Heurich, Benjamin; Lukács, Bence; Weidener, Lukas

Article

Science-on-chain: How can we trust science again?

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Heurich, Benjamin; Lukács, Bence; Weidener, Lukas (2026) : Science-on-chain: How can we trust science again?, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 15, Iss. 1, pp. 1-26, https://doi.org/10.14763/2026.1.2070

INTERNET POLICY REVIEW

Volume 15 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Science-on-chain: How can we trust science again?

Benjamin Heurich *Institute for Applied Blockchain (IABC)*
Bence Lukács *Institute for Applied Blockchain (IABC)*
Lukas Weidener
UMIT Tirol - Private University for Health Sciences and Health Technology

DOI: https://doi.org/10.14763/2026.1.2070

Published: 26 January 2026
Received: 30 September 2023 **Accepted:** 24 July 2024

Funding: The authors did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Heurich, B., Lukács, B., & Weidener, L. (2026). Science-on-chain: How can we trust science again? *Internet Policy Review*, *15*(1). https://doi.org/10.14763/2026.1.2070

Keywords: Trust, Open science, Decentralisation, Systems theory, Blockchain

Abstract: Over the last few decades society has lost significant trust in the work of the scientific community and debated the trustworthiness of scientific findings and (policy) implications. In response, an open science framework has been proposed based on accessibility and transparency of data and increased collaboration and participation among the scientific community and society at large. We argue that this can restore trust within society, and science itself. Following the proposed framework innovative scientists discovered the affordances of blockchain technology (e.g. inherent transparency, immutability, data security). However, since this issue describes a fundamental trend in society as a whole, it is worthwhile to conduct a sociological analysis through Niklas Luhmann's Systems Theory that focuses on both the functional areas and the purpose of trust in modern societies and the overall approach to disruptive technologies. This paper focuses on two key texts, the Bitcoin and Bloxberg white papers, used here as case studies to examine the theoretical underpinnings of trust in blockchain-based systems. We argue that while blockchain offers potential solutions, the term 'trust' is often misused in these discourses, overshadowing the need for a robust sociological framework. By critically analysing these technologies, we highlight their potential to reshape scientific practices and restore trust through a decentralised, transparent infrastructure.

Introduction: (why) does science have a trust problem?

The COVID19 pandemic put significant strain on the relationship of the scientific community and society at large. However, even before this global event shined a bright light on potentially serious issues within the scientific community, the so-called 'Replication Crisis' ignited debates about entire fields of scientific inquiry (Ioannidis, 2015). These debates extend to the implications for action items and related policies, as well as the fundamental concept of empirical analysis (Baker, 2016). Apart from the question of research data and its availability, the scientific community has been dealing with internal processes that can significantly alter how certain processes are perceived by society at large, e.g. the overwhelming leverage of journals with regard to the advancement of researchers' careers, the peer-review process and its misused incentive structure, as well as the in-transparency of scientific funding (see COPE & STM, 2022; Petrescu & Krishen, 2022; Fong et al., 2023).

In the following paper we will briefly address historical and current methods and mechanics available to the scientific community that were introduced to combat the aforementioned issues, namely the Open Access (OA) and especially the Open Science (OS) movement, as well as the general concept of decentralising technological infrastructure for science. Among the infrastructures proposed for such decentralisation, permissionless distributed ledger technology, of which blockchain is the most widely adopted form, first outlined in 2008, is particularly relevant. By establishing a consensus without trusted intermediaries, blockchain can safeguard the integrity and accessibility of scientific records, thereby operationalising the normative commitments of OS.

The concept of trust is pivotal not only in societal and scientific contexts but also in technological innovations, such as blockchain. In the well-known Bitcoin whitepaper published by Satoshi Nakamoto in 2008, the term 'trust' or its variation (e.g., trusted) is mentioned in 11 sentences. Given that the whitepaper is only nine pages long and primarily technical in nature, this frequent emphasis on trust reveals it to be a central design concern, rather than a peripheral consideration. With the whitepaper, Nakamoto (2008) addresses an important problem of the current financial system – the reliance on 'trusted third parties.' Through the prism of Luhmann's conceptualisation of trust, a deeper analysis of the whitepaper illuminates the paradigms inherent in blockchain technology. These paradigms are increasingly being applied beyond financial systems, including Decentralized Science (DeSci), to address critical issues of trust in scientific publishing and research processes (Weidener & Spreckelsen, 2024). But to thoroughly analyse these proposed im-

provements, it is key to first gain an understanding of how 'trust' functions in society and in relation to technological developments. In this regard, Niklas Luhmann's sociological Systems Theory not only serves this perspective but, due to its high degree of abstraction, also brings far-reaching new problem-solving approaches to the surface (Luhmann, 1993). Luhmann (2014) emphasises the close relation between trust, risk and sustainability, and moreover that trust is considered to be the most reliable mechanism for reducing complexity in all areas of modern societies. In addition, the inherent and important distinction between trust and familiarity (Luhmann, 2014) provides a new perspective on the actual functioning and importance of trust regarding the implementation of new technologies, thereby revealing interfaces and links that meet the demands of OS. To conclude our discussion, we apply this theoretical framework to a contemporary use case from the scientific community. We then examine whether, and in what ways, the Open Science and Decentralised Science (DeSci) communities can leverage technological developments to address public critiques and 're-store' trust in science.

Luhmann's systems-theoretical lens strengthens trust in three distinct ways. First, it widens the discursive horizon by integrating observations from different functional systems and lay public, which supports inclusivity (Luhmann, 1993). Second, it renders epistemic premises explicit by obliging observers to name the codes and programmes through which communication is selected, thereby enhancing transparency (Luhmann 1992). Third, its high level of abstraction allows the same framework to be reapplied as social or technological conditions change, making it possible to reassess and validate knowledge over long periods of development (Luhmann, 1998, 2014). Building on these three mechanisms, Luhmann (2014) argued that trust rests on stable expectations, which grow stronger when scientific knowledge circulates widely and remains accessible. Broad dissemination exposes findings to scrutiny from diverse audiences, a process that enhances credibility and curbs the monopolisation of knowledge. Luhmann (1993, 1998, 2014) further maintained that trust in any social system, the functional system of science, depends on the system's capacity to manage complexity and uncertainty. He notes, "The more inclusive the system is, the more it can reduce complexity and increase its capacity to produce reliable expectations" (Luhmann, 1992, p. 88). When science extends its reach, it demonstrates accountability and openness, qualities that sustain public trust, and encourages collaboration across societal boundaries.

Theories of this scope and complexity largely elude empirical research and inductive research approaches. We choose this approach in order to give substance to a research direction that we believe has not been sufficiently pursued and to create

a robust foundation for further social theory research in the field of open science, blockchain technology and society.

Can openness and decentralisation alleviate distrust?

The access to scientific knowledge has been guarded by various stakeholders for centuries of knowledge creation, first based on illiteracy and later through privileges and institutions. With the introduction of the printing press, and more recently, the internet, the dissemination of knowledge on a technical level became much easier. Unfortunately, these changes in the mechanisms of access did not automatically yield a wide societal participation in knowledge creation. Over the past several decades, there has been a growing consensus among institutions, governments, and researchers about the necessity of fostering broader and more genuine "openness" in both the creation of knowledge and access to scientific discoveries. This shift reflects a commitment to increasing transparency, inclusivity, and accessibility in the dissemination of research findings, thereby enhancing collaboration and innovation across disciplines (Peters & Roberts, 2015; Suber, 2012). Advocates for open science argue that unrestricted access to scientific knowledge not only accelerates discovery but also democratises information, ensuring that it benefits society as a whole (Willinsky, 2006).

Then in 2002, the first major initiative regarding OA was formulated ("Budapest Open Access Initiative"; BOAI, 2002) and in 2003 made more explicit through the *Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities* (Berlin Declaration, 2003). These statements not only raised awareness for the need of more inclusive processes, but also articulated an understanding and started a definitory work regarding OA. To this day, the definition provided in the Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities is widely used and referenced globally by institutions and organisations (Max Planck Society, 2003; Peters & Roberts, 2015; Suber, 2012). But as history has shown, simply declaring OA and OS a (policy) priority in knowledge creation processes, does not lead to immediate qualitative changes about the perception and quality of science, e.g. in some scientific communities OA could have impact by introducing a more diverse set of researchers and topics (Nagaraj et al., 2020), but in other communities of the Global South, which is a main target of OS policy, it can remain ineffective (Figueiredo et al., 2024). The further development of 'openness' principles, i.e. OS, institutions such as UNESCO, explicitly aim to alleviate distrust through opening up more (infra-)structure, mechanisms and processes:

> Increased openness leads to increased transparency and **trust in scientific information** and reinforces the fundamental feature of science as a distinct form of knowledge based on evidence and tested against reality, logic and the scrutiny of scientific peers. (UNESCO, 2022, p. 18)[1]

The declaration of such principles goes even further, by suggesting that the connection of opening up science and generating trust in society form a causal relationship:

> Dissemination of scientific information through scientific journalism and media, popularization of science, open lectures and various social media communications **builds public trust in science** while increasing the engagement of societal actors beyond the scientific community. (UNESCO, 2022, p. 27)[2]

Achieving societal engagement as envisioned in the UNESCO Recommendation on Open Science (2022) depends, at least in part, on the infrastructure through which scientific information circulates. Permissionless distributed ledger technology, as exemplified by blockchain technology, offers a decentralised architecture that can store, trace, and publish research data in a transparent and tamper-proof manner (Bartling, 2018; Ali et al., 2023). By lowering barriers to participation and opening research workflows, such systems invite the broader public to contribute directly to the creation of scientific knowledge.

Decentralised infrastructure provides a missing link between openness and public trust in science. UNESCO recognises that achieving openness requires specific infrastructural commitments: "[o]pen science infrastructures should be organized and financed upon an essentially not-for-profit and long-term vision, which enhances open science practices and guarantees permanent and unrestricted access to all, to the largest extent possible" (UNESCO, 2022, p. 19). Permissionless DLT meets these requirements. DLT can ensure records that are immutable, continuously replicated, and permanently available, so that the provenance of datasets and analyses can be audited at any moment. Distribution across many independent nodes removes single points of failure and ensures that data remain available even if a particular server, funder, or nation withdraws its support. By embedding these guarantees in the technical layer rather than in policy statements alone, de-

1. Emphasis added by authors
2. Idem

centralisation turns openness from an aspiration into an enforceable property, thereby strengthening public trust in scientific records.

More recently, a community of researchers has adopted these open-science principles and incorporated their use within their revolutionary technological stack (i.e. blockchain) and began to operate their scientific processes in a decentralized manner. This DeSci community and DeSci itself do not currently have a properly defined theory but can loosely be seen as OS principles extended by a Web3 technological stack (Ethereum Foundation, 2023). Early implementations exemplify how this translation potentially operates in practice. For example, ResearchHub operates on the principle of accessibility, incentivizing scientific discourse via a decentralised reward system based on blockchain technology. Ants-Review, utilising the Ethereum blockchain, tackles replication and trust issues through a transparent, community-driven peer review process (Lu et al., 2020; Trovò & Massari, 2021). These initiatives show how blockchain technology-enabled designs aim to foster trust; however, whether they succeed remains an open empirical question. The challenges and limitations of DeSci's technological stack and operational models underscore the need for further theoretical and empirical work (Heurich, Lukács, & Weidener, 2023). Therefore, this study focuses on a foundational theoretical analysis of trust, examining key texts such as the Bitcoin whitepaper and Bloxberg's whitepaper to bridge sociological theory and technological application.

However, these initiatives often overlook a critical element: a robust theoretical understanding of 'trust.' The assumption that mechanisms such as decentralized rewards or transparency inherently build trust remains insufficient without deeper scrutiny. Trust is not merely a byproduct of technological systems but a complex sociological construct that requires explicit theoretical frameworks for evaluation and validation (Luhmann, 2014). This gap underscores the importance of foundational analyses, such as the present study, to connect trust theory with practical technological solutions in DeSci.

Importance of trust in modern societies

Why is trust so valuable, and why does it seem to have become even more important in modern times? Sociologists such as Max Weber and Georg Simmel were already grappling with the concept and the immensely important role of trust at the beginning of the last century. Weber emphasised that actors can navigate highly complex social environments with the help of trust without needing to know much about them. Simmel (1907/2011) focused on the realm between knowledge and ignorance: trust compensates for lack of knowledge. In his book *The Philosophy of*

Money, Simmel (1907/2011) made it clear that without trust in the acceptance of a currency, all global financial transactions would quickly collapse.

For sociologist Niklas Luhmann, trust is primarily a "mechanism for reducing social complexity" (2014, p. 9). It helps us navigate modern societies in the face of an overwhelming world filled with possibilities, uncertainties, risks, and a completely undetermined future. In situations where there isn't enough information available to make a rational decision, or where there simply isn't enough time to evaluate the existing information, trust helps to make decisions nevertheless, even if it proves to be a risky proposition. The terms trust and risk are thus inseparable: trust is risky, meaning it carries the risk of having one's own expectations disappointed (Luhmann, 2014).

Niklas Luhmann, in his seminal work *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität* (2014), explores the dynamics of trust and distrust as essential mechanisms for managing social complexity. Luhmann argues that trust is not merely a personal sentiment but a structural necessity in social systems, enabling individuals to navigate an uncertain world. While trust facilitates cooperation and reduces complexity, distrust plays a critical role in safeguarding individuals and systems from potential harm by identifying and mitigating risks. According to Luhmann, distrust arises when the stability of expectations is undermined. In situations where trust is violated or where individuals perceive the likelihood of betrayal, distrust becomes a rational response to uncertainty. He highlights that distrust is not inherently negative; instead, it functions as a protective mechanism, allowing individuals and institutions to adapt and recalibrate expectations in response to perceived threats or inconsistencies. Luhmann moreover emphasises that distrust, like trust, is a way to manage the future's unpredictability. However, excessive distrust can lead to social fragmentation, as it prevents the formation of stable relationships and undermines the coordination necessary for collective action. Thus, Luhmann views distrust as both a necessary and potentially disruptive force within social systems, one that reflects the complexity and ambivalence of human interactions (Luhmann, 2014).

Years of research and analysis on the concept of trust have yet to yield a universally accepted definition. One of the reasons for this lies in the examination of trust across various scientific levels, leading to a contextual shaping of its meaning. The elusive nature of trust defies easy categorisation or a one-size-fits-all definition. Instead, scholars have approached it from multiple angles, recognising that trust operates differently in various contexts and scenarios. Referring to the deep psychological approach of Erik Erikson (1950) and the learning theory approach of Ju-

lian B. Rotter (1967), trust is analysed as a personal variable and considered a personality trait. This level of trust examination is rooted in a normative and structural-oriented perspective. It reflects their predisposition to rely on others and is often linked to their upbringing and experiences. This normative and structural-oriented approach draws from the works of Erikson and Rotter's learning theory. Moving to a more practical perspective, trust can also be viewed as a situational variable that influences decision-making (Erikson, 1950). This utilitarian approach to trust can be described as a situational variable in relation to decision-making processes. It is rooted in economic game theory and examines how individuals make choices based on the level of trust they have in others. However, these two perspectives have no explicit relevance for a theoretical discussion of the scope presented in this paper. This is because the layers of complexity that can be revealed by the definitional power of these two individualistic and personality-based approaches do not do justice to the challenges facing society as a whole and to the issues that hold promise for the years to come.

Therefore, we approach the subject via a third definitory framework, which is based on the social theoretical foundation of Niklas Luhmann's Sociological Systems Theory. Luhmann (2014) provides a broader systemic view of trust as a variable that reduces complexity in social interactions. In an increasingly complex and dynamic environment, trust serves as a stabilising force, allowing social structures and behavioural norms to emerge and persist. This systemic and difference-theoretical approach develops its analytical value in the context of an environment that is constantly increasing in complexity. Luhmann (2014; 1993) states that any societal system would not function without trust as a variable for psychological and social risk reduction, as social structures and behavioural orientations are not constant in the light of continuing technological advances and ongoing modernisation processes. Consequently, even trust in an individual cannot completely eliminate risks because one cannot acquire complete information about the expected behaviour of other individuals. The other person is always just another ‘self’ who may experience the same things but can distance themselves from what one personally perceives as true. Therefore, trust does not form towards a person, but only towards an expectation and what is experientially observable. Luhmann (2014) elaborates further on trust in terms of temporality by stating that the "future contains many more possibilities than can be realized in the present and transferred into the past" (p. 33). Consequently, the future holds more risks than an individual can be aware of at a given moment. Here, Luhmann agrees with Ulrich Beck (1992) in considering risk minimization and complexity reduction as constitutive elements of the progressive dynamics of modern societies.

Risk, trust and familiarity

With a focus on dealing with future risks, it becomes clear that the establishment of trust is primarily a complex psychological process initiated by individuals during times when ontological security is no longer guaranteed. These transitional situations are often driven by technology and characterised by the fact that trust, the belief in predictability of actions and social relations, is not a given certainty but must be actively created by the actors involved. Luhmann (2014) draws a line regarding trust and predictability, emphasising that there is no absolute security regarding the non-occurrence of future disadvantages. Drawing on his analysis of how trust operates through "fictions that function" (p. 78) — social constructs that work despite their contingent nature — security itself can be understood as a working fiction that enables social coordination He goes one step further and contrasts trust with the concept of familiarity, as a sustainable condition that enables individuals to reasonably expect something at all. Familiarity is not a category for categorising expectations; “it is merely a prerequisite for both trust and mistrust” (Luhmann, 2014, p. 31). This does not provide a definitive assessment of whether a system's operations are good or bad, but rather an agreement on how this qualitative assessment can be made. Familiarity with societal processes allows the recognition of favourable and risky life situations, which are then integrated into personal decision-making situations. This demonstrates that, in familiar situations, the past generally prevails over the present. Luhmann emphasises that, in addition to familiarity, trust heavily depends on society members' experience-based knowledge. However, trust is not generated by extrapolating future events from past knowledge, but rather by "overlapping the information it possesses from the past and risking a determination of the future" (Luhmann, 2014, p. 26). Only this kind of knowledge is suitable for minimising future risks, and its application and value must persist into the future. However, relying on the past, especially in the era of digitalization, is not very effective because the structure and functioning of the Internet or blockchain technology for that matter, as well as the cultural, societal, or intentional attributes of communication participants, cannot be confidently placed into future decision-making situations. Here it becomes clear that familiarity is not a guarantee that something is secure or trustworthy. Familiarity is merely a form of observation where the familiar is distinguished from the unfamiliar. Each person makes this distinction and labels what is familiar or unfamiliar to them individually. In a continuous examination, familiar forms and meaningful constructs are assessed for their value within one's own life world. A sense of security that may accompany familiarity is not a sociologically manageable concept, but rather a sentiment that can dissolve with each further examination of life world contexts.

Within this framework, which constitutes itself as the unity of the difference between familiarity and unfamiliarity, constructivist knowledge is developed in dealing with new technologies and their influence on daily decisions in societal interactions. This implies that the handling of what is familiar always occurs within the entire society, which is observed as a unity without necessarily being conceptually graspable as a unity. Familiarity arises with the awareness that what one person applies in their everyday life, which may provide them with a sense of security or enduring trust, can represent risky unfamiliarity for another person and likely generate mistrust. Familiarity does not, therefore, give rise to a universal claim of normative action, as it can serve as the basis for both trust and mistrust.

In sociological systems theory, both trust and distrust can be constitutive for a social system. Experiences with 'NFT rug pulls', network outages, or complications in the governance structures of DAOs leads to the emergence of mistrust, but also to the formation of new social connections and the creation of new familiarity. The event of a personal or societal consequence has to occur for the first time before it is recognised as a risk by individuals and subsequently renegotiated within (digital) society. Beck (1992) refers to this process as the identification of "socially accepted risks" (p. 31). Ongoing engagement of this kind strengthens trust and generates resilience in social systems that, for instance, utilise the functionality of blockchain technologies. Therefore, when trust is discussed in this context, it refers to the consistent and familiar environment that constitutes itself at each present moment of decision or action (Luhmann, 2014). This situation is filled with expectations and knowledge that are continuously reviewed and updated. When expectations are disappointed, once-held trust is also called into question.

Blockchain technology and society

In contemporary discourse, technology is typically framed as a purely instrumental tool for achieving predefined objectives (Luhmann 2005). This interpretation suggests the idea that one can choose technologies to achieve certain goals as efficiently and cost-effectively as possible. "A technology is a tried and tested simplification, but that does not make it a rational way of transforming nature or society" (Luhmann, 2005, p. 74). In the end, one is confronted with unintended side-effects (risks) that give rise to the invention of new ends and new technologies that maintain these end-means relationships (Luhmann, 1998). Ultimately, the complexity of the tasks determines the limit of the plannability and technical feasibility of non-natural states (Hofmann & Williams, 2017). Failures then encourage the redesign of technological arrangements and divide observers into inventors and users of the technologies on one hand and those who reject technology or want to see it re-

duced on the other (Luhmann, 1992). This process creates an asymmetry of information as well as a knowledge and/or competence gap, resulting in risks for members of society when it comes to the usability of technology (Mukherjee, 2006).

As Luhmann (1992) argues, technological systems inherently generate complexity, which requires continuous adaptation and can lead to societal divides as different groups respond to the uncertainty and unpredictability that accompany new technologies. This asymmetry of knowledge between innovators and skeptics, he suggests, produces a "differentiation of perspectives" that influences how technology is accepted or rejected by different social groups (Luhmann, 1992, p. 74). It remains undisputed that technologies are to a large extent developed intentionally, i.e., designed with the intention of achieving a certain effect, and this is true even if the objective is only brought into its final form during the development phase. For example, railways were designed not only for freight but also for passenger travel. Similarly, the earliest telephones permitted communication in only one direction. Within a few years, they were redesigned so that the callers could speak and hear simultaneously.

At the same time, Luhmann's perspective on technology views artifacts chiefly as products of social evolution, in which purposeful intentions emerge only after situations are already sufficiently pre-structured (Luhmann, 1998; 2005). The ends/means perspective of the inventors, financiers and users is then only the play material of this (social) evolution, the effects of which are determined by whether sufficient causal isolation is achieved or not. Thus, the inventive path that began with cryptography and led via Bitcoin, the development of further consensus mechanisms and smart contracts to the general imperative of decentralisation can also be seen as a technology-driven social evolution. This approach makes it possible to focus on the social components of technological development processes and to ask about its functionality for society as well as its contribution to other social systems such as education, law, politics, economics and science (Luhmann, 1993).

Over time, the original purpose of any technology must align with the evolving problems faced by modern society. The trust in natural technologies as formulated by the laws of the natural sciences and the trust in tried and tested artificial technologies had offered a kind of stability and halt to an increasingly complex world that had disregarded all kinds of ecological, economic and educational side-effects for a long time (Luhmann, 1998); nor was sufficient attention paid to global interdependencies. Thus, centralised structures have been consolidated for decades. Only in recent decades have the ecological consequences of technological developments become the subject of public attention. This has led to a rapidly increas-

ing aversion to technology, which is additionally fed by the old humanistic resentments of technology and science. The emerging question in many people's minds is how the great purpose of a new technology can be to revolutionize everything that is traditionally accepted and apparently functioning? One can hold any opinion regarding the fundamental principle of decentralisation that underlies this argument, but one thing is certain: current social problems can certainly not be solved by rejecting technologies. For it is and ultimately remains a problem of the complexity of the world (Luhmann, 2005).

Science (and) blockchain

The emergence of blockchain technology has generated renewed optimism within the scientific community, particularly regarding its potential to enhance transparency, data integrity, and trust in research processes (Bartling, 2018; Lukács et al., 2023). Its potential to address the 'trust-issue' that permeates through society is being increasingly recognised and harnessed in innovative ways. From blockchains developed by universities to DeSci projects reimagining the landscape of scientific publishing, the applications of this technology are as diverse as they are promising. Amid this enthusiasm, it is especially crucial to critically examine the discourse surrounding 'trust' as it relates to blockchain technology based on the theoretical discussion presented above. This technology offers significant potential for transforming the practice of science and counteracting the previously mentioned structural issues within the scientific community, though realizing this potential depends on addressing fundamental questions of governance and trust. Therefore, changing societal interactions with science itself, by providing a secure and transparent infrastructure for verifying and sharing scientific data, blockchain can help to foster greater confidence in scientific research. However, to be able to establish this trust in the long term, both a familiarity with the technological structures and a future-oriented and sustainable approach to recognised risks and dangers must be learned. This approach must then immediately become part of blockchain education. Even if blockchain education is not part of the discussion in this paper, this connection to trust must not be ignored and can be considered an important desideratum.

Origins of trustless infrastructure

The omission of a formal definition or exploration of the term 'trust' in the Bitcoin white paper is both intriguing and significant, especially considering the pivotal role trust plays in the proposed system. This absence might suggest that Nakamoto presumed a universal understanding of 'trust', implying that its definition was

self-evident and universally shared, rendering further elaboration unnecessary. As the Bitcoin whitepaper marks the beginning of blockchain technology, its foundational ideas have significantly influenced subsequent developments and innovations in the field. The paper set the stage for a new era of decentralised systems, where intermediaries were no longer deemed essential, challenging the traditional notions of trust in the process. In this context, it becomes especially important to engage with the concept of 'trust', particularly from Luhmann's perspective. His theories on trust can offer valuable insights into how the notion of trust is interpreted and understood in a decentralised world based on blockchain technology and Nakamoto´s vision.

TABLE 1: Bitcoin white paper and mentions of 'trust'

PAGE NUMBER	CITATIONS OF THE TERM 'TRUST' AS PART OF THE WHITE PAPER (EMPHASIS ADDED BY AUTHORS)
1	Digital signatures provide part of the solution, but the main benefits are lost if a **trusted** third party is still required to prevent double-spending
1	Commerce on the Internet has come to rely almost exclusively on financial institutions serving as **trusted** third parties to process electronic payments
1	While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the **trust** based model
1	With the possibility of reversal, the need for **trust** spreads
1	These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a **trusted** party
1	What is needed is an electronic payment system based on cryptographic proof instead of **trust**, allowing any two willing parties to transact directly with each other without the need for a **trusted** third party
2	A common solution is to introduce a **trusted** central authority, or mint, that checks every transaction for double spending
2	After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are **trusted** not to be double-spent
2	To accomplish this without a **trusted** party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received
6	The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the **trusted** third party
8	We have proposed a system for electronic transactions without relying on **trust**

In the context of trust, two sentences from the Bitcoin whitepaper seem especially

important and should be used for further analysis and discussion:

> *What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.* (Nakamoto, 2008, p. 1)

> *We have proposed a system for electronic transactions without relying on trust.* (Nakamoto, 2008, p. 8)

Reconceptualising trust in decentralised systems

Both these sentences encapsulate Nakamoto's revolutionary proposition, which is to redefine the traditional understanding of trust in financial transactions. From Luhmann's perspective, trust is a mechanism to reduce social complexity, enabling individuals to make decisions without having full information or certainty. In traditional banking, we place trust in the bank, a central entity, to handle our financial transactions faithfully and securely. However, Nakamoto's vision challenges this by suggesting that this form of trust can be replaced or at least supplemented by mathematical proofs and decentralised consensus mechanisms. What this implies is that trust is not eliminated, but rather transformed. Instead of placing trust in a single, centralised, 'closed-operating' (Luhmann, 1993, p. 65) entity (like a bank), users place trust in the operating mode of the technology itself – its algorithms, cryptographic methods, and the decentralised network of peers. This shift is profound as it decentralises trust, spreading it across a network rather than concentrating it in a single institution. With the loss of the bank as a direct addressee, the level of responsibility for actions and decisions also shifts. Due to the newly gained autonomy and control of the individuals, responsibility therefore also shifts to a personal level. With every use of blockchain technology, a certain level of familiarity is created, which serves as the basis for trust, but also mistrust. Such a reconfiguration of trust raises numerous questions: Can mathematical and cryptographic proofs truly replace the trust we place in human institutions? How does the decentralisation of trust affect the broader socio-economic landscape? And perhaps most importantly, as the technology matures and becomes more ubiquitous, how will society's understanding of trust evolve in response?

As framed in this analysis, the reconfiguration of trust in blockchain technology aligns with, and extends, the discourse surrounding the complex dynamics of trust and technology. Zavolokina et al. (2023) emphasise that while blockchain is often

touted as a “trust-free” system, it actually shifts the focus of trust from centralised institutions to the transparency and immutability of its algorithms, creating new trust expectations centered on system design and user understanding (Zavolokina et al., 2023, p. 1). Ali et al. (2023) highlight blockchain's defining characteristics – such as reliability, tamper-proofing, and decentralization – as essential components in fostering trust but caution that these technical features alone are insufficient for comprehensive trust formation (Ali et al., 2023). This complements Bodó’s (2021) argument that the mediation of trust by digital technologies, including blockchain, introduces new risks and responsibilities, particularly as technology itself becomes the mediator of trust (Bodó, 2021). Moreover, Duenas-Cid and Calzati (2023) critiqued the societal legitimation of trust in data-driven systems, underscoring how blockchain’s decentralisation complicates the translation of trust from institutional contexts into new socio-technical ecosystems (Duenas-Cid & Calzati, 2023). Together, these studies underscore the interplay between technical design, user understanding, and broader societal structures in the evolution of trust in the blockchain. By situating the transformation of trust within Luhmann’s framework of reducing social complexity, this analysis deepens the understanding of blockchain’s socioeconomic implications, particularly the redistribution of trust and responsibility to individuals navigating these systems.

A science blockchain: Bloxberg

In seeking answers to these profound inquiries about trust in the digital age, it becomes imperative to examine real-world applications that embody the shift from traditional trust mechanisms towards a more decentralized model. DeSci provides a variety of practical solutions within the scientific domain, especially those related to the challenges of the scientific publishing system and its trust dynamics. To better understand the potential conflicts and implications of using blockchain technology in science, particularly considering Luhmann's views on trust, we will examine one particular solution – claiming to be the ‘Blockchain for Science’.

Infrastructure design and trust architecture

Motivated by the expectation that distributed ledger infrastructures can provide an alternative to the existing scientific system, *Bloxberg* was founded by the Max Planck Society in February 2019 as a consortium of 11 research organisations across nine countries. The Bloxberg blockchain operates on a permissioned Ethereum implementation utilising a Proof of Authority (PoA) consensus algorithm. Unlike the traditional Proof of Work mechanisms, PoA relies on pre-approved authority nodes operated by trusted research organisations. This allows for greater

efficiency, security, and scalability while minimising computational overhead. The infrastructure provides key functionalities such as timestamping, certification, and verification of research data through decentralised applications (dApps), such as Certify and Verify. These tools enable researchers to generate proof of existence and authorship, protecting intellectual property rights, while enhancing transparency. Viewed through Luhmann's framework of trust, these design choices embed expectations of reliability at the infrastructural level, which allows participants to act despite limited direct oversight.

In Luhmann's (2014) view, trust is a leap of faith that allows individuals to navigate an uncertain and complex world. It is a form of 'confidence' that enables us to act despite the inherent risks and uncertainties in social life. In the scientific community, trust is typically established through rigorous peer review processes, reputation of research institutions, and personal credibility of researchers. It is "trust in the present of those researching at the same time" (Luhmann, 1992, p. 558). However, these traditional mechanisms of trust are not without limitations and vulnerabilities. In the end, the scientific system places trust in itself. It assumes that existing knowledge is subject to continuous scrutiny and that it would no longer exist if it could not be upheld in the present. The social system of science, therefore, evaluates not its own past but itself. It counts on scientists to be honest, to not suppress doubts but to report and verify them. It assumes itself to be a system that does not deceive itself (Luhmann, 1992).

The Bloxberg Association seeks to address the challenges surrounding trust by leveraging the power of blockchain technology. Bloxberg seeks to realise these trust-related objectives by reducing the risk of data manipulation, enhancing the transparency of research processes, and facilitating the verification of research outputs. However, as Luhmann reminds us, trust is not simply a technical or procedural issue, but fundamentally a social and relational phenomenon. Therefore, the success of the Bloxberg Association and similar DeSci projects will depend not only on the technical robustness of their blockchain solutions, but also on their ability to navigate the complex social dynamics of the scientific community, the interdependencies and structural couplings (Luhmann, 1993) between all social systems and society at large. This includes addressing the issues of power and inequality, fostering a culture of openness and collaboration, and building strong relationships with a diverse range of stakeholders.

Despite its strengths, Bloxberg's governance model raises critical questions regarding trust and centralisation. While described as "permissioned public," its PoA structure inherently depends on a limited number of authority nodes. These nodes,

vetted and maintained by selected research organisations, consolidate significant power, potentially creating familiarity-based trust rather than the broader systemic trust envisioned by blockchain advocates. As Luhmann (2014) differentiates trust from familiarity, this reliance may reinforce the existing hierarchies in the scientific community, undermining the decentralised ethos of blockchain technology. Moreover, the phrase 'trusted network' in Bloxberg's whitepaper appears to emphasize procedural trust in the blockchain's technical framework while glossing over relational trust in the organisations managing it.

This dynamic prompts critical reflection: who monitors Bloxberg in its role as the *de facto* gatekeeper of the consortium, and, by extension, over the authority nodes and research institutions that operate them? By narrowing the governance structure to a select group, Bloxberg risks replicating the power imbalances it seeks to disrupt. Furthermore, while the PoA consensus mitigates risks, such as '51% attacks', it also centralises decision-making authority within the network's founding members. Such a model requires transparent mechanisms for onboarding new nodes, resolving conflicts, and ensuring accountability to avoid eroding trust among stakeholders.

Science without trust?

To further illustrate the potential conflicts that can occur due to an insufficient consideration of the definition of trust and the associated consequences for science as defined by Luhmann (1992; 2014), the whitepaper of the Bloxberg Association should be analysed. Within the first version of the Bloxberg whitepaper published in February 2019 (Vengadasalam et al., 2019), the term 'trust' is mentioned four times.

TABLE 2: Bloxberg whitepaper and mentions of 'trust'

PAGE NUMBER	CITATIONS OF THE TERM 'TRUST' AS PART OF THE WHITEPAPER (EMPHASIS ADDED BY AUTHORS)
1	Bloxberg – The **Trusted** Research Infrastructure
5	By establishing the permissioned, public blockchain Bloxberg the network is safeguarded against the cryptographic power of third entities, as the credibility of the research organizations maintaining the network, constitute **trust** in the system.
5	For example, with consented transactions on the Bloxberg infrastructure, research claims need not to be limited to one institution alone, but can be confirmed by the whole **trusted** network.
19	With Bloxberg, research claims need not be limited to one institution alone, but can be confirmed by the whole **trusted** network.

It should be emphasised that despite trust being an integral part of the Bloxberg Association's and DeSci's narrative, highlighted by the description in the subheading, no definition of 'trust' is provided in the first version of the whitepaper. This omission is surprising, especially considering the weight and centrality of the term in the entire concept of a 'Trusted Research Infrastructure'. Trust, in its multifaceted nature, has significant implications not only in the realm of technology, but also in the sociocultural dynamics of the scientific community. A clear and comprehensive definition would provide stakeholders – from researchers to institutions – with a foundational understanding upon which they can base their interactions and expectations. Furthermore, as the initiative seeks to revolutionise the scientific research landscape through the utilisation of blockchain, it becomes imperative to delineate what 'trust' means in this context.

Interestingly, in the updated whitepaper published in February 2024 (Kleinfercher et al. 2024), 'trust' is only mentioned once[3]. Although the rationale for this rebranding has not been disclosed, examining the shift is analytically valuable because it reveals how the project now treats trust. What had been an explicit promise ("Trusted Research Infrastructure") is recast as an implicit attribute of the technology itself ("The Blockchain for Science"). This rhetorical move offers a concrete case for tracing how DeSci initiatives renegotiate the meaning of trust over time and how those renegotiations align (or fail to do so) with Luhmann's distinctions.

Potential reasons could be some of the following:

- The evolution of trust in technology: The change in emphasis from "The Trusted Research Infrastructure" to 'The Blockchain For Science' may reflect a maturing understanding of blockchain within the scientific community. As blockchain becomes more widely understood and accepted, the explicit need to label it as a 'trusted' system may diminish. Instead, the focus on the technology itself can be seen as a statement that trust is an inherent quality of the blockchain.
- The challenges of defining trust: The lack of explicit definition of 'trust' in the Bloxberg whitepapers may exemplify the difficulty in pinning down this multifaceted concept, especially in a rapidly evolving field like blockchain technology. Trust is not merely a technical issue but a complex social phenomenon (Luhmann, 2014). This might explain why it is challenging to encapsulate 'trust' within a whitepaper, as it involves interpersonal relationships, cultural norms, institutional credibility, and

3. Citation: With Bloxberg, research claims need not be limited to one institution alone, but can be confirmed by the whole **trusted** network (p. 17, 2024) (emphasis added by authors)

more.
- Implications for collaboration and openness: By referring to Bloxberg as 'The Blockchain For Science,' the initiative might be signalling a broader, more inclusive approach. This aligns with the contemporary drive in the scientific community for increased collaboration and open access to research.

The Bloxberg initiative, as outlined in their 2019 whitepaper, 'Bloxberg - The Trusted Research Infrastructure', proposed a blockchain-based solution to address challenges faced by contemporary science, including the verification of research authenticity. The emphasis was firmly on trust, yet intriguingly, the concept remained undefined in the whitepaper. By contrast, the 2024 updated whitepaper titled 'The Blockchain For Science' notably reduces its emphasis on trust, despite its ongoing significance (Kleinfercher & Vengasasalam, 2024). Although the initial phrase "By establishing the permissioned, public blockchain Bloxberg the network is safeguarded against the cryptographic power of third entities, as the credibility of the research organizations maintaining the network, constitutes trust in the system" (2020, p. 5) was omitted in the updated whitepaper, Bloxberg's blockchain continues to be described as 'public, permissioned'. This terminology, "permissioned, public blockchain," presents a seeming discrepancy in the context of trust and inclusivity.

Examined through Luhmann's lens of trust, Bloxberg's trust architecture reveals a clear duality. On one side, there is procedural trust in the blockchain's technical foundation. On the other, there is a relational trust placed in the network-maintaining research organisations. Yet, this bifurcation poses a potential risk: by narrowing network maintenance to authorised research organisations, could Bloxberg unintentionally sustain the scientific realm's existing power imbalances? This is accentuated by the updated whitepaper's mention of security, asserting that "Security is guaranteed by distributed Authority nodes… preventing a malicious 51% attack" (Kleinfercher et al., 2024, p. 7). Such a statement emphasises the criticality of these select 'Authority nodes'.

This raises the following questions: Who monitors the monitors? How can we ensure that these organisations themselves are trustworthy and act in the best interests of the scientific community? This shift points to a notable shift in familiarity with given structures and the consistency with which trust can be formed. The risk that distrust could develop as a result of this shift increases. Here, the added value of Luhmann's definitional distinction between trust and familiarity becomes clear. Moreover, Luhmann's (2014) framework underscores that trust is not just about simplification; it is also a leap of faith. In Bloxberg's model, these 'trusted' organi-

sations assume that leap, taking on a pivotal role in anchoring the credibility and reliability of the entire system for its users.

The statement “With Bloxberg, research claims can be confirmed by the whole trusted network” still features in the updated whitepaper (Kleinfercher et al., 2024, p. 17). Although it insinuates broad validation, it is potentially misleading. The network merely timestamps data, ensuring 'proof of existence' and 'proof of authorship'. It doesn't ascertain the research claim's veracity, underscoring the multifaceted nature of trust in blockchain frameworks. While Bloxberg's updates signal an evolution in its stance, the underlying challenges and complexities of merging technology with trust remain. The intertwining of these domains necessitates continuous scrutiny and reflection.

Discussion

DeSci has the potential to challenge traditional hierarchies and inefficiencies within scientific systems, leveraging blockchain technology to enhance transparency, reproducibility, and inclusivity. However, the mere deployment of blockchain technology does not inherently address the multidimensional challenges of trust in science. By design, blockchain technology offers procedural guarantees through features such as immutability, cryptographic security, and decentralised validation mechanisms (Ali et al., 2023; Zavolokina et al., 2023). For example, platforms such as Bloxberg rely on timestamping to provide ‘proof of existence’ and authorship for the research data. However, practical implementation reveals significant operational complexities: DeSci-DAOs struggle to balance token-weighted governance against scientific expertise, manage hybrid on-chain/off-chain accounting, and navigate institutional interfaces such as university Technology Transfer Offices (Weidener & Boltz, 2025). Therefore, while such mechanisms aim to enhance procedural transparency, they fail to address relational trust – public confidence in the intentions and credibility of the individuals and institutions governing these systems (Bodó, 2020; Luhmann, 2014).

The dual nature of trust in decentralised science

To counteract public skepticism, DeSci initiatives must move beyond procedural guarantees and engage directly with relational trust. This includes addressing the fundamental questions: Who governs blockchain platforms? Are these entities accountable to the public, and how is the misuse of authority prevented? Transparency regarding governance processes and explicit public-facing commitments to inclusivity are essential. Furthermore, platforms can incorporate mechanisms for in-

teractive public engagement such as citizen oversight panels, which can review node governance and platform decisions (e.g. Danish consensus conferences (Joss, 1998). This participatory approach aligns with Luhmann's (2014) emphasis on reducing complexity through trust-building within interdependent systems.

The Bloxberg blockchain exemplifies the duality inherent in the existing applications of blockchain technology in science and DeSci. On the one hand, its Proof of Authority (PoA) consensus mechanism minimises computational overhead and secures data integrity through pre-approved authority nodes (Bloxberg Whitepaper 3.0, 2024). However, this reliance on a limited set of research institutions introduces significant governance centralisation. By narrowing the governance structure to select organisations, Bloxberg risks reinforcing pre-existing hierarchies and undermining the decentralised ethos of blockchain technology (Bodó, 2020). This centralisation raises critical questions: Who decides which institutions qualify as authority nodes? How are their decisions scrutinised, and by whom? As Shapiro (1987) and Sztompka (1999) highlight, trust in institutional systems requires checks and balances, including mechanisms for managing distrust (Duenas-Cid & Calzati, 2023). Without such measures, platforms such as Bloxberg risk creating a veneer of decentralisation, while inadvertently replicating the same structural inequities that undermine their stated goals of transparency and open access . To mitigate these risks, DeSci platforms can adopt hybrid governance models inspired by decentralised autonomous organisations (DAOs). For example, voting mechanisms for node inclusion could involve not only founding members, but also independent stakeholders and public representatives. Such models would distribute power more equitably and align with UNESCO's (2022, p. 17) call for open science infrastructures that are "inclusive, sustainable and equitable."

Policy recommendations: a framework for institutional and technical reforms

- Diversified governance structures: DeSci platforms must go beyond token inclusivity by instituting mandatory diversity benchmarks in their governance frameworks. Authority nodes or equivalent decision-making entities should include institutions from the Global South and underrepresented research disciplines. This can be achieved through a rotating system of node selection and quotas for participation, ensuring that centralized power does not perpetuate the existing hierarchies. Platforms such as Bloxberg could pioneer such initiatives by providing transparent criteria for node selection that prioritize inclusion alongside scientific excellence.
- Interoperability standards: Fragmentation remains a significant impediment to the scalability of the DeSci technologies. International

organisations such as UNESCO and the OECD should convene multi-stakeholder working groups to develop universal interoperability protocols for blockchain-based scientific infrastructures. These standards would cover the seamless exchange of data and metadata, while requiring transparent reporting of governance decisions, node activity logs, and audit trails to align procedural transparency with relational trust.

- Enhanced verification mechanisms: Blockchain platforms must expand beyond timestamping functionalities to integrate independent layers of verification that directly address replication crises. One approach could be embedding reproducibility metadata within blockchain records or linking claims to independently verified peer review data. This integration would foster trust not only in the data's existence but also in its scientific validity, addressing the concerns highlighted in both Bitcoin and Bloxberg whitepapers.
- Public engagement initiatives: Public skepticism often stems from a lack of understanding of the technical applications of blockchains in science. Governments, academic institutions, and private platforms should co-invest in blockchain literacy programs that target scientists, educators, and the general public. DeSci platforms can develop user-friendly dashboards that visualize blockchain operations (e.g., node activity and data verification processes) to make procedural trust more accessible and intuitive. Public workshops and collaborations with media outlets can further clarify the role of blockchain in fostering transparency and reliability.
- Dynamic feedback and oversight mechanisms: Trust in decentralised systems requires not only transparency but also accountability. Platforms such as Bloxberg should implement mechanisms for dynamic feedback, such as user-reported audits or peer-led reviews of node activities. Oversight boards comprising independent researchers, ethicists, and public representatives can be established to periodically evaluate platform governance and ensure alignment with scientific and societal values.

Although DeSci offers a compelling vision for the future of scientific collaboration, its transformative potential remains constrained by unresolved governance and relational trust challenges. The reliance on permissioned systems such as Bloxberg highlights the difficulty of achieving true decentralisation in practice. Without rigorous oversight and inclusive governance, DeSci risks perpetuating the very inequities it seeks to address (Duenas-Cid & Calzati, 2023; Bodó, 2020). Nevertheless, the integration of blockchain into scientific systems presents unprecedented innovation opportunities. By embedding decentralised technologies into a broader framework of institutional reforms, DeSci can democratise access to scientific resources, enhance collaboration across disciplines and rebuild public trust. Achieving these goals will require not only technological advances, but also systemic cul-

tural shifts within the scientific community, supported by robust policy frameworks and public engagement.

Conclusion

Trust in science remains a cornerstone of societal progress; however, it faces unprecedented challenges in the modern era. Decentralised technologies such as blockchain present a promising avenue for addressing structural weaknesses in scientific processes, offering solutions for transparency, reproducibility, and accessibility. However, as this study has shown, trust cannot be engineered solely through technical systems. It is fundamentally a social construct that requires a nuanced approach that integrates technology with systemic reform. By examining key case studies such as Bitcoin and Bloxberg whitepapers through the lens of Luhmann's sociological theory, this study underscores the dual nature of trust in decentralised systems: procedural trust in the technology itself and relational trust in the stakeholders governing it. Both forms must coexist and be continuously nurtured to ensure the credibility of the science. Looking forward, DeSci must expand its vision beyond operational improvements, striving to address deeper sociopolitical issues such as inclusivity, equity, and public engagement. By integrating decentralized systems into a broader ecosystem of trust-building measures, the scientific community counteracts public skepticism and ensures its relevance to the 21st century.

References

Ali, V., Norman, A. A., & Azzuhri, S. R. B. (2023). Characteristics of blockchain and its relationship with trust. *IEEE Access*, *11*, 15364–15374. https://doi.org/10.1109/ACCESS.2023.3243700

Baker, M. (2016). 1,500 scientists lift the lid on reproducibility. *Nature*, *533*(7604), 452–454. https://doi.org/10.1038/533452a

Bartling, S. (2018). *Blockchain for science and knowledge creation*. https://doi.org/10.5281/zenodo.60223

Beck, U. (1992). *Risk society: Towards a new modernity* (repr). Sage.

Bence, L., Heurich, B., & Weidener, L. (2023). *Opportunities and limitations of decentralization in decentralized science*. 170 KB, 6 pages. https://doi.org/10.48446/OPUS-14635

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

Budapest Open Access Initiative. (2002). *Read the declaration – Budapest Open Access Initiative*. http

s://www.budapestopenaccessinitiative.org/read/

Committee on Publication Ethics (COPE) and STM. (2022). *Paper mills research*. Committee on Publication Ethics and STM. https://doi.org/10.24318/jtbG8IHL

Duenas-Cid, D., & Calzati, S. (2023). Dis/Trust and data-driven technologies. *Internet Policy Review*, *12*(4). https://doi.org/10.14763/2023.4.1727

Erikson, E. H. (1950). *Childhood and society* (1st ed). W. W. Norton & Company, Incorporated.

Ethereum Foundation. (2023). *Dezentrale Wissenschaft (DeSci) [Decentralised science (DeSci)]*. ethereum.org. https://ethereum.org/de/desci/

Figueiredo, C., Neves, A. A. B., Pimentel, F., Pimentel, D., Mota-Araujo, H. P., Bem, A. F. D., A.D. Neto, B., & Mcmanus, C. (2024). Impact of open access policy on Brazilian science and global trends. *Anais Da Academia Brasileira de Ciências*, *96*(2), e20231068. https://doi.org/10.1590/0001-37652024 20231068

Fong, E. A., Patnayakuni, R., & Wilhite, A. W. (2023). Accommodating coercion: Authors, editors, and citations. *Research Policy*, *52*(5), 104754. https://doi.org/10.1016/j.respol.2023.104754

Hofmann, A. G., & Williams, B. C. (2017). Temporally and spatially flexible plan execution for dynamic hybrid systems. *Artificial Intelligence*, *247*, 266–294. https://doi.org/10.1016/j.artint.2015.0 2.007

Ioannidis, J. P. A. (2005). Why most published research findings are false. *PLoS Medicine*, *2*(8), e124. https://doi.org/10.1371/journal.pmed.0020124

Joss. (1998). Danish consensus conferences as a model of participatory technology assessment: An impact study of consensus conferences on Danish Parliament and Danish public debate. *Science and Public Policy*. https://doi.org/10.1093/spp/25.1.2

Kleinfercher, F., & Vengadasalam, S. (2024). *Bloxberg: The blockchain for science (White Paper 3.0)*. ht tps://bloxberg.org/wp-content/uploads/2024/02/bloxberg_whitepaper_3.0.pdf

Lu et al. (2020, July 31). *The ResearchCoin whitepaper*. ResearchHub. https://researchhub.com/paper/ 819400/the-researchcoin-whitepaper

Luhmann, N. (1992). *Die Wissenschaft der Gesellschaft [The science of society]* (8. Auflage). Suhrkamp.

Luhmann, N. (1993). *Soziale Systeme: Grundriß einer allgemeinen Theorie [Social systems: Outline of a general theory]* (18. Auflage). Suhrkamp.

Luhmann, N. (2005). *Soziologische Aufklärung. 5: Konstruktivistische Perspektiven [Sociological Enlightenment. 5: Constructivist perspectives]* (2. Aufl). Westdt. Verl.

Luhmann, N. (2014). *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität [Trust: a mechanism for reducing social complexity]* (5. Aufl). UVK Verlagsgesellschaft.

Luhmann, N., Whobrey, W., & Luhmann, N. (1998). *Observations on modernity*. Stanford University Press.

Max Planck Society. (2003). *Berlin Declaration*. https://openaccess.mpg.de/Berlin-Declaration

Mukherjee, I. (2008). Understanding information system failures from the complexity perspective. *Journal of Social Sciences*, *4*(4), 308–319. https://doi.org/10.3844/jssp.2008.308.319

Nagaraj, A., Shears, E., & De Vaan, M. (2020). Improving data access democratizes and diversifies science. *Proceedings of the National Academy of Sciences*, *117*(38), 23490–23498. https://doi.org/10.1073/pnas.2001682117

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Peters, M., & Roberts, P. (2015). *The virtues of openness: Education, science, and scholarship in the digital age*. Paradigm publ.

Petrescu, M., & Krishen, A. S. (2022). The evolving crisis of the peer-review process. *Journal of Marketing Analytics*, *10*(3), 185–186. https://doi.org/10.1057/s41270-022-00176-5

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust1. *Journal of Personality*, *35*(4), 651–665. https://doi.org/10.1111/j.1467-6494.1967.tb01454.x

Sandra, V., Frederike, K., & James, L. (2019). *Bloxberg: The trusted research infrastructure (White Paper 1.0)*. https://www.mpg.de/13416733/bloxberg_whitepaper.pdf

Shapiro, S. (1987). The social control of impersonal trust. *American Journal of Sociology*, *93*(3), 623–658. https://www.jstor.org/stable/2780293

Simmel, G., Frisby, D., & Simmel, G. (2011). *The philosophy of money* (3. enl. ed., repr). Routledge.

Suber, P. (2012). *Open access*. The MIT Press.

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge university press.

Trovò, B., & Massari, N. (2021). Ants-Review: A privacy-oriented protocol for incentivized open peer reviews on Ethereum. In B. Balis, D. B. Heras, L. Antonelli, A. Bracciali, T. Gruber, J. Hyun-Wook, M. Kuhn, S. L. Scott, D. Unat, & R. Wyrzykowski (Eds), *Euro-Par 2020: Parallel Processing Workshops* (Vol. 12480, pp. 18–29). Springer International Publishing. https://doi.org/10.1007/978-3-030-71593-9_2

UNESCO. (2021). *UNESCO Recommendation on open science*. UNESCO. https://doi.org/10.54677/MNMH8546

Weidener, L., & Boltz, L. (2025). Challenges of DAOs in decentralized science: A qualitative analysis of expert interviews. *Frontiers in Blockchain*, *8*, 1641294. https://doi.org/10.3389/fbloc.2025.1641294

Weidener, L., & Spreckelsen, C. (2024). Decentralized science (DeSci): Definition, shared values, and guiding principles. *Frontiers in Blockchain*, *7*, 1375763. https://doi.org/10.3389/fbloc.2024.1375763

Willinsky, J. (2006). *The access principle: The case for open access to research and scholarship*. MIT Press.

Zavolokina, L., Zani, N., & Schwabe, G. (2023). Designing for trust in blockchain platforms. *IEEE Transactions on Engineering Management*, *70*(3), 849–863. https://doi.org/10.1109/TEM.2020.3015359

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

RESEARCH
FOR THE
DIGITAL AGE

in cooperation with

UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies