for trust, but *try to eliminate the social, institutional practices of traditional trust production*. While not inherently trustless, those technologies can be viewed as actively contributing to the cultivation of societal and interpersonal trustlessness, both through removing the need for trust, and through the elimination of centralized intermediaries and institutions, together with their trust-producing functions. The question, therefore, is not just about how human actors engaging in trust-necessitating transactions within the system trust each other under the new, technologically defined conditions. It is about how trust between

(1989) and Hughes (1987). Confidence in blockchain technologies, for instance, may thus be challenged by the decisions of human actors in the system, such as influential core developers working on the blockchain protocol, or miners. See De Filippi et al. (2020).

[3] See Beck et al. (2016) and Hawlitschek et al. (2018).

[4] See Christin (2016).

[5] See Bodó (2021a, b), Botsman (2017), and Keymolen (2016).

these actors, both interpersonal and institutional, is being affected by (un)intended consequences of the technology destroying the traditional modes and institutions of trust production. Thereby, the inquiry into how these systems produce impersonal trust takes on an additional role. The greater the ability of their technical features to instill confidence in users and convey a feeling of predictability[6] of future events—independent of the traditional, institutional forms of impersonal trust—the stronger their impact is on societal trust in general. As we argue in this chapter, the impact of these technical features deserves extra scrutiny, if that impact is a growth of some form of trustlessness, which implies, in other words, the loss of (the need for) impersonal trust.

Despite the hype and the alleged revolutionary potential of these algorithmic digital technologies, they have yet to fully materialize. But, perhaps they don't need to. Their impact is measurable even if they don't fulfill their promises, and the disruption, as imagined, will not ultimately happen. The potential for damage is already there if individual consumers, citizens, public and private institutions embrace the unsubstantiated, never-to-be fulfilled claims about technological solutionism, the efficiency claims, the desirability of innovation at all costs, and the benefits of disruption.[7] For this reason, in this chapter, we will not look as much into whether decentralized and automated socio-technical decision-making systems will effectively replace our existing institutional methods of producing trust. Instead, we focus on the following question: What kind of dynamics are set into motion by the introduction of these systems into societal trust production logics?

The next section will introduce the social labor of trust production. We will then line out how in the realm of identity management, pursuits towards trustlessness, enabled through decentralization, automation, and verification, may discard, what we refer to as, the 'second dimension' of societal trust, which encompasses the procedures, interactions, and safeguards to ensure not only trust, but also a sense of community.

2 The Social Labor of Trust Production

The initial source of trust in other people and institutions may be inherited, developed through repeated interactions and long-term experiences, or provided by external references. Thus, trust is typically earned through reliable behavior, positive experiences, or good reputation. Known actors garner trust through personal experiences, while trust in unknown actors may arise from the positive experiences of others, recommendations, or the safeguards given by external institutional intermediaries. At the other end, trust collapses quickly, if and when the other breaches that

[6] Predictability in this context is instilled through machines and artefacts, and is not coming from the act of trust, which is built from reliable, benevolent, and corrective behavior of societal actors.

[7] See Bodó and Janssen (2022) and Janssen et al. (2018).

trust. But what happens between the birth and death of trust? *What kind of investment, upkeep, and maintenance work are necessary to maintain and support both personal, interpersonal trust, and abstract, societal trust?*

For the purposes of this chapter, we do not discuss in detail how that process takes place in face-to-face, interpersonal trust relations, as this has already been extensively discussed.[8] Instead, we will focus on the labor required to maintain the abstract and impersonal societal trust. Some of that trust is certainly the aggregate of interpersonal trust relations. If the members of a community generally trust each other in their micro-transactions, the overall, communal social trust should also be high. However, in modern societies, much of impersonal trust is produced by institutions, and through the interactions between citizens and institutions.[9] Let us briefly sketch the societal labor necessary to maintain impersonal trust.

2.1 The Social Labor of Impersonal Trust as a Shared and Social Resource

We define impersonal trust as a societal, broadly accessible resource, that facilitates the co-existence, collaboration, and cooperation of strangers within a particular polity, usually the nation state.[10] Such impersonal trust is produced by various public and private institutions and practices. As Zucker put it, when the mechanisms of trust production "*are reconstructed as intersubjective and as part of the "external world known in common" they can generalize beyond that transaction. This process of reconstruction has been called institutionalization: the process of redefining acts as exterior when intersubjective understanding causes them to be seen as part of the external world and objective when they are repeatable by others without changing the common understanding of the acts.*"[11] The source of such impersonal trust is external to the trust relation it supports. Such trust can rely on many sources, infrastructures, such as the media system or public education producing shared epistemic frameworks, the justice system producing reliable contracting and conflict resolution regimes, or the private sector providing risk management opportunities. Thus, impersonal trust can be considered a *shared* resource, as it should be accessible to everyone.

[8] See Gambetta (1988), Goffman (1990), Greif (1989), and Hardin (2002). Let it suffice to say that potential trustees (i.e.: all of us) have to act in accordance with the formal and informal expectations of trustworthiness. This includes demonstrating one's competence in certain tasks, performing a social role that demonstrates reliability, benevolence, care for others near and far, and acting with general integrity. Good social standing is a synonym for trustworthiness, and that social standing needs to be upheld both in the concrete, everyday social, economic interactions, as well as beyond them, in face of general social entropy and forgetfulness.

[9] See Zucker (1985).

[10] See Giddens (1990), Misztal (1996), and Sztompka (1999).

[11] See Zucker (1985).

There have been attempts to quantify the amount of resources spent on the production of such impersonal trust.[12] The study selected a number of professions in the US economy, such as managers (in business, finance, education, healthcare), service occupations (food preparation, care, etc.), sales, natural resource management, and transportation, and estimated how much time each profession spends with upholding trust. They found that around one third of the employment in the US is in one way or another related to upholding trustful economic relationships. This study frames this finding as the "cost of trust" and goes on to argue that at least some of this cost can be saved by relying on blockchains, smart contracts, and other algorithmic systems to produce the same trust, but cheaper. For the authors, trust production is first and foremost an economic question centered around costs and efficiency. However, reducing complex social, cultural phenomena to the question of economic efficiency robs them of all their non-economic functions. Fast food restaurants may be more efficient than cooking for friends, or maintaining a food service for the homeless, but it is also obvious what the more efficient alternative lacks.

The economic efficiency framing dis-embeds the practice it is applied to from the social relations it otherwise is embedded into.[13] This also applies to how we see the labor spent on producing trust in society. The efficiency approach removes many of those considerations that socially embedded and controlled trust production practices embody and follow, such as care, maintenance of social relations, and ultimately the *maintenance and reproduction* of interpersonal and impersonal trust. Hence, impersonal trust is also a *social* resource, implying that economic and quantifiable considerations are unable to capture the multifaceted and abstract nature of trust.

2.2 The Social Labor of Trust as a Shared Responsibility

Since centuries, public institutions are the primary producers of impersonal trust, and the social labor of trust production takes place in the frameworks they offer. Schools don't just teach children to read and write, they produce trust through diversity in the classroom, and creating the shared epistemic frameworks above and beyond individual, and group-based (racial, religious, linguistic) differences. Public service media doesn't simply provide news and entertainment. While doing so, it's mandate is to provide a continuously and freely accessible baseline in the cacophony of opinions, partisan debates, polarized info-bubbles. Likewise, a transparent, accountable, unbiased public administration doesn't just manage communal resources, but while doing so, it allows trust to develop between those who rely on and contribute to those resources. Let's take this latter trust production logic as an example to see in more detail how their trust production function may be affected

[12] See Davidson et al. (2018).

[13] See Polanyi (1944).

by external pressures which don't take into account the disruption of the indirect trust related functions of public institutions.

The fate of the once lauded, but now dwindling New Public Management (NPM) approach highlights recent changes in the public governance and maintenance of trust. By introducing NPM, governments started to treat citizens as customers through mimicking private sector management models and leaning on market- and profit-oriented ideals, such as efficiency and performance measurements.[14] NPM seeks to enhance public service delivery by promoting decentralization, competition, and customer-centric service provision. On the surface these goals are commendable, but the effect they had on trust relations only became evident long after their introduction. See, for example, the strategy brief on trust in the government by the City of Amsterdam, signed by the Mayor and the Secretary of Amsterdam:

> In the 1980s, government organizations were seen as too cumbersome, bureaucratic, and slow. The government had to be 'run' like a business. Effective and efficient: achieving goals with as few people and resources as possible. Values such as humanity, fairness and openness became less important. The human dimension disappeared to the background. Citizens were seen as consumers and that had an effect on how governments treated citizens. Namely, as individuals who are mainly concerned with their own self-interest, people who cannot be trusted and therefore must be checked. If we want to increase residents' confidence in the municipality, we must take the first step and embrace a different, more positive view of humanity. Where we think and act as a starting point assume that Amsterdam residents are of good will. Trust instead of suspicion is the basis to act as a reliable government that primarily serves the citizen.[15]

This problem statement highlights the complexity of the role of public institutions as sources of impersonal trust. On the one hand, their mandate is to maintain trust in a community. For that, however, they need to be trusted by their constituents: the community they serve. Yet, this trust collapses, if the citizens see them as only focusing on efficiency, or in the name of the NPM ethos, they try to base their activities on control rather than trust.

Private institutions, such as banks, credit rating agencies, PR, marketing, and communications agencies also produce societal trust, either as their main area of activities, or as a byproduct of providing trust-requiring services. Unlike public institutions, their focus is not first and foremost to produce societally optimal levels and forms of trust. Instead, they must balance their economic interests, shareholder value, profits, market dominance with the kind of trust they are ultimately producing. Though the assumption of neoliberal economic theory is that economic self-interest, coupled with market competition would ultimately lead to trustworthy behavior in general, and in the case of trust producers, a steady and reliable supply of trust as a product, this does not always work in practice. The 2008 financial crisis was the result of financial institutions (investment banks, credit rating agencies)

[14] See Ferlie et al. (1996).

[15] Halsema and Teesink (2022).

prioritizing short-term profits over their long-term mandate[16] to produce trust in economic relations, despite them being also heavily regulated to ensure their trustworthy behavior.

This conflict of interest is greatly aggravated in the case of technology companies in the business of trust production, where platforms, search engines, communication services, dating apps, self-driving car companies are repeatedly caught breaching their users' trust by selling their data, eavesdropping their conversations, feeding them misinformation, or putting them in physical danger, because profitability concerns seem to be more important than being trustworthy in all those relations they service.

2.3 Algorithmic Technologies and the Social Labor of Trust

The amount and nature of societal trust is the outcome of a constantly shifting balance between different trust production approaches: trust produced in interpersonal relations, trust produced by public institutions, and by private institutions. For example, if trust in public institutions is dwindling, which means that citizens rely less on the impersonal trust safeguards produced by the government, they may rely more on interpersonal trust relations.[17] Consumers may be happy to replace some of the trust they feel towards other humans with trust produced by private actors, when, for example, they let their car drive itself, rather than grabbing the wheel themselves. Public institutions are increasingly outsourcing their trust production functions to private entities. The closure of schools during the COVID pandemic, and the increased reliance of private education technologies (from Zoom and Google classroom to various learning platforms) outsourced many functions of the school (instruction, practice, assessment) to these technological actors. There is also a constant shift between various private trust producers, such as the one between traditional banks and neobanks,[18] or between traditional news organizations and social media.

Some of these shifts are less controversial than others. At the time, the shift from Encyclopedia Britannica to Wikipedia as a source of trustworthy and trusted information seemed outrageous, by now we know that ultimately there is little difference between the two in terms of the level of editorial control over individual articles, or the selection mechanisms producing the editors.[19] Other shifts are way more controversial. Replacing seasoned journalists and newsrooms with AI and social media

[16] In this sense, a mandate is not to be understood as a legal mandate, but for financial institutions to function properly in the financial system, trust is the very foundation. Without trust, customers would not deposit their money, seek financial advice, or use banking services.

[17] See Fukuyama (1996).

[18] See Ferrari (2022).

[19] See the (self-)evaluation of Wikipedia on trustworthiness criteria: https://en.wikipedia.org/wiki/Wikipedia:Evaluating_Wikipedia_as_an_encyclopedia, its complex administrative structure:

may save costs for news producers or consumers but apparently results in a breakdown of some of the fundamental shared epistemic frameworks, from science to politics.[20] Replacing human social workers with algorithmic decisions can harm everyone: citizens, whose needs are denied; public institutions, who are reinforcing rather than lessening inequalities through their algorithmic tools; and the rest of society, outside of these relationships.[21] The algorithmization of the public sector, when it fails, leads to a breakdown of social trust relations between citizens and institutions; and through the growing distrust in the institutions tasked to produce impersonal trust, it can end with a general breakdown of societal trust.[22] Finally, the responsibilization of the citizen under the neoliberal state shifts responsibilities from public institutions to individuals and impersonal economic processes,[23] also in terms of trust production. The neoliberal subject is increasingly left to their own devices to find an answer to the question whether the unknown other is trustworthy, and to prove their own trustworthiness towards the others.

Blockchain-based systems present a particularly nasty configuration of these issues. They are designed to serve an arbitrary, ad-hoc cloud of anonymous, individual subjects, under the assumption that no one *in the system* is trustworthy; the users, due to their disposable identities cannot form a community (the problem of so-called “on chain governance” is still unresolved, and the governance of communities—if they exist—happens at least in part separately from what is happening on the decentralized infrastructure); and as a result, there is neither a need, nor a possibility for social trust in the system. This assumption of course is incredibly corrosive, if the system is deployed in a setting where social trust is still present. First, such a system in and by itself, does not, because it cannot, contribute anything to the maintenance of that pre-existing trust. Second, it may actively destroy social trust by injecting the assumption of untrustworthiness into the community and replacing trust by control. Third, to the extent it actually replaces (the functions) of a public institution, it removes this institution’s trust-producing labor from the maintenance of social trust.

For any of these reasons, efforts that aim to disrupt and replace trusted societal middlemen with trustless, algorithmic, or confidence-based systems deserve extra scrutiny. Identity management systems, described in the next section provide a comprehensive case study to just do that.

https://en.wikipedia.org/wiki/Wikipedia:Administration, its overview of editorial control: https://en.wikipedia.org/wiki/Wikipedia:Editorial_oversight_and_control.

[20] See Laufer and Nissenbaum (2023).

[21] See Eubanks (2017).

[22] See Bodó and Janssen (2022).

[23] See Brown (2017) and Weigl et al. (2023).

3 Identity Management as a Case Study for Trust Labor

Identification, both digital and analogue, is essential for parties who do not know or trust each other, but want to, or need to collaborate, or simply co-exist. There are multiple ways how identity information can be managed, maintained, disclosed, each contributing differently to the social production of trust. Although more granular distinctions are possible, we will adopt a general approach in this chapter and lay out three of them: paper-based public identity management, and privatized, so-called federated models (Sect. 3.1), and decentralized identity management systems, also known as self-sovereign identity systems (Sect. 3.2). In the following we will compare these alternatives from the perspective of their trust related functions.

3.1 Trust and Distrust in Public and Private Centralized Digital Identity Systems

3.1.1 Public Identity Infrastructures

The history of identification, public administration, and the collection of personalized information dates back thousands of years. During this time, governments emerged as the primary identity providers to maintain social order, manage taxation, and deliver public services. As societies grew in complexity, governments took on the role of centralizing and regulating identity documentation, leading to the development of formal identity information, such as date of birth, address, or nationality.[24] Given that identity information is largely rooted in the confirmation of an individual's citizenship, most types of personal identification have thus remained under the authority of governments.[25] An instance of an established instrument for confirming citizenship are paper-based passports. Serving as government-issued and globally acknowledged documents, passports enable individuals to, for instance, verify their identity when crossing international borders, and thereby facilitate travel.[26] When not coupled with surveillance technologies (such as biometrics, facial recognition systems, or GPS tracking) or politically and ideologically motivated misuse, they are also a trust anchor for public authorities and other service providers. The personal identification enabled through these official documents plays a relevant role for individuals engaging with public administrations, but also for accessing services provided by commercial entities, such as opening a bank account.

However, using physical documents for identity proofing can come with security risks, including the potential for breaches, identity theft, personal data misuse, and

[24] See Lips (2019).

[25] See Wihlborg (2013).

[26] See van Dijck and Jacobs (2020).

compromised privacy.[27] The digitization of identification systems signified a move toward fostering a more transparent and trustworthy information society and a step toward modernizing administrative and bureaucratic processes. This, however, introduced new risks and challenges to the public administration of identities, such as (growing threats of) cybercrimes, and a subsequently enhanced need to safeguarding users' privacy and security.

3.1.2 Private Identity Providers

With the advent of Facebook in the early 2000s, and various commercial services requiring user identification online, the traditional perception of identity management as a prerogative preserved for public authorities was substantially weakened. In the private sector, a digital identity management approach emerged, known as the 'federated' identity management system. In this system, private companies act as central trust authorities, enabling users to verify their identity through a single-sign-on process on the platform where they first registered their accounts. The system requires all involved parties to have a mutual sense of trust, since it is based on an arrangement between multiple domains that enables users to use the same identification data to access different networks. Hence, for commercial services, major private trust mediators like Google or Meta started to offer convenient identity management systems that store users' access credentials. Users 'only' need to establish a single account with one of these digital intermediaries, or identity providers in this case, to gain access to a diverse array of portals and services.

3.1.3 Trust Related Issues with Centralized Identity Management Systems

Both public and private digital identity management systems are in effect centralized repositories of personal data. This gives rise to issues of privacy, security, surveillance, and misuse, as the following examples testify.

Centralized data repositories of identity information are vulnerable to security breaches and data leaks, in some cases affecting billions of users, exemplified by cases such as those involving Yahoo!, LinkedIn, and Meta. Private actors are also prime targets for state surveillance, such as those revealed by Edward Snowden in 2013.[28] Classified documents exposed details about an electronic mass surveillance data mining initiative led by the NSA, with the collaboration of major tech companies such as Microsoft, Yahoo!, Google, Facebook, YouTube, and Apple, aimed at acquiring real-time data about US citizens. Private identity providers are also sensitive to how well, and by what values they are managed. Elon Musk's 2022 takeover

[27] Ibid.

[28] See Königs (2022).

of Twitter illustrates how the commercialization of the platform's user identity verification system, and the introduction of a subscription-based system can lead to the proliferation of fake accounts with verification checks, enabling the spread of misinformation and undermining the original purpose of the 'blue check' as a seal of authenticity of the account holder.

Despite all these concerns, users seem to have confidence in these systems to manage their (digital) identities. In case of the public systems, they have little choice. What is more surprising is their continued use of those private identity management systems which already proved themselves to be untrustworthy.

The reasons behind users' continued reliance on untrustworthy identity management systems can vary. Some users believe that they can manage and take safeguards against security and privacy risks, leading them to continue using the services of digital trust mediators with a strong belief in making informed decisions.[29] Digital service providers also do a lot to appear as trustworthy. Instances of such practices are (1) a strong focus on user experience and user-centric features, (2) some investment in internal governance mechanisms to increase trustworthiness, (3) relying on external signals and attestation of trustworthiness, (4) inviting regulation, or (5) building powerful (meta) narratives of trustworthiness, often without, or directly contradicting real world facts, and experiences.

These trust building practices, however, are quite different from actual, verifiable *trustworthiness*. Governments and private technology companies can only earn trustworthiness by being reliable and consistent in their behavior. Otherwise, these practices only produce misplaced trust: convincing users to trust something which isn't actually *worth* their trust. While trust-building actions can certainly enhance perceived, but possibly misguided trustworthiness, building and maintaining actual trustworthiness requires an often much more costly ongoing commitment and integrity.

The difference between investing in trustworthiness perceptions, and investing in actual, verifiable trustworthiness is what differentiates between the lack, and the presence of the social labor of trust production. The former ultimately decreases social trust by investing in deception, the latter actually contributes the social trust by investing in trustworthy trust producers.

The social labor of trust production in this latter case can take many forms. Trustworthiness of both public and private digital intermediaries in identity systems can be gained through, for example, user data and privacy protection through encrypted communication, compliance with data protection regulations, and the prioritization and demonstrated commitment to the proper and ethical use of any collected user information, at the cost of monetary gains, as well as other commercial and political interests.

[29] See Bodó et al. (2023).

3.2 Trustlessness in Decentralized Digital Identity Management Systems

Historically, institutional trust has experienced ups and downs. The last decades witnessed several downturns, marked by trust-shattering events invoked by political, digital and also financial actors.[30] These socio-economic conditions prompted technological responses that envisioned a disruption of traditional governance structures.[31] Decentralized technologies like blockchain constituted an alternative governance model grounded in cryptographic code rather than contracts and legal frameworks, and verification mechanisms rather than institutional trust.[32] The foundational technology of blockchain initially emerged within the cyberlibertarian realm of the internet, marked by a deep skepticism towards both public and private institutions.[33]

The sphere of digital identity management was not left untouched, as engineers and a small circle of identity management experts called for a decentralized infrastructure as an approach to solve the trust issues provoked by centralized actors. With blockchain gaining prominence as a hype technology, a new libertarian blockchain-based digital identity paradigm touted as ‘self-sovereign identity’ (SSI) emerged. Taking into account the conceptual analysis of a variety of scholars studying this concept,[34] self-sovereignty can be understood as a concept in which data subjects exert control over their data and can determine how data are collected, processed, stored, and shared.

According to the SSI philosophy, safeguarding user privacy and security can thus only be achieved by removing any centralized entity involved in the exchange of user data. Essentially, data control should be decentralized, and this could be accomplished on a technical level through public key cryptography. Public key cryptography operates with key pairs, comprising a public key and a corresponding private key. The ownership of the key pair can be mathematically proven without disclosing the private key itself. Public key cryptography enables users to generate their own identifiers known as decentralized identifiers (DIDs), which facilitate encrypted communication between users and service providers without the necessity of a central authority for registering or revoking the identifiers. Similarly, verifiable credentials are a frequently observed technical feature of SSI. The validity of the credentials can be assessed without the involvement of the credential issuer and simply by controlling the digital signature of the issuer and a public revocation registry. For this purpose, a distributed ledger acting as a single source of truth regarding public information on credential issuers is recommended.[35] Users can then store DIDs,

[30] See Earle (2009), Levi and Stoker (2000) and Werbach (2018)

[31] See Davidson et al. (2016).

[32] See Werbach (2017).

[33] See Golumbia (2016), Karlstrøm (2014), and Reijers and Coeckelbergh (2018).

[34] See Couture and Toupin (2019), Herian (2020), Ishmaev (2021), and Weigl et al. (2023).

[35] See Mühle et al. (2018).

associated cryptographic keys and credentials on their devices or in the cloud, in a so-called 'digital wallet'. For enhanced user privacy, computer scientists, cryptography researchers in particular, explored cryptographic methods for the selective disclosure of identity credentials. The assumption that, in general, centralized institutions would typically ask for more data than necessary, led to the integration of zero-knowledge proofs (ZKPs) as tools to minimize information exposure during a verifiable presentation and reveal only the attributes relevant to the specific purpose. ZKPs would also avoid the disclosure of an associated identifier, such as the public key of the issuer's signature.[36]

Thus, in order to verify someone's claim or identity, the holder or user of the information that needs to be verified can provide verifiable credentials, that is cryptographic proofs, generated from their wallet to the verifier. These proofs contain information that was attested by an issuer beforehand. Attestation in SSI systems is enabled by the issuance of verifiable credentials, which are digitally signed by the issuer, and thereby assure the accuracy and authenticity of the information. Verifiers can independently check for the veracity and validity of these credentials by checking the cryptographic signatures of the issuer's public keys, without the involvement of a centralized entity or authority.

Essentially, the technical characteristics of SSI are designed to bridge the high level of distrust in centralized entities and seek to grant individuals greater power and control over their personal data. From a normative point of view, however, it is worthwhile to critically scrutinize the moral and ethical feasibility of decentralized data control, and the replacement of digital intermediaries and institutions and their trustworthiness. Two main points within the context of trust disruption merit particular attention.

The first pertains to the *infrastructural* challenge stemming from what we can delineate as the '*ledger society*'.[37] The second involves an *individual*-level concern arising from the strong pursuit of *user empowerment* and control. The ledger society is characterized by great expectations and hopes regarding blockchain technology to solve societal issues. SSI, in this context, is "an idea that arguably assumes the retreat or abject failure of institutions, including intersubjective trust".[38] Thereby, SSI does not necessarily seek to recalibrate or enhance social cohesion or political integrity. Instead, its objective lies in disrupting trust and establishing verification mechanisms and control as the bedrock for societal transactions encompassing both impersonal interactions and institutional relationships.[39] Secondly, as a user-centric identity management model, SSI aims to empower users with increased control and ownership of their personal information. However, the proponents of SSI, evidenced by the case of digital COVID-19 immunity passports, neglected ethical problems

[36] See Sedlmeir et al. (2022).

[37] See Herian (2020).

[38] Herian (2020), p. 157.

[39] See Bodó (2021a).

such as social stratification, discrimination, or deliberate self-infection.[40] SSI can thus be described as an economic model that establishes self-constituted markets for credentials and identity verification. Ideally, users and consumers feel autonomous and sovereign as they control the methods and avenues of data exploitation, practices that, however, inherently remain unchanged.[41]

These two dynamics on the infrastructural and the individual level eliminate the need for trust by establishing an ecosystem that is characterized by transparency, immutability, and user autonomy, and thereby eliminating the reliance on trusted intermediaries.

4 A Lost Sense of Community

4.1 Trust Production in Identity Management

As mentioned above, at a more abstract level, we can discern three distinct approaches to managing digital identity (public, private, and decentralized systems) and the underlying production of impersonal trust. However, to begin with, it is important to acknowledge that next to any public administrative function, such as identity management, trust is needed for a democratic state to operate in the first place. Well-placed trust is feeding into the legitimacy a state needs to function on behalf of its citizens. For public identity management in democratic societies, trust production relies on democratic control, the rule of law, and the accountability and legitimacy of public institutions. In turn, trustworthy identity management in the public realm is important as it allows the justice system to operate, it allows public registries to be trustworthy, and it allows public administration to fulfill its tasks to develop and implement just, equitable, accountable policies.

In the privatized or federated models, identity information is managed by private, profit-driven companies. They operate in a different territory as public institutions, and they are able to provide trust safeguards for interactions across jurisdictional boundaries at scale. How they do that, however, is only in part defined by the needs of the users and the specific interactions they mediate. Of course, on a technical level, they need to manage identity information in a safe, secure, and reliable manner, by protecting users' personal data and privacy, using encryption, and complying with data protection laws, as well as integrating multi-factor authentication or privacy-enhancing technologies. Yet, private actors have their own incentives: balancing safety and legal compliance against costs and following economic incentives which often result in identity information being used for purposes that benefit the identity provider and not always the users. They also don't have societal concerns in mind when they decide whom to issue a federated identity, what kind of compliance

[40] See Halpin (2020).

[41] See Herian (2020).

they enforce, when and how they monitor bad behavior, and when to deny authentication to services. Their practices, norms, and rules may be oblivious to, or in some cases, in direct conflict with the purposes and goals of public identity providers.

If these practices are not effective enough, or if institutions are not perceived as trustworthy anymore, a third option to govern digital identities emerges; the decentralized identity paradigm. Decentralized identity systems aim to empower individuals to act autonomously without the interference of institutional middlemen. The trust placed in any central actor is minimized, despite the consequence of disconnecting from the broader societal system. In the evolving landscape of digital identity management, the desire to reduce the influence of untrustworthy federated and public intermediaries, particularly in the era of datafication, is a recurring theme. The incentive behind this shift is clear—a response to the numerous instances where trust has been betrayed through security breaches, personal data misuse for behavioral manipulation, microtargeting, data-driven profiling, mismanagement, and through political or ideological differences. All of that accumulates and results in institutional mistrust. The rationale behind embracing a trustless approach appears comprehensible. However, the notion of entirely removing intermediaries for digital identification and verification purposes raises several questions when analyzing trust from a sociological and philosophical perspective. This is because the function of trust goes beyond its role in facilitating and economizing interactions.

4.2 Two Sides of Two Different Coins: Technical and Societal Trust Mechanisms

In this section, we will contrast some of the self-sovereign identities' (SSI) technical features with the relevance of societal trust-building mechanisms. SSI, on a general technical level, is characterized by individual empowerment through enhancing privacy and anonymity, and the detachment from centralized systems. The infrastructure needs to be a decentralized network, such as a public or private blockchain or any decentralized public key infrastructure.[42] Embedding identity verification (of citizens) in a trustless network comes with societal consequences, especially when considering the role trust plays in various interpersonal and institutional interactions in social and political life.

[42] Although recent implementations of SSI systems have moved away from extensive blockchain integration, some still argue blockchains could be useful for hosting the public key infrastructure for certificate issuers and public registries that contain information on the revocation status of credentials. Regardless of the implementation of a blockchain, the SSI system always exercises some degree of decentralization with the usage of digital wallets operating on local devices and containing users' identity data.

4.2.1 The Disruption of Social Capital

First, for several reasons, life becomes more manageable in a community equipped with *social capital*. This term, as defined by Putnam, refers to "connections among individuals—social networks and the norms of reciprocity and trustworthiness that arise from them".[43] Social networks cultivate norms of generalized reciprocity, enabling coordination and communication, enhancing reputations, and ultimately providing a means to resolve collective action dilemmas. Taking the idea of self-sovereign identities further will make social capital difficult to accumulate. Self-sovereignty enforces individual control and autonomy over personal data.

In a society where identity is managed by individuals through decentralized systems, the traditional bonds of trust and reciprocity, which are essential for the formation of social capital, become hardcoded as obligations and crypto-economic incentives into an infrastructure layer. Self-sovereign identity infrastructures may or may not be the future of many social, economic interactions and trust relations in the future, but in some way or another, the affordances of the technology will shape those relations. A technology built on the assumption of anonymity, zero-knowledge proofs, distrust, and libertarian ideas of control and individuality will frame the interactions where this technology is put in use. Whether in interpersonal relations, or vis-à-vis public institutions, a technology of distrust will shape and constrain the interaction. It is hard to imagine how such a framework would be conductive to the emergence of collective trust necessary for social cohesion. In addition, rules, hard-coded into the infrastructure layer make it difficult for a community to adjust its own norms to changing circumstances because such capacity is now tied to the restricted technological domain of protocol development.

Another aspect is how such technologies can contribute to the development of shared epistemic frameworks. Lynne Zucker argues that trust emerges from a complex set of background expectations, the attitudes of daily life, reciprocal perspectives, and socially warranted knowledge.[44] This is a two-way interaction. Common background expectations produce trust, and it is the social labor of trust production which to a large extent forms shared background expectations. These expectations are constantly challenged and reassessed according to fast-changing global and societal circumstances. In the epistemological framework of SSI-based trustlessness, this process, the formation and modification of background expectations, is reduced to the mere impression of confidence that the system works. The interactions individuals build through such systems also do not allow for the production of background expectations, or for an update thereof, as SSI does not produce trust, it produces verification mechanisms, such as cryptographic protocols and attestations, due to distrust. With each interaction, we calibrate what we can expect from each other and the environment. In the absence of a functional trust system based on common expectations, society may fragment into tribal trust networks. The danger

[43] See Fukuyama (1996) and Putnam (2001), p. 19.

[44] See Zucker (1985).

of such fragmentation becomes apparent as societal systems lose their coherence. This results in dysfunctional interactions, hindering the development of broader, interconnected communities.

4.2.2 The Disruption of Civic Culture

Secondly, trust is also a central element of *civic culture*. As Sztompka argues, “its presence is an indispensable precondition of a viable political system”.[45] The foundation of the political system rests on active participation, where the crucial role of engagement lies in incorporating practices that allow everyone to witness and contribute to the system’s trustworthiness—often by participating in practices of distrust: control, oversight, verification. Consequently, trustworthiness becomes an experience of engagement. From a certain perspective, distrust can be seen as beneficial as it implies a sense of guardianship, wherein we scrutinize those who are in positions of authority.

In SSI systems, zero-knowledge proofs (ZKPs) are optimized to empower users by enhancing anonymity through privacy-enhancing features. Identities are verified through cryptographic protocols (cryptographic hash functions and mathematical proofs), which allow the holder of identity data to demonstrate knowledge of a secret to a verifier without revealing that information itself. While ZKP can allow for identity verification without oversharing specific information, this goal comes at the expense of being able to participate in the production of collective societal goods, such as trustworthiness, which relies on some levels of visibility and legibility.[46] For instance, in the context of law enforcement, excessive anonymity resulting from their use might impede investigations into criminal activities.[47] Healthcare institutions may face challenges in efficiently managing public health crises if they cannot access anonymized data for epidemiological analysis.[48] Moreover, since ZKPs have to date no legal development under EU regulation, there is a risk of impeding regulatory efforts. Hence, while ZKPs provide a cryptographic means to validate information without revealing it and constitute an essential feature in a zero-trust environment, the use of such systems contributes little to the operation and maintenance of a trustworthy system itself. If we delegate this responsibility to an algorithm of trustlessness, we forfeit the ability to uphold trust through vigilant skepticism. SSI is unable to provide this process because this task has been rendered irrelevant by delegating it to the protocol level.

[45] Sztompka (1999), p. 14; and see also Almond and Verba (1963).

[46] See Golman et al. (2017), Kahneman and Tversky (1979), Pozen (2018), and Prat (2005).

[47] See Garland (2001), Hert and Gutwirth (2006), and Jardine (2015).

[48] See Abouelmehdi et al. (2018) and Gille and Brall (2021).

4.2.3 The Disruption of Societal Interactions

Thirdly, trust is also an important dimension of *civil society interactions* in general. The existence of a functioning community of citizens, dedicated to political authority, relies on both mutual trust among individuals and a trusting relationship with public institutions. Institutions thereby also serve as the catalysts for a continuous calibration process between individuals. This calibration process involves language, concepts, and the establishment of a shared understanding. Removing or neglecting this capacity, which is fundamental to trust, disrupts the process of building a common understanding. Emerging decentralized systems like self-sovereign identity further underscore the effect of postmaterialism on societal trust, whereby individual values shift from physical and economic principles to values like autonomy and self-expression.[49] Thus, while typically supportive of democratic ideals, postmaterialism also embodies perspectives and actions that challenge the establishment, along with growing discontent with authority within contemporary democracies. This resonates particularly with the perspective of blockchain evangelists who argue that the technology has the potential to provide internationally recognized self-sovereign legal identities to everyone. This could, in turn, empower individuals to establish virtual communities in cyberspace, dedicated to political decision-making and the formulation of laws, surpassing the confines of (national) institutions.[50] It is plausible that individuals supporting such views largely contest authority and exhibit a heightened pursuit of trustlessness.[51]

In conclusion, while the desire to reduce the power of trust intermediaries in the evolution of digital identity management is understandable, a nuanced approach is necessary. Trust is not just a procedural safeguard but a vital element in civic culture and civil societies in general. Institutions and collective practices play a crucial role in this process. Various forms of identity management encourage specific forms of trust production and societal reproduction and discourage others. The choice between the different approaches thus has consequences beyond identification and verification of different aspects of our identities in narrowly defined settings. Replacing public identity infrastructures with self-sovereign ones means abolishing certain forms of trust labor, and thereby risking societal fragmentation and the breakdown of cohesive communities.

It can finally also be argued that if SSI was really able to foster trust by making issuers, verifiers, and users more trustworthy, a significant contradiction arises. The paradox lies in the potential resistance from entities, such as private verifiers, who may have vested interests in monetizing data or exploiting extensive data collection practices. In this scenario, the implementation of mechanisms to verify credentials and empower users with ZKPs and control over their digital identities could face pushback from those accustomed to traditional data-centric models. Furthermore,

[49] See Catterberg and Moreno (2006) and Inglehart (1990).

[50] See Orgad (2018).

[51] See Catterberg and Moreno (2006).

when governments or supranational actors, like the EU, adopt SSI, there exists a possibility that these entities might embrace SSI simply to demonstrate a commitment to principles of transparency and individual empowerment, which they are already perceived to uphold. On the other side of the coin, if the SSI technology lived up to its promise of state 'disempowerment' and individual autonomy, would untrustworthy surveillance and authoritarian states adopt SSI and fully relinquish the control to citizens, just to become trustworthy?

5 Conclusion

In the realm of digital identity management, small circles of experts have advocated for a decentralized infrastructure as a solution to address the trust issues arising from centralized actors. With the rise of blockchain as a 'trustless' technology, a novel libertarian digital identity paradigm known as SSI has surfaced. Decentralized systems like SSI alter the form, content, shape, and amount of impersonal trust in often unforeseen and unforeseeable ways. The aggregate impact of the changes is hard to assess. Yet, in this chapter, we asked what kind of dynamics are set into motion by the introduction of trustless systems into societal trust production logics?

We posit that societal, impersonal trust facilitates the co-existence among strangers within a specific political entity. This form of trust is generated through diverse public and private institutions and practices as laid out in Sect. 2. From this, we formulated some normative goals, when it comes to the social production of impersonal trust. First, impersonal trust is a *shared* social resource. This means that ideally, it is equally accessible to all members of the community, without discrimination. Second, impersonal trust is a shared *social* resource. This means that the nature, form, and amount of that trust should be defined by social, rather than purely or predominantly economic considerations and/or technological limitations. Private trust producers' contribution to impersonal trust should also be assessed and ensured from the perspective of the community. And third, the production of impersonal trust is a shared *responsibility* of the community. This means that no member should face a barrier to, or completely excuse themselves from participating in the practices of trust production. Also, public institutions' mandate should include this responsibility, both directly or through their regulatory and oversight functions vis-a-vis private parties.

In the case of SSI, two main elements of trust disruption clash with at least one of the normative goals above. The first revolves around the *infrastructural* disruption due to decentralization, which clashes with the second (*social*) and third (*responsibility*) normative goal. In this context, the objective of SSI is to disrupt trust and establish verification mechanisms and control as the fundamental basis for societal transactions, encompassing both impersonal interactions and institutional relationships. This removes trust as a *social* resource and as a shared *responsibility*. Specifically, digital wallets and DIDs eliminate the need to trust central entities by allowing users to control their data and communicate directly by leveraging cryptography instead of relying on intermediaries. Distributed ledger technology eliminates the need to trust issuing entities, allowing to verify issuers' signatures for the integrity of credentials. Verifiable credentials eliminate the need to trust users, by making credentials tamper-evident and cryptographically verifiable, reducing the risk of forgery. ZKPs eliminate the need to trust verifiers, by minimizing the amount of personal data exchanged during verification processes and the potential for misuse of information.

The second clash pertains to *individual*-level concerns stemming from the intense pursuit of user empowerment and control. This user empowerment, from the perspective of trust labor, however, seems one-sided and superficial, and conflicts with the first (*shared*) and the second (*social*) normative goal. Some users may be empowered in a technical sense if they control their own identity information, but this does not translate into bargaining power vis-à-vis private entities trying to extract as much information from them as possible, and certainly results in disempowerment when it comes to participating in the social practices of trust production and trust development. Moreover, empowering users comes with attributing a significant responsibility to them. This responsibility also comes with accountability, but through the distribution of power and decision-making capacity, accountability can no longer be exercised by a protective central entity. Consequently, how is that entity supposed to be trustworthy when it cannot be held accountable? In essence, the pursuit of user empowerment requires careful consideration of the broader societal context, acknowledging the inherent challenges and responsibilities associated with empowering individuals within existing power structures. Simply providing users with technological tools does not automatically address the underlying power imbalances. To conclude, it remains unlikely that decentralized technologies will ever fully substitute the sense of community and belonging for individuals, even if these individuals harbor distrust towards societal institutions.

In this chapter, we used decentralized identity management as a case study for zero-trust technologies to show how, regardless of the numerous trust breaches, trust cannot be replaced by a techno-centric approach. It can, at best, make existing procedures more efficient and, if implemented correctly, sometimes more transparent. However, when sold under the premise of improving trust and contributing to a more trustworthy society, this does not fly. Though electronic identification is but one activity of governmental and commercial interactions with citizens and customers, it is of course also linked to the bigger picture of the democratic state and rule of law. This is because, electronic identification, if misused and exploited, easily lingers around infringements of data protection, privacy, and security, and therefore plays an important role in the connection between the state, its political system, and societal trust.

The right approach to address the perceived or actual untrustworthiness of institutional intermediaries is to be more engaged in the production of trust, instead of abandoning them to a trustless, protocol-based, self-sovereign alternative. The labor of individuals and communities to voice criticism and hold entities accountable is the means of advancing toward improvement. Ultimately, it should also not be left unsaid that a well-functioning society relies on the establishment of mutual institutional trust. Institutions will find it hard to effectively offer good governance, services, assistance, security, and support to an anonymous society. In an era where alienation, social fragmentation, polarization, discrimination, and growing distrust are major societal issues, it seems strange to try to solve these challenges by moving to an identity infrastructure that is built upon the exact same premises, with no intention, or technical affordance to address or overcome them. Instead of disproportionately channeling efforts into replacing institutions and disrupting entire systems through trustless technologies, a more sustainable approach for the greater societal good would involve identifying untrustworthy individual actors and patterns, while concurrently directing resources towards rebuilding and regaining trust within the existing framework.

References

Abouelmehdi K, Beni-Hessane A, Khaloufi H (2018) Big healthcare data: preserving security and privacy. J Big Data 5(1):1. https://doi.org/10.1186/s40537-017-0110-7

Almond GA, Verba S (1963) The civic culture: political attitudes and democracy in five nations. Princeton University Press. https://www.jstor.org/stable/j.ctt183pnr2

Beck R, Czepluch J, Lollike N, Malone S (2016) Blockchain - the gateway to trust-free cryptographic transactions

Bijker WE, Hughes TP, Pinch TJ (1989) The social construction of technological systems: new directions in the sociology and history of technology. MIT Press

Bodó B (2021a) Mediated trust: a theoretical framework to address the trustworthiness of technological trust mediators. New Media Soc 23(9):2668–2690. https://doi.org/10.1177/1461444820939922

Bodó B (2021b) The commodification of trust. SSRN Electron J. https://doi.org/10.2139/ssrn.3843707

Bodó B, Janssen H (2022) Maintaining trust in a technologized public sector. Policy Soc 41(3):414–429. https://doi.org/10.1093/polsoc/puac019

Bodó B, Bene M, Boda Z (2023) Standing naked in the storm– European citizens' trust in social media, users, information. SSRN Scholarly Paper. Rochester, NY, February 23, 2023. https://doi.org/10.2139/ssrn.4368419

Botsman R (2017) Who can you trust? How technology brought us together and why it might drive us apart, 1st edn. Public Affairs, New York

Brown W (2017) Undoing the Demos: Neoliberalism's Stealth Revolution. First paperback edition, this Edition corrects errors in previous printings. Near Futures. Zone Books, New York

Catterberg G, Moreno A (2006) The individual bases of political trust: trends in new and established democracies. Int J Public Opin Res 18(1):31–48. https://doi.org/10.1093/ijpor/edh081

Christin A (2016) From daguerreotypes to algorithms: machines, expertise, and three forms of objectivity. ACM SIGCAS Comput Soc 46(1):27–32. https://doi.org/10.1145/2908216.2908220

Couture S, Toupin S (2019) What does the notion of 'sovereignty' mean when referring to the digital? New Media Soc 21(10):2305–2322. https://doi.org/10.1177/1461444819865984

Davidson S, De Filippi P, Potts J (2016) Disrupting governance: the new institutional economics of distributed ledger technology. SSRN Scholarly Paper. Rochester, NY, July 19, 2016. https://doi.org/10.2139/ssrn.2811995

Davidson S, Novak M, Potts J (2018) The cost of trust: a pilot study. J Br Blockchain Assoc 1(2):1–7. https://doi.org/10.31585/jbba-1-2-(5)2018

De Filippi P, Mannan M, Reijers W (2020) Blockchain as a confidence machine: the problem of trust & challenges of governance. Technol Soc 62:101284. https://doi.org/10.1016/j.techsoc.2020.101284

Earle TC (2009) Trust, confidence, and the 2008 Global Financial Crisis. Risk Anal 29(6):785–792. https://doi.org/10.1111/j.1539-6924.2009.01230.x

Eubanks V (2017) Automating inequality: how high-tech tools profile, police, and punish the poor. St. Martin's Press, New York, NY

Ferlie E, Ashburner L, Fitzgerald L (1996) The new public management in action. Oxford University Press

Ferrari MV (2022) The platformisation of digital payments: the fabrication of consumer interest in the EU FinTech Agenda. Comput Law Secur Rev 45:105687. https://doi.org/10.1016/j.clsr.2022.105687

Fukuyama F (1996) Trust: the social virtues and the creation of prosperity. 1. Free Press paperback ed. A Free Press Paperbacks Book. Free Press, New York

Gambetta D (1988) Can we trust trust. In: Gambetta D (ed) Trust: making and breaking cooperative relations. Basil Blackwell, Oxford, England, pp 213–237

Garland D (2001) The culture of control: crime and social order in contemporary society. Oxford University Press, Oxford, New York

Giddens A (1990) The consequences of modernity. Polity Press, Cambridge

Gille F, Brall C (2021) Limits of data anonymity: lack of public awareness risks trust in health system activities. Life Sci Soc Policy 17(1):7. https://doi.org/10.1186/s40504-021-00115-9

Goffman E (1990) The presentation of self in everyday life. 1. Anchor Books ed., rev. Ed. Anchor Books, New York

Golman R, Hagmann D, Loewenstein G (2017) Information avoidance. J Econ Lit 55(1):96–135. https://doi.org/10.1257/jel.20151245

Golumbia D (2016) The politics of bitcoin: software as right-wing extremism. University of Minnesota Press, Minneapolis

Greif A (1989) Reputation and coalitions in medieval trade: evidence on the Maghribi traders. J Econ Hist 49(4):857–882. https://doi.org/10.1017/S0022050700009475

Halpin H (2020) A critique of immunity passports and W3C decentralized identifiers. arXiv, November 30, 2020. https://doi.org/10.48550/arXiv.2012.00136

Halsema F, Teesink P (2022) Werken aan meer vertrouwen tussen Amsterdammers en de gemeente. Raadsinformatiebrief. City of Amsterdam, Amsterdam. July 30, 2022. https://openresearch.amsterdam/nl/page/89681/werken-aan-meer-vertrouwen-tussen-amsterdammers-en-de-gemeente

Hardin R (2002) Trust and Trustworthiness. The Russell Sage Foundation Series on Trust, vol 4. Russell Sage Foundation, New York

Hawlitschek F, Notheisen B, Teubner T (2018) The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron Commerce Res Appl 29:50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Herian R (2020) Blockchain, GDPR, and fantasies of data sovereignty. Law Innov Technol 12(1):156–174

Hert P, Gutwirth S (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. Privacy, Data Protection and Law Enforcement, Opacity of the Individuals and Transparency of Power, Privacy and Criminal Law 18. https://doi.org/10.11117/rdp.v18i100.6200

Hughes TP (1987) The evolution of large technological systems. In: Bijker WE, Pinch TJ (eds) The social construction of technological systems: new directions in the sociology and history of technology. MIT Press, Cambridge

Inglehart R (1990) Culture shift in advanced industrial society. In: Culture shift in advanced industrial society. Princeton University Press, pp 1–2. https://doi.org/10.1515/9780691186740-003

Ishmaev G (2021) Sovereignty, privacy, and ethics in blockchain-based identity management systems. Ethics Inf Technol 23(3):239–252. https://doi.org/10.1007/s10676-020-09563-x

Janssen M, Rana NP, Slade EL, Dwivedi YK (2018) Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. Public Manag Rev 20(5):647–671. https://doi.org/10.1080/14719037.2017.1305689

Jardine E (2015) The Dark Web Dilemma: Tor, Anonymity and Online Policing. SSRN Scholarly Paper. Rochester, NY, September 30, 2015. https://doi.org/10.2139/ssrn.2667711

Kahneman D, Tversky A (1979) Prospect theory: an analysis of decision under risk. Econometrica 47(2):263–291

Karlstrøm H (2014) Do libertarians dream of electric coins? The material embeddedness of bitcoin. Distinktion: Scand J Soc Theory 15:23–36. https://doi.org/10.1080/1600910X.2013.870083

Keymolen ELO (2016) Trust on the line: a philosophical exploration of trust in the networked era. Erasmus University Rotterdam. hdl.handle.net/1765/93210

Königs P (2022) Government surveillance, privacy, and legitimacy. Philos Technol 35(1):8. https://doi.org/10.1007/s13347-022-00503-9

Laufer B, Nissenbaum H (2023) Algorithmic Displacement of Social Trust. 23-12 Knight First Amend. Inst. (blog), November 29, 2023. http://knightcolumbia.org/content/algorithmic-displacement-of-social-trust

Levi M, Stoker L (2000) Political trust and trustworthiness. Annu Rev Polit Sci 3(1):475–507. https://doi.org/10.1146/annurev.polisci.3.1.475

Lips M (2019) Digital government: managing public sector reform in the digital era, 1st edn. Routledge

Misztal BA (1996) Trust in modern societies: the search for the bases of social order. Polity Press, Cambridge

Mühle A, Grüner A, Gayvoronskaya T, Meinel C (2018) A survey on essential components of a self-sovereign identity. Comput Sci Rev 30:80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Orgad L (2018) Cloud communities: the dawn of global citizenship? In: Bauböck R (ed) Debating transformations of national citizenship, IMISCOE Research Series. Springer International Publishing, Cham, pp 251–260. https://doi.org/10.1007/978-3-319-92719-0_46

Polanyi K (1944) The great transformation: the political and economic origins of our time. Beacon Press

Pozen D (2018) Transparency's Ideological Drift. SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3120807

Prat A (2005) The wrong kind of transparency. Am Econ Rev 95(3):862–877. https://doi.org/10.1257/0002828054201297

Putnam RD (2001) Bowling alone: the collapse and revival of American community, 1st edn. Touchstone Books by Simon & Schuster, London

Reijers W, Coeckelbergh M (2018) The blockchain as a narrative technology: investigating the social ontology and normative configurations of cryptocurrencies. Philos Technol 31(1):103–130. https://doi.org/10.1007/s13347-016-0239-x

Sedlmeir J, Barbereau T, Huber J, Weigl L, Roth T (2022) Transition pathways towards design principles of self-sovereign identity. ICIS 2022 Proceedings, December 12, 2022. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4

Sztompka P (1999) Trust: a sociological theory. Cambridge University Press

van Dijck J, Jacobs B (2020) Electronic identity services as sociotechnical and political-economic constructs. New Media Soc 22(5):896–914. https://doi.org/10.1177/1461444819872537

Weigl L, Barbereau TJ, Fridgen G (2023) The construction of self-sovereign identity: extending the interpretive flexibility of technology towards institutions. Gov Inf Q 40(2)

Werbach K (2017) Trust, but verify: why the blockchain needs the law. SSRN Scholarly Paper. Rochester, NY, August 1, 2017. https://doi.org/10.2139/ssrn.2844409

Werbach K (2018) The blockchain and the new architecture of trust. Illustrated Edition. The MIT Press, Cambridge, London, England

Wihlborg E (2013) Secure Electronic Identification (eID) in the intersection of politics and technology. Int J Electron Gov 6:143–151. https://doi.org/10.1504/IJEG.2013.058371

Zucker LG (1985) Production of trust: institutional sources of economic structure, 1840 to 1920. In: Cummings LL, Staw B (eds) Research in organizational behavior. JAI Press, Greenwich, Conn