Transparency as an Instrument for Fraud Prevention in the Digital Business Ecosystem

Nada Zhafira Almira[1], Widyasari[2]

[1,2] Faculty of Economics and Business, Universitas Tarumanegara

ABSTRACT: Digital transformation has reshaped the global business landscape, increasing efficiency while also giving rise to new risks in the form of digital fraud. This research aims to analyze the role of transparency as a strategic instrument in preventing fraud in the Indonesian digital business ecosystem. Using a qualitative multiple case study approach, data was collected through interviews, observations, and analysis of policy documents from technology-based companies. The results show that transparency significantly contributes to increased accountability and the effectiveness of internal controls. The implementation of digital audit systems, real-time monitoring, and blockchain technology has proven to reduce information asymmetry and the opportunities for fraud. However, its effectiveness is still influenced by institutional factors, digital ethics, and collaboration among regulators. Therefore, further research is recommended to develop a quantitative model that measures the impact of transparency on reducing fraud risk longitudinally across various digital business sectors in Indonesia.

KEYWORDS: Accountability, Corporate Governance, Digital Transparency, Fraud Prevention.

INTRODUCTION

Digital transformation brings fundamental changes for a company in carrying out its business activities. The shift from manual systems to information technology-based automation has not only improved operational efficiency, but also given rise to a new paradigm in data management and decision-making. The digital era requires companies to adapt to the utilization of technologies such as *cloud computing*, *artificial intelligence*, and *blockchain* (Laksono et al., 2024; Ramadani & Firdaus, 2024). This technology allows for faster and more accurate integration of business processes. This phenomenon shows that digitalization is no longer just a strategic choice, but a structural need that determines the competitiveness of an organization in the global market (Porter & Hepperman, 2014). However, these changes also have consequences for how companies maintain the honesty, integrity, and security of information in their systems.

The development of digitalization has also encouraged the emergence of various online business platforms and electronic transactions that change the pattern of interaction between companies, consumers, and their business partners (Melisa et al., 2025). Financial reporting systems can now be done in *real-time* and integrated through big data-based software (*big data analytics*) that demands high openness and accountability (Dharma & Hendri, 2022; Panjaitan et al., 2025). This condition indicates that information disclosure is an important aspect in maintaining public trust and preventing deviations in organizational behavior (Tapscott & Tapscott, 2016). However, on the other hand, automation and digitalization actually create new potential for system abuse and data manipulation that are not easily detected by conventional mechanisms.

Although digitalization brings various innovative opportunities, the ease of data manipulation and weak internal supervision systems are challenges in digital business governance. Cases of misuse of customer data, manipulation of digital financial statements, as well as system-based fraud such as algorithmic engineering show that fraud in the digital context has more complex and difficult to identify characteristics compared to *conventional fraud* (Ali et al., 2022). Phenomena such as *cyber fraud* and *data breaches* have become a central issue in the *Association of Certified Fraud Examiners* modern *corporate governance practices* (ACFE, 2024) . Therefore, the issue of digital integrity is now an integral part of corporate governance strategies that are oriented towards sustainability and public trust.

Table 1. Fraud cases in Indonesia since 2021-2024.

No	Year	Number of cases	Types of fraud
1	2021	612 cyber cases	*Phishing, Malware Ransomware*
2	2022	4,860 cybercrime cases	Crypto Investment Scams, *Social Engineering*
3	2023	3,758 cybercrime cases	Sniffing (APK Mode), *Phishing* (Wedding Invitation/Ticket Mode), Illegal Loans, Illegal Investment
4	2024	3,331 cybercrime cases	Online Gambling (closely related to money laundering & fraud), *Ransomware* (including National Data Center/PDN cases), Crypto Fraud, *Deepfakes*

Source: Pusiknas polri, 2023; Central Statistics Agency, 2024

Based on the table, the data shows a significant spike in cybercrime cases in Indonesia from 612 cases (2021) to 4,860 cases (2022). This surge reflects two things: the increase in people's digital activities after the COVID-19 pandemic and the increased detection and reporting capabilities of law enforcement officials. However, after the peak of 2022, the number of cases decreased to 3,758 cases (2023) and 3,331 cases (2024). This decrease does not necessarily mean a decrease in threats, but rather describes a shift in crime modes that are increasingly sophisticated and hidden. Fraud based cybercrime has a systemic impact on national financial stability. Cases such as crypto fraud and illegal loans not only cause direct financial losses, but also lower public trust in digital financial institutions (Stengos, 2025).

Transparency emerged as a fundamental principle of *good corporate governance* that ensures information disclosure and minimizes opportunities for irregularities. Transparency is not only understood in administrative dimensions such as the disclosure of financial statements, but also includes the openness of systems, algorithms, and access to digitally auditable transaction data (Hendra & Fahlevi, 2024). Transparency serves as a social and technological control mechanism that allows various stakeholders to verify the validity of information. Thus, digital transparency is not only an indicator of organizational accountability, but also a strategic instrument in preventing *fraud* through reducing *information asymmetry* and improving the *traceability of* business processes (Healy & Palepu, 2001).

Based on these problems, a number of important research questions arise: to what extent has the principle of transparency been applied in the digital business ecosystem in Indonesia? What factors affect the effectiveness of transparency in preventing digital fraud? How are transparency, accountability, and internal controls related in a technology-based business environment? Also, what kind of policy models can encourage the sustainable implementation of digital transparency? These questions are the conceptual basis for building an empirical analysis framework that focuses on the application of transparency as an instrument for fraud prevention in the digital era.

As a conceptual solution, a digital transparency system needs to be developed through the integration of automated auditing technology, *real-time monitoring*, and *blockchain-based verification*. This approach can strengthen internal oversight and reduce the chance of fraud through early detection of data anomalies. Based on *the Fraud Triangle Theory* (Cressey, 1953), fraud occurs due to pressure, opportunity, and rationalization; in this context, transparency plays a role in reducing opportunities and rationalizing fraudsters through an openness mechanism that increases individual and organizational accountability. In addition, through the lens of *Stakeholder Theory* (Freeman, 1984), information disclosure to all stakeholders is an important element in building public reputation and trust. By presenting the latest empirical data on the implementation of digital transparency in the Indonesian business sector, this research is expected to make a theoretical and practical contribution to strengthening digital business governance with integrity and sustainability.

METHODS

This research uses a qualitative approach with multiple case study designs, which aims to understand in depth how transparency plays a role in fraud prevention in the digital business ecosystem. This approach was chosen because the phenomenon being studied

is complex, contextual, and cannot be measured quantitatively. In line with the view, the case study method allows researchers Yin Robert K (2003), to explore the social processes and dynamics that underlie digital transparency practices in various organizations. Data was obtained through in-depth interviews, participatory observations, and analysis of digital documents and corporate policies related to the application of *good corporate governance principles* and digital audit mechanisms (Creswell & James, 2018). The focus of the analysis is directed to identify behavioral patterns, supervisory strategies, and ethical challenges in the application of transparency as a fraud prevention instrument.

Furthermore, data were analyzed using thematic analysis techniques (Braun & Clarke, 2006) to extract key themes that reflect the relationship between transparency, accountability, and digital risk control. The validity of the findings was maintained through triangulation of sources and methods, by comparing the results of interviews from industry players, regulators, and independent auditors. An interpretive approach is used to interpret the meanings that emerge from the data, taking into account the social and institutional contexts in which digital business practices take place (Creswell & Poth, 2018). Thus, this method is expected to produce a comprehensive understanding of how transparency can be formulated into a strategic instrument in preventing *fraud* and strengthening digital business governance with integrity.

RESULTS AND DISCUSSION

A. Level of Implementation of Transparency Principles in the Digital Business Ecosystem in Indonesia

The application of transparency principles in the digital business ecosystem in Indonesia has shown significant developments, especially since the increase in information technology penetration after the COVID-19 pandemic. Based on empirical data from the National Police and BPS, the increase in cyber cases that occurred in 2022 reached 4,860 cases from 612 cases in 2021 is a momentum for the public and private sectors to strengthen good corporate governance policies through digitization of reporting systems, data-based audits, and transaction openness. Many companies are starting to implement real-time financial reporting and blockchain systems to suppress potential data manipulation. The implementation of this transparency is also strengthened by government initiatives through personal data protection regulations and cross-sector digital system integration policies (Mashudin, 2024).

However, the level of transparency implementation still varies between sectors. The financial industry, especially banking and fintech, tends to be more advanced due to strict supervision from the Otoritas Jasa Keuangan (OJK) and Bank Indonesia. The sector implements a digital audit system that can trace suspicious transactions automatically (Healy & Palepu, 2001). In contrast, the digital SME, mid-scale e-commerce, and startup sectors still face challenges in building an efficient transparency system due to limited resources and technological literacy (Margama & Fasa, 2025; Ramadhani et al., 2025). This shows that the implementation of transparency in Indonesia is not yet structural, but is still reactive to external pressure or fraud incidents that have occurred.

In addition, interviews with X1, the Compliance Manager, revealed that the company actually has a transparency policy, particularly regarding financial reporting and compliance with OJK regulations. However, the implementation of this policy is still administrative in nature. Transparency has not truly become part of the company's cultural values, so employees view data disclosure as a legal obligation rather than a form of ethical commitment to the public.

X2, the internal auditor, explained that the digital audits they conduct are actually running well, but the mechanisms for public transparency are still very limited. He gave an example that transaction data can only be accessed by internal teams and certain regulators, without an independent audit system that allows third parties to assess data integrity. According to him, in digital business, openness to external parties can actually increase customer and investor trust. However, many companies are still cautious and consider the reputational risks if their data is too open.

Based on interviews and document analysis, it was found that transparency is often perceived as limited to administrative reporting, not as a corporate culture. Some companies only selectively open data to meet regulations, without providing public access or adequate independent audit mechanisms. In fact, as emphasized by Freeman & McVea (2005) Stakeholder Theory, transparency is actually a means of ethical communication between organizations and all stakeholders to maintain business trust and reputation. Therefore, although the principle of transparency has been recognized as important, its application still needs to be expanded into managerial practices inherent in organizational values.

B. Factors Affecting the Effectiveness of Transparency in Preventing Digital Fraud

The effectiveness of transparency in preventing digital fraud is determined by the complex interaction between institutional, technological, and cultural factors of the organization. Institutionally, the success of transparency depends on the strength of systematically built internal and external oversight systems (Rosidah et al., 2023). Organizations with mature digital governance generally integrate automated auditing technologies, blockchain-based verification, and real-time monitoring to ensure the authenticity of data and prevent transaction manipulation (Indraprakoso & Haripin, 2023; Rijal et al., 2024). Empirical studies show that companies that adopt blockchain-based digital auditing systems tend to have lower fraud incidence rates, as they allow for early detection of data anomalies (Tapscott & Tapscott, 2016). On the other hand, organizations that still carry out manual oversight or have not integrated the principle of transparency in corporate governance policies are more vulnerable to misuse of access and digital data engineering. The phenomenon of increasing cases of APK sniffing and phishing in 2023 is evidence of the weak openness and supervision system in a number of digital companies in Indonesia.

In addition, the competency factor of human resources and the culture of digital ethics play an important role in the effectiveness of transparency. Transparency is not only technical, but also moral and cultural. Its implementation demands individuals who understand the values of accountability, information security, and ethical responsibility in data management. Based on the Fraud Triangle Theory (Cressey, 1953), fraud arises because of pressure, opportunity, and rationalization. In the context of digital business, strong transparency is able to suppress two key aspects of opportunity and rationalization through the implementation of open reporting policies and verifiable digital audit systems (Ratna et al., 2025). However, weak digital literacy and lack of corporate ethics training have caused many organizations to fail to instill a culture of transparency in a sustainable manner. This is especially true in companies with rigid hierarchical structures, where access to information is limited and internal reporting is not effective, so the risk of fraud remains high even though surveillance technology is available.

The last factor is regulatory support and collaboration between stakeholders. The Government of Indonesia through the Otoritas Jasa Keuangan (OJK), the Ministry of Communication and Information Technology (Kominfo), and Badan Siber dan Sandi Negara (BSSN) have built a regulatory foundation through the Personal Data Protection Law (2022) and the establishment of the Indonesia Anti-Scam Center (IASC) in 2024. This policy strengthens the legal environment that supports information disclosure and the integrity of digital systems. However, its effectiveness is still constrained by cross-sector coordination and resistance from companies that are reluctant to share audit data due to concerns about corporate reputation. This condition shows that transparency cannot function optimally without an interconnected governance ecosystem between regulations, technology, and public ethics as affirmed by the Association of Certified Fraud Examiners (ACFE, 2024). Thus, synergy between parties is the main requirement for the realization of effective transparency in preventing digital fraud and maintaining the sustainability of public trust in Indonesia's digital business ecosystem.

C. The Relationship between Transparency, Accountability, and Internal Control in a Technology-Based Business Environment

The results show that digital transparency has a direct correlation with increased organizational accountability and the effectiveness of internal controls. Based on empirical findings from interviews with internal auditors and compliance managers at several fintech companies, the implementation of a reporting system based on real-time data analytics speeds up the process of verifying transactions and detecting irregularities early. Transparency, in this context, is not only realized through the disclosure of financial statements, but also through traceability of data on digital systems that can be audited by internal and external parties. These findings strengthen the agency's theory (Healy & Palepu, 2001) that information disclosure can reduce information asymmetry between management and stakeholders, thereby minimizing the opportunity for abuse of authority that is the root cause of fraud.

Digital transparency also serves as a means of forming accountable behavior in a technology-based business environment. Companies that implement digital tracking and automated audit systems show a higher level of compliance with good corporate governance policies (Gaffar, 2024). Based on empirical data from the National Police and BPS in Table 1, the increase in fraud cases in 2022 which reached 4,860 cases is an indicator that weak transparency and internal control are still the main gaps in digital business practices. However, in 2023 and 2024 there will be a significant decrease in cases to 3,758 and 3,331 cases, which can be attributed to the start of the implementation of digital openness policies and automated supervision systems in several financial and online trade sectors. This indicates that transparency contributes to strengthening a more responsive and data-based internal control system.

From an organizational social perspective, the relationship between transparency and accountability is symbiotic. Transparency encourages a culture of information disclosure, while accountability ensures the information is used for ethical oversight and performance evaluation (Fadhilah et al., 2025; Padang et al., 2025). In a technology-based business environment, the openness of algorithms and auditing of transaction data plays an important role in creating a robust digital governance. This approach is in line with the view in Freeman & McVea (2005) Stakeholder Theory, that information disclosure not only strengthens the relationship between companies and capital owners, but also with consumers and regulators. Therefore, digital transparency is not just an administrative tool, but a strategic mechanism that ensures the effectiveness of internal controls through increased individual and collective responsibility at all levels of the organization.

D. Policy Models That Drive the Sustainable Implementation of Digital Transparency

The results of the study show that an effective policy model to encourage digital transparency must be based on three main components: (1) integration of digital audit technology, (2) adaptive information disclosure regulation, and (3) improving organizational digital literacy. From case studies conducted in the banking and e-commerce sectors, companies that adopt blockchain-based audit systems and real-time monitoring tools show better ability to prevent cyber fraud and transaction errors. This implementation reinforces the internal control function in layers and provides proof of audit that cannot be manipulated, in line with the principle of immutability in blockchain systems (Tapscott & Tapscott, 2016). Empirically, this model has been proven to reduce the potential for internal fraud because every digital activity is recorded and can be verified publicly and internally.

At the national policy level, the existence of the Indonesia Anti Scam Center (IASC) and increased coordination between the OJK, Kominfo, and the National Police in the 2023-2024 period show the government's commitment to strengthening the digital transparency ecosystem. Based on the OJK report (2024), the integration of public complaint data through CekRekening.id and banking digital reporting systems has helped identify more than 572 thousand digital fraud reports from 2017 to 2024. This initiative proves that cross-agency data collaboration-based policies can be a catalyst for the sustainable implementation of transparency. However, the main challenge still lies in the consistency of law enforcement and the availability of human resources who are able to manage audit technology effectively.

In addition to structural factors, the sustainability of digital transparency also depends on a corporate culture that places openness and digital ethics as core values. The implementation of a digital code of conduct, cyber literacy training, and an incentive system for internal reporting (whistleblowing system) are important parts of the policy model that supports long-term fraud prevention. Transparency must be understood not only as an external demand from regulators, but as a reputational investment and competitive advantage for companies in the digital age. This is in line with the idea in Cressey (1953) the Fraud Triangle Theory, where transparency is able to suppress the two main elements that trigger fraud opportunity and rationalization through the creation of an open, measurable, and integrity business environment.

CONCLUSION

Based on the results of research on the role of transparency as an instrument of fraud prevention in the digital business ecosystem, it can be concluded that transparency has a strategic contribution in strengthening the accountability and effectiveness of internal control of the organization. The implementation of technology-based reporting systems such as *real time analytics*, *blockchain verification*, and *digital audits* has been proven to be able to reduce information asymmetry between management and stakeholders, thereby reducing the chance of fraud. Transparency not only functions as an administrative tool, but also forms an organizational culture that upholds openness, integrity, and public trust. In addition, this study shows that the decrease in digital fraud cases in Indonesia between 2022 and 2024 correlates with the increasing application of transparency principles and system openness policies in the digital business sector.

As a follow up, it is necessary to strengthen national and corporate policies that are oriented towards digital transparency in a sustainable manner. The government and supervisory institutions such as OJK, Kominfo, and BSSN need to expand information disclosure regulations by encouraging cross-agency data integration and the application of blockchain and AI-based audit technology to detect indications of fraud early. At the organizational level, it is important to instill the value of digital ethics, cyber literacy, and a transparent internal reporting system such as the whistleblowing system so that transparency becomes part of corporate culture, not just a regulatory obligation. With this collaborative and adaptive approach, transparency can serve as the foundation for integrity, innovative, and sustainable digital business governance in facing fraud challenges in the digital transformation era.

REFERENCES

1. ACFE. (2024). The Nations Occupational Fraud 2024 :A Report To The Nations. *Association of Certified Fraud Examiners*, 1–106.

2. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences (Switzerland)*, *12*(19). https://doi.org/10.3390/app12199637

3. Braun, V., & Clarke, V. (2006). Qualitative Research in Psychology Using thematic analysis in psychology Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. http://www.tandfonline.com/action/journalInformation?journalCode=uqrp20%5Cnhttp://www.tandfonline.com/action/jour nalInformation?journalCode=uqrp20

4. Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Free Press.

5. Creswell, J. W., & James, D. C. (2018). *Qualitative, quantitative, and mixed methods approaches*. Sage Publication Ltd.

6. Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry & Research Design Choosing Among Five Approaches Fourth Edition John. In *Journal of Physics A: Mathematical and Theoretical* (Vol. 44, Issue 8).

7. Dharma, A., & Hendri, N. (2022). The Urgency of Using Big Data Analytics in Public Sector Audits. *Acquisition: Journal of Accounting*, *18*(02), 107–120. http://www.fe.ummetro.ac.id/ejournal/index.php/JA

8. Fadhilah, Abiyu, F., Ariesta, A., & Alfaruqi, D. M. (2025). Transparent and Accountable School Financial Management. *Journal of Management and Education Sciences*, *02*(01), 419–424.

9. Freeman, R. E. E., & McVea, J. (2005). A Stakeholder Approach to Strategic Management. *SSRN Electronic Journal*, *January 2001*. https://doi.org/10.2139/ssrn.263511

10. Gaffar. (2024). *Financial Transparency and the Role of Audit* (Issue February). Hosted by Innovatix Labs.

11. Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, *31*(1–3), 405–440. https://doi.org/10.1016/S01654101(01)00018-0

12. Hendra, & Fahlevi, A. H. (2024). Implementation of Good Corporate Governance Principles in Pt . *IAPA International Conference 2024*, 1138–1153. https://doi.org/10.23920/jphp.v1i2.292.1

13. Indraprakoso, D., & Haripin. (2023). Exploring the Potential Use of Blockchain in Port Management Optimization in Indonesia: A Review of the Literature. *Sanskara Management and Business*, *1*(03), 140–160. https://doi.org/10.58812/smb.v1i03.131

14. Laksono, A., Nur Wijayani, Q., Raya Telang, J., Kamal, K., Bangkalan, K., Timur, J., & author, K. (2024). The role of the latest technology in improving the effectiveness of business communication. *Jma)*, *2*(1), 1680–1694.

15. Margama, A. L., & Fasa, M. I. (2025). DIGITAL TRANSFORMATION IN E-BUSINESS: OPPORTUNITIES AND CHALLENGES FOR MSMES DIGITAL TRANSFORMATION IN E-BUSINESS: OPPORTUNITIES AND CHALLENGES FOR SMES. *Journal of Intellectual and Scholars of the Archipelago*, *2*(2), 924–931. https://jicnusantara.com/index.php/jicn

16. Mashudin, A. (2024). Transformation of Public Administration in the Digital Era: Innovations and Challenges. *Journal of Artificial Intelligence and Digital Business (RIGGS), 4*(1), 449–456. https://www.kompasiana.com/anandaagustin2773/659294dec57afb45221eb6b2/transformasi-asuransi-syariah-inovasi-dantantangan-di-era-digital

17. Melisa, O.:, Faisal, T., & Fasa, M. I. (2025). The Role of E-Commerce in the Growth of the Digital Economy in Indonesia. *Jma)*, *3*(4), 3031–5220.

18. Padang, N. N., Padang, W. S., Padang, N. N., Padang, W. S., & Gultom, L. L. (2025). The effect of accountability and transparency on the quality of financial statements at the General Election Commission (KPU) in North Sumatra Province 1.3. *Journal of Accounting & Financial Research*, *10*(1), 70–80.

19. Panjaitan, C., Nayma, S., Afriliyani, I., & Yani Panggabean, F. (2025). Analysis of Financial Statements in the Digital Era: Challenges and Opportunities for Modern Companies (Journal Review Study). *Journal of Financial and Business Accounting*, *3*(2), 121–125. https://jurnal.ittc.web.id/index.php/jakbs/index

20. Porter, M. E., & Hepperman, J. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*, *92*, 64–88.

21. Ramadani, D. P., & Firdaus, R. (2024). Evolusi Sistem Informasi Manajemen Dari Manual ke Otomatis The Evolution of Information Management System From Manual to Automatic. *Journal of Intellectual and Scholars of the Archipelago*, *1*(3), 4131. https://jicnusantara.com/index.php/jicn

22. Ramadhani, N., Sugesti, A. I., Sagita, D. N., & Purwanto, E. (2025). The Utilization of Digital Marketplace in Improving MSME Performance through Communication Facilities in the Digital Era. *Journal of Business and Digital Communication*, *2*(2), 20. https://doi.org/10.47134/jbkd.v2i2.3560

23. Ratna, A., Devi, S., Prahasti, K., Putri, K., Dewi, R., Kusumaningtias, R., Kusumaningsih, A., & Research, A. (2025). Transparansi dan Akuntanbilitas: Strategi Dalam Mencegah Fraud di PT Multi Karya Liftindo Transparency and Accountability: Strategy in Preventing Fraud at PT Multi Karya Liftindo. *Collaborative Journal of Science*, *8*(5), 2357–2368. https://doi.org/10.56338/jks.v8i5.7479

24. Rijal, S., Devi, E. K., Saputra, A. E., Fatimah, S., & Sarwono, S. (2024). The Influence of Blockchain Technology Integration and Organizational Structure on Accounting Audit Efficiency in XYZ Companies in Indonesia. *Sanskara Accounting and Finance*, *2*(03), 175–183. https://doi.org/10.58812/sak.v2i03.389

25. Rosidah, I., Gunardi, Priatna Kesumah, & Royke Bahagia Rizka. (2023). Transparency and Accountability in Fraud Prevention in Government Agencies (Case Study of Ciwidey District Office). *Journal of Business Management Economics and Accounting: EMBA, 2*(1), 137–156. https://doi.org/10.59820/emba.v2i1.110

26. Stengos, T. (2025). *Abstract from the 1st International Online Conference on Risk and Financial Management*. 1. https://doi.org/10.3390/proceedings2025125001

27. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.