Literature Review

Eduardo Oliveira

March 26, 2025

1 Addressing the Reproducibility Crisis in Science Through Open Science and Decentralized Technologies

1.1 The Pervasive Challenge of Reproducibility in Science

1.1.1 Defining Reproducibility and Replicability

The terms reproducibility and replicability are central to the integrity of the scientific method, often used interchangeably in common discourse, yet possessing distinct technical meanings [?]. For the purpose of this literature review, reproducibility will be understood as the ability to obtain consistent results using the same input data, computational steps, methods, and code [?]. This definition aligns with the concept of computational reproducibility, which is particularly relevant when considering the application of digital technologies to scientific research.

In contrast, replicability refers to the capacity to achieve consistent results across different studies designed to answer the same scientific question, where each study involves the collection of new, independent data [?]. The distinction between these two concepts is crucial as it frames the nature of the reproducibility crisis and influences the types of solutions that can be effectively proposed and evaluated. The focus on computational reproducibility, which decentralized technologies are well-positioned to address through enhanced data sharing and methodological transparency, provides a clear and manageable scope for this literature review.

1.1.2 Quantifying the Crisis: Statistical Evidence of Reproducibility Failures

The scientific community is facing a significant challenge, evidenced by a substantial body of research indicating a widespread inability to reproduce published findings across numerous disciplines [?]. A notable survey published in *Nature* revealed that over 70% of researchers have attempted and failed to reproduce the experimental results of other scientists [?]. This failure rate is

particularly high in fields such as chemistry, where 87% of researchers reported such issues, followed by biology at 77%, and medicine at 67% [**?**]. These figures highlight that the problem is not isolated to specific areas but rather permeates the scientific landscape.

Further evidence comes from a study in *PLOS Biology*, which found that only 22% of papers published in top-tier journals could be replicated [**?**]. Similarly, a review in *Nature* indicated that a mere 15% of studies reported high levels of reproducibility [**?**]. Metastudies corroborate these findings, suggesting that the reproducibility rate across scientific literature may range from a high of 40% to a low of just 10% [**?**]. Moreover, studies indicate that up to 70% of attempts to replicate high-profile experiments end in failure [**?**]. The challenge is further underscored by data from preclinical cancer research, where only approximately 11% of studies could be successfully replicated [**?**].

Table 1: Reproducibility Failure Rates Across Scientific Disciplines

Scientific Field	Failure Rate (%)
Chemistry	87
Biology	77
Medicine	67
Top-tier Journal Studies	78
Preclinical Cancer Research	89

The consistently high rates of reproducibility failures across diverse scientific fields strongly suggest that this is not a collection of isolated incidents but a systemic issue demanding urgent and effective solutions.

Table 2: Scope of the Reproducibility Crisis in Science

Scientific Discipline	Reported Reproducibility/Replication Rate	Source
General Science	> 70% failure rate in replication attempts	Nature Survey [**?**]
Top-Tier Journal Publications	22% replicable	PLOS Biology [**?**]
General Science	15% high reproducibility	Nature Review [**?**]
Biomedical Research	10-40% reproducible	Metastudies [**?**]
High-Profile Experiments	Up to 70% replication failure	[**?**]
Preclinical Cancer Research	∼ 11% successfully replicated	[**?**]
Chemistry	87% failure to reproduce	Nature Survey [**?**]
Biology	77% failure to reproduce	Nature Survey [**?**]
Medicine	67% failure to reproduce	Nature Survey [**?**]

1.1.3 Exploring the Multifaceted Causes of the Reproducibility Crisis

The lack of reproducibility in scientific research stems from a complex interplay of several contributing factors [?]. Methodological limitations represent a significant category, encompassing flawed study designs that may overlook critical variables or employ inadequate control groups [?]. Issues with data quality, unreliable measurement tools, and inconsistencies in research practices further exacerbate these challenges [?]. Additionally, studies with small sample sizes and insufficient statistical power are more prone to producing results that cannot be reliably replicated [?].

Publication bias also plays a crucial role, as scientific journals often show a preference for publishing novel and positive findings, leading to the underreporting or neglect of negative results and replication studies [?]. This phenomenon is often referred to as the *file drawer problem*, where non-significant or negative findings remain unpublished [?]. Furthermore, the prevalence of questionable research practices (QRPs) such as p-hacking, where researchers manipulate data to achieve statistical significance, and HARKing (hypothesizing after results are known), significantly contribute to the crisis [?].

The intense pressure on researchers to consistently publish in high-impact journals, often described as the *publish or perish* culture, can incentivize rushed research, cutting corners, and a prioritization of quantity over methodological rigor and quality [?]. Finally, a lack of transparency in research practices, such as insufficient reporting of methods and limited access to raw data and research materials, severely hinders the ability of other researchers to independently verify and replicate published findings [?]. The convergence of these methodological, systemic, and cultural factors within the scientific ecosystem underscores the multifaceted nature of the reproducibility crisis.

1.1.4 Analyzing the Far-Reaching Consequences of Irreproducible Research

The consequences of the reproducibility crisis extend far beyond the confines of the scientific community, impacting public trust, economic efficiency, and the overall advancement of knowledge [?]. The inability to replicate scientific findings erodes confidence in the reliability of individual researchers, academic institutions, and the scientific enterprise as a whole [?]. This erosion of trust can have significant implications for public perception and support of scientific endeavors.

Economically, irreproducible research represents a substantial waste of financial resources. Estimates suggest that billions of dollars are spent annually on preclinical research in the United States alone that ultimately cannot be replicated [?]. Some analyses indicate that the direct costs of unreliable biomedical research in the U.S. could be near $28 billion annually, with indirect effects potentially inflating this figure to hundreds of billions yearly [?]. Furthermore, reliance on irreproducible results can significantly impede scientific progress by

misdirecting research efforts, delaying critical breakthroughs, and hindering the cumulative development of scientific understanding [**?**].

In fields such as medicine, the consequences can be particularly severe, as irreproducible research can lead to patient harm through the development of ineffective or unsafe treatments [**?**]. Therefore, the reproducibility crisis poses a significant threat not only to the integrity of science but also to societal well-being and economic stability.

1.2 The Open Science Movement: A Paradigm Shift in Research

1.2.1 Unpacking the Core Tenets of Open Science

The Open Science movement represents a fundamental shift in the way scientific research is conducted and disseminated, advocating for principles and practices that make scientific inquiry and its outcomes accessible to everyone [**?**]. At its core, Open Science is built upon several key tenets. Transparency is paramount, emphasizing openness at all stages of the research lifecycle, including the sharing of data, methodologies, and the processes of peer review [**?**]. Accessibility is another crucial principle, aiming to make research outputs, such as publications and datasets, freely available without financial, legal, or technical barriers [**?**]. Open Science also strongly promotes collaboration, encouraging cooperation and the sharing of knowledge among researchers, as well as engagement with the wider public [**?**]. Intrinsically linked to these principles is reproducibility, as Open Science practices are designed to enhance the verifiability and repeatability of research findings [**?**]. This movement signifies a paradigm shift towards a more open, inclusive, and collaborative approach to scientific inquiry.

1.2.2 Highlighting the Goals and Potential Benefits of Open Science

Embracing Open Science is intended to yield numerous positive outcomes and advantages for both the scientific community and society at large. Increased access to research and data has the potential to significantly accelerate discovery by allowing researchers to build upon existing knowledge more efficiently and avoid unnecessary duplication of effort [**?**]. Furthermore, Open Science can foster innovation by stimulating new ideas, products, and collaborations across various sectors through broader access to research findings [**?**]. By making research accessible to the public, Open Science can also enhance societal impact by increasing transparency, building trust in scientific endeavors, and facilitating the translation of research findings into practical solutions for pressing global challenges [**?**]. A key goal of Open Science is to improve research quality and reproducibility through practices such as open data sharing and open peer review, which enhance the rigor and verifiability of scientific work [**?**]. Finally, Open Science promotes increased collaboration and efficiency by fostering both national and international partnerships and reducing the duplication of research efforts [**?**]. Realizing these substantial benefits, however,

necessitates a concerted effort to address the existing challenges that hinder the widespread adoption of Open Science principles.

1.2.3 Examining the Barriers to Widespread Adoption of Open Science

Despite its significant potential, the widespread adoption of Open Science faces several notable barriers. Financial constraints represent a primary challenge, particularly concerning the costs associated with open access publishing. Article Processing Charges (APCs) required by many open access journals can be prohibitive for researchers with limited funding, creating an economic barrier to participation [?]. The financial implications also extend to the infrastructure needed for data sharing and the maintenance of open repositories [?]. Social norms and cultural resistance within academia also impede progress, as deeply ingrained practices may resist the shift towards more open methodologies [?]. A significant aspect of this resistance is the lack of strong incentives and recognition for researchers who engage in time-consuming open science practices such as comprehensive data sharing and the conduct of replication studies [?]. Infrastructure limitations, especially in regions with less developed technological resources and internet connectivity, pose another substantial hurdle to global participation in open science initiatives [?]. Equity concerns arise from financial barriers and the dominance of the English language in scientific communication, potentially disadvantaging researchers from lower-income countries or those whose primary language is not English [?]. Furthermore, misconceptions about the quality of open access resources can discourage researchers from utilizing these platforms for publishing or accessing research [?]. Finally, some researchers express concerns about data sharing, fearing that their work might be prematurely used by others or that their intellectual property could be compromised [?]. Overcoming these multifaceted barriers is essential to fully realize the transformative potential of the Open Science movement.

1.3 Decentralized Technologies: Revolutionizing Data Management and Collaboration

1.3.1 Blockchain Technology: Principles and Applications in Scientific Research

Blockchain technology has emerged as a transformative innovation, offering a distributed ledger system that enhances data security and transparency through its fundamental characteristic of immutability [?]. The core principles underpinning blockchain include its nature as a distributed ledger, where data is not stored in a single location but is instead shared across a network of computers, thereby eliminating the risks associated with centralized systems [?]. Immutability ensures that once data is recorded on the blockchain, it becomes virtually impossible to alter without the consensus of the entire network, providing a high degree of data integrity [?]. Security is achieved through the use

of cryptographic hashing and robust consensus mechanisms, which protect the data from unauthorized access and tampering [**?**].

Depending on the specific type of blockchain implementation (e.g., public or permissioned), the system can also offer a high degree of transparency, allowing transactions and data to be auditable by network participants [**?**]. These inherent properties make blockchain technology particularly relevant to scientific research, with applications ranging from ensuring the integrity and provenance of research data [**?**] to facilitating secure data sharing and collaboration among researchers [**?**]. Blockchain also holds promise for enhancing the peer review process by improving its integrity, transparency, and overall efficiency [**?**], as well as for managing research outputs and intellectual property through secure and verifiable records [**?**]. Furthermore, blockchain can enable decentralized funding mechanisms for research projects, fostering transparency and community involvement in resource allocation [**?**]. Despite its numerous benefits, it is important to acknowledge the limitations of blockchain technology, including potential scalability issues, transaction costs, and the evolving landscape of legal and regulatory frameworks [**?**].

1.3.2 InterPlanetary File System (IPFS): Decentralized Storage for Research Data

The InterPlanetary File System (IPFS) presents a novel approach to data storage, functioning as a peer-to-peer network designed for storing and sharing hypermedia in a decentralized and content-addressed manner [4]. A key feature of IPFS is content addressing, where each file is uniquely identified based on a cryptographic hash of its content, ensuring data integrity and facilitating efficient retrieval [**?**]. The decentralized architecture of IPFS means that data is distributed across a network of interconnected nodes, eliminating single points of failure and enhancing the overall resilience of the storage system [**?**].

IPFS also supports persistence and versioning, allowing users to access previous versions of files and track changes over time, which is particularly valuable in the context of evolving research data [**?**]. Furthermore, IPFS is designed for scalability and efficiency, capable of handling large datasets and potentially reducing bandwidth costs associated with data transfer [**?**]. In the realm of scientific research, IPFS offers significant advantages for decentralized and persistent data storage, providing a robust and accessible infrastructure for housing research datasets, protocols, and publications [4].

It also facilitates data sharing and collaboration by enabling researchers to easily distribute and access large files without the need for centralized servers [4]. The use of content addressing in IPFS also contributes to ensuring data integrity and verifiability, as it allows for straightforward confirmation that the retrieved data has not been altered since it was originally stored [4]. One limitation of IPFS when used in isolation is the lack of inherent access control mechanisms, which can be addressed through integration with other technologies like blockchain [**?**].

1.3.3 Smart Contracts: Automating Agreements and Workflows in Research

Smart contracts are self-executing agreements where the terms of the contract are directly encoded into program code and stored on a blockchain [52]. A defining feature of smart contracts is automation, as they automatically execute predefined actions once specific conditions outlined in the code are met [52]. The code of smart contracts is typically transparent, visible on the blockchain for all participants to inspect [52]. Once a smart contract is deployed on the blockchain, it becomes immutable, meaning its code and terms cannot be altered [52]. This immutability, combined with the decentralized nature of the blockchain, enables trustless execution, as smart contracts operate without the need for intermediaries, fostering trust among parties involved in an agreement [52].

In the context of scientific research, smart contracts hold significant potential for various applications. They can be used for automating data sharing agreements, ensuring that research data is shared according to predefined policies and conditions [?]. Smart contracts can also facilitate the management of intellectual property rights, automating processes related to the transfer and licensing of research findings [?]. Furthermore, they can be employed in facilitating decentralized funding by automating the distribution of research grants based on the achievement of specific milestones [?].

Smart contracts could also play a role in verifying research processes and results by automating certain aspects of validation and ensuring adherence to predefined protocols [?]. Additionally, they can be used to incentivize peer review and reproducibility by automatically rewarding researchers for conducting reviews or successfully replicating studies [52]. While offering numerous advantages, the development of secure and reliable smart contracts can be complex, and the potential for errors in the code necessitates careful design and auditing [?].

1.4 Bridging the Gap: Open Science as a Framework for Reproducible Research

1.4.1 Analyzing How Open Science Principles Currently Address the Reproducibility Crisis

The Open Science movement provides a robust framework of principles and practices that directly aim to mitigate the reproducibility crisis in scientific research [?]. A cornerstone of this approach is the emphasis on open data and methods, which involves making research data, methodologies, and analysis code publicly available. This transparency allows other researchers to independently verify the original findings and attempt to replicate the study [?].

Another important practice is pre-registration, where researchers publicly document their study protocols and analysis plans before conducting the research. This helps to increase transparency and reduces the potential for ques-

tionable research practices such as HARKing and p-hacking [**?**]. Open access publishing, which makes research publications freely available to all, ensures that findings are widely accessible for scrutiny and potential replication by the broader scientific community [**?**].

The format of registered reports represents an innovative approach where study protocols are peer-reviewed and accepted for publication prior to data collection, thereby significantly reducing the influence of publication bias on the dissemination of research outcomes [**?**]. Finally, open peer review, which introduces transparency into the evaluation process, can further enhance the rigor and accountability of scientific publishing [**?**]. Through these various practices, Open Science directly addresses many of the factors contributing to the reproducibility crisis by promoting transparency and enabling the verification of research findings.

1.4.2 Evaluating the Limitations of Current Open Science Implementations in Fully Resolving the Crisis

While Open Science offers a powerful framework for improving research reproducibility, its current implementations face certain limitations that prevent it from fully resolving the crisis [**?**]. Many Open Science practices rely on the voluntary participation of researchers and may lack robust automation and enforcement mechanisms to ensure consistent adherence and data integrity. Furthermore, the incentive structures within academia often do not adequately reward the time and effort required for comprehensive Open Science practices, such as thorough data sharing and conducting replication studies [**?**].

While open data sharing increases transparency, it does not inherently guarantee the integrity and trustworthiness of the data itself, as manipulation could potentially occur before the data is shared. Current Open Science infrastructures may also face challenges in terms of scalability and complexity when it comes to managing and verifying the growing volume of large and intricate datasets produced by modern scientific research. Finally, deeply entrenched cultural and systemic barriers, such as the strong emphasis on publishing novel findings in high-impact journals within the "publish or perish" system, can still undermine the effectiveness of even the most well-intentioned Open Science practices [**?**]. These limitations suggest that while Open Science provides a crucial foundation, complementary approaches may be necessary to fully address the persistent challenges of the reproducibility crisis.

1.5 The Synergistic Potential of Decentralized Technologies and Open Science

1.5.1 Exploring the Theoretical Alignment of Decentralized Technologies and Open Science

Decentralized technologies, particularly blockchain, IPFS, and smart contracts, exhibit a strong theoretical alignment with the core tenets of the Open Science

movement, offering the potential to reinforce and enhance its impact on research reproducibility [4]. Blockchain technology, with its inherent transparency and immutability, can significantly enhance the verifiability and trustworthiness of research data and processes within the Open Science framework. The permanent and auditable nature of blockchain records ensures that research outputs remain tamper-proof and their history is easily traceable [4].

The InterPlanetary File System (IPFS), with its decentralized and content-addressed storage, directly supports the Open Science principle of open access by providing a robust and persistent infrastructure for storing and sharing research outputs, ensuring their long-term availability and accessibility to the global scientific community [4]. Finally, smart contracts offer a powerful mechanism for automation and trustless execution that can be leveraged within Open Science to automate data sharing agreements, manage intellectual property rights in a transparent manner, and potentially incentivize reproducible research practices through automated reward systems [52]. In essence, decentralized technologies provide concrete technical solutions that can address some of the key limitations of current Open Science implementations by offering enhanced mechanisms for ensuring data integrity, accessibility, automation, and trust within the scientific research ecosystem.

1.5.2 Investigating Existing Research and Initiatives Leveraging Decentralized Technologies for Open and Reproducible Science

The intersection of decentralized technologies and Open Science in addressing the reproducibility crisis is an active area of research and development, with a growing number of initiatives exploring the potential of blockchain, IPFS, and smart contracts [4]. Several Decentralized Science (DeSci) platforms have emerged, such as VitaDAO, ResearchHub, and OriginTrail, which leverage these technologies to create more open and collaborative research environments [4]. These platforms are exploring decentralized solutions for various aspects of the research lifecycle, including open access publishing, secure data sharing, transparent funding mechanisms, incentivized peer review processes, and the management of intellectual property rights through IP-NFTs [4].

Prior research by the author has also explored the use of blockchain technology to improve the reproducibility of preclinical research experiments [?]. Furthermore, there are initiatives focused on utilizing blockchain to enhance the integrity and transparency of the peer review process [?], and IPFS is being investigated and implemented as a decentralized storage solution for research data, offering persistence and accessibility [?]. This growing body of work indicates a significant interest in and exploration of how decentralized technologies can be practically applied within the Open Science framework to tackle the challenges of research reproducibility.

1.5.3 Highlighting the Potential Benefits of the Synergistic Approach

The integration of decentralized technologies within the Open Science framework offers a powerful synergistic approach with the potential to significantly enhance research reproducibility. By leveraging the unique capabilities of blockchain and IPFS, the integrity of research data can be substantially improved. Blockchain ensures immutability and provides an auditable trail of data provenance, while IPFS offers content-based addressing, guaranteeing that data remains verifiable and free from tampering [4]. The use of blockchain and smart contracts can also lead to more transparent research workflows, creating auditable processes from data collection and analysis to publication and peer review [?]. Smart contracts further enable automated verification of certain research processes and results, increasing efficiency and reducing the potential for human error [52].

Decentralized platforms can also employ tokens and smart contracts to create incentives for collaboration and reproducibility, rewarding researchers for sharing data, conducting replication studies, and participating in open peer review [52]. Finally, IPFS offers a robust solution for improved accessibility and long-term preservation of research outputs by providing decentralized and persistent data storage [4]. The convergence of these benefits underscores the significant potential of this synergistic approach to foster a more transparent, reliable, and trustworthy scientific ecosystem, directly addressing the core challenges posed by the reproducibility crisis.

1.6 Identifying Knowledge Gaps and Charting Future Research Directions

1.6.1 Synthesizing the Literature to Pinpoint Unanswered Questions and Areas for Further Investigation

The comprehensive review of existing literature reveals several key gaps in the current understanding of how decentralized technologies can be effectively leveraged within the Open Science framework to address the reproducibility crisis. While the theoretical alignment and potential benefits are increasingly recognized, more empirical evidence is needed to rigorously evaluate the effectiveness and impact of decentralized platforms on research reproducibility across diverse scientific disciplines [?].

Further research is also crucial to address the scalability and performance limitations of blockchain and IPFS when handling the large datasets and high transaction volumes characteristic of modern scientific research [?]. Understanding and overcoming user adoption barriers for decentralized research tools is another critical area requiring more investigation, including the development of intuitive and user-friendly interfaces tailored to the needs of researchers with varying levels of technical expertise [?]. The development and evaluation of effective governance models for decentralized science platforms are also essential to ensure quality control, prevent the spread of misinformation, and foster meaningful community participation [?].

Furthermore, the legal and ethical implications of using blockchain and IPFS for scientific research data, particularly concerning data privacy, security, ownership, and compliance with evolving regulations, warrant further in-depth analysis [?]. Research on achieving interoperability and seamless integration between decentralized platforms and existing scientific infrastructure and workflows is also necessary for broader adoption [?]. Finally, comprehensive cost-benefit analyses are needed to assess the economic feasibility and long-term sustainability of implementing decentralized solutions for promoting Open Science and research reproducibility. Specific challenges related to the implementation of decentralized peer review systems, such as scalability, cost, legal risks, standardization, resistance to change, and perceived uncertainty, also require further exploration. These identified gaps highlight the need for continued and focused research to fully realize the potential of decentralized technologies in advancing Open Science and addressing the reproducibility crisis.

1.6.2 Proposing Potential Avenues for Future Research

Based on the identified knowledge gaps, several promising avenues for future research emerge. A key direction involves the development and rigorous evaluation of novel decentralized platforms that integrate blockchain, IPFS, and smart contracts to specifically support Open Science principles and enhance reproducibility within various scientific disciplines. Conducting in-depth case studies and empirical assessments of existing and emerging DeSci platforms will be crucial for understanding their real-world impact on research outcomes and user experience.

Future research should also focus on the investigation and proposal of effective governance models for decentralized science platforms that can ensure the quality, accountability, and active participation of the research community. Addressing the complex legal and ethical challenges associated with the use of decentralized technologies for scientific research data requires interdisciplinary collaboration and the development of practical solutions. Furthermore, research efforts should be directed towards developing standards and solutions that enable seamless interoperability and integration between decentralized research platforms and the established scientific infrastructure.

Conducting thorough cost-effectiveness studies will be essential for evaluating the economic viability and sustainability of decentralized solutions for promoting Open Science and reproducibility. Investigating and evaluating strategies to promote user adoption of decentralized research tools within the broader scientific community is also a critical area for future work. Finally, research should focus on defining and developing appropriate metrics that can effectively measure and track improvements in research reproducibility on decentralized platforms. These research directions collectively aim to bridge the existing knowledge gaps and pave the way for the effective utilization of decentralized technologies in advancing Open Science and fostering a more reproducible scientific ecosystem.

2 Conclusion

The literature reviewed in this chapter underscores the pervasive and multifaceted nature of the reproducibility crisis in science, highlighting its significant impact on the credibility and progress of scientific knowledge. The Open Science movement offers a promising framework for addressing this crisis by promoting transparency, accessibility, collaboration, and reproducibility. However, current implementations of Open Science face limitations related to automation, incentives, data integrity, scalability, and cultural barriers.

Decentralized technologies, including blockchain, IPFS, and smart contracts, present a compelling set of tools that align with the principles of Open Science and have the potential to overcome some of its inherent limitations. Existing research and emerging Decentralized Science initiatives demonstrate the growing interest in leveraging these technologies to enhance data integrity, transparency, automation, and collaboration within the scientific ecosystem. Despite the promise, significant knowledge gaps remain regarding the practical implementation, effectiveness, and broader implications of this synergistic approach.

Future research should focus on developing and evaluating novel decentralized platforms, addressing user adoption challenges, establishing effective governance models, navigating legal and ethical considerations, and assessing the overall cost-effectiveness of these solutions. By systematically addressing these gaps, the scientific community can move towards a more transparent, reliable, and trustworthy research environment, ultimately strengthening the foundations of scientific progress.

References

[1] Maher Alharby and Aad van Moorsel. Blockchain-based smart contracts: A systematic mapping study. *Computer Science & Information Technology*, pages 125–140, 2017.

[2] Ahmed Alkhateeb, Cagatay Catal, Gorkem Kar, and Alok Mishra. Hybrid blockchain platforms for the internet of things (iot): A systematic literature review. *Sensors*, 22(4), 2022.

[3] Dave Bayer, Stuart Haber, and W. Scott Stornetta. Improving the efficiency and reliability of digital time-stamping. *Sequences II: Methods in Communication, Security, and Computer Science*, pages 329–334, 1993.

[4] Juan Benet. Ipfs - content addressed, versioned, p2p file system. *arXiv preprint*, arXiv:1407.3561, 2014.

[5] Juan Benet. Ipfs - the interplanetary file system, 2015.

[6] D.J. Bernstein, T. Lange, and R. Niederhagen. High-speed high-security signatures. *Journal of cryptographic engineering*, 2(2):77–89, 2012.

[7] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings - IEEE Symposium on Security and Privacy*, pages 104–121, 2015.

[8] C. L. Borgman. The conundrum of sharing data. *Journal of the American Society for Information Science and Technology*, 63(1):105–118, 2012.

[9] G. Boulton, L. Allen, and M. H. Brooks. Open science: A new era for the future of research. *Science*, 348(6237):29–32, 2015.

[10] D.R. Brown. Standards for efficient cryptography (sec) 1: Elliptic curve cryptography. Technical report, Certicom Research, 2010.

[11] Mihai Budiu and Brian J. Schwartz. *Designing Distributed Systems: A Service-Oriented Approach*. Prentice Hall, 2007.

[12] Christian Cachin. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL)*, 2016.

[13] Christian Cachin. Blockchains: The magic of cryptographic protocols. *IEEE Security & Privacy*, 14(2):56–62, 2016.

[14] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, pages 173–186, 1999.

[15] George Coulouris, Jean Dollimore, Tim Kindberg, and Jonathon Blair. *Distributed Systems: Concepts and Design*. Addison-Wesley, 2011.

[16] David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134:91–109, 2019.

[17] C.F. Fan, Y. Chen, R. Chen, H. Zhou, and L. Chen. Analysis of elliptic curve cryptography for blockchain. *Future Generation Computer Systems*, 89:735–743, 2018.

[18] Hyperledger Foundation. Hyperledger fabric now supports ethereum, 2018. Accessed: 2025-03-17.

[19] Hyperledger Foundation. Burrow - the boring blockchain, 2019. Accessed: 2025-03-17.

[20] Hyperledger Foundation. Iroha special instructions dsl, 2020. Accessed: 2025-03-17.

[21] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991.

[22] D. Hankerson, A.J. Menezes, and S.A. Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[23] Hyperledger Foundation. *Hyperledger Iroha Documentation*, 2025. Accessed: 2025-03-17.

[24] D. Johnson, A. Menezes, and S. Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1(1):36–63, 2001.

[25] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 3rd edition, 2020.

[26] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In J Katz and H Shacham, editors, *ADVANCES IN CRYPTOLOGY - CRYPTO 2017, PT I*, volume 10401 of *Lecture Notes in Computer Science*, pages 357–388. Int Assoc Cryptol Res; NSF; Fujitsu; Western Digital; Mozilla, 2017. 37th Annual International Cryptology Conference (Crypto), Univ Calif, Santa Barbara, CA, AUG 20-24, 2017.

[27] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[28] Leslie Lamport. Time, clocks, and the ordering of events in a distributed system. *Commun. ACM*, 21(7):558–565, July 1978.

[29] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[30] A. Langley, M. Hamburg, and M. Naehrig. Curve25519: new diffie-hellman speed records. *International Association for Cryptologic Research*, 2016.

[31] S. Leonelli. The practices and politics of open science. In *Springer Handbook of Science and Technology Studies*, pages 1–19. Springer, 2016.

[32] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996.

[33] Ralph Merkle. A certified digital signature. *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pages 24–34, 1989.

[34] Ralph C. Merkle. A digital signature based on a conventional encryption function. In *Advances in Cryptology — CRYPTO '87*, volume 293, pages 369–378. Springer Berlin Heidelberg, Berlin, Heidelberg, 1988.

[35] R.C. Merkle. A digital signature based on a conventional encryption function. *Advances in cryptology—CRYPTO'87*, pages 369–378, 1988.

[36] Arthur Miller, David S. Rowe, and Alex Papageorgiou. Scaling blockchain storage and its applications. *Journal of Computer Science and Technology*, 31(4):873–886, 2016.

[37] V.S. Miller. Use of elliptic curves in cryptography. *Advances in cryptology—CRYPTO'85*, pages 417–426, 1986.

[38] Monax. Hyperledger burrow, 2020. Accessed: 2025-03-17.

[39] Fedor Muratov, Andrei Lebedev, Nikolai Iushkevich, Bulat Nasrulin, and Makoto Takemiya. YAC: BFT Consensus Algorithm for Blockchain, September 2018. arXiv:1809.00554 [cs].

[40] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[41] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton university press, Princeton (N.J.), 2016.

[42] B. A. Nosek, M. E. Ebersole, K. M. DeHaven, and D. L. Mellor. The preregistration revolution. *Proceedings of the National Academy of Sciences*, 112(5):1–8, 2015.

[43] National Institute of Standards and Technology. Fips pub 180-4: Secure hash standard (shs), 2012. Accessed: 2025-03-17.

[44] Sina Pilehchiha. Improving reproducibility in smart contract research. Master's thesis, Concordia University, 2022. Accessed: 2025-03-17.

[45] H. A. Piwowar. Who shares? who doesn't? *PLoS ONE*, 6(7):e18657, 2011.

[46] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[47] Tim Roughgarden. *Twenty-One Lectures on Algorithmic Game Theory*. Cambridge University Press, 2016.

[48] Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. The Energy Consumption of Blockchain Technology: Beyond Myth. *Bus Inf Syst Eng*, 62(6):599–608, December 2020.

[49] Simplilearn. What is a smart contract in blockchain and how does it work?, 2022. Accessed: 2025-03-17.

[50] Mathis Steichen, Beltran Fiz, Robert Norvill, Wazen Shbair, and Radu State. Blockchain-based, decentralized access control for ipfs. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1499–1506, 2018.

[51] Nick Szabo. Smart contracts: Building blocks for digital markets. *EX-TROPY: The Journal of Transhumanist Thought*, 16, 1996.

[52] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[53] Don Tapscott and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. Penguin Random House, 2016.

[54] Marko Vukolić. Rethinking permissioned blockchains. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, BCC '17, page 3–7, New York, NY, USA, 2017. Association for Computing Machinery.

[55] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum White Paper*, 2014.

[56] Y. Wu, X. Zheng, J. Ren, K. Zhang, and Y. Shen. Blockchain-based secure key management scheme with high availability. *IEEE Access*, 6:27766–27774, 2018.

[57] X. Xu, L. Yang, and L. Zhao. A survey of blockchain data storage issues and solutions. *Journal of Computer Networks and Communications*, 2018:1–17, 2018.

[58] X. Zhang, H. Li, and B. Xu. Decentralized data storage systems: Blockchain and beyond. *Journal of Blockchain Research*, 3(2):45–56, 2020.

References

[1] Maher Alharby and Aad van Moorsel. Blockchain-based smart contracts: A systematic mapping study. *Computer Science & Information Technology*, pages 125–140, 2017.

[2] Ahmed Alkhateeb, Cagatay Catal, Gorkem Kar, and Alok Mishra. Hybrid blockchain platforms for the internet of things (iot): A systematic literature review. *Sensors*, 22(4), 2022.

[3] Dave Bayer, Stuart Haber, and W. Scott Stornetta. Improving the efficiency and reliability of digital time-stamping. *Sequences II: Methods in Communication, Security, and Computer Science*, pages 329–334, 1993.

[4] Juan Benet. Ipfs - content addressed, versioned, p2p file system. *arXiv preprint*, arXiv:1407.3561, 2014.

[5] Juan Benet. Ipfs - the interplanetary file system, 2015.

[6] D.J. Bernstein, T. Lange, and R. Niederhagen. High-speed high-security signatures. *Journal of cryptographic engineering*, 2(2):77–89, 2012.

[7] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings - IEEE Symposium on Security and Privacy*, pages 104–121, 2015.

[8] C. L. Borgman. The conundrum of sharing data. *Journal of the American Society for Information Science and Technology*, 63(1):105–118, 2012.

[9] G. Boulton, L. Allen, and M. H. Brooks. Open science: A new era for the future of research. *Science*, 348(6237):29–32, 2015.

[10] D.R. Brown. Standards for efficient cryptography (sec) 1: Elliptic curve cryptography. Technical report, Certicom Research, 2010.

[11] Mihai Budiu and Brian J. Schwartz. *Designing Distributed Systems: A Service-Oriented Approach*. Prentice Hall, 2007.

[12] Christian Cachin. Architecture of the hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL)*, 2016.

[13] Christian Cachin. Blockchains: The magic of cryptographic protocols. *IEEE Security & Privacy*, 14(2):56–62, 2016.

[14] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, pages 173–186, 1999.

[15] George Coulouris, Jean Dollimore, Tim Kindberg, and Jonathon Blair. *Distributed Systems: Concepts and Design*. Addison-Wesley, 2011.

[16] David Easley, Maureen O'Hara, and Soumya Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134:91–109, 2019.

[17] C.F. Fan, Y. Chen, R. Chen, H. Zhou, and L. Chen. Analysis of elliptic curve cryptography for blockchain. *Future Generation Computer Systems*, 89:735–743, 2018.

[18] Hyperledger Foundation. Hyperledger fabric now supports ethereum, 2018. Accessed: 2025-03-17.

[19] Hyperledger Foundation. Burrow - the boring blockchain, 2019. Accessed: 2025-03-17.

[20] Hyperledger Foundation. Iroha special instructions dsl, 2020. Accessed: 2025-03-17.

[21] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991.

[22] D. Hankerson, A.J. Menezes, and S.A. Vanstone. *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[23] Hyperledger Foundation. *Hyperledger Iroha Documentation*, 2025. Accessed: 2025-03-17.

[24] D. Johnson, A. Menezes, and S. Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1(1):36–63, 2001.

[25] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC, 3rd edition, 2020.

[26] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In J Katz and H Shacham, editors, *ADVANCES IN CRYPTOLOGY - CRYPTO 2017, PT I*, volume 10401 of *Lecture Notes in Computer Science*, pages 357–388. Int Assoc Cryptol Res; NSF; Fujitsu; Western Digital; Mozilla, 2017. 37th Annual International Cryptology Conference (Crypto), Univ Calif, Santa Barbara, CA, AUG 20-24, 2017.

[27] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[28] Leslie Lamport. Time, clocks, and the ordering of events in a distributed system. *Commun. ACM*, 21(7):558–565, July 1978.

[29] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

[30] A. Langley, M. Hamburg, and M. Naehrig. Curve25519: new diffie-hellman speed records. *International Association for Cryptologic Research*, 2016.

[31] S. Leonelli. The practices and politics of open science. In *Springer Handbook of Science and Technology Studies*, pages 1–19. Springer, 2016.

[32] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996.

[33] Ralph Merkle. A certified digital signature. *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pages 24–34, 1989.

[34] Ralph C. Merkle. A digital signature based on a conventional encryption function. In *Advances in Cryptology — CRYPTO '87*, volume 293, pages 369–378. Springer Berlin Heidelberg, Berlin, Heidelberg, 1988.

[35] R.C. Merkle. A digital signature based on a conventional encryption function. *Advances in cryptology—CRYPTO'87*, pages 369–378, 1988.

[36] Arthur Miller, David S. Rowe, and Alex Papageorgiou. Scaling blockchain storage and its applications. *Journal of Computer Science and Technology*, 31(4):873–886, 2016.

[37] V.S. Miller. Use of elliptic curves in cryptography. *Advances in cryptology—CRYPTO'85*, pages 417–426, 1986.

[38] Monax. Hyperledger burrow, 2020. Accessed: 2025-03-17.

[39] Fedor Muratov, Andrei Lebedev, Nikolai Iushkevich, Bulat Nasrulin, and Makoto Takemiya. YAC: BFT Consensus Algorithm for Blockchain, September 2018. arXiv:1809.00554 [cs].

[40] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[41] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton university press, Princeton (N.J.), 2016.

[42] B. A. Nosek, M. E. Ebersole, K. M. DeHaven, and D. L. Mellor. The preregistration revolution. *Proceedings of the National Academy of Sciences*, 112(5):1–8, 2015.

[43] National Institute of Standards and Technology. Fips pub 180-4: Secure hash standard (shs), 2012. Accessed: 2025-03-17.

[44] Sina Pilehchiha. Improving reproducibility in smart contract research. Master's thesis, Concordia University, 2022. Accessed: 2025-03-17.

[45] H. A. Piwowar. Who shares? who doesn't? *PLoS ONE*, 6(7):e18657, 2011.

[46] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[47] Tim Roughgarden. *Twenty-One Lectures on Algorithmic Game Theory*. Cambridge University Press, 2016.

[48] Johannes Sedlmeir, Hans Ulrich Buhl, Gilbert Fridgen, and Robert Keller. The Energy Consumption of Blockchain Technology: Beyond Myth. *Bus Inf Syst Eng*, 62(6):599–608, December 2020.

[49] Simplilearn. What is a smart contract in blockchain and how does it work?, 2022. Accessed: 2025-03-17.

[50] Mathis Steichen, Beltran Fiz, Robert Norvill, Wazen Shbair, and Radu State. Blockchain-based, decentralized access control for ipfs. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1499–1506, 2018.

[51] Nick Szabo. Smart contracts: Building blocks for digital markets. *EX-TROPY: The Journal of Transhumanist Thought*, 16, 1996.

[52] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[53] Don Tapscott and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World.* Penguin Random House, 2016.

[54] Marko Vukolić. Rethinking permissioned blockchains. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, BCC '17, page 3–7, New York, NY, USA, 2017. Association for Computing Machinery.

[55] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum White Paper*, 2014.

[56] Y. Wu, X. Zheng, J. Ren, K. Zhang, and Y. Shen. Blockchain-based secure key management scheme with high availability. *IEEE Access*, 6:27766–27774, 2018.

[57] X. Xu, L. Yang, and L. Zhao. A survey of blockchain data storage issues and solutions. *Journal of Computer Networks and Communications*, 2018:1–17, 2018.

[58] X. Zhang, H. Li, and B. Xu. Decentralized data storage systems: Blockchain and beyond. *Journal of Blockchain Research*, 3(2):45–56, 2020.