Deloitte. Insights

A report from the
Deloitte Center for Integrated Research

Earning digital trust: Where to invest today and tomorrow

Leaders can invest in these four emerging digital trust solutions to enable more trusted data and information for the foreseeable future

About the Deloitte Center for Integrated Research

The Deloitte Center for Integrated Research (CIR) offers rigorously researched and data-driven perspectives on critical issues affecting businesses today. We sit at the center of Deloitte's industry and functional expertise, combining the leading insights from across our firm to help leaders confidently compete in today's ever-changing marketplace.

Connect

To learn more about the vision of the Center for Integrated Research, its solutions, thought leadership, and events, please visit www.deloitte.com/us/cir.

Contents

Introduction

IN AN ERA of ever-present digital threats that can undermine and erode stakeholder trust, organizations should invest to earn "digital trust," that is, protect their data and information from fraud and bad actors to safeguard their relationships, reputation, and revenue. This task could be more difficult than ever before as technology and the threats to digital trust it enables continue to evolve. For example, deepfakes—fake digital images, videos, or audio that can be generated using artificial intelligence (AI) at the click of a button—can already be used to impersonate individuals. Such an impersonation caused a CEO of an energy company to approve a US$243,000 wire transfer to a fictional supplier in 2019.[1] While deepfake scams are still a relatively new threat, they grew more than 900% annually between 2017 and 2019,[2] and were estimated to have cost businesses more than US$250 million in 2020.[3]

The stakes are high, and any misstep can impact customer loyalty, financial performance, brand equity, and ultimately undermine an organization's ability to build and maintain trust. Surveys suggest that 81% of consumers lose trust in a brand after a breach, while 25% completely stop interacting with it.[4] The stakes became even higher as the pandemic accelerated digital work infrastructures[5] and drove spending on emerging tech security strategies and solutions.[6]

While many leaders understand the threats to digital trust, they may find it difficult to augment traditional cybersecurity measures with more advanced solutions. What will best address today's digital trust needs? When preparing for tomorrow, what investments in digital trust solutions are the most effective bets? There are certainly many options—our analysis found at least 2,000 patents related to digital trust filed annually[7] between 2015 and 2020—illustrating why it can be hard to choose the right tools.

The stakes are high, and any misstep can impact customer loyalty, financial performance, brand equity, and ultimately undermine an organization's ability to build and maintain trust.

As leaders consider where to place their investments to improve digital trust, it's important to note that addressing digital trust should include an end-to-end interdisciplinary approach across people, process, governance, and regulation, with technology being a key enabler. In this study, we focus on advanced technology enablers that organizations can explore, over and beyond existing cyber measures, to enhance digital trust. Our interviews with 15 global subject matter specialists and leaders found four promising technology solutions—AI-based data monitoring, cloud-enabled data trusts, blockchain, and quantum technologies. We further validated these findings by analyzing the trends in digital trust–related patents granted over the last five to six years to gauge the maturity of these emerging technologies vis-à-vis digital trust. While there are many innovations in commercially available solutions that are unpatented, for this study, we look at patents as they help provide a window into broad innovation areas and maturity. And we exclusively analyze granted patents, rather than including the patent applications, as they are better indicators of truly differentiated, credible innovation to watch (see appendix, "Digital trust innovation research"). Based on the maturity of these solutions, two of them seem able to meet today's needs. The other two are future bets for the near and long term, which may help organizations stay ahead of evolving threats for the foreseeable future.

WHAT DO WE MEAN BY DIGITAL TRUST?

Building on Deloitte's definition of trust,[8] we define digital trust as the confidence among customers, employees, partners, and other stakeholders in an organization's ability to create and maintain the integrity of all digital assets (including data/information, architectures, applications, and infrastructure) across stakeholder experiences, strategic insights, organizational platforms, and network connectivity.[9] This digital trust ensures transparency and accessibility, security and reliability, privacy and control, and ethics and responsibility.[10]

Solutions that enhance digital trust today

ORGANIZATIONS LOOKING TO enhance digital trust today can already invest in relatively mature, common solutions; however, advanced solutions that may currently be limited to select industries or use cases have the potential to offer new capabilities. These advanced solutions should not replace existing cyber measures; rather, they can provide complementary and additive digital trust advantages. Our research revealed two advanced solutions that organizations can consider adopting today: AI-based data monitoring and data trusts.

AI-based monitoring of data, its access and use

Of the many applications where AI could be applied to improve digital trust, our research uncovered some business cases where AI monitoring can help, especially when validating contextual data accuracy and governing data access and usage by participants across an ecosystem.

AI can help make sure data is correct and isn't tampered with and, therefore, can be trusted. Manually identifying and cleaning poor-quality data, including incorrect, stale, missing, or poorly labelled data, can be time-consuming and expensive.[11] It costs organizations an average of US$13 million annually.[12] Furthermore, if a bad data model is ingested, it can compromise outcomes and amplify the effects of bad information.[13] AI can help validate information accuracy, authenticity, and reliability for data in context.[14] Today, AI-based solutions can detect missing data, anomalies, or unexpected data in real time.[14] Emerging AI solutions are able to identify fake or manipulated documents, images, deepfake videos, and more.[16] Deepfake-detection algorithms can check for digital integrity such as the presence of grayscale pixels at the boundaries of manipulated sections.[17] They can also check for physical irregularities such as inaccurate shadows and reflections, and biometric irregularities such as lip movement, blinking, and pupil shape.[18] Facebook and Michigan State University's model identifies deepfakes with reportedly 70% accuracy, by reverse-engineering aspects of the AI used to create it.[19] Such solutions can help build trust in the data, related processes, and the insights generated from it.

AI can improve identity and access management. It can help flag and prevent unauthorized data access, detect abnormal user behavior, or other anomalies.[20] Behavioral solutions can establish authorized user identities and block bot accounts based on users' interaction patterns with devices.[21] Spam filters based on machine learning (ML) reduce the risk of unauthorized access attempts via phishing or social engineering attacks[22]—some of the most common ways to infect systems with malware or ransomware and gain access to data. A survey found that 75% of respondents agree that behavior-based analytics is the only way to catch complex ransomware attacks.[23] Behavior analytics, when combined with unsupervised ML algorithms, can enable more proactive security measures.[24] In fact, organizations with fully deployed AI solutions can have up to an 80% lower cost impact from data breach incidents, compared to those without.[25]

AI can make sure that data is used as intended. For example, organizations can monitor public sites or platforms to identify intellectual property or

copyright infringements on digital assets such as text, music, images, and more. YouTube's AI-driven Content ID platform helps identify copyrighted content and facilitates payouts to rightful owners, to the tune of billions of dollars annually.[25]

Organizations can consider emerging privacy-preserving techniques as they think about leveraging digital trust AI use cases.[27] Homomorphic encryption allows AI solutions to directly analyze encrypted data to generate insight without having to decrypt and expose the underlying data.[28] And federated learning–based solutions can analyze data and train algorithms, across decentralized devices and servers, without necessitating actual data access or exchange.[29] For example, Secure AI Labs leverages federated learning for analyzing sensitive health data,[30] and Google Ads shifted to a federated model to locally and anonymously analyze users' interests.[31] These approaches enable outcomes such as generating insights without data misuse, ensuring greater data privacy and security, and simplifying data access and usage management, thus making AI increasingly viable for highly regulated industries.

AI isn't a digital trust cure-all, and it still has a lot of room to grow. Our research found some vulnerabilities related to AI's applicability for certain use cases. For instance, it can perform poorly when policing text due to its inadequate understanding of context. In such instances, a more human-AI collaborative setup could prove helpful. Additionally, unethical and biased AI is a digital trust issue itself. Deloitte's research has shown that AI biases can be either active (due to human action) or passive and may be more pervasive than organizations realize. Apart from education and a human-first approach, technology is one of the ways in which this challenge can be mitigated; some AI solutions are being developed that can uncover biases and ensure model fairness.[32] Even then, despite these challenges, our analysis shows that AI innovations related to digital trust have been growing at a brisk pace over the years.[32] With further advancements in AI algorithms and the availability of robust, extensive training datasets and correlations, more mature and automated solutions are expected across use cases.

AI isn't a digital trust cure-all, and it still has a lot of room to grow.

Data trusts as an approach for digital information-sharing

Data is the new currency. According to Alex "Sandy" Pentland, director of MIT's Connection Science Lab, "We have banks for money, but we don't have the same infrastructure for data." He suggests that data trusts can fill that void.[34]

Much in the same way a bank holds and manages financial assets, data trusts or cooperatives manage data for others. They're a business model in which independent third parties validate, control, secure, and share information, governing the data's proper use and managing legal data rights on behalf of its beneficiaries.[35] While there are various approaches to empowering customers with greater security and control for their data-sharing and usage, data trusts emerge as an interesting techno-legal approach. Data trusts can come in many forms, from a single entity storing data and only sharing collective insights to a group of trusted third parties working together for collective benefit.[36] For example, MIDATA, a health data cooperative, allows members to control their own personal data flow to actively contribute to medical research globally.[37] Construction Data Trust is set up in the United Kingdom to facilitate trusted information-sharing across the sector.[38] While the benefits of

data trusts from a data producer or customer perspective are clear, the third party's role may not be transparent, or inherently trusted; therefore, organizations should think carefully about who their customers will accept to manage their data, how to communicate about it, and where and when to engage the customer in the process.[39]

From a business perspective, data trusts can help unlock a range of benefits such as reduced data silos, greater control, and access to trusted and audited information, along with improved brand reputation from ethical and transparent data collection and use. Our interviews suggest that digital trust is enhanced by data trusts because organizations can gain greater confidence in that data and the insights generated from it.

From an IT perspective, data trusts can enhance digital trust by validating a single source of trusted information, making data management and sharing easier and more trusted. And organizations can avoid data bloat and gain access to only necessary data and insights through intermediaries, providing an added layer of privacy and protection,[40] while minimizing the risks of data loss, breaches, mismanagement, or fraud.[41] Data trusts are also emerging as a relevant solution for managing and sharing huge volumes of IoT (the Internet of Things) and sensor data.[42] Open Data Institute is piloting data trusts for various smart city use cases in London.[43] Cloud technology is making data trusts more effective at managing digital information that needs to be shared across networks with greater digital trust. For instance, Mastercard, with IBM, has established an independent data trust, Trūata, to manage customer financial information securely and anonymously; and cloud allows for the use of that data across other trusted digital solutions.[44]

Our interviews suggest that digital trust is enhanced by data trusts because organizations can gain greater confidence in that data and the insights generated from it.

Although an important model to maintain digital trust, data trusts come with challenges. Distributed cloud systems enable easier data-sharing, but they can also lead to data sovereignty and compliance issues if not properly governed. For example, data stored in one country may get replicated to a data center located in another country for business continuity and disaster recovery purposes, creating issues with local data standards and privacy laws, that is, when proper governance and control measures are not set. Also, data trusts aggregate high-value data; so even if the data is physically distributed, it is still a target for cyberattacks. A federated cloud security model can be considered to help address this issue. Organizations can use a cloud-data fabric—data seamlessly stitched together across different sources and infrastructures—to create a tiered security model that helps abstract and better protect data as it is being consumed.[45] With such measures in mind, data trusts are a viable model that organizations across industries can pursue to enhance digital trust.

Innovations that may transform digital trust tomorrow

CLOUD-ENABLED DATA TRUSTS and AI monitoring are rapidly maturing innovations that can help build digital trust for data and information beyond core cyber solutions. However, organizations also need to understand where technology is heading and be prepared for what's next to disrupt or enhance digital trust—not just for today's infrastructure, but also for tomorrow's future-readiness. So based on our qualitative research, coupled with a patent analysis, we examine two such topics: blockchain and quantum technologies. Both should be on organizations' radars now given their innovative and transformative potential for digital trust.

Blockchain and data provenance and ownership

Often referred to as a trust-less solution, blockchain provides a mechanism to trust individuals, organizations, and contractual details through an independently verifiable, immutable, and trusted database or ledger. This can reduce the need for trusted third parties as organizations trust the technology instead. Uniform, continually auditable systems could eventually replace the current patchwork of separate systems—streamlining permissions, security, and privacy.[46] Rapid innovation is happening around blockchain technology, and projects are gradually moving beyond early proofs-of-concept or pilots.[47] Digital fingerprinting, digital identity, digital assets, and smart contracts are some of blockchain's top use cases and are intertwined to provide a robust framework for trusted relationships.[48]

Blockchain and quantum technologies should be on organizations' radars now given their innovation and transformative potential around digital trust.

Blockchain can help maintain a trusted record of transactions. By tracking data and its fingerprint, stakeholders gain greater transparency and can easily establish data authenticity and integrity. There is a gradual increase in adoption of blockchain-based systems that can track products and corresponding information across complex global supply chains.[49] Norwegian aluminum manufacturer Hydro and global certification body DNV piloted a blockchain solution to allow urban furniture users to simply scan a barcode and trace the sustainable aluminum used in a park bench or a litter bin and ascertain the CO_2 emission from its raw material.[50] The media industry is also exploring the use of blockchain to counter challenges such as misinformation and to establish digital trust in publicly available information. The Safe.press consortium adds a blockchain-linked digital seal of approval to member publications.

Whenever these news sources are appended to stories or references, its key gets tracked, enabling consumers to track its origin and making it difficult to falsify news articles.[51]

Blockchain can help with trusted identities. This is a key component when it comes to any digital relationship or transaction. Blockchain can verify credentials without revealing details behind that identity and enables decentralized, tamper-proof self-sovereign identities,[52] which can be used for various commercial and government services. For example, the government of Zug, Switzerland, created a digital, decentralized, sovereign identity for its citizens, enabling them to partake in activities like casting votes and accessing government services.[53] Likewise, MIT piloted blockchain-based, verifiable, tamper-proof diplomas that graduates can securely and easily share externally.[54]

Blockchain can establish asset ownership. Digital assets, especially cryptocurrencies, comprise a use case currently adopted at scale. According to Deloitte's 2021 Global Blockchain survey, around 40% of respondents say digital assets will have a significantly positive impact on improving compliance and transparency, reducing risk, and enhancing trust.[55] Non-fungible tokens (NFTs)—unique, non-interchangeable data units stored on a blockchain—are emerging as a viable solution to authenticate and certify ownership of digital assets.[56] Even though NFTs can be copied, their creator and owner will still be publicly displayed.[57] Currently, they're gaining popularity in the art market and with sports memorabilia[58] but have the potential for broader application across industries. For example, NFTs can mark health data belonging to a particular person as a form of identification and guarantee of ownership. This also enables patients to know how their data is being used and potentially monetize it.[59]

Lastly, blockchain can enable faster legal agreements and automate trust. Blockchain-based smart contracts can help parties agree on terms and transact without any third-party intermediary or escrow, and trust that they will be executed automatically with reduced risk of error or manipulation.[60] Partior, a joint venture between Temasek, DBS, and a leading US-based financial services company, is piloting a cross-border payment system based on blockchain and smart contracts in an effort to improve efficiency and trust.[61] The company predicts a three-to-five-year time frame for the mass adoption of this platform.[62] The technology can also be used for automatic validation of information and digital funds by ports to enable faster processing and releasing of ships.

Despite these wide-ranging use cases, blockchain for digital trust is still in its early days. Technological constraints such as limited transaction throughput, user obfuscation, platform interoperability, along with nontechnical constraints such as limiting incentive mechanisms in public blockchains and the lack of industry standards and regulatory harmony, among others,[63] can limit the ability to construct a robust solution that enhances digital trust. However, ongoing rapid innovation and increasing maturity and understanding among stakeholders suggest that we can expect many of these limitations to be addressed in the coming years, resulting in a transformative change to digital trust. Hence, organizations should begin understanding this upcoming digital infrastructure now to incubate future solutions.

Quantum technologies

Quantum technologies will likely impact digital trust in three distinct ways.[64] First, the immense computing power that quantum computers promise can be applied to perform vast analytics on cyber and privacy data to detect anomalous or suspicious behavior. Second, quantum technologies' physical properties may offer

enhanced components to cyber systems such as cryptographic key generation and distribution. Third, when fully mature, quantum computing may be able to implement Shor's algorithm,[65] which would render some common encryption techniques easy to crack, making data and transactions more vulnerable to attackers.[66] Maintaining digital trust in a postquantum world will likely leverage a number of capabilities,[67] most notably the use of encryption techniques that are "quantum-resistant," also referred to as postquantum cryptography (PQC). PQC runs on classical computers and uses complex mathematical problems believed to be unsolvable by quantum computers. PQC is expected to be interoperable with current communication protocols and networks, making it more cost-effective and easier to maintain.[68] The National Institute of Standards and Technology (NIST) aims to standardize quantum-resistant algorithms by 2024.[69] Furthermore, as organizations review their underlying cryptographic processes in anticipation of PQC, it's likely that they will move toward a more crypto-agile state with an improved level of overall cyber hygiene.[70] This enhanced awareness of cryptographic reliance could contribute toward improved digital trust.

As mentioned previously, quantum principles can also potentially enhance data-encryption systems,[71] using methods such as quantum key distribution (QKD).[72] QKD uses quantum mechanics to distribute encryption keys between two parties. Due to the inherent tamper-evident properties of quantum physics, any attempt to eavesdrop the keys would be detected.[73]

But QKD technology has some limitations, including complex processes, oversized special equipment, and high costs.[74] The fragile state of quantum particles involved can significantly limit its coverage and reach.[75] Some small-scale, experimental implementations of QKD have been publicized—for example, the integrity and security of the election process in a Swiss canton was protected by incorporating QKD.[76] QKD's commercial approval or use for critical systems is challenged unless its limitations are overcome. The US National Security Agency, for example, has currently refrained from supporting the usage of QKD to protect communications in national security systems.[77]

Because it will be hard to predict when today's internet becomes vulnerable to tomorrow's quantum hackers, and because that moment would be catastrophic for digital trust, it's important that leaders gain awareness and begin to prepare as early as possible. Although the implementation of Shor's algorithm is predicted to be on the order of 10 to 15 years away,[78] the time required to gather a full cryptographic inventory, institute a governance process,[79] and select and implement PQC algorithms is significant. Hence, organizations should keep a pulse on quantum technology and the related cryptography landscape and ensure timely technology and talent investment for developing the needed crypto-agility and infrastructure.[80]

There's no silver bullet

WHILE THERE'S NO single solution to solve the digital trust puzzle, AI-based monitoring, data trusts, blockchain, and quantum technologies are some of the solutions that can play a valuable role. How might these digital trust tech approaches protect you? Consider the danger that deepfakes pose to organizations. Let's say you've been targeted by bad actors who pose as your company's CEO and attempt a false transaction or data breach. An AI-based monitoring solution that's integrated across your organization's network and applications could alert you to a potential deepfake as a first line of defense and block further attempts. If missed, a robust blockchain-based solution could help easily verify the transaction details and establish fail-safe mechanisms within a smart contract. Additionally, through a data-trust setup, the amount of compromised data could be minimized. Lastly, if your organization someday implements quantum-resistant safeguards within network and communications channels, other organizations can have much stronger confidence in the integrity of your data and transactions.

Given the rising business impacts, digital trust is not merely a CIO or CISO issue anymore; it requires the CEO and other business leaders to be engaged in technology investments now and into the future. Leaders can't afford to play the waiting game. Rapid technology innovation is enabling new digital threats too quickly. Leaders need to be proactive, sense innovation opportunities, and invest accordingly to weave them into their digital-trust fabric. This should be an ongoing activity—like a regular rhythm—to maintain and advance digital trust today and tomorrow.

Appendix: Digital trust innovation research

OUR PATENT ANALYSIS found a gradual rise (approximately 15% year over year) in the overall number of digital trust–related patents granted between 2015 and 2020.[81] But, the data shows that certain emerging technology families are growing at a much faster rate, indicating their relative importance and popularity. Upon further analysis, the following trends emerge (figure 1):

- Cloud technology has relatively matured in its innovation cycle. And given cloud's ability to enable other technologies—and, in some instances, improve their security and effectiveness—it might be an essential technology for an organization's digital trust strategy.

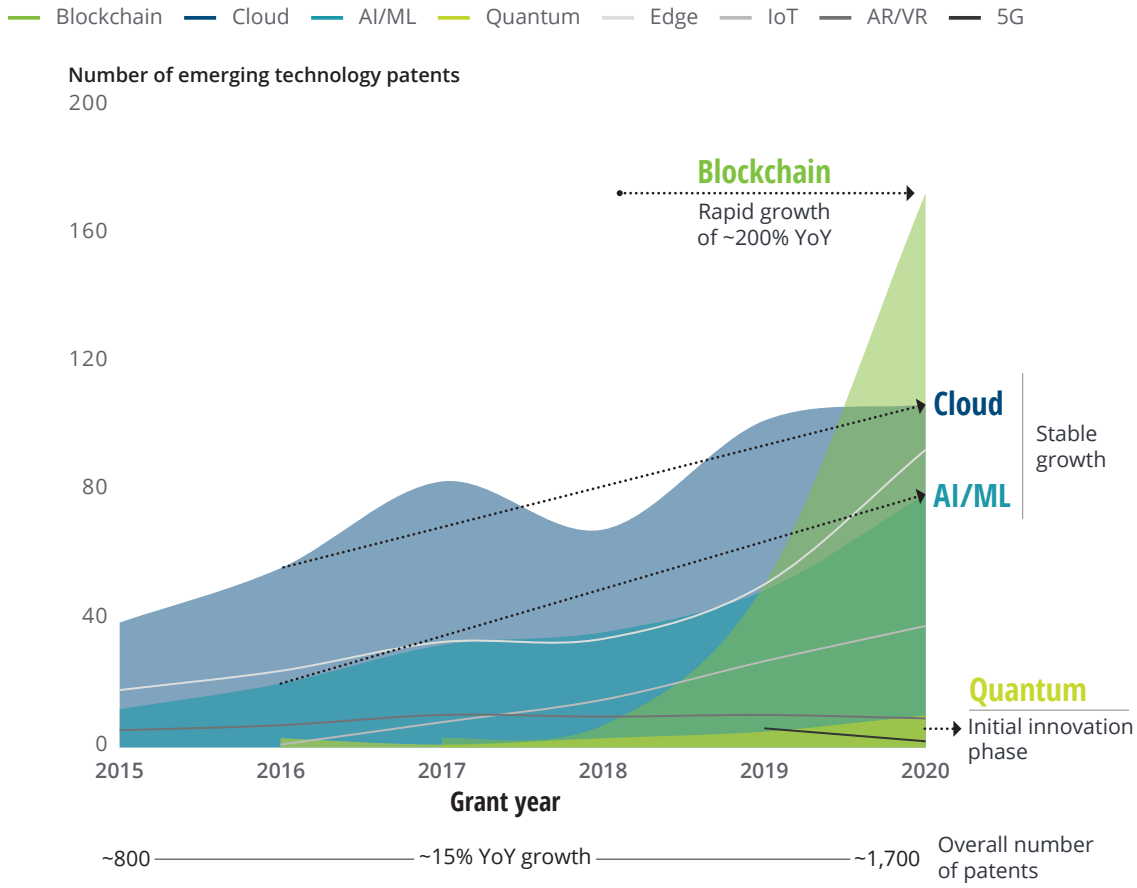
- AI and ML patents are growing at a brisk pace (35%) and provide numerous avenues today for organizations to enhance digital trust across applications and use cases.

- Blockchain, on the other hand, appears to be in its initial, rapid-growth phase. Blockchain patents have grown by almost 200% YoY over the last three years. This indicates that blockchain may have promising growth potential as an increasingly viable digital trust solution—but has not yet reached peak maturity. Blockchain projects are gradually moving from early proofs-of-concept or pilots to full-scale implementations;[82] thus, in the near future, blockchain could play a truly foundational role in establishing digital trust across the enterprise and ecosystem.[83]

- Quantum technologies are much earlier in their innovation curve; but specialists suggest that they could become vital to ensuring the security of sensitive digital assets as core quantum-computing capabilities mature.[84]

FIGURE 1

Digital trust patents granted annually between 2015 and 2020



Notes: All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review any individual patents in preparing this analysis.

Source: Deloitte analysis.

Endnotes

1. Catherine Stupp, “Fraudsters used AI to mimic CEO’s voice in unusual cybercrime case,” *Wall Street Journal*, August 30, 2019.
2. Johannes Tammekänd, John Thomas, and Kristjan Peterson, *Deepfakes 2020: The tipping point*, Sentinel, October 2020.
3. Jeff Pollard, “Predictions 2020: Cyberattacks influence society in a broader way,” Forrester, October 30, 2019.
4. Ping Identity, *2019 Consumer survey: Trust and accountability in the era of data misuse*, October 8, 2019.
5. David Linthicum et al., *The future of cloud-enabled work infrastructure: Making future business infrastructure ready*, Deloitte Insights, September 23, 2020.
6. Spiceworks Ziff Davis, *The 2022 State of IT*, accessed January 21, 2022.
7. All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review individual patents while preparing this analysis.
8. Deloitte defines organizational trust as the foundation of a meaningful relationship between an entity and its stakeholders, at both individual and organizational levels. Trust is built through actions that demonstrate a high degree of *competence* and the right *intent*, which result in demonstrated capability (possessing the means to meet expectations), reliability (consistently and dependably delivering upon promises made), transparency (openly sharing information, motives, and choices in plain language), and humanity (genuinely caring for the experience and well-being of others). For more information, please visit: Importance of Trust in your organization | Deloitte US.
9. Rich Nanda et al., *A new language for digital transformation*, Deloitte Insights, September 23, 2021.
10. Nancy Albinson, Sam Balaji, and Yang Chu, *Building long-term trust in digital technology*, Deloitte Insights, September 23, 2019.
11. Gil Press, “Cleaning big data: Most time-consuming, least enjoyable data science task, survey says,” *Forbes*, March 23, 2016.
12. Manasi Sakpal, “How to improve your data quality,” Gartner, July 14, 2021.
13. Don Fancher et al., *AI model bias can damage trust more than you may know. But it doesn’t have to*, Deloitte Insights, December 8, 2021.
14. Debbie Walkowski, “What is the CIA Triad?,” F5, July 9, 2019.
15. Ira Cohen, “The end to a never-ending story? Improve data quality with AI analytics,” Anadot, accessed January 21, 2022.
16. Sensity, “Fraudulent documents detection,” accessed January 21, 2022; Sentinel, “Defending against deepfakes and information warfare,” accessed January 21, 2022.
17. Mina Tocalini, “Living in a deepfake world,” Arts Management & Technology Laboratory, October 21, 2021.
18. Matt Groh, “Detect DeepFakes: How to counteract misinformation created by AI,” MIT Media Lab, accessed January 21, 2022; Tammekänd, Thomas, and Peterson, *Deepfakes 2020*; Nadeem Sarwar, “Scientists discover trick to spotting deepfakes, but it’s not easy,” *Screen Rant*, September 13, 2021.
19. Jeremy Kahn, “Facebook says it’s made a big leap forward in detecting deepfakes,” *Forbes*, June 16, 2021.

20. Curt Aubley et al., *Cyber AI: Real defense*, Deloitte Insights, December 7, 2021.
21. Avi Turgeman, "Machine learning and behavioral biometrics: A match made in heaven," *Forbes*, January 18, 2018.
22. Ben Dickson, "How machine learning removes spam from your inbox," TechTalks, November 30, 2020.
23. Sentinel One, *Global ransomware study 2018*, accessed January 21, 2022.
24. Aubley et al., *Cyber AI: Real defense*.
25. IBM, *How much does a data breach cost—Cost of a data breach report 2021*, accessed January 21, 2022.
26. John Paul Titlow, "YouTube is using AI to police copyright—to the tune of $2 billion in payouts," *Fast Company*, July 13, 2016.
27. Duncan Stewart, Gillian Crossan, and Ariane Bucaille, *Keeping AI private: Homomorphic encryption and federated learning can underpin more private, secure AI*, Deloitte Insights, December 1, 2021.
28. VentureBeat, "Meet the new twist on data encryption that promises better privacy and security for AI," January 16, 2020; Bernard Marr, "What is homomorphic encryption? And why is it so transformative?," *Forbes*, November 15, 2019.
29. Brendan McMahan and Daniel Ramage, "Federated learning: Collaborative machine learning without centralized training data," Google AI Blog, April 6, 2017.
30. Zach Winn, "Enabling AI-driven health advances without sacrificing patient privacy," *MIT News*, October 7, 2021.
31. Dieter Bohn, "Privacy and ads in Chrome are about to become FLoC-ing complicated," *Verge*, March 30, 2021.
32. Fancher et al., *AI model bias can damage trust more than you may know. But it doesn't have to*. Deloitte Insights, December 08, 2021.
33. All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review individual patents while preparing this analysis.
34. Jeffery Weirens, Michael Bondar, and Jennifer Lee, *New models for building digital trust: An interview with MIT's Sandy Pentland*, Deloitte Insights, April 5, 2021.
35. Sylvie Delacroix and Jess Montgomery, "Data trusts and the EU data strategy," Data Trusts Initiative, June 8, 2020; The Open Data Institute, "How do we unlock the value of data while preventing harmful impacts?," accessed January 21, 2022.
36. Geoff Mulgan and Vincent Straub, "The new ecosystem of trust," Nesta, February 21, 2019.
37. MIDATA, "My data—Our health," accessed January 21, 2022.
38. Construction Data Trust website, accessed January 21, 2022.
39. Deloitte interview.
40. Deloitte, "To build trust, take data protection to the bank," *Wall Street Journal*, July 14, 2021.
41. Weirens, Bondar, and Lee, *New models for building digital tru*st.
42. Monique Crichlow and David Castle, "Examining the role of data trusts in smart cities," Canadian Science Policy Centre, November 2019.
43. The Open Data Institute, "Greater London Authority and Royal Borough of Greenwich pilot: What happened when we applied a data trust," April 15, 2019.
44. Tanya Andreasyan, "Mastercard and IBM join forces for new "data trust," Truata," *FinTech Futures*, March 19, 2018.

45. Deloitte interview; TIBCO, "What is data fabric?," accessed January 21, 2022.

46. Deloitte, "To build trust, take data protection to the bank."

47. Avivah Litan and Adrian Leow, *Hype cycle for blockchain technologies, 2020,* Gartner, July 13, 2020; Avivah Litan, "Hype cycle for blockchain 2021; More action than hype," Gartner, July 14, 2021.

48. Deloitte interview.

49. Thomas Jensen, Jonas Hedman, and Stefan Henningsson, "How TradeLens delivers business value with blockchain technology," *MIS Quarterly Executive* 18, no. 4 (2019): pp. 221–43; TradeLens, "Together, we can set trade free," accessed January 19, 2022.

50. Elinar Stabel, "Hydro and DNV GL launch blockchain for greener metals," Norsk Hydro ASA, March 1, 2021; Ledger Insights, "Aluminium firm Hydro pilots DNV blockchain solution for sustainable traceability," March 2, 2021.

51. Safe.press, "News certification operated by blockchain," accessed January 21, 2022.

52. Jai S. Arun and Alexander Carmichael, *Digital identity on blockchain,* IBM, April 1, 2017; Tykn B.V., "Self-sovereign identity: The ultimate beginners guide!," accessed January 21, 2022.

53. Consensys, "Blockchain in digital identity," accessed January 21, 2022.

54. Elizabeth Durant and Alison Trachy, "Digital diploma debuts at MIT," *MIT News*, October 17, 2017.

55. Linda Pawczuk, Richard Walker, and Claudina Castro Tanco, *Deloitte's 2021 Global Blockchain Survey: A new age of digital assets*, Deloitte Insights, 2021.

56. Sam Dean, "$69 million for digital art? The NFT craze explained," *Los Angeles Times*, March 11, 2021.

57. Rebellion Research, "Why NFTs could be the solution to the DeepFake problem," April 11, 2021.

58. Paul Lee et al., *From trading cards to digital video: Sports NFTs kick sports memorabilia into the digital age,* Deloitte Insights, December 1, 2021.

59. Chrissa McFarlane, "Tokenized blood? How NFTs are transforming healthcare," *Forbes*, June 2, 2021.

60. Deloitte, "Getting smart about smart contracts," accessed January 19, 2022.

61. Alex Rad, "Partior enters cross-border payments ecosystem as newcomer with big backers," The Asian Banker, September 23, 2021.

62. Ledger Insights, "JP Morgan, DBS blockchain payment platform Partior launches first pilot," October 26, 2021.

63. William D. Eggers and Ruth Hickin, *Global technology governance report 2021: Harnessing Fourth Industrial Revolution technologies in a COVID-19 world*, World Economic Forum, December 2021; Matthew Niemerg, "Private vs. public blockchains for enterprise business solutions," InfoQ, September 21, 2021; Shea Ketsdever and Michael Fischer, "Incentives don't solve blockchain's problems," accessed January 21, 2022.

64. Scott Buchholz, Deborah Golden, and Caroline Brown, *A business leader's guide to quantum technology*, Deloitte Insights, April 15, 2021.

65. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," IEEE Xplore, August 6, 2002.

66. Deborah Golden et al., *Preparing the trusted internet for the age of quantum computing*, Deloitte Insights, August 6, 2021.

67. World Economic Forum, *Quantum personas: A multistakeholder approach to quantum cyber risk management,* 2021.

68. Buchholz, Golden, and Brown, *A business leader's guide to quantum technology*; National Security Agency, "Quantum key distribution (QKD) and quantum cryptography (QC)," accessed January 21, 2022.

69. NIST, "Post-quantum cryptography (PQC)," June 14, 2021.
70. Golden et al., *Preparing the trusted internet for the age of quantum computing*.
71. Ibid.
72. Buchholz, Golden, and Brown, *A business leader's guide to quantum technology*.
73. QuantumXchange, "Quantum cryptography, explained," accessed January 21, 2022; Toshiba Clip, "Securing the future of a digital society: Achieving secure transfer of sensitive data between remote facilities on a single fiber," April 20, 2021.
74. NSA, "Quantum key distribution (QKD) and quantum cryptography (QC)."
75. Deloitte, "With quantum computing's rise, cybersecurity takes center stage," *Wired*, accessed January 21, 2022.
76. QuantumXchange, "Quantum communications in real world applications," accessed January 21, 2022.
77. NSA, "Quantum key distribution (QKD) and quantum cryptography (QC)."
78. Kylie Robison, "Here's how quantum computing could transform the future," *Business Insider*, March 2, 2021. Michele Moska and Marco Piani, *Quantum threat timeline report 2020*, Global Risk Institute, January 27, 2021.
79. Colin Soutar et al., "How the world can prepare for quantum-computing cyber risks," World Economic Forum, September 28, 2021.
80. Duncan Stewart et al., *Quantum computing in 2022: Newsful, but how useful?*, Deloitte Insights, December 1, 2021; Golden et al., *Preparing the trusted internet for the age of quantum computing*, Deloitte Insights, August 6, 2021.
81. The number of granted digital trust patents analyzed was approximately 7,000 (between 2015–20). All information on patents is sourced from Derwent World Patents Index via Quid (https://quid.com). The purpose of the analysis is to identify general themes in digital trust. Deloitte did not review individual patents while preparing this analysis.
82. Litan and Leow, *Hype cycle for blockchain technologies, 2020,* Gartner, July 13, 2020; Litan, "Hype cycle for blockchain 2021; More action than hype," Gartner, July 14, 2021.
83. Gartner, "Gartner 2019 hype cycle shows most blockchain technologies are still five to 10 years away from transformational impact," press release, October 8, 2019; Deloitte interview.
84. Deloitte interview.

Acknowledgments

The authors would like to thank **Alex "Sandy" Pentland** from MIT's Connection Science lab for sharing his thoughts and ideas. They would also like to thank the following individuals for sharing their contributions: **Bilyana Lilly, Eric Dull, Nirmal Kumar, Asad Ahamad, Kevvie Fowler, Nick Galletto, Beth Dewitt, Lukas Kruger, Michelle Lee, Charlotte Gribben, Tyler Welmans,** and **David Linthicum.**

The authors would also like to thank **Kiran Nagaraj, Colin Soutar, Linda Walsh, Hallie Miller, Andy Bayiates, Natasha Buckley, Jonathan Holdowsky, Negina Rood, Siri Anderson,** and **Wasim Sarang** for their support.

About the authors

Deborah Golden I debgolden@deloitte.com

Deborah Golden, a principal at Deloitte & Touche LLP, is the US Cyber & Strategic Risk leader for Deloitte Risk & Financial Advisory. She has more than 25 years of cross-industry experience, focused predominantly within government, life sciences and health care, and financial services industries. Golden primarily helps commercial organizations and government agencies navigate multifaceted cyber problems and transform business or mission strategies and operations. Recognizing the ubiquitous, sophisticated nature of cyber, she uses a values-driven approach to help clients align cybersecurity imperatives with cyber risk and strategic business priorities to strengthen cyber resilience.

Jesse Goldhammer I jgoldhammer@deloitte.com

Jesse Goldhammer is a managing director in Deloitte's cyber security practice and leads the firm's Trustworthy Institutions initiative. He is deeply committed to the safeguarding of public and private sector data, networks, systems, and people from a wide range of cyber threats. An accomplished instructor, author, and speaker, he has written articles and given presentations on a variety of cyber- and trust-related topics.

Jay Parekh I japarekh@deloitte.com

Jay Parekh is a senior analyst with the Deloitte Center for Integrated Research. He has over six years of experience in research and analysis focused on emerging technologies and digital innovations related to cloud computing, augmented & virtual reality, the Internet of Things (IoT), and other advanced technologies. He also focuses on developing Deloitte's perspectives on cross-industry topics such as climate change and sustainability.

Diana Kearns-Manolatos I dkearnsmanolatos@deloitte.com

Diana Kearns-Manolatos is a senior manager in the Deloitte Center for Integrated Research where she analyzes market shifts and emerging trends across industries. She leads Deloitte's global research on digital transformation. Additionally, Kearns-Manolatos draws on almost 15 years of award-winning marketing communications expertise to align insights with business strategy.

Curt Aubley I caubley@deloitte.com

Curt Aubley is Deloitte's Cyber and Strategic Risk Groups managing director and general manager for the Threat Detection & Response. He leads the development of the vision, strategy, solution development, roadmap, go-to-market, sales, ecosystem, alliances, and overall execution in alignment with Deloitte's strategy.

Michael Morris I micmorris@deloitte.com

Michael Morris is a managing director in Deloitte's Cyber and Strategic Risk practice where he leads Engineering for Detect and Respond. He is responsible for the technical vision, technological development, operations engineering, and was the chief architect behind the Adversary Pursuit platform and methodology. He has experience in intelligence operations, advanced offensive and defensive cyber operations, and tactics and tool development.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Jesse Goldhammer
Managing director | Deloitte Risk & Financial Advisory
+1 415 783 7681 | jgoldhammer@deloitte.com

Jesse Goldhammer is a managing director in Deloitte's Cyber Security practice and leads the firm's Trustworthy Institutions initiative. He specializes in helping clients build new cyber and trust capabilities using cutting-edge technologies.

Linda Walsh
Managing director | Deloitte & Touche LLP
+1 973 255 9295 | lwalsh@deloitte.com

Linda, a managing director at Deloitte & Touche LLP, is the Cyber Risk Services Data solution leader for Deloitte Risk & Financial Advisory. She is working to maximize the go-to-market strategies for Deloitte's Privacy, Protection, and Data Management solution offerings.

David Mapgaonkar
Principal | Deloitte & Touche LLP
+1 415 783 7681 | jgoldhammer@deloitte.com

David Mapgaonkar, a principal at Deloitte & Touche LLP, is the Identity practice leader, and, the TMT Industry leader for the Cyber & Strategic Risk practice.

Deloitte Center for Integrated Research

Diana M. Kearns-Manolatos
Senior manager, subject matter specialist | Deloitte Services LP
+1 212 436 3301 | dkearnsmanolatos@deloitte.com

Diana M. Kearns-Manolatos is a senior manager with Deloitte Services LP's Center for Integrated Research, where she leads Deloitte's global research on digital transformation.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Andy Bayiates, Emma Downey, Dilip Poddar, and Arpan Kumar Saha

Creative: Jaime Austin and Rahul Bodiga

Audience development: Alexandra Kawecki, Nikita Garia, and Hannah Rapp

Cover artwork: Jaime Austin

Deloitte's Center for Integrated Research focuses on developing fresh perspectives on critical business issues that cut across industries and functions, from the rapid change of emerging technologies to the consistent factor of human behavior. We look at transformative topics in new ways, delivering new thinking in a variety of formats, such as research articles, short videos, in-person workshops, and online courses.

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte