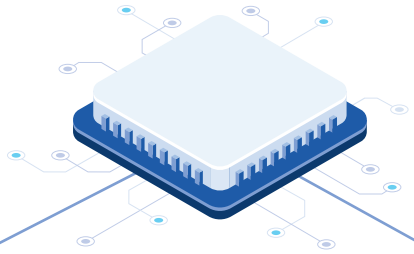
United Nations Development Programme



New Technologies for Sustainable Development:

PERSPECTIVES ON INTEGRITY, TRUST AND ANTI-CORRUPTION

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow @UNDP.

One United Nations Plaza, New York, NY 10017, USA

ACKNOWLEDGEMENTS

New Technologies for Sustainable Development: Perspectives on integrity, trust and anti-corruption was developed by the United Nations Development Programme's Anti-Corruption for Peaceful and Inclusive Societies (ACPIS) Global Project, under the overall guidance and supervision of Anga R Timilsina, UNDP Global Programme Advisor on Anti-Corruption.

The publication was authored by Charlene Lui (UNDP) and edited and reviewed by Anga R Timilsina (UNDP). The publication received helpful contributions and inputs from the following ACPIS team members: Aida Arutyunova and Jungoh Son.

We are thankful to Sarah Lister and Jennifer McEneaney from the UNDP Governance Team for their support and review of the publication. We would also like to express our appreciation to the following staff from UNDP for their valuable insights and contributions in reviewing the publication: Robert Opp, Daria Asmolova, Tariq Malik, Niall McCann, Calum Handforth, Sonja Stefanovska-Trajanoska, Sarah Dix, Irakli Kotetishvili, Mark Dibiase and Brook Horowitz.

We would also like to thank the following experts for serving as external peer reviewers: Per Aarvik (U4 Anti-Corruption Resource Centre), Kristen Sample and Victoria Welborn (National Democratic Institute), Mark Lovatt and Jayasantini Pandian (Trident Integrity).

The production of this publication was made possible through generous funding from the Australian Government Department of Foreign Affairs and Trade (DFAT), Norwegian Agency for Development Cooperation (Norad) and Swedish International Development Cooperation Agency (Sida); however the views expressed in this publication do not necessarily reflect the views or policies of the Governments of Australia, Sweden and Norway.

Contact:
Anga R Timilsina (anga.timilsina@undp.org)
Charlene Lui (charlene.lui@undp.org)

Copyediting by Alexandra George
Design by Peter Ørntoft

TABLE OF CONTENTS

FOREWORD

In the past decades, technology has revealed its potential for transforming the world and accelerating the pace of sustainable development. During the Fourth Industrial Revolution, the development, adaptation and application of new technologies are bringing benefits to almost every area of the economy, society, culture and institutions. Today, with data growing at an exponential pace, we have more information than at any other point in history, which therefore enables us to better address complex global challenges.

Amid the COVID-19 pandemic, artificial intelligence and data analytics have improved the ways in which healthcare is delivered, by increasing the accuracy of diagnosis and treatment, quality of patients' experience, and access to healthcare services. As the pandemic continues to unravel the unresolved tensions between people and the planet, technology has also enhanced transparency in complying with the Paris Agreement. For example, the Pacific Alliance has piloted a publicly shared digital ledger of carbon credits to boost transparency and accountability in climate action[1].

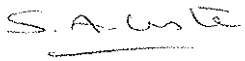
At the same time, however, the adoption and application of new technologies have posed new challenges for policymakers, including issues related to ethics, trust, human rights, data privacy, and data protection. In addition, inequalities in the form of the 'haves' and 'have-nots' in reaping the benefits of digital transformation undermine the central promise of the 2030 Agenda to 'Leave No One Behind' and threaten to widen the digital divide.

UNDP recognizes the huge potential of new technologies for sustainable development, and through its Digital Strategy[2], focuses on using digital technologies to solve development challenges through innovation in delivery, co-creation, collaboration, and advocacy. As part of our commitment to leave no one behind and ensure that the benefits of technological innovation are shared by all, UNDP is engaging with governments, the private sector, civil society and communities to address challenges from both a programmatic and policy perspective.

New Technologies for Sustainable Development: Perspectives from integrity, trust and anti-corruption explores the immense opportunities new technologies bring in improving the access and quality of service delivery and in mitigating corruption risks and enhancing transparency and accountability. It also highlights new avenues in which technologies could be misused or abused for corrupt, criminal and unethical conduct, including the use of cryptocurrencies for illicit trade and money laundering, or AI-driven decisions that could be used for manipulation or discrimination due to algorithmic bias.

We hope that this study contributes to identifying and developing effective digital governance strategies, to maximize the benefits of new technologies for sustainable development and minimize the risks of abuse and misuse in the application and adoption of new technologies.

I would also like to take this opportunity to thank all who have contributed to this study, which should be considered an initial contribution to a fast-moving field. We also look forward to feedback on this publication.



Sarah Lister
Head of Governance
Bureau for Policy and Programme Support
United Nations Development Programme

1 Pacific Alliance: Market and non-market approaches for achieving the NDCs, August 2019. https://www.transparency-partnership.net/news/pacific-alliance-market-and-non-market-approaches-achieving-ndcs
2 UNDP Digital Strategy. https://digitalstrategy.undp.org/strategy.html

EXECUTIVE SUMMARY

The **2030 Agenda for Sustainable Development** has embraced the spread of technology and global interconnectedness as having great potential to accelerate human progress, bridge the digital divide and develop knowledge societies. With growing challenges to sustainable development – from poverty and inequality, to conflict, climate change and global health threats such as the COVID-19 pandemic – the 2030 Agenda has brought immense opportunities to leverage scientific and technological innovation to meet many development challenges in the 21st century.

Over the past two decades, the evolution of technology has dramatically transformed economies, societies and cultures. Digitalization can propel us towards achieving the Sustainable Development Goals (SDGs)[3]. The rapid advancements in technology – from Information and Communication Technology (ICT) to new technologies such as artificial intelligence (AI) – have profoundly changed the ways people interact with one another, with businesses and with governments. This has been evident during the COVID-19 pandemic, when many governments have taken unprecedented measures using new technologies and advanced analytics to respond to and recover from the crisis[4]. Countries that have maintained low per-capita COVID-19 mortality rates have had similar pandemic management strategies, including early surveillance, testing, contact tracing and strict quarantine measures. In particular, in many countries the adoption of technology and its integration into policies and healthcare service delivery has significantly helped in coordination, data management and effective implementation of COVID-19-related national strategies[5].

"Technology has become one of the greatest allies for preventing and tackling corruption."

In the area of anti-corruption, technology has become one of the greatest allies for preventing and tackling corruption, defined as 'the abuse of entrusted power for private gain'[6] by global development actors. The most common internationally-agreed forms of corruption, as identified in Articles 15 to 25 of the United Nations Convention against Corruption (UNCAC), include, but are not limited to: bribery, illicit financial flows, money laundering, kickbacks, nepotism, patronage, embezzlement, clientelism, abuse of functions and trading in influence.[7]

Around the world, technology is increasingly being harnessed for anti-corruption efforts, focusing not only on tackling specific forms of corruption (such as bribery, illicit financial flows, money laundering, embezzlement, nepotism and others), but also on enhancing transparency, accountability, integrity, openness, participation and inclusion. This is most evident in innovations in corruption reporting, monitoring, advocacy and e-government initiatives, including open contracting and e-procurement.

The opportunities in the use of digital technologies for integrity and anti-corruption are vast, and can be grouped into two main approaches: a **direct approach to prevent and tackle corruption,** such as using digital tools to detect, analyse, investigate, predict, and monitor corruption; and an **indirect approach through promoting effective, accountable and inclusive institutions** and governance processes for efficient and effective service delivery, such as e-government for efficient service delivery; digital

3 United Nations Secretary-General's Task Force on Digital Financing of the Sustainable Development Goals (2020) People's Money: Harnessing Digitalization to Finance a Sustainable Future (Final Report), August 2020. https://unsdg.un.org/sites/default/files/2020-08/DF-Task-Force-Full-Report-Aug-2020-1.pdf

4 B.Busetto and A. Timilsina, "The role of technology and anti-corruption measures in fighting COVID-19" (Blog) UNDP, 15 September 2020. https://www.undp.org/content/undp/en/home/blog/2020/the-role-of-technology-and-anti-corruption-measures-in-fighting-.html

5 S. Whitelaw et al. "Applications of digital technology in COVID-19 pandemic planning and response", The Lancet, 29 June 2020. https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30142-4/fulltext

6 UNDP, Corruption and Development: A Primer, 2008. http://www.undp.org/content/undp/en/home/librarypage/democratic-governance/anti-corruption/corruption.html

7 United Nations Convention against Corruption (UNCAC). https://www.unodc.org/unodc/en/corruption/uncac.html

tools to promote advocacy and awareness; and open data for monitoring and access to information. Moreover, over the years, ICTs have played an instrumental role in empowering citizens, by simplifying administrative procedures and enabling governments to move towards a more citizen-centric approach to offering public services. These, in turn, have significant implications for public trust in governance institutions to serve public interests, as well as social cohesion and trust within society, necessary conditions for inclusive and sustainable development.

Based on lessons learned from the use of ICTs over the past two decades, the effectiveness of technology to achieve development goals depends on the following factors:

- A long-term national e-government/digital policy or strategy
- Sustained investments in technological capacity/capabilities and digital infrastructure
- Continuous innovation, adaptation and experimentation over time, including building on best practices around the world
- Implementation of digital governance and ICT strategies, programmes and projects with a clear monitoring and evaluation framework
- Technology education and digital literacy, advocacy efforts and raising public awareness of the use of digital technologies
- Building trust in digital systems, in terms of public confidence, transparency and accountability

These critical elements hold important lessons for new technologies, such as AI, blockchain and big data analytics, whose development, practical applications and regulatory mechanisms are still largely unrealized in the field of anti-corruption in many countries. New technologies are often cited as the 'Next Big Things' and have vast potential for sustainable development, by transforming agriculture, education, energy, health and public services, identifying, reversing and mitigating the effects of climate change, ensuring food security, reducing disaster risks, preventing humanitarian crises, monitoring natural resources and reducing poverty.

> **"Given that the development of new technologies and digital solutions adds a new dimension of vulnerability, there is a need to address the risks of misuse and abuse of technology."**

However, a clear understanding is needed of how new technologies might shape the global economy, society and politics over the next decade. Given that the development of new technologies and digital solutions adds a new dimension of vulnerability, there is a need to address the risks of misuse and abuse of technology, including corrupt activities that could be facilitated by technology, such as money laundering, fraud and cybercrime; the balance between regulation and innovation; ethical and human rights considerations; trust and integrity; the digital divide among and within countries, especially in access to these technologies; and challenges in governing multinational corporations dominating a largely unregulated space. Thus, the effectiveness and risks surrounding the use of new technologies or digital solutions also depend on several prerequisites for **effective digital governance and digital infrastructure.**

This study, based on desk research, explored the following new technologies in relation to integrity, trust and anti-corruption: AI, machine learning and deep learning tools; blockchain technology; big data analytics; robotic process automation; the Internet of Things; and cloud computing.

This study sought to enhance the understanding of the opportunities offered by new technologies to prevent and tackle corruption, while recognizing the risks and challenges that exist. The study also explored current regulatory mechanisms in the use of the technologies, building on the practices around the world. The study provided policy recommendations to address risks, promote effective digital governance and support partnerships and dialogue among key stakeholders, including governments, technologists and innovators, regulators, development practitioners, anti-corruption actors, the private sector and civil society.

Regardless of whether technologies are traditional or new, their efficiency and effectiveness tend to largely depend on the enabling environment for their use. The discussion in each chapter also addresses the following issues: digital governance, institutional

architecture and an effective set of rules to complement traditional policy, regulation and governance processes; implications and ethical issues surrounding the use of technology; data and privacy issues, including data collection, storage, sharing, protection and security; the applicability, relevance and transferability of technology across contexts; the principle of leaving no one behind; and collaborative platforms to advance the understanding of new technologies.

The key takeaways of this study are summarized as follows:

- **Technology is an important tool to enhance anti-corruption efforts,** not only in promoting increased transparency, accountability, openness, accessibility and citizen participation, but also in its potential to detect, analyse, predict, and therefore deter and prevent corruption. To harness its full potential, the application of technology for anti-corruption efforts should also take into account a major lesson learned: technology alone cannot solve corruption, which is also dependent on the wider political economy context and requires ethics and integrity to be embedded in systems, institutions and society.

- **Effective digital governance is necessary to ensure ethics and integrity in the use of new technologies,** including data-driven digital transformations and data quality management. The outcomes generated by technologies such as AI highly depend on the design and implementation of the algorithms and data used. These will generate outcomes that are inherently biased to some extent, whether systemic or random. In that regard, governments and policymakers need to work together with the technologists and data scientists to produce data and services that ensure ethics and integrity are built in.

- **Along with the need to encourage innovation and the application of new technologies, there is an increasingly clear recognition that regulation is necessary to govern the responsible use of technologies and data.** This includes integrating the principles of transparency, accountability, ethics, non-discrimination, integrity, access, inclusion and human rights. Regulation is crucial to protect users and ensure security, but it should also create an environment that is conducive to continuous innovation. Without appropriate legal and regulatory frameworks in which technologies operate, the usefulness of technology may be limited or susceptible to abuse at the hands of those who design them. Therefore, through digital governance, governments have a crucial role to play in guiding technological change proactively alongside technologists and other stakeholders, a much different approach to traditional decision-making and policymaking processes.

- **While, on the one hand, digital technologies can play a key role in driving transparency, on the other hand, we need to build trust in the technology sector.** From the perspectives of integrity and trust, technology and anti-corruption measures have a mutually reinforcing relationship: technology for integrity and trust; and integrity and trust for technology. The ability of digital technologies to create platforms for data transparency and open information, which are useful for monitoring services, improving products and improving citizen engagement, can help build trust. Yet, privacy and security breaches, with wide-ranging implications for human rights and accountability, have led to declines in trust, not only in technology products but also in the whole technology sector.

- **Participatory approaches to digital governance, including public engagement, dialogue and consultation** of a wide range of stakeholders, particularly between technology and digital solution providers, regulators and oversight institutions and users of digital technologies, are necessary to build trust, safeguard human rights and ensure accountability. In addition, promoting a ‘culture of openness’ is important alongside promoting a ‘culture of innovation’. Open resources, processes and standards can drive the internet ecosystem and promote continuous technology-based innovation globally.

- **Good quality data is necessary to provide meaningful insight, information and intelligence in any area.** However, the wide-ranging opportunities and applications of data must be balanced with its ethical use, including measures to ensure data privacy and protection in its collection, storage, sharing and management. Addressing these issues would promote trust in digital systems and encourage innovation.

- **Investments in digital infrastructure need to be in place in order to reap the benefits of new technologies, accompanied by a strong political commitment to change existing systems and mechanisms.** To promote advancement in technologies, all technologies need to undergo experimentation, innovation, adaptation and a process of disruption. These require sustained and significant investments in order to turn disruptions into positive change.

- **Digital transformations should ensure inclusive, people-centred and human rights-based social contracts built on accountability and trust.** The widening digital divides between developed and developing countries, urban and rural areas, the rich and poor and men and women – such as in the capabilities for harnessing digital data and new technologies, or in the basic opportunities to participate in digital society – threaten to exacerbate inequalities and leave developing countries even further behind. Digital education and digital literacy are thus necessary, including strengthening equal access and ownership of technology within populations, so that no one is left behind.

1.

INTRODUCTION

1.1 CONTEXT: TECHNOLOGY AND INNOVATION FOR SUSTAINABLE DEVELOPMENT

The 2030 Agenda for Sustainable Development has embraced the spread of technology and global interconnectedness as having great potential to accelerate human progress, bridge the digital divide and develop knowledge societies to accelerate the achievement of the SDGs. With the growing challenges to sustainable development – from poverty and inequality, to fragility and conflict, climate change and global health threats such as the COVID-19 pandemic – the 2030 Agenda has brought immense opportunities to leverage scientific and technological innovation to meet many development challenges.

Over the past two decades, technology has evolved dramatically and transformed economies, governance, societies and cultures. Digitalization and advancements in technology can propel us towards achieving the SDGs[8].

During the COVID-19 pandemic, rapid innovations in response to and to recover from COVID-19 have been evident worldwide[9]. Some countries have leveraged new technologies in responding to different areas of the pandemic: from surveillance, prevention and containment, to diagnosis and treatment of patients. In Singapore, the government employed extensive contact-tracing using 'digital signatures' to identify the close contacts of those infected with COVID-19, which has been effective in containment and preventing further transmission[10]. In the Republic of Korea, open data is used to disclose real-time information to alert residents giving them detailed information of the itineraries of confirmed COVID-19 patients, to enable them to take precautionary measures and to monitor and report on their conditions if they have visited the 'infection points' at the same hours as the confirmed patients and developed symptoms[11]. Open data portals have also been used to monitor COVID-19 information in Serbia[12], while digital payment platforms reduced the risk of fraud and corruption by authenticating COVID-19 cash transfers in Malawi[13].

The growing use of digital technologies as a means to respond to crises, tackle development challenges and achieve the SDGs is unsurprising, given that digital technologies have advanced more rapidly than any innovation in history, reaching around 50 percent of the developing world's population in only two decades,[14] and transforming societies by enhancing connectivity, access to financial services, trade and public services. The growth of new technologies and technological innovation will continue to

8 People's Money. https://unsdg.un.org/sites/default/files/2020-08/DF-Task-Force-Full-Report-Aug-2020-1.pdf
9 B. Busetto and A. Timilsina. "The role of technology and anti-corruption measures in fighting COVID-19" (Blog), UNDP, 15 September 2020. https://www.undp.org/content/undp/en/home/blog/2020/the-role-of-technology-and-anti-corruption-measures-in-fighting-.html
10 C. Handforth, "What Singapore can teach about an effective coronavirus response" (Blog), UNDP, 25 March 2020. See https://www.undp.org/content/undp/en/home/blog/2020/what-singapore-can-teach-about-an-effective-coronavirus-response.html
11 UNDP Seoul Policy Centre, "Public Information Disclosure on COVID-19", 22 April 2020. https://www.undp.org/content/seoul_policy_center/en/home/presscenter/articles/2019/Collection_of_Examples_from_the_Republic_of_Korea/covid-public-information-disclosure.html
12 UNDP Serbia, "How is UNDP helping Serbia fight the coronavirus epidemic", 31 March 2020. https://www.rs.undp.org/content/serbia/en/home/presscenter/articles/2020/kako-undp-poma_e-srbiji-u-borbi-sa-epidemijom-korona-virusa.html
13 UNDP Malawi, "Promoting E-payment systems as a COVID-19 Preventative Strategy", UNDP Digital Responses to COVID-19. https://airtable.com/shrGXLJECotnZa1Ou/tblwPhDJfiisTMNg6/viwRoWh6lu99wyzz7/rec1n5BVkcc5iiU3O?blocks=bipVDslkfppjON6Dh
14 United Nations, The Age of Digital Interdependence, Report of the Secretary-General's High-Level Panel on Digital Cooperation, 2019. https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

drive the global economy in the next decade. For example, it is estimated that by 2021, 60 percent of Gross Domestic Product (GDP) in the Asia-Pacific region will be derived from digital products or services resulting from digital transformation[15]. The United Nations Task Force on Digital Financing of the SDGs also highlighted that governments in developing countries could gain US$220-320 billion annually from increasing transparency in public budgets and contracts through digitalizing payments[16].

The multitude of opportunities new technologies bring could reinvent the economy, society and the environment, although many challenges would arise, including bridging the digital divide and access to technologies, increasing workforce redundancy as more efficient digital processes are put in place, increasing risks of surveillance, and the increasing power of technology firms and of the 'tech-elite'. Importantly, governments worldwide also recognize the power of technology and e-government for the advancement and transformation of the public sector landscape, owing to the enormous potential of improving the efficiency and effectiveness in public administration and service delivery, and of increasing transparency, accountability, accessibility and citizen participation.

1.2 ICTS AND NEW TECHNOLOGIES FOR INTEGRITY, TRUST AND ANTI-CORRUPTION

In the area of anti-corruption, technology – from ICTs to new technologies – has become one of the greatest allies for preventing and tackling corruption. While there is no universal definition of corruption, it is commonly defined as the 'abuse of entrusted power for private gain'. The UNCAC, as the global legally-binding instrument against corruption, identifies many forms of corrupt conduct in Articles 15 and 25 of the Convention, including, but not limited to: bribery, illicit financial flows, money laundering, kickbacks, nepotism, patronage, embezzlement, clientelism, abuse of functions and trading in influence.

While anti-corruption is essential for achievement across the 2030 Agenda, anti-corruption is most directly related to five SDG targets:

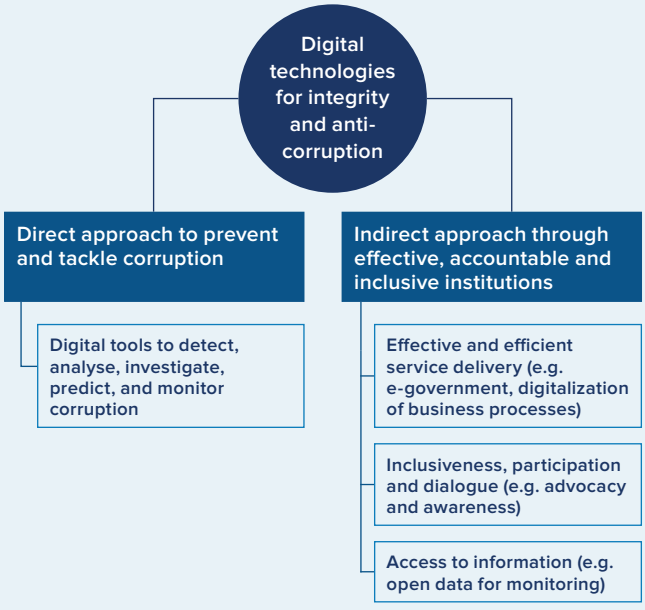
- 16.4: Significantly reduce illicit financial flows and strengthen the recovery and return of stolen assets
- 16.5: Substantially reducing corruption and bribery
- 16.6: Developing effective, accountable and transparent institutions
- 16.7: Ensuring responsive, inclusive, participatory and representative decision-making at all levels
- 16.10: Ensuring public access to information

Most importantly, anti-corruption focuses on the principles of transparency, accountability, integrity, openness, participation and inclusion. These, in turn, have significant implications for trust in governance institutions to meet the needs of people, and for social cohesion and trust within society, necessary conditions for inclusive and sustainable development.

Around the world, technology is increasingly being harnessed for anti-corruption efforts, most evidently in innovations for corruption reporting, monitoring, advocacy and e-government initiatives. The opportunities in the use of digital technologies for integrity and anti-corruption are vast. As presented in **Figure 1.1,** digital technologies could contribute to preventing and tackling corruption, both directly and indirectly.

Over the past two decades, ICTs have proven to be critical in improving the efficiency and effectiveness of public administration and service delivery by making services more accessible, relevant and intelligible for citizens. **Figure 1.2** presents key applications of several ICTs for integrity and anti-corruption.

Figure 1.1: Digital technologies for integrity and anti-corruption



15 UNDP, Recovering from COVID-19: Lessons from past disasters in Asia and the Pacific, 2020. https://www.undp.org/content/undp/en/home/librarypage/crisis-prevention-and-recovery/recovering-from-COVID-19-lessons-from-past-disasters-in-asia-pacific.html

16 United Nations Secretary-General's Task Force on Digital Financing of the Sustainable Development Goals, People's Money: Harnessing Digitalization to Finance a Sustainable Future, 2020, p.51.

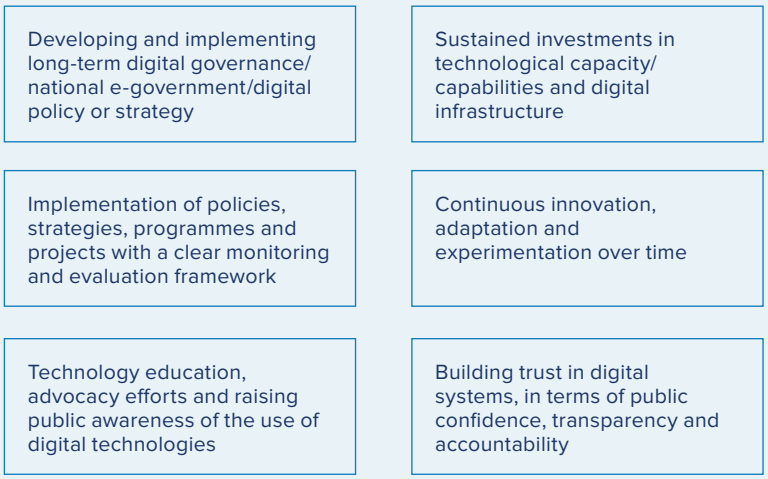
Figure 1.2: Examples: ICTs for integrity and anti-corruption

	Key applications for anti-corruption
E-government	• Promote efficiency in delivery of public services through digitization and digitalization • Promote transparent and accessible services intelligible to citizens • Enhance social accountability and citizen oversight through opportunities for monitoring • Participatory budgeting as a tool to engage in the decision-making process • Reduce or eliminate human discretion through automation of services • Remove intermediaries that create opportunities for bribery • Solicit feedback and reports from citizens
Corruption reporting mechanisms	• Provide a channel/platform for reporting suspicions of corruption, including anonymously • Support the investigation of corrupt acts • Facilitate complaint handling and grievance mechanisms
Crowdsourcing platforms	• Identify trends of the frequency and nature of corruption • Deter corrupt acts by exposing them • Increase the visibility of corruption
Open data	• Promote transparency of government activities (e.g. budgets, expenditures) • Encourage citizen participation for social accountability • Create disincentives for engaging in corrupt acts

Adapted from Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ), Embracing Digitalization: How to use ICT to strengthen Anti-Corruption, March 2018.

Reflecting on the wide array of projects and programmes which have used ICTs to promote integrity and anti-corruption at different levels of governance and through different stakeholders (e.g. government, civil society, media and private sector), the effectiveness of technology to achieve development goals depends on the following:

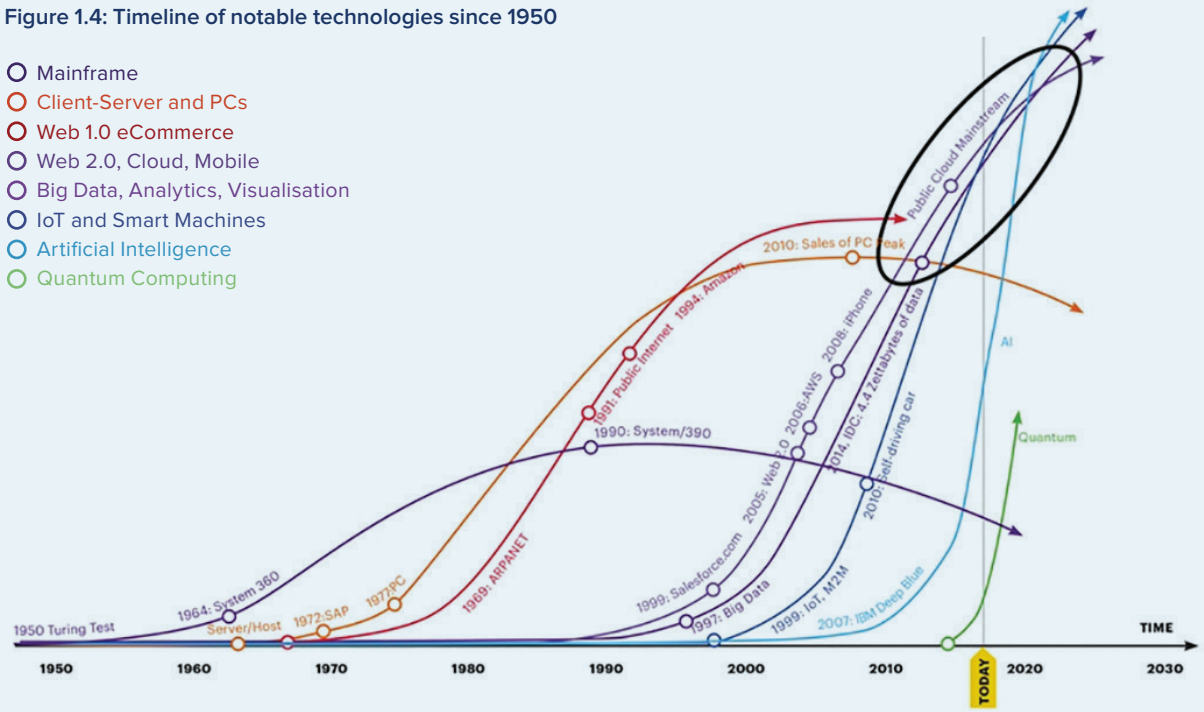
Figure 1.3: Lessons learned from ICTs for development



These critical elements hold important lessons for new and emerging technologies, whose development and practical applications are still largely unrealized and are not widely used in the field of anti-corruption, although they have provided many new opportunities in tackling corruption. These technologies are characterized by productive techniques that offer significant improvements over the established (older) technology for a given process in a specific context. For example, these improvements could be in the form of increased effectiveness or cost savings. What is termed as a 'new' technology can be continuously redefined, given that successive changes and innovations in technology are being undertaken with technological advancements.

Moreover, the rapid development of these new technologies is impacting each other, causing 'combinatorial effects and creating huge opportunities for innovation'[17]. Presenting a timeline of notable technologies since 1950, **Figure 1.4** clearly shows that the more recent technologies are developing and transforming the world at an unprecedented rate, compared to older technologies, which took decades to mature.

Figure 1.4: Timeline of notable technologies since 1950



Source: Accenture Research[18]

Emerging solutions and digital technologies, which have enormous potential for ensuring transparency or enhancing integrity, include AI, blockchain technology and big data analytics. Yet the development of new technologies and digital solutions further adds a new dimension of vulnerability, and calls for conversations surrounding digital governance.

Key considerations in the development of new technologies include:

- **Corruption risks and the misuse or abuse of technology:** Some technologies can be misused to facilitate corruption, such as the use of cryptocurrencies for illicit financial flows, money laundering, embezzlement, or fraudulent activity.

- **Regulation:** Most of the discussions surrounding technology tend to be led by technology providers – technologists and innovators, rather than regulators or digital governance policymakers, who have different incentives and objectives.

- **Ethics and human rights:** Governments and stakeholders may also not be well-equipped to venture into the many ethical or regulatory issues, and mitigate the risks that arise from the use of technology, including sufficient safeguards for human rights and personal data privacy.

- **Innovation:** Continuous innovation, adaptation and experimentation are necessary for the advancement of technology. There needs to be a balance with the level of regulations, which should encourage but not stifle innovation.

- **Digital divide:** Given the widening digital divide and lack of digital infrastructure and technological capabilities in many countries, the applicability and transferability of digital tools are limited, and threaten to leave many developing countries even further behind. Moreover, within countries, the digital divide between the urban and rural population, rich and poor, and men and women, among other groups, needs to be addressed.

17 B. Fanning, "The Future of Work is coming. FS leaders admit they are not ready", Accenture, 2 April 2019. https://talentorganizationblog.accenture.com/financialservices/the-future-of-work-is-coming-fs-leaders-admit-they-are-not-ready
18 Diagram source: U-Hopper https://blog.u-hopper.com/2020/01/10/mega-trends-digital-transformation/

- **Deploying public interest technologies[19] with proper testing:** Before its public roll-out, public interest technological solutions should also undergo proper testing to ensure their effectiveness and to earn public trust. This is particularly relevant when deploying technologies in emergency responses.

The effectiveness and risks surrounding the use of new technologies or digital solutions also depend on several prerequisites for effective digital governance and digital infrastructure. Digital governance, digital infrastructure and digital solutions are, naturally, closely linked. The development of new technologies and digital solutions is dependent on the **capacity and infrastructure** supporting it, implying the need for sustained investments, a long-term digital governance and digital transformation strategy, a strong political will and the government's commitment to technological innovation, capacity and infrastructure. Continuous **innovation, experimentation and adaptation** are processes that drive the advancement of technology.

Regulation of these processes and the technologies themselves is important in promoting accountability, safeguarding human rights and ensuring ethics and integrity in the development and use of new technologies and digital solutions. At the same time, regulation has important implications for the processes needed for technological advancement: encouraging innovation, providing effective guidance for experimentation, innovation, adaptation and preventing the misuse and abuse of new technological solutions.

Therefore, taken together, effective digital governance drives the advancement of technology by developing digital infrastructure and capacity, while promoting accountability and openness, building trust, safeguarding human rights and ensuring ethics and integrity is built into systems, to maximize the benefits and positive impact for all, in the context of the 2030 Agenda.

With the dynamic nature of digital transformations and the many unexplored risks that are present in the use of new technologies, there is therefore an increasing need to understand how to ensure effective digital governance, to harness opportunities to unlock the benefits of new technologies, prevent their misuse for private gain and build just, inclusive and sustainable digital societies.

1.3 HARNESSING TECHNOLOGY AND INNOVATION: UNDP'S APPROACH

UNDP is uniquely positioned to support stakeholders in implementing the 2030 Agenda for Sustainable Development. Innovation is at the heart of UNDP's work, across strategy, context analysis, programme design and operational implementation. For example, the UNDP Innovation Facility has provided seed funds to over 140 experiments across 87 countries[20]. Many of these initiatives have tested the potential of frontier technologies – from drones to artificial intelligence. UNDP is also exploring the potential use of distributed ledger technology to advance the SDGs[21] and to address global development challenges. UNDP's **Digital Strategy**[22] set UNDP on the path to harness new technologies and innovation to deliver more and better results in countries and communities, and to use digital technologies to solve development challenges and improve the quality, relevance and impact of UNDP's work.

To address the emerging challenges posed by COVID-19, UNDP's response, **'Beyond Recovery: Towards 2030'**[23] is helping decision-makers to make choices and manage complexity during uncertainty, in four integrated areas: governance, social protection, green economy and digital disruption. Contributing to UNDP's COVID-19 response, UNDP's global anti-corruption team published two guidance notes[24] to support United Nations Country Teams, UNDP Country Offices and partners in integrating transparency, accountability and anti-corruption in their response and recovery priorities to build forward better, including through the use of technology.

19 Public interest technologies refer to the application of technologies to advance public interests to generate public benefits. See, for example: https://pitlab.stanford.edu/pit
20 UNDP Innovation Facility. https://www.undp.org/content/undp/en/home/2030-agenda-for-sustainable-development/partnerships/sdg-finance--private-sector/innovation.html
21 UNDP, "Beyond bitcoin: Using blockchain to advance the SDGs". https://feature.undp.org/beyond-bitcoin/
22 UNDP Digital Strategy. https://digitalstrategy.undp.org/
23 UNDP, Beyond Recovery: Towards 2030, 2020. https://www.undp.org/content/undp/en/home/librarypage/hiv-aids/beyond-recovery--towards-2030.html
24 UNDP, Transparency, Accountability and Anti-Corruption Service Offer for COVID-19 Response and Recovery, 2020. https://www.undp.org/content/undp/en/home/librarypage/democratic-governance/anti-corruption/transparency--accountability-and-anti-corruption-service-offer-f.html and UNDP, Integrating Transparency, Accountability and Anti-Corruption in Socio-Economic Impact Analyses. Needs Assessment and Response to the COVID-19 Pandemic, 2020. https://www.undp.org/content/undp/en/home/librarypage/democratic-governance/anti-corruption/integrating-transparency--accountability-and-anti-corruption-in-.html

UNDP recognizes the important role of the governance of digital technologies, not only in response to the pandemic but also in accelerating progress on the SDGs, and UNDP has been supporting efforts in its programmes across countries. It recognizes that effective digital governance is needed not only to harness the power of digital technologies to achieve specific SDG targets, but also to leverage digital transformation itself as a pathway to sustainable development.

UNDP/Sumaya Agha

As part of #NextGenUNDP to accelerate progress towards the SDGs, UNDP's Next Generation of Anti-Corruption Programming focuses on four priority areas: **SDG 16 implementation, integration and monitoring; technology and innovation; business integrity;** and **social accountability.** UNDP's global and regional anti-corruption teams are continuing to leverage innovation and technology in their support to countries across the world. New technologies have the potential to enable more effective and participatory forms of accountability and transparency, but they are largely unexplored, as compared to the more 'traditional' forms of technology such as Information and Communications Technology (ICT) and digitization. Efforts must thus be continued to unlock the opportunities that new technologies present in the collective fight against corruption.

1.4 OBJECTIVES OF THE STUDY

In this context, the main objectives of this study are:

1. To enhance the understanding of stakeholders in the opportunities of new technologies to prevent and tackle corruption, while recognizing the risks and challenges that exist.
2. To provide policy recommendations that promote effective digital governance and address the risks in the use of new technologies for integrity, trust and anti-corruption.
3. To support and promote partnerships and dialogue among stakeholders, including governments, technologists and innovators, regulators, development practitioners, anti-corruption actors, the private sector and civil society.
4. To connect the technology community with the governance and anti-corruption community by promoting a sound regulatory environment to prevent corruption risks in the use of new technologies and to promote integrity, trust and anti-corruption.

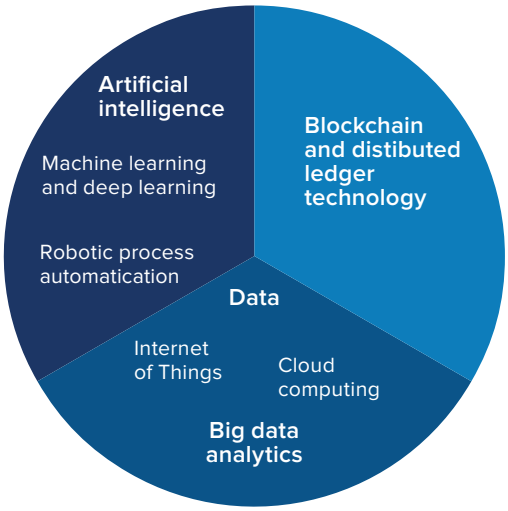
The insights and recommendations in this study will inform UNDP's work on using innovation and technology for anti-corruption policy and programming, specifically:

- **To explore** innovative responses to anti-corruption efforts that can be adopted in and adapted to different contexts.
- **To understand** how innovative approaches to anti-corruption can effectively contribute to achieving the SDGs.
- **To feed into** the design of UNDP's research, policy and advocacy agenda, and to support programming guidance at the regional and country levels.

1.5 OUTLINE OF THE STUDY

This study explores in-depth the following new technologies to promote integrity, trust and anti-corruption: AI, machine learning and deep learning tools (Section 2.1), blockchain and distributed ledger technology (Section 2.2) and big data analytics (Section 2.3).

It will also include brief analyses of the opportunities, risks and limitations of robotic process automation, the Internet of Things and cloud computing.



Each section:

- ✓ Provides an **overview** of the technology in the context of integrity, anti-corruption and sustainable development
- ✓ Highlights the **opportunities** the technology brings to prevent and tackle corruption
- ✓ Identifies the **corruption risks** and **limitations** in the use of the technology to promote integrity and anti-corruption
- ✓ Explores the **current regulatory mechanisms** surrounding the use of the technology, building on the practices around the world
- ✓ Outlines **the way forward** by highlighting key points to note

The issues addressed include, but are not limited to:

- Digital governance, the institutional architecture and effective set of rules for new technologies to complement traditional policy, regulation and processes
- Implications and ethical issues surrounding the use of technology
- Data and privacy issues, including data collection, storage, sharing, protection and security
- Applicability, relevance and transferability of technology across contexts
- The principle of leaving no one behind to address the digital divide
- Collaborative platforms to advance the understanding of new technologies

1.6 LIMITATIONS

The limitations of this study are as follows:

- This study is limited to exploring the specified digital technologies and providing perspectives from an integrity and anti-corruption point of view.
- The technologies mentioned in this study could be defined by different names/terminology. For example, 'new technologies', 'emerging technologies' and 'frontier technologies' refer to the same category, but for consistency the term 'new technologies' is used throughout the study.
- A few types of new technologies have been grouped into three categories on the basis of their characteristics. The objective of this study is not to detail their similarities or differences, but to explore the policy implications in regard to the opportunities and risks represented by each category.
- This study looks at the opportunities and risks of the new technologies from the policy perspectives of anti-corruption efforts. It does not attempt to discuss the technical aspects of the technologies themselves, which is beyond the scope of this study.

2.

NEW TECHNOLOGIES FOR INTEGRITY, TRUST AND ANTI-CORRUPTION

The Fourth Industrial Revolution, driven by new technologies, is continuously transforming the ways in which we live, work and connect with each other. It builds on the Third Industrial Revolution's vast use of electronics and information technology to automate production, but the Fourth Industrial Revolution is evolving at an exponential pace, disrupting every industry, and transforming systems of production, management and governance. As summarised by the World Economic Forum,

> **"The possibilities of billions of people connected by mobile devices, with unprecedented processing power, storage capacity and access to knowledge, are unlimited. And these possibilities will be multiplied by emerging technology breakthroughs in fields such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage and quantum computing."[25]**

These new technologies present many opportunities for the achievement of the SDGs – improving health outcomes, providing economic opportunities, addressing climate change and allowing for rapid flows of ideas, knowledge and data for innovative solutions. In the area of anti-corruption, as this study seeks to focus on, new technologies could enhance integrity, for example, through information transparency and predictive analytics.

Artificial intelligence and machine learning are key drivers of the Fourth Industrial Revolution, with applications across all aspects of daily life, potentially bringing societal benefits for individuals, households, businesses and the public sector. In the past decade, a rise in AI has been observed globally. For example, the McKinsey Global AI Survey 2019[26] finds a nearly 25 percent year-over-year increase in the use of AI in standard business processes, with its adoption increasing in nearly all industries – 58 per cent of respondents report that their organizations have embedded AI capabilities in at least one function or business unit, and 30 percent report that such capabilities have been embedded in multiple functions or business units **(Figure 2.1).**

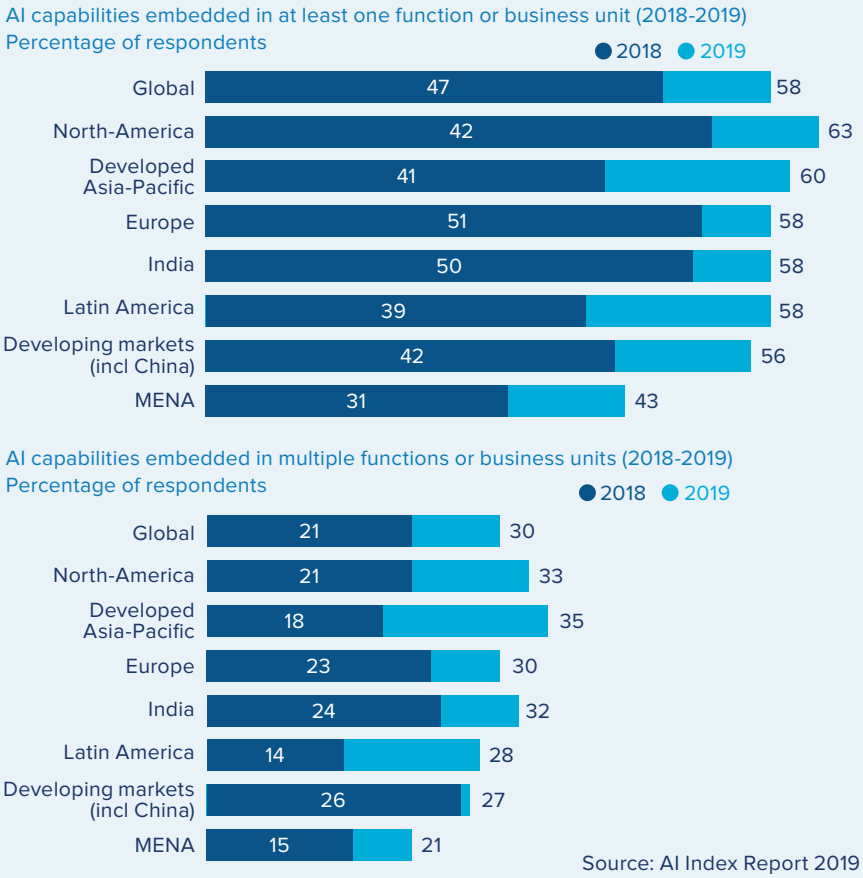
Blockchain technology has gained traction over the past decade, with a growing demand now to develop and utilise the technology to solve business issues and to deliver value[27].

25 K. Schwab, "The Fourth Industrial Revolution: what it means, how to respond", World Economic Forum, 14 January 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/
26 McKinsey Global AI Survey 2019. https://www.mckinsey.com/featured-insights/artificial-intelligence/global-ai-survey-ai-proves-its-worth-but-few-scale-impact
27 Deloitte, "C-Suite Briefing. 5 Blockchain Trends for 2020", March 2020. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Consulting/Blockchain-Trends-2020-report.pdf

It is forecasted to deliver $3.1 trillion in value by 2030 (Figure 2.2)[28]. For example, GIZ has presented promising use cases of blockchain for the 2030 Agenda[29], across a spectrum of economic, social and environmental aspects, including land registries[30], climate accountability and facilitating trade. The application of blockchain in supply chains and across sectors has the potential for transforming systems, and it is particularly relevant for preventing and combatting corruption due to its potential for providing transparency, a higher level of security and integrity of the records and information it manages.

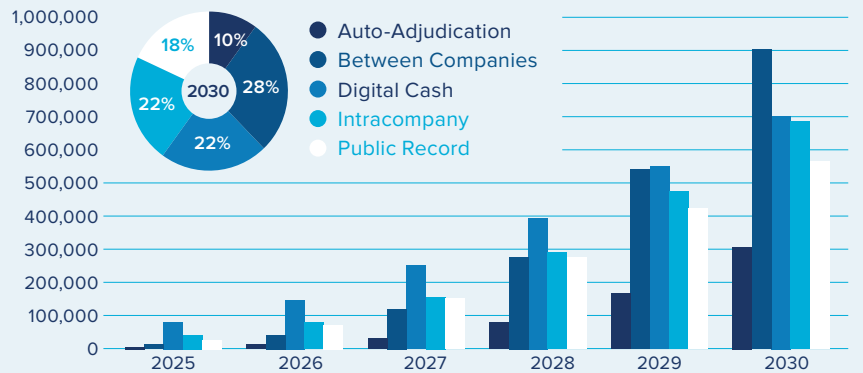
Data and analytics form the core of the Fourth Industrial Revolution, with an unprecedented amount of big data continuously being generated globally, including on Internet of Things devices that capture data and help improve the places we live in **(Figure 2.3).**

Figure 2.1: Increase in AI adoption in business functions



Source: AI Index Report 2019

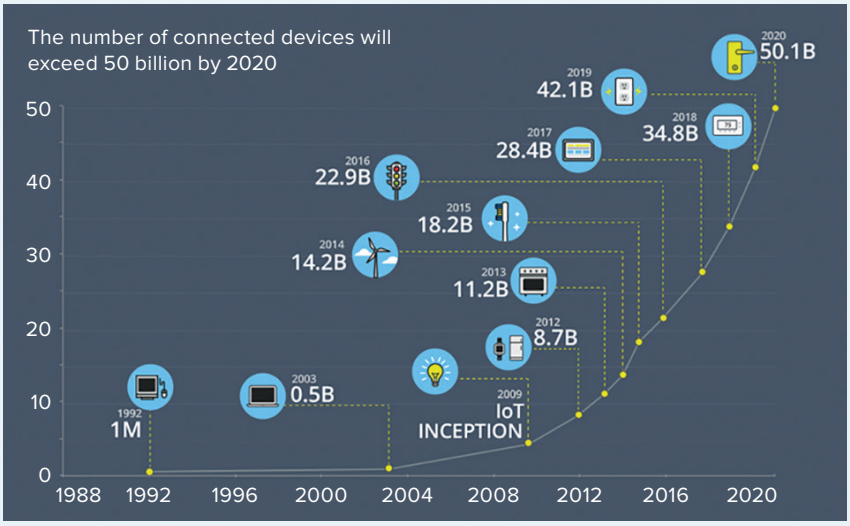
Figure 2.2: Business value-added of blockchain – $176 billion by 2025, $3.1 trillion by 2030



Source: ConsenSys

28 ConsenSys, "Gartner: Blockchain Will Deliver $3.1 Trillion Dollars in Value by 2030", 6 June 2019. https://media.consensys.net/gartner-blockchain-will-deliver-3-1-trillion-dollars-in-value-by-2030-d32b79c4c560
29 Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, "Blockchain for Sustainable Development: Promising use cases for the 2030 Agenda", 2019. https://www.giz.de/en/downloads/giz2019-EN-Blockchain-Promising-Use-Cases.pdf
30 GIZ, "Concept Note. Land registries on a distributed ledger", 2019. https://www.giz.de/en/downloads/giz2019-en-distributed-land-registry.pdf

Figure 2.3: Growth in the Internet of Things

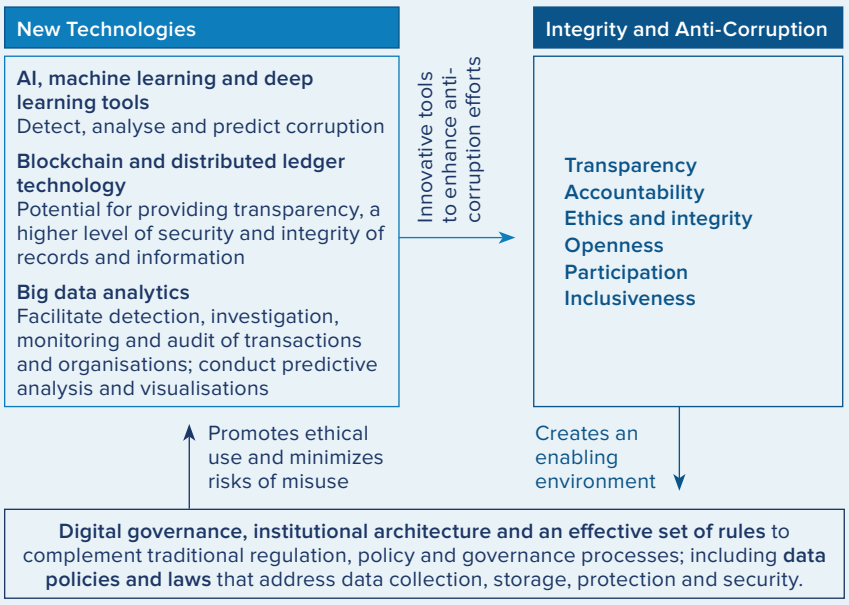


Source: World Economic Forum[31]

The increasingly pervasive use of big data and new technologies has created many opportunities for transparency, accountability and integrity. Yet these principles must be instilled in the technologies themselves to prevent risks of abuse and misuse, such as concerns over privacy and personal data protection, and they must ensure responsible digital governance to maximize their impact on society.

New technologies have a mutually reinforcing relationship with integrity and anti-corruption **(Figure 2.4)**. On the one hand, different innovative tools can help facilitate the detection, analysis, investigation, prediction and monitoring of corruption. On the other hand, the principles of transparency, accountability, integrity, openness, participation and inclusiveness contribute to creating a conducive and enabling environment for effective digital governance, digital infrastructure and digital transformation – factors which further harness the benefits of new technologies while minimizing risks of abuse and misuse of data or misuse of the technologies themselves.

Figure 2.4: The linkages between new technologies and integrity and anti-corruption



31 D. Wellers, "'Is this the future of the Internet of Things?", World Economic Forum, 27 November 2015. https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things/?utm_content=buffer10b03&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

In addition to digital, legal, regulatory and other infrastructures, trust in new technologies also plays a vital role in the transformative nature of AI, blockchain and other new technologies. If one considers, for example, the evolution of online trading and online shopping, many consumers may have been sceptical or suspicious about e-commerce when it first launched, including having concerns about opaque processes, the quality of products and the potential for fraud, as compared to conventional and non-virtual marketplaces. However, over time, advancements in cyber security for e-commerce, combined with efforts to build trust through higher quality and experience, have increased consumers' confidence. This experience will be equally valuable in the case of new technologies.

This chapter will explore these three new technologies in depth (AI, blockchain technology and big data analytics) in the context of integrity, trust and anti-corruption. It will also include brief analyses of the opportunities, risks and limitations of robotic process automation, the Internet of Things and cloud computing.

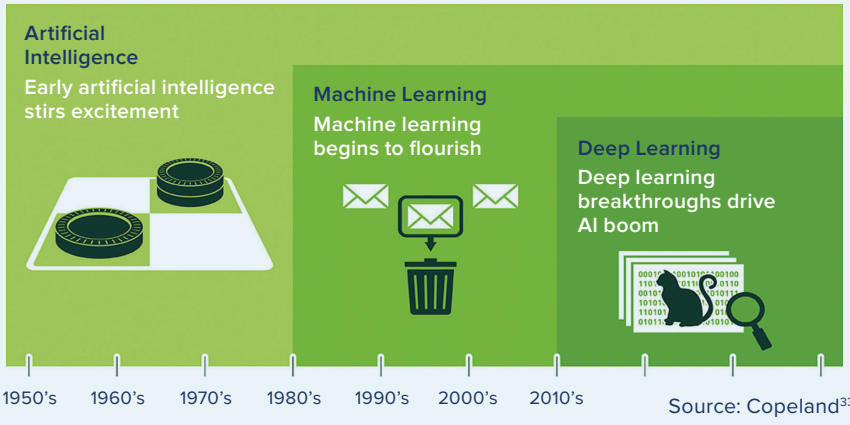
2.1 ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DEEP LEARNING

AI broadly refers to software that is capable of learning and making decisions almost in the same way as human beings. AI enables machines, devices, programmes, systems and services to function in a manner that is sensible in light of the given task and situation. Machine learning is a subset of AI, in which a computer can act without explicit instruction or human intervention, analysing large quantities of data to identify patterns, and performing tasks and making predictions when confronted with new information. In other words, machine learning automatically learns and improves from experience without each step being explicitly programmed.

Over the past decade, AI techniques have emerged as technological forces affecting all disciplines, economies and industries. While there are relatively few examples of how AI has been deployed in anti-corruption work[32], they are increasingly being used in this field. For example, AI systems are being used in the financial and tax sectors to detect money laundering, tax evasion and fraudulent patterns. More importantly, there is huge potential for designing novel AI-assisted processes to address corruption-prone procedures and hence prevent corruption in both the public and private sectors.

More advanced **deep learning** is a class of machine learning algorithms which use multiple layers of artificial neural networks to simulate human decision-making. Deep learning breakthroughs have driven the AI boom **(Figure 2.5). Neural networks,** which are a framework for many different machine learning algorithms to work together and process complex data inputs, have been a novel technique of AI used to collect and analyse cases of corruption. For example, Lopez-Iturriaga et al (2017) created a model based on neural networks that calculates the probability of corruption in Spanish provinces and the conditions that favour it. By predicting where corruption may happen, models based on neural networks will allow the authorities to take preventive measures to mitigate corruption risks.
AI technologies present many opportunities to fight corruption and promote integrity, although there is a need to take into account their limitations and risks. In addition to im-

Figure 2.5: AI, machine learning and deep learning: Early flush of optimism in the 1950s to larger disruptions in the recent decade



Source: Copeland[33]

32 P. Aarvik, Artificial Intelligence – a promising anti-corruption tool in development settings? Anti-Corruption Resource Centre, CMI Chr. Michelsen Institute, Norway, U4 Report 2019:1. https://www.u4.no/publications/artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings.pdf

33 M. Copeland, "What's the Difference Between Artificial Intelligence, Machine Learning and Deep Learning?" NVIDIA, 29 July 2016. https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

proving the efficiency and effectiveness of service delivery by designing faster and better processes through automation and AI-assistance, the main appeal of AI, machine learning and deep learning is in their ability to detect, analyse, predict, and thereby deter and prevent corruption, which would have otherwise been difficult or slow to uncover without AI-assistance. As highlighted by Oxford Insights, AI is the next frontier in anti-corruption[34]. However, there is also a need to recognise its limitations, risks and potentially negative effects.

AI TECHNOLOGIES: OPPORTUNITIES FOR INTEGRITY, TRUST AND ANTI-CORRUPTION

AI has the ability to analyse large amounts of data to reveal complex relationships or patterns that are difficult for humans alone to identify. By accelerating large amounts of data analysis, AI allows humans to focus on scrutinizing potential corrupt activities and to follow up on unusual patterns and 'red flags'. This not only increases accuracy and reliability, but also efficiency in terms of time and cost. From the perspective of promoting integrity and anti-corruption, AI has the potential to be deployed as an early warning system to prevent and detect anomalies, red flags and patterns with a satisfactory level of precision.

In the area of regulatory compliance, AI and machine learning tools have increasingly been used as a regulation technology (RegTech) by both the regulators and the regulated **(Figure 2.6).** It can assist entities in understanding compliance requirements, notifying stakeholders of regulatory changes and also assisting regulators to monitor entities' compliance with regulations. For example, Shield FC, a Tel Aviv start-up, specializes in reducing compliance risks through intelligent automated reporting. The company's compliance platform utilizes AI, natural language processing and visualization capabilities to automate and orchestrate the complete communications compliance lifecycle, mitigate risk and make surveillance efficient[35].

Figure 2.6: Examples of Global RegTech Initiatives by Jurisdiction

Source: UNSGSA[36]

34 A. Petheram and I. Asare, "From open data to artificial intelligence: the next frontier in anti-corruption", Oxford Insights, 27 July 2018. See https://www.oxfordinsights.com/insights/aiforanticorrduption
35 Shield FC. "Moving Compliance Forward". https://www.shieldfc.com/
36 United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA) FinTech Working Group and Cambridge Centre for Alternative Finance, Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech, 2019. https://responsiblefinanceforum.org/publications/early-lessons-regulatory-innovations-enable-inclusive-fintech-innovation-offces-regulatory-sandboxes-regtec

This is particularly useful given the rapid pace of new regulations and modifications of existing regulations during the Fourth Industrial Revolution, which complicates the enforcement process for regulators and creates difficulties for businesses to track changes and comply with regulations[37]. AI can increase the efficiency and accuracy of compliance and due diligence by allowing the regulated entities to improve their workflow management, and by helping regulators to verify the compliance of these entities and identify any discrepancies or deliberate attempts of fraud and non-compliance, which would allow them to take legal action.

AI and machine learning have also been used to detect money laundering activities or fraud in public procurement. In 2018, Transparency International Ukraine launched Dozorro, an online monitoring platform and a set of intelligence tools which help to detect and prevent misuse of public funds in public procurement. This has dramatically increased the efficiency of identifying violations in public tenders.

The system assesses the likelihood of corruption risks in tenders, and then sends them to the Dozorro community. If the suspicions were correct, the software remembers its choice; if they were wrong, the system forgets it. This increases the accuracy of the AI algorithm's assessment of corruption risks in tenders.[38] In the case of Dozorro, oversight and prosecuting bodies are then able to check for violations in public procurement, detect uncompetitive behaviour in a timely manner and investigate them at an early stage[39]. From 2016-2018, 22 criminal charges and 79 sanctions were issued as a result of the platform's ability to detect violations[40].

UNDP/Cyril Ndegeya

With its ability to pick up unusual patterns or 'red flags' and to predict potential corrupt activities that may happen, AI allows authorities to take pre-emptive and preventive measures. In particular, where the resources available to combat corruption are limited, authorities can use an early corruption warning system to deter and prevent corruption before it happens.

In the Czech Republic, Mazrekaj et al (2019) analysed the publicly available financial and industry data of all contracting firms from the country to predict which firms were politically connected. Using machine-learning techniques, they found that over 75 percent of firms with political connections could be accurately identified. Further, this approach could be used by public institutions to identify firms whose political connections could represent major conflicts of interest. Moreover, with the ability of machine learning algorithms to rely on patterns and inference to learn and adapt, algorithms can improve reliability, accuracy and efficiency over time, with the ever-increasing amounts of data that are processed.

The alert system modelled by Lopez-Iturriaga et al (2017) using neural networks found that the number of years of government by the same political party is positively correlated to the probability of corruption. The data indicates that some of the variables that induce public corruption include real estate taxes, inflated real estate prices, the opening of bank branches and the creation of new companies. When all four factors exist in a region, more rigorous control of public accounts may be necessary. In this case, the early corruption warning system categorizes each province according to its corruption profile, which helps to better implement preventive and corrective policies within each province. In addition, the model predicts corruption cases long before they are discovered, which enhances anticipatory measures. Lopez-Iturriaga et al (2017) have stated that this is especially relevant and useful in countries suffering from the most severe corruption problems.

37 N. Joshi, "Why regulatory compliance can be complicated and how AI can simplify it", Forbes, 22 July 2019. https://www.forbes.com/sites/cognitiveworld/2019/07/22/why-regulatory-compliance-can-be-complicated-and-how-ai-can-simplify-it/#400cc55e377e

38 Transparency International Ukraine, "DoZorro artificial intelligence to find violations in ProZorro: How it works", 2018. https://ti-ukraine.org/en/news/dozorro-artificial-intelligence-to-find-violations-in-prozorro-how-it-works/

39 Organisation for Economic Co-operation and Development (OECD) Observatory of Public Sector Innovation, "OECD Open Government, DoZorro Case Study," 2018. https://oecd-opsi.org/innovations/dozorro/

40 K. Granickas, "Learning insights: The latest impacts emerging from Ukraine's Prozorro reforms", Open Contracting Partnership, 12 January 2018. https://www.open-contracting.org/2018/01/12/learning-insights-latest-impacts-emerging-ukraines-prozorro-reforms/

USING AI TO COMBAT COVID-19: UNDERSTANDING INTEGRITY RISKS

AI has been an important tool in combatting the COVID-19 pandemic.

- **Predicting the spread of the outbreak:** BlueDot[41], a Canadian company that uses AI to detect disease outbreaks, was among the first in the world to identify the emerging risk of a respiratory illness outbreak in Hubei province. It used AI and machine learning algorithms to predict the spread of an outbreak, and provided these insights to epidemiologists, public health officials, airlines and hospitals to help them anticipate and better manage risks.

- **Virtual assistants:** AI-driven tools such as chatbots are used as virtual assistants to update doctors and healthcare workers with the latest fast-changing information on COVID-19. AI-powered apps and wearable technology that harvest location, usage and the health data of device owners are also useful for patients to receive tailored information or advice from their medical providers virtually, when there is high clinical demand.

- **Tracking and tracing contacts:** AI has been an important tool in tracking and tracing contacts during COVID-19. AI-driven contact-tracing algorithms are being deployed in many countries to instruct individuals to quarantine after being in contact with someone with a positive diagnosis. SQREEM Technologies, a Singapore AI solutions company, developed a software Channel Sqreem, which can track people using their mobile device ID down to a 5 sqm grid, without needing to know any personal information of the device owner. It then uses AI and machine-learning models to automatically determine how many devices carried by other people had risky contact with that person over the previous 14 days[42].

However, numerous considerations related to tracking, surveillance, privacy, civil liberties and data protection must be taken into account.

- The ability of AI in tracking and surveillance, for example, through the use of CCTV cameras, facial recognition systems and AI-powered drones and robots to detect population movement and social gatherings[43], has raised concerns over **the protection of personal data and privacy.** Moreover, there is a need to recognise and address the implicit bias of AI algorithms, including gender bias, racial prejudice and age discrimination in facial recognition systems, for example.

- Where systems are able to link data from a geographic location, CCTVs, facial scans, temperature monitors, medical records and individuals' credit card payments, there is a risk that **privacy** will be **curtailed** during times of emergency.

- Many applications of AI for COVID-19 raise **privacy protection issues** in the collection, use, aggregation, analysis and disclosure to third parties of datasets that may include de-identified or re-identifiable data[44].

In extraordinary times with uncharted circumstances, AI regulation, ethics and data protection regulations therefore remain crucial not only to instil public trust and confidence in systems, but also to ensure appropriate AI governance architectures are embedded in transparency and accountability, to achieve the intended benefits and to avoid harm even under emergency measures.

41 BlueDot, "Anticipate outbreaks. Mitigate risk. Build resilience". https://bluedot.global/
42 T. Tan, "Tapping AI to battle Covid-19", The Straits Times, Singapore, 29 April 2020. https://www.straitstimes.com/tech/tapping-ai-to-battle-covid-19
43 S. Greenman, "Governments must build trust in AI to fight COVID-19 – Here's how they can do it", World Economic Forum, 21 April 2020. https://www.weforum.org/agenda/2020/04/governments-must-build-trust-in-ai-to-fight-covid-19-here-s-how-they-can-do-it
44 B. Sookman, "COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic", 14 April 2020. https://www.mccarthy.ca/en/insights/blogs/techlex/covid-19-and-privacy-artificial-intelligence-and-contact-tracing-combatting-pandemic#page=1

PROMOTING ACCESS TO INFORMATION THROUGH "C BOT" IN RUSTAVI MUNICIPALITY, GEORGIA

In Georgia, with support from UNDP, the Rustavi municipality launched "C Bot", an AI-powered "civil servant" that provides round-the-clock online information on municipal services to local citizens. The Rustavi Chatbot for Municipal Services was developed by the municipality and Rustavi Innovations Hub to respond to citizens' needs during the COVID-19 pandemic, including sharing updates; connecting volunteers with vulnerable groups; and listing available delivery, medical and other services. General information on municipal services, now consolidated into a single database, is also provided. are embedded in transparency and accountability, to achieve the intended benefits and to avoid harm even under emergency measures.

AI-ENABLED ROBOTIC PROCESS AUTOMATION (RPA)

What is it?
RPA enables the automation of repetitive, rules-based processes by emulating human execution on high-volume transactions, based on artificial intelligence workers or software "bots", designed to increase operational capacity and improve process efficiencies. AI-enabled RPA can create a fully autonomous process from end to end,or can help improve an RPA process once it has been deployed. When AI is integrated with RPA, the result is increased productivity and efficiency.

How can it be used to fight corruption and fraud?

- ✓ **Detecting fraud and corruption.** RPA uses an ''if-then'' method for identifying 'red flags' of potential corruption or fraud. For example, 'if several transactions are made within a short amount of time in a different state, then send the account for manual review'[45]. Such rules can be set up to flag potential risks and provide additional analysis for unusual transaction behaviour. RPA can be applied in a range of processes, including to analyse transactions, payments and disbursements.
- ✓ **Reducing human interaction and discretion.** Opportunities for corruption are present when humans interact with data as part of a process, and they can manipulate data for private gain. When RPA is enabled, the frequency of human interaction with data is diminished, reducing opportunities for humans both to tamper with data and to manipulate data or the processes.

What are its limitations in anti-corruption efforts?

- **Using AI-enabled RPA does not eliminate the need for building or rethinking core platforms. AI-enabled** RPA can help automate manual processes, improve productivity, save costs and detect unusual activities. However, its usefulness is also dependent on the design of each component within the tool and on the design of the technology infrastructure. If integrity is not built into the platforms, it could also be manipulated or corrupted for private gain.
- **RPA may be less useful than other emerging technologies as the amount of big data produced increases over time.** The amount of data produced today and the complexity of analysis has grown to unprecedented levels. The manual process of building and maintaining rules, which RPA is built on, is expensive, time intensive and less predictive. In this regard, machine learning and deep learning technologies can be more useful to autonomously learn, predict, act and explain without being explicitly programmed.

45 Rajat Vig, "Perspectives. Automation is the future of fraud risk management", Deloitte India. https://www2.deloitte.com/in/en/pages/finance/articles/automation-is-the-future-of-fraud-risk-management.html

CORRUPTION AND INTEGRITY RISKS IN THE USE OF AI TECHNOLOGIES

While there is huge potential in using AI to promote integrity and to fight corruption, at the same time, AI-assisted procedures can be used to facilitate corrupt activities. As the use of AI applications increase, so does the risk for algorithms being used, intentionally or unintentionally, for fraud and corrupt activities. For example, the emergence of 'deepfake' videos have presented the many dangers that accompany sophisticated artificial intelligence – in this case, manipulated videos using deep learning techniques that fabricate images and sounds that appear to be real.

There are urgent and challenging policy, technology and legal issues that need to be addressed. Without clear governance mechanisms or regulation to guide the use of AI and machine learning tools, AI may be vulnerable to the few who design the processes. For example, democratic elections could be manipulated to distort the political discourse and control electoral outcomes, and facial recognition systems could be abused to violate the rights of citizens. These have a widespread impact on society at large.

> **"Without clear governance mechanisms or regulation to guide the use of AI and machine learning tools, AI may be vulnerable to the few who design the processes."**

The outcomes generated by AI and their usefulness depend on the design of the algorithms and the data used. Datasets are often built through collection methods that have limitations, leading them to hold biases (whether systemic or random), including gender and racial biases[46]. Because all data are inherently biased, algorithms will generate outcomes that are biased to some extent, reflecting the background and bias of the source that has programmed them. Moreover, by learning based on the data fed to them, AI-driven decisions can be "used, intentionally or not, for manipulation, censorship or discrimination"[47] and may reinforce existing inequalities.

Moreover, the unethical collection and use of data may pose huge challenges over privacy concerns, safety, surveillance issues and opaque decision-making processes. Access to data is fundamentally important to AI systems. Yet, the privacy of data may not be protected by those who use them. More fundamentally, even in the more developed countries, there is a lack of data to train AI and other technological solutions. In developing countries, this issue is compounded by the lack of data infrastructure.

The complexity of "black box" algorithms makes it impossible to tell exactly how the calculation resulting in a given output is performed. This inevitably results in a lack of transparency that makes it difficult to explain and interpret the reasons for decisions made as a result of deep learning. AI is limited in explaining the process it has undergone to reach such a conclusion, which can inevitably result in a lack of trust in the system.

For example, China's 'Zero Trust' Anti-Corruption AI System is an experimental anti-corruption AI system that can access more than 150 protected databases in central and local governments for cross-reference in order to monitor, evaluate or intervene in the work and personal life of public servants. The system is able to draw sophisticated, multiple layers of social relationship maps to derive behaviour analyses of government employees, which is can detect suspicious property transfers, infrastructure construction, land acquisitions and house demolitions. The system can immediately detect unusual increases in bank savings, for instance, or if there has been a new car purchase or bidding for a government contract under the name of an official or one of his family or friends. Once its suspicions have been raised it will calculate the chances of the action being corrupt. If the result exceeds a set marker, the authorities are alerted.

Since 2012, Zero Trust has caught 8,721 government employees engaging in misconduct such as embezzlement, abuse of power, misuse of government funds and nepotism. However, while AI may quickly point out a corrupt official, it is limited in its ability to explain the process it has undergone to reach such a conclusion. Some local governments have also decommissioned the machine as, according to reports, they "may not feel quite comfortable with the new technology".[48]

---

46 Privacy International and ARTICLE 19, Privacy and Freedom of Expression in the Age of Artificial Intelligence, April 2018. https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf

47 Aarvik, Artificial Intelligence – a promising anti-corruption tool in development settings?

48 S. Chen, "Is China's corruption-busting AI system 'Zero Trust' being turned off for being too efficient?" South China Morning Post, Hong Kong, 4 February 2019. https://www.scmp.com/news/china/science/article/2184857/chinas-corruption-busting-ai-system-zero-trust-being-turned-being
J. Christian, "China built an AI to detect corruption and officials shut it down", The Byte, 4 February 2019. https://futurism.com/the-byte/china-ai-corruption

Moreover, humans must also work carefully with all AI systems, using results as a reference to check and verify their validity. 'Ground truth', a term used in statistical models, refers to checking the accuracy of machines' results against the real world. This reiterates the point that AI alone cannot overcome corrupt activities and has to be accompanied by human capacity, although it is a useful tool that can drastically improve the efficiency, accuracy and reliability of analysing large amounts of data to detect, analyse and predict corruption.

Given the above-mentioned corruption and integrity risks, several areas of concern need addressing.

First, humans must steer AI systems when designing and developing them. This is crucial to address algorithmic and data bias, to ensure that ethics and integrity are built into AI systems and to mitigate corruption risks in the use of different AI technologies. Currently, many countries lack the regulations and legislation to responsibly govern the behaviour of non-human systems. More fundamentally, there is a need to caution against overconfidence and optimism, and question the validity and accuracy of these tools, while recognizing the limitations of steering systems that humans do not necessarily fundamentally understand.

Second, investments in good quality data are crucial to reap the benefits of AI. Data collection and the lack of standardized and machine-readable data are huge problems in many countries. To benefit from using AI on a broad scale, many countries will need reforms in the areas of data collection, data privacy, open data, infrastructure and governance. Moreover, algorithms need to be trained on more complex and diverse datasets in a search for deeply hidden corruption indicators. In this regard, both developers and anti-corruption bodies must also develop a rigorous understanding of which datasets can most help AI practitioners in detecting corruption.

Third, given the 'black box' problem, efforts must be made to address gaps in transparency, accountability and trust in AI technologies. In this regard, establishing strong governance and controls in the design, development and deployment of AI is critical to its safe and effective use and to build the trust that people have for the technologies themselves, which humans cannot comprehend at the algorithmic level. As such, transparency, ethics and integrity in AI and its underlying algorithms are important to build trust in the systems.

Fourthly, business models based on AI and machine learning tools that facilitate peer-to-peer transactions in service-based industries without a centralized body (known as 'Uberisation') raise concerns regarding protection of rights and ensuring safety and security. For example, in many cities, customers and passengers increasingly turn to business organisations such as Uber, Lyft and Airbnb to directly receive services from providers, through digital technologies powered by AI technologies. As highlighted by U4, "passengers trust a ride with Uber more than they trust ordinary taxi services", given that AI and digitalization has enabled these transactions and procedures to be less prone to cheating or fraud, and there are fewer or no disputes over the fare or best route to take[49]. Yet, 'Uberisation' has also been criticized for its role in facilitating the decline of labour-intensive industries and threatening jobs. In addition, these business models operate in a largely unregulated territory, often sidestepping corporate regulations, labour rights and tax obligations.

REGULATORY MECHANISMS GOVERNING THE USE OF AI

There is an increasingly clear recognition that regulation is necessary to govern the responsible use of AI. The regulatory and policy landscape for AI is an emerging issue globally, but it should be noted that regulation is required not just to mitigate corruption risks in the use of AI, but also to encourage trustworthy and human development-centred AI.

Although regulation of AI is still in its infancy and no global regulatory mechanism or global norms and standards exist as such, a growing number of countries are issuing national strategies and policies governing the use of AI, albeit many are doing so without passing substantive laws. Such strategies and policies address overarching concerns related to anti-corruption that cut across different industries and sectors. These include addressing transparency, accountability, ethics, non-discrimination, integrity, access, inclusion and human rights, among others.

To address algorithmic bias and data protection in legal frameworks, the European Union (EU) has taken huge steps in protecting consumer data with the General Data Protection Regulation Act (GDPR), which requires companies to ensure they have a

49 Aarvik, Artificial Intelligence – a promising anti-corruption tool in development settings?

data consent management process. Transparency is an overarching obligation under the GDPR, requiring organizations to inform individuals about what personal data they collect and why, as well as the rights that they have as data subjects.

ADDRESSING RISKS IN THE USE OF AI IN THE EUROPEAN UNION

In February 2020, the EU released its White Paper on AI[50], which set out policy options on how to promote the uptake of AI and address the risks associated with certain uses of AI, while emphasising fundamental rights such as human dignity and privacy protection. It sets out the key elements of a future regulatory framework for AI in Europe that will create a unique 'ecosystem of trust', building on the work of the High-Level Expert Group on Artificial Intelligence (AI HLEG)[51] and, in particular, the Ethics Guidelines for Trustworthy AI[52], which were tested by companies in late 2019. The AI HLEG is also the steering group for the European AI Alliance, a multi-stakeholder forum for engaging on all aspects on AI development.

As highlighted in the White Paper, AI systems must be developed and used in a way that respects EU law and fundamental rights, while breaches of fundamental rights must be addressed by national authorities. The European Strategy for Data[53], which was also released, reiterates the importance of a strong legal framework – in terms of data protection, fundamental rights, safety and cyber security.

In 2019, lawmakers in the United States of America proposed a bill, the Algorithmic Accountability Act, to govern the use of algorithms by tech companies[54]. Its main purpose is to address the AI biases in the algorithms powering the tools created by these companies. The Act empowers the Federal Trade Commission (FTC) to regulate AI technologies by requiring covered entities to conduct an impact assessment for any existing or new high-risk automated decision systems or information systems. This automated decision system impact assessment consists of a study evaluating the development process of an automated decision, including the design and data used.

Under the Algorithmic Accountability Act, the impact assessment of a high-risk automated decision system will have to address whether the algorithms pose risks to privacy, and whether they may result in inaccurate, unfair or discriminatory decisions. In addition, the Act refers to the need to conduct a Data Protection Impact Assessment, that is an evaluation of the protection offered by information systems to the privacy and security of personal data. The Act is the first federal legislative effort to regulate AI systems across industries in the United States, and it reflects a growing and legitimate concern regarding the lawful and ethical implementation of AI.

Many governments have also embarked on establishing national strategies to govern the ethical and responsible use of AI. According to PricewaterhouseCoopers' (PwC) National AI Strategy Radar[55], which uses natural language processing to read through AI strategy documents, AI Governance has been mentioned in over 42 percent of 48 official AI strategy documents that were analysed[56]. The World Economic Forum (2019) sets out a framework for developing a national AI strategy in its White Paper[57], emphasizing that governments have a crucial role to play in guiding technological change proactively, a much different approach to traditional policymaking processes.

As part of its broader Artificial Intelligence Programme, Finland was the first EU country to put in place a national AI strategy[58], in October 2017. In particular, the Finnish Presidency of the Council of the EU has invested in people's future skills, through education and training in AI using Massive Open Online Courses (MOOCs). Finland's 'Elements of AI' online course[59] is freely available in all official EU languages, with the aim of educating 1 per cent of European citizens about artificial intelligence by 2021.

54 U.S. Congress, H.R.2231, "The Algorithmic Accountability Act of 2019", 116th Congress, First Session, 10 April 2019 . https://www.congress.gov/bill/116th-congress/house-bill/2231/text
55 PwC, "Gaining National Competitive Advantage through Artificial Intelligence (AI)", 2019. https://www.pwc.lu/en/advisory/digital-tech-impact/technology/gaining-national-competitive-advantage-through-ai.html
56 Stanford University, Human-Centred Artificial Intelligence, Artificial Intelligence Index Report 2019. https://hai.stanford.edu/research/ai-index-2019
57 World Economic Forum, A Framework for Developing a National Artificial Intelligence Strategy, Centre for Fourth Industrial Revolution, August 2019. http://www3.weforum.org/docs/WEF_National_AI_Strategy.pdf
58 EC, Finland AI Strategy Report, 2020. https://ec.europa.eu/knowledge4policy/ai-watch/finland-ai-strategy-report_en#aistrategy
59 Finland "Elements of AI" (Massive Open Online Course) https://www.elementsofai.com/eu2019fi

Singapore's National AI Strategy[60], in line with the country's Smart Nation journey, spells out its plans to broaden the use of AI technology in transforming the economy, rethinking business models and creating new areas of growth. It also released its Model AI Governance Framework, which provides detailed and readily implementable guidance to private sector organizations for addressing key ethical and governance issues when deploying AI solutions[61]. In addition, the Government of Singapore is working with the World Economic Forum's Centre for the Fourth Industrial Revolution to help drive the ethical and responsible deployment of AI technologies in order to prevent its misuse.

MODEL AI GOVERNANCE FRAMEWORK IN SINGAPORE

Singapore's Model AI Governance Framework[62] provides detailed guidance to private sector organizations to address key ethical and governance issues when deploying AI solutions. By explaining how AI systems work, building good data accountability practices and creating open and transparent communication, the Model Framework aims to promote public understanding and trust in technologies.

Two guiding principles underlie this framework:

- ✓ Decisions made by AI should be explainable, transparent and fair.
- ✓ AI systems should be human-centric.

In addition to the Model Framework, the Government of Singapore has released an Implementation and Self-Assessment Guide for Organisations (ISAGO)[63], in collaboration with the World Economic Forum's Centre for the Fourth Industrial Revolution, to help organizations assess the alignment of their AI governance practices with the Model Framework. It also provides an extensive list of useful industry examples and practices to help organizations implement the Model Framework.

A Compendium of Use Cases[64] was also published to provide practical illustrations of the Model AI Governance Framework, including how local and international organizations across different sectors and sizes implemented or aligned their AI governance practices with all sections of the Model Framework.

Germany launched its Artificial Intelligence Strategy in November 2018, jointly developed by the Federal Ministry of Education and Research, the Federal Ministry for Economic Affairs and Energy and the Federal Ministry of Labour and Social Affairs. In contributing to the implementation of Germany's High-Tech Strategy 2025, the AI Strategy focuses on making Germany and Europe a leading centre for AI, developing and using AI to serve the good of society and integrating AI in society in ethical, legal, cultural and institutional terms. For example, the Federal Government will work with data protection authorities and business associations to develop joint guidelines for developing and using AI systems, with the commitment of guiding the entire development process and the use of AI based on the principles of ethics and the rule of law.

The United States launched its American AI Initiative in 2019, the national strategy on AI to promote and protect national AI technology and innovation. As part of the American AI Initiative, Federal agencies are directed to establish guidance for AI development and use across different types of technology and industrial sectors. This guidance will help Federal regulatory agencies develop approaches for the safe and trustworthy creating and adoption of AI technologies, which will help foster public trust in AI systems[65]. In line with the national strategy, the AI R&D Strategic Plan[66], focuses on understanding and addressing the ethical, legal and societal implications for AI, and ensuring the safety and security of AI, among other issues.

60 Government of Singapore "National Artificial Intelligence Strategy". https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4
61 Government of Singapore, Personal Data Protection Commission, "Model AI Governance Framework", 2020. https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governartnce-framework
62 Government of Singapore, Model Artificial Intelligence Governance Framework: Second Edition, 2020. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf
63 World Economic Forum, Companion to the Model AI Governance Framework – Implementation and Self-Assessment Guide for Organizations (Prepared in collaboration with the Info-communications Media Development Authority of Singapore), January 2020. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf
64 Government of Singapore, Compendium of Use Cases: Practical Illustrations of the Model AI Governance Framework, 2020. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGAIGovUseCases.pdf
65 White House Office of Science and Technology Policy, American AI Initiative 2019, "Accelerating America's Leadership in Artificial Intelligence", 11 Febuary 2019. https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/
66 U.S. National Science and Technology Council, "National Artificial Intelligence Research and Development Strategic Plan: 2019 Update", June 2019. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

Increasingly, international organizations are also working on AI policies and principles. For example, the International Telecommunication Union (ITU) leads the 'AI for Good' Global Summit, the leading United Nations platform for global and inclusive dialogue on AI. It brings together United Nations agencies and partners to discuss their roles in AI to improve their responses to global challenges[67].

UNITED NATIONS ACTIVITIES ON AI

The UN system has taken steps in identifying practical applications of AI to accelerate progress towards meeting the Sustainable Development Goals. UN agencies have increasingly experimented with AI to improve their responses to global challenges.

The 2019 Compendium 'United Nations Activities on Artificial Intelligence'[68] presents a compilation of examples of how different UN agencies are using AI to fight hunger, ensure food security, mitigate climate change, advance health for all and facilitate the transition to smart sustainable cities.

The United Nations' High Level Committee on Programmes (HLCP) on the Ethics of Artificial Intelligence was formed to develop a better internal understanding of the impact of AI-related technologies on the work of the entire UN system. In line with the decision of the United Nations Educational, Scientific and Cultural Organization's (UNESCO) General Conference at its 40th session, an Ad Hoc Expert Group (AHEG), comprising 24 international experts, was tasked with producing a draft[69] of a global standard-setting instrument, in the form a 'Recommendation on the Ethics of Artificial Intelligence'.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) PRINCIPLES ON ARTIFICIAL INTELLIGENCE

The OECD provides five recommendations to governments on the use of AI[70]:

- Facilitate public and private investment in research and development to spur innovation in trustworthy AI
- Foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge
- Ensure a policy environment that will open the way to deployment of trustworthy AI system
- Empower people with the skills for AI and support workers for a fair transition.
- Co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI

The OECD and partner countries adopted the OECD Principles on Artificial Intelligence in May 2019[71], the first international standards agreed by governments for the responsible stewardship of trustworthy AI. The Principles include concrete recommendations for public policies and strategies, and complement existing OECD standards in areas such as privacy, digital security risk management and responsible business conduct[72]. Drawing from the OECD principles and recommendations, the Group of Twenty (G20) also adopted AI Principles in June 2019, focusing on principles aimed at responsible stewardship of trustworthy AI and on national policies and international cooperation for trustworthy AI.[73]

67 United Nations Activities on Artificial Intelligence 2019. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2019-1-PDF-E.pdf
68 Ibid.
69 United Nationals Educational, Scientific and Cultural Organization (UNESCO), Ad Hoc Expert Group (AHEG) for the Preparation of a Draft text of a Recommendation the Ethics of Artificial Intelligence, 2020. https://unesdoc.unesco.org/ark:/48223/pf0000373434
70 OECD, "What are the OECD Principles on AI". http://www.oecd.org/going-digital/ai/principles/
71 OECD, "Forty-two countries adopt new OECD Principles on Artificial Intelligence", 22 May 2019. https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm
72 OECD Principles on Artificial Intelligence.
73 "G20 Ministerial Statement on Trade and Digital Economy". https://www.mofa.go.jp/files/000486596.pdf

PARTNERSHIP ON AI

The Partnership on AI (PAI)[74] is a multi-stakeholder organization that brings together academics, researchers, civil society organizations, companies building and utilizing AI technology and other groups working to better understand AI's impacts. The Partnership was established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, to serve as an open platform for discussion and engagement about AI and its influences on people and society and to identify and foster AI efforts for socially beneficial purposes.

THE WAY FORWARD

Governments, law enforcement agencies and anti-corruption actors still have much to do to be AI-ready for anti-corruption efforts. Often, the bottlenecks to reaping the full benefits of AI is not in the readiness of the technology, but in the ability to redesign processes, systems and regulation to deploy them. The transformative power of AI technology must be combined with responsible and ethical human efforts to realize the potential AI technology brings to enable governments, investigators, anti-corruption actors and relevant stakeholders to promote transparency, accountability, integrity and anti-corruption.

"The transformative power of AI technology must be combined with responsible and ethical human efforts to realize the potential AI technology brings."

At the same time, it is important to recognize that while AI is an important tool for anti-corruption efforts, particularly in predicting, detecting and analysing corruption, it cannot solve corruption on its own no matter how effective it may be in revealing corrupt conduct. While it can aid in the investigation process, it is not sufficient to rely on technology alone, and needs to be complemented by decision-making of the analysts, investigators and compliance officers, for whom this technology provides greater insight and eliminates labour-intensive tasks[75].

Nevertheless, when AI technology is developed ethically, governed responsibly and trust is built in the system, the benefits of AI can be harnessed for integrity, trust and anti-corruption. In this regard, all stakeholders have important roles to play in governing the responsible use of AI.

74 The Partnership on AI. https://www.partnershiponai.org/
75 IBM, Fighting financial crime with AI, 2019. https://www.ibm.com/downloads/cas/WKLQKD3W

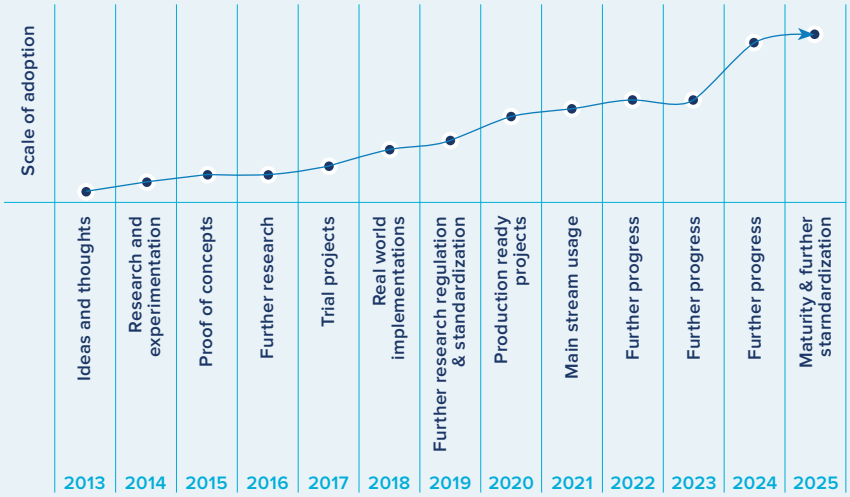
2.2 BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY

With the invention of Bitcoin, introduced as a cryptocurrency in 2008, **blockchain** started gaining recognition for its technological prowess to serve as the public transaction ledger of cryptocurrencies. Today, cryptocurrencies are just one of the many applications that use blockchain technology to record transactions. Blockchain is expected to progress more quickly as the technology matures **(Figure 2.7),** although there are many legal and regulatory challenges that need to be addressed to prevent the misuse of blockchain for criminal activities.

Blockchain is a type of **distributed ledger technology (DLT)** in which information is stored in 'blocks' in a digital ledger. Each block contains encrypted data about a transaction, time-stamped and cryptographically sealed. The blockchain is theoretically tamperproof – as long as there are no successful attacks on the system that compromise any of the system nodes that verify transactions via the agreed consensus mechanism, no data entered in the blockchain can later be changed or deleted, and all data can be traced back to the exact moment it was added to the blockchain. Depending on the choice of consensus mechanism, therefore, and whether the blockchain is a public, private or commissioned blockchain, the decentralised nature of how a blockchain operates can bring transparency, providing arguably a higher level of security and integrity of the records and information it manages. While different types of blockchain have different implications and applications in addressing corruption risks, discussing the types of blockchain in more detail is beyond the scope of this study.

Some of the features and stated aims of blockchains, therefore, are closely linked with anti-corruption principles[76] – transparency, accountability, integrity and trust. As such, blockchain has been deployed for anti-corruption efforts in areas such as land registries, budget transparency, enforcing contracts, conducting transactions, and supply chain managemen[77].

Figure 2.7: Blockchain's progress towards adoption and maturity



Source: Bashir, 2018

BLOCKCHAIN TECHNOLOGY: OPPORTUNITIES FOR INTEGRITY, TRUST AND ANTI-CORRUPTION

Depending on the type of blockchain chosen, and the consensus mechanism agreed upon, blockchain can make it difficult for corrupt actors to manipulate data and conduct fraudulent or corrupt activities, given its potential for transparency, immutability, verifiability and security. At the same time, the encrypted nature of the transactions means that trust is assured, as long as data itself is not compromised and that inaccurate or potentially fraudulent transactions are kept out of the database. Therefore, there are several ways to realize the transformative role of blockchain technology for integrity and anti-corruption.

76 GIZ, The potential of distributed ledger technologies in the fight against corruption, 2020. https://www.giz.de/en/downloads/Blockchain_Anticorruption-2020.pdf
77 Transparency International, Bitcoin Blockchain and Corruption: An Overview, 2018. https://knowledgehub.transparency.org/helpdesk/bitcoin-blockchain-and-corruption-an-overview

First, depending on the choice of blockchain chosen and the consensus mechanism agreed upon, it can create a transparent and accountable system where information can be verified. As such, it is increasingly being adopted in a range of development contexts, and leveraged to solve development challenges, from humanitarian aid, to financial inclusion, to quality education.

As an example of the application of blockchain, the World Food Programme (WFP), as part of its 'Building Blocks' pilot, used blockchain technology to explore whether direct cash transfers to refugees can be made more efficient, secure and transparent, given that the practice of money transfers has many challenges and risks. For example, given that refugees may not have an official identity or bank account needed for the transfer of money, this pilot sought to eliminate the need for intermediaries (e.g. banks, central registries), which also reduced an additional layer of cost (e.g. transaction fees), time, and corruption risks (e.g. bribery and extortion through interaction and discretionary practices with intermediaries).

WORLD FOOD PROGRAMME 'BUILDING BLOCKS' PILOT

In this initiative, WFP used blockchain and biometrics to enable refugees to receive direct cash transfers, without the need for identification or bank documents. Refugees' biometric scans allow them to have a digital identity, which helps them apply for and receive other aid and facilities.

In this initiative, refugees can pay for a transaction through an eye scanner, which verifies their identity and recognizes the amount of money they have, and then processes the transaction, which is stored on the blockchain.

This initiative helped to increase the speed and efficiency of cash transfers and facilitated cash transfers with increased transparency and security. The system could also identify potentially suspicious transactions in real time, which limited the space for corrupt and fraudulent activities.[78]

In Malta, blockchain technology has been used to issue academic credentials and verify workers' skills and credentials. Malta is the first country to standardize the use of Blockcerts across its academic institutions, by allowing students' academic certificates, diplomas and transcripts to be delivered in an instantly verifiable digital and portable format. The access and verification of credentials is possible without paying fees or relying on a software vendor's platform. This increases efficiency and reduces the costs for employers to verify any worker's skills and credentials. In addition, it allows institutions to prevent academic fraud and tampering of certificates, while ensuring authenticity and integrity.[79]

Second, blockchain ensures a complete and public record of alterations, as transactions and documents stored on the blockchain cannot be changed or deleted, as long as the integrity of the system nodes that verify transactions via the agreed consensus mechanism is not compromised. Tokenisation, for example, has the ability to protect sensitive data by replacing them with security 'tokens', which are algorithmically randomly-generated numbers that can serve as reference to the original data, but cannot be used to guess those values. This is highly valuable in ensuring integrity in sectors and administrative areas that are susceptible to or rife with corruption and fraud.

In Georgia, the National Agency of Public Registry (NAPR), in cooperation with the Bitfury Group, has implemented a Blockchain land-titling project, with technical assistance from

78 S. Sayers, Code to Integrity, Ministry of Foreign Affairs of Denmark, 2018. https://um.dk/~/media/UM/English-site/Documents/News/Code%20to%20Integrity_Enkeltsider_Web.pdf?la=en
World Food Programme, Innovation Accelerator, "Building Blocks: Blockchain for Zero Hunger" https://innovation.wfp.org/project/building-blocks
G. Dhameja, "UN World Food Programme uses Parity Ethereum to aid 100,000 refugees", 18 February 2019. https://www.parity.io/un-world-food-programme-uses-parity-ethereum-to-aid-100-000-refugees/
A. Smith, "How the World Food Programme uses blockchain to better serve refugees", ITU News, 11 April 2019. https://news.itu.int/how-the-world-food-programme-uses-blockchain-to-better-serve-refugees/

79 Malta Chamber, "Employers In Malta Will Soon Be Able To Verify Skills And Credentials Through Blockchain", 21 February 2019. https://www.maltachamber.org.mt/en/employers-in-malta-will-soon-be-able-to-verify-skills-and-credentials-through-blockchain
K. Micallef, "Malta begins multiyear roll out of Blockcerts", AIBC News, 26 February 2019. https://maltablockchainsummit.com/news/malta-begins-multiyear-roll-out-of-blockcerts/
G. Watson, "Malta first to introduce Blockcerts for academic credentials", Newsbook, 21 February 2019. https://newsbook.com.mt/en/malta-first-to-introduce-blockcerts-for-academic-credentials/

GIZ[80]. Through a distributed digital timestamping service, the NAPR can verify and sign a document containing a citizen's essential information and proof of property ownership. This timestamping service also allows citizens to ensure their documents are legitimate without exposing confidential information. This project will continue to advance to include smart-contract capabilities to streamline business operations for NAPR, including the sale of property, transfer of ownership and more.

In India, UNDP has supported a project to build a land registry using blockchain technology for the city of Panchkula, in the state of Haryana, India. Many land registries in the world suffer from rife corruption and inefficiencies, with unprotected citizens bearing the brunt of these issues. With blockchain technology, land registries can benefit from immutability, verifiability and security of transactional records, since no one can tamper or forge records. Using the Ethereum blockchain, the land registry has a single source of ownership status and the history of a property. The buyer will be assured that the land being bought is the correct plot, and that the seller is the owner. This reduces the potential for disputes, mitigates the inherent corruption risks and saves costs and time for any given transaction. Transparency and traceability are embedded into the system, which will enhance data security and ensure authenticity of land records[81].

TRUBUDGET BLOCKCHAIN PLATFORM

KfW, the German Development Bank, developed TruBudget[82], an open source blockchain-based platform aimed at making donor-financed development cooperation projects more efficient and effective. The blockchain-based platform makes it possible to trace all work, approval steps and processes, in real time. This includes tracking all activities in the implementation of a project, such as drafting contracts, tendering and disbursement processes, budget allocation, and more.[83] In this way, TruBudget reduces corruption risks and promotes transparency and accountability in project implementation and among project partners.

The main benefits of TruBudget for partner countries and donors are[84]:

1. The reduction of transaction costs on both sides
2. The increasing transparency and efficiency of donor-funded projects
3. The strengthening of domestic governance structures and of public financial management systems

TruBudget is currently being implemented by KfW through different pilot phases in Brazil, Burkina Faso, Ethiopia and Georgia.

Third, blockchain is able to track the precise movement of money more accurately. It can be a valuable tool in supply chain management, where blockchain can be useful in record keeping and provenance tracing and tracking. For example, blockchain technology can track corrupt activities, counterfeiting and trafficking in different sectors and industries.

Everledger, an independent technology company, was formed with the objective of building transparency, trust, compliance and sustainability in assets such as diamonds, gemstones and wine. In collaboration with IBM, Everledger built a blockchain platform which provides a secure record of an asset's origin and journey by bringing transparency to its 'lifetime journey'. For diamonds, this means tracing its steps from mining, to sorting and pricing, to manufacturing, to cutting, polishing and producing, to selling and retailing.

Blockchain technology has helped overcome the corruption risks, including those associated with human interaction and discretion, as well as fraudulent activities, by using

80 Bitfury, "The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project", 7 February 2016. https://bitfury.com/content/downloads/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf
81 A. Oprunenco and C. Akmeemana, "Using blockchain to make land registry more reliable in India" (Blog), UNDP, 1 May 2018. https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html
82 TruBudget, https://openkfw.github.io/trubudget-website/
83 KfW Development Bank, "Blockchain creates more transparency in development cooperation", 17 December 2018. https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Pressemitteilungen-Details_500800.html
84 KfW Development Bank, "TruBudget Project Information", 2018. https://www.kfw-entwicklungsbank.de/PDF/Entwicklungs-finanzierung/Themen-NEU/Digitalisierung/2018_TruBudget.pdf

digital signatures on diamonds. When a certified mine puts a diamond on the blockchain, it signs the transaction with its private key, which can be verified. This means that the source of the diamond cannot be altered, and it is impossible to change previous records without invalidating the entire chain. Not only can blockchain technology improve the supply chain transparency of diamonds, but it also increases the value of luxury items as authenticity throughout their entire lifetime history can be ensured.

Blockchain technology has similarly been used to overcome illegal and corrupt activities in fisheries. It can track the journey of a single fish, recording information from when and where it was caught, how it was processed, to its sale to consumers. The World Wildlife Fund partnered with the global blockchain venture studio ConsenSys[85], ICT implementer TraSeable Solutions Pte Ltd.[86] and the tuna fishing and processing company, Sea Quest Fiji Ltd., to prevent illegal activities in the Pacific Islands tuna industry.

The global tuna industry has historically suffered from corrupt practices, illegal fishing practices and modern slavery practices. As such, the project used a combination of radio-frequency identification (RFID) tags, quick response (QR) tags and scanning devices to collect information about the journey of a tuna at various points along the supply chain, which is then recorded using blockchain technology. Blockchain technology ensures a digital, transparent and tamper-proof record of information that is accessible to everyone; and consumers can have the certainty that they are buying legally caught, sustainable tuna with no slave labour or other harmful practices involved.[87]

Figure 2.8 presents a summary of the examples of how blockchain can be applied across sectors and thematic areas to promote integrity and anti-corruption.

Figure 2.8: Summary: Applications of blockchain for integrity and anti-corruption

Sector/thematic area	Example of potential application of blockchain	Examples of the contribution to integrity and anti-corruption
Medical and healthcare	Track and trace transactions and payments related to procurement, tendering and contracting of healthcare	• Enhance integrity and accountability of direct contract modalities • Prevent fraud and corruption in procurement of products
Land management	Distributed digital timestamping service to verify and sign documents containing citizen information and proof of property ownership	• Prevent corruption in the sale of property, transfer of ownership and more • Increase security and privacy by allowing the proof of legitimacy of documents without exposing confidential information
Digital and legal identity	Enable record and storage of identity documentation	• Prevent fraud in identification • Reduce the burden of paperwork
Financial inclusion	Enable direct cash transfers through blockchain and biometrics	• Eliminate possibilities for corruption and fraud in disbursement of cash transfers • Increase efficiency, transparency and security in transferring money
Education	Enable verification of academic certificates, diplomas and transcripts instantly through digital and portable format	• Prevent academic fraud and tampering of certificates • Increase efficiency and integrity in verification of workers' skills and credentials
Diamonds	Tracking digital signatures on diamonds and verifiable transactions using private key	• Improve supply chain transparency • Prevent fraud by ensuring authenticity in items
Fisheries	Tracking and recording the journey of fish throughout the entire supply chain using blockchain technology	• Increased certainty for consumers about the integrity of fishing practices • Prevent corruption and modern slavery practices in fisheries

85 ConsenSys, "The Most Trusted Ethereum Blockchain Solutions". https://consensys.net/
86 TraSeable Solutions, "Transforming Pacific Fisheries and Agriculture through Collaborative Transparent Traceability". https://traseable.com/
87 C. Visser and Q. Hanich, "How blockchain is strengthening tuna traceability to combat illegal fishing", 201 (2018) 22 January, The Conversation 1-4, University of Wollongong, Australia.
K. Whiting, "Blockchain could police the fishing industry - here's how", World Economic Forum, 12 February 2020. https://www.weforum.org/agenda/2020/02/blockchain-tuna-sustainability-fisheries-food-security/
World Wildlife Fund (WWF), "New blockchain project has potential to revolutionise seafood industry", 8 January 2020. https://wwf.panda.org/?320232/New-Blockchain-Project-has-Potential-to-Revolutionise-Seafood-Industry
WWF-New Zealand, "Blockchain Tuna Project". https://www.wwf.org.nz/what_we_do/marine/blockchain_tuna_project/

HEALTH PROCUREMENT UNDER COVID-19 EMERGENCY PROTOCOLS: POTENTIAL OPPORTUNITIES FOR BLOCKCHAIN-BASED E-PROCUREMENT SYSTEMS

In response to the COVID-19 health crisis, many governments have relaxed safeguards on transparency, oversight and accountability mechanisms for speed and flexibility under emergency protocols. This is particularly pertinent in procurement, tendering and contracting processes as emergency protocols in many countries allow for fast-tracking the sourcing of essential goods and services, including emergency direct contracting.

Yet, the procurement of medicines and supplies in health systems is one of the most vulnerable areas for corruption. Given that direct modalities and fast-track mechanisms are put in place in some countries, if there are inadequate oversight and accountability mechanisms, corrupt actors may capitalise on the global shortages in both medicines and medical supplies during the pandemic.

Examples of corruption risks include:

- Manipulation of specifications and TORs to favour suppliers
- Bribery and favours between suppliers and procurement officials to gain advantage in a tender process
- Price gouging/demanding higher prices for products
- Procurement of products without a justifiable medical reason
- Nepotism during the bidding process

The World Economic Forum's report on 'Exploring Blockchain Technology for Government Transparency'[88] highlighted that blockchain-based e-procurement systems could be considered in enhancing integrity and accountability of direct contract modalities, particularly pertinent in the wake of the COVID-19 pandemic.

With its features of transparency, immutability, verifiability and security, blockchain technology could potentially serve as a valuable tool in emergency procurement processes during a crisis or pandemic, allowing for corruption and fraud detection and analytics and for tracing and tracking transactions and payments.

Blockchain technology therefore provides potentially huge benefits for curbing corruption in emergency procurement processes; for enhancing efficiency in procuring or contracting essential goods and services; and for promoting effectiveness in crisis management and response.

TRUST IN THE CONTEXT OF BLOCKCHAIN TECHNOLOGY

Trust is often cited as one of the key aspects of blockchain. The technical characteristics of blockchain present a number of key benefits to ensure trust, given the potential for transparency, immutability, verifiability and security. The encrypted nature of the transactions means that trust is assured, and inaccurate or potentially fraudulent transactions are kept out of the database, as long as the integrity of the system nodes are not compromised.

It is often noted that blockchain technology would be successful in a society with a high trust in technology, since blockchain ensures tamper-proof records that corrupt actors cannot modify or falsify. However, it should be noted that if blockchain technology is applied to secure physical records – for example, land records, diamonds, digital identity, inter alia – then, in addition to the trust in technology, there needs to be trust in those who enter records in the blockchain[89]. This implies that the incentives for good behaviour does not only reside in the transformative nature of blockchain for integrity and transparency, but also in the government bodies or institutions responsible for matching information with reality.

88 World Economic Forum, Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption, 2020. https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption

89 P. Aarvik, Blockchain as an anti-corruption tool: Case examples and introduction to the technology, Anti-Corruption Resource Centre, CMI Chr Michelsen Institute, Norway, U4 Report 2020:7. https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf

CORRUPTION AND INTEGRITY RISKS IN THE USE OF BLOCKCHAIN TECHNOLOGY

While blockchain technologies present many opportunities for preventing corruption and promoting transparency and integrity, they could also be misused for private gain, such as using cryptocurrency for money laundering, illegal (e.g. black market) transactions and tax evasion.

The use of cryptocurrencies by criminals for illicit activities has attracted the attention of financial regulators, legislative bodies, law enforcement and the media over the years. Some have argued that bitcoin's anonymity encourages money laundering and other crimes. Foley et al (2019) estimate that around US$76 billion of illegal activity per year involve bitcoin (46 percent of all bitcoin transactions), and suggest that cryptocurrencies are transforming the black markets by enabling "black e-commerce". For example, the Silk Road, an online black market and first modern darknet market, best known for selling illegal drugs, used bitcoins as the form of transactions between buyers and sellers, due to its level of anonymity.[90]

Yet, others have argued that money laundering using bitcoin or other cryptocurrencies can easily lead investigators to identify criminal actors due to the nature of cryptocurrency transactions. These transactions rely on DLT and are recorded on a permanent, public and immutable ledger, which, while it has a certain degree of anonymity, can actually offer unprecedented transparency into financial transactions. Because one of the goals of money laundering or other illicit activities is to create a chain of transactions that cannot be traced, the vast majority of cryptocurrencies makes these activities difficult, given that they are designed to have an indelible public record of all transactions. Thus the properties of DLT can potentially facilitate law enforcement.[91]

Nevertheless, criminals will continue their attempts at circumventing or exploiting the blockchain of cryptocurrencies, such as through unregulated cryptocurrency exchanges or decentralized peer-to-peer networks, where criminals can take advantage of exchanges that have little or no anti-money laundering regulations.[92] Attacks from malicious actors could occur either within the blockchain, or via software clients and third-party applications (e.g. cryptocurrency wallets).

While blockchain can be a very secure method of recording data due to its encryption, the data that is within the blockchain can hold sensitive information linked with an individual identity, which may be susceptible to cyberattacks and also raise concerns about data privacy and the misuse of data. For example, retailers may capture a mass of data about customer preferences and store data about what they buy and how they pay for it. In this regard, corporate blockchains are likely to contain a lot of information about individuals, even if pseudonyms are used, data is encrypted and data is only available to authorized parties.

While it is true that no names, addresses, telephone numbers or any other information can make it readily possible to identify participants in the corresponding transaction data entries in the blockchain without significant effort, there are various possibilities for the de-anonymisation of corresponding entries.[93] If data governance and privacy issues are not adequately addressed, blockchain can be used as a tool to abuse power and gain dominant control of the system.

Moreover, many have noted the tension and incompatibility that exists between the nature of blockchain technologies and data protection laws. For example, the EU's GDPR mandates that systems (not limited to blockchain technology) used to capture and store personal data must be built to ensure data privacy. Yet, in principle, the nature of blockchain technology is that blockchain data is stored permanently, and no data entered in the blockchain can later be changed or deleted. Removing all evidence of a person's transactions, as per the GDPR, would compromise the integrity of the blockchain and falsify the record. Thus, there are concerns regarding the inherent incompatibility between transparency and privacy and the violation of the 'right to be forgotten'.

90 D. Adler, "Silk Road: The Dark Side of Cryptocurrency" (Blog). Fordham Journal of Corporate and Financial Law, 21 February 2018. https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/
91 M. De Silva, "Bitcoin money laundering is a classically dumb crime", Quartz, 5 December 2019. https://qz.com/1761343/bitcoin-money-laundering-is-a-classically-stupid-crime/
92 Elliptic, "Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act)", 18 September 2019. https://www.elliptic.co/our-thinking/bitcoin-money-laundering
93 Deloitte, "Blockchain and GDPR: from practice to theory and back." https://www2.deloitte.com/nl/nl/pages/legal/articles/blockchain-and-gdpr-from-practice-to-theory-and-back.html

Cyberattacks and 'privacy poisoning' may also render blockchain technologies unusable. 'Privacy poisoning' refers to loading private data or illegal material into a blockchain, which puts the blockchain in conflict with data privacy laws. The result is that the affected chain with all the data it contains cannot be used unless expensive and time-consuming steps are taken.[94]

Some have argued that the transformative nature of blockchain technology lies with the fully distributed ledgers, which can prevent powerful actors from controlling a market or sector, and thereby prevent corruption[95]. Yet, Aggarwal and Floridi (2018) find evidence that the network power on the Bitcoin blockchain is highly concentrated (the number of validation nodes is steadily decreasing), demonstrating that political power on the blockchain is recentralized in a 'tech-elite' rather than truly 'distributed', which could create new avenues for corruption[96].

UNDERSTANDING BLOCKCHAIN VS. CRYPTOCURRENCY

In 2008, Bitcoin was introduced as a cryptocurrency without a central bank or single administrator, but managed by a network of stakeholders. Bitcoins are awarded from a process known as 'mining', and can be exchanged for products, services and other currencies. It is one of the most well-known cryptocurrencies, but is susceptible to illegal transactions, money laundering, black market activities and other corruption activities. Cryptocurrencies have also been vulnerable to theft through hacking and scams, with more than US$1.4 billion stolen just in the first half of 2020[97]. These illicit activities have attracted widespread negative public attention in the past years, including from financial regulators, legislative bodies, law enforcement and the media.

Blockchain and distributed ledger technology are the technological innovation powering Bitcoin and other cryptocurrencies. However, over time, the potential use of blockchain technology for other transactions and uses was explored in applications beyond cryptocurrencies, known as 'Blockchain 2.0'.

In other words, while there are ongoing arguments for and against cryptocurrencies, these comprise just one application of blockchain technologies, which are also used in other applications, including for smart contracts, supply chain management, among others (as discussed in this study), with wide-ranging benefits for promoting transparency and integrity.

Moreover, the use and misuse of cryptocurrencies also depend on the legal and regulatory environment. In some countries, provisions are in place for ensuring compliance with Know Your Customer (KYC) regulations, which guarantees the verification of customer identities during the opening and maintaining of accounts to assess and monitor customer risk. This is intended as an anti-money laundering measure.

REGULATORY DEVELOPMENTS SURROUNDING BLOCKCHAIN TECHNOLOGIES

The purpose of regulation is to have legal oversight of the business on the blockchain and not the underlying technology itself.[98] Many countries have increasingly established frameworks for regulation, in order to provide safeguards and also to encourage innovation and growth in the use of blockchain technologies. However, most of the tangible regulatory responses to date relate to components of blockchain, such as cryptocurrencies, and to specific legal issues, such as anti-money laundering (AML) and counterterrorism-financing (CTF). A comprehensive regulatory response to the use of blockchain as a whole does not currently exist.

94 H. Kenyon, "Privacy 'poisoning' poses threat to companies using blockchain", PhysOrg, 10 April 2019. https://phys.org/news/2019-04-privacy-poisoning-poses-threat-companies.html#:~:text=Known%20as%20privacy%20%22poisoning%2C%22,in%20conflict%20with%20local%20laws.
95 Aarvik, Blockchain as an anti-corruption tool: Case examples and introduction to the technology.
96 N. Aggarwal and L. Floridi, "The Opportunities and Challenges of Blockchain in the Fight against Government Corruption", Digital Ethics Lab, Oxford Internet Institute, 2018. https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article_AggarwalFloridi.pdf
97 D. Nelson, "Crypto Criminals Have Already Stolen $1.4B in 2020, Says CipherTrace", COINDESK, 2 June 2020. https://www.coindesk.com/crypto-criminals-have-already-stolen-1-4b-in-2020-says-ciphertrace
98 OECD, Blockchain Technology and Corporate Governance, Directorate for Financial and Corporate Affairs, Corporate Governance Committee, 6 June 2018. https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/CA/CG/RD(2018)1/REV1&docLanguage=En

In terms of implementing crypto regulations, the EU's Fifth Anti-Money Laundering Directive (AMLD5) requires crypto exchanges and custodial service providers to register with their local regulator and demonstrate compliance with AML and CTF processes. The AMLD5 has mostly aligned with the Financial Action Task Force (FATF) recommendations.

Many countries around the world have aligned with the FATF recommendations on virtual assets. The FATF is an inter-governmental body established to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Finalised in 2019, FATF's "travel rule" requires virtual asset service providers, including wallet providers and exchanges, to share user information with one another every time funds are transferred. This aims to prevent terrorists and money launderers using cryptocurrencies to bypass existing controls and sanctions.

FINANCIAL ACTION TASK FORCE 'TRAVEL RULE' ON VIRTUAL ASSETS

Many FATF member states and G20 economies have already adopted the FATF's 'travel rule'. For example, the new Financial Services Act (FinSA) and Financial Institutions Act (FinIA) in Switzerland came into force at the start of 2020. These oblige the Swiss Financial Market Supervisory Authority (FINMA) to pass a number of implementing provisions. In line with implementing the FATF's travel rule, FINMA has lowered the threshold value for exchange transactions in cryptocurrencies, from CHF 5,000 to CHR 1,000, in its Anti-Money Laundering Ordinance (AMLO-FINMA), thereby acknowledging the heightened money-laundering risks in this area.

In Singapore, the Payment Services Act, which was passed in 2019, gives the Monetary Authority of Singapore formal supervisory authority over payment firms, and it has brought all crypto businesses and exchanges based in Singapore under current anti-money laundering and counterterrorist-financing rules.[99] These businesses are required to register and apply for a licence to operate in Singapore. The Payment Services Act provides a forward-looking and flexible regulatory framework for the payments industry, which will mitigate risk and foster confidence in digital payments, while encouraging continued innovation and growth of payment services and FinTech. In line with the FATF guidance, Singapore set its travel rule threshold at S$1,500.

Similarly, Japan and South Korea have aligned with the FATF directives, with Japan's Payment Services Act, passed in 2017, and a similar bill passed by South Korea in 2019 that provides a legal basis for cryptocurrencies in the country, and aims to prevent money laundering and protect investments.

Overall, with the regulatory developments surrounding blockchain technologies, such as the FATF guidance, many countries have been urged to make progress on developing and enacting cryptocurrency regulation in order to mitigate risks of illicit activities, encourage growth and innovation and foster confidence in blockchain technologies.

In addition, international organisations have also been working on frameworks for the use of blockchain technologies. The International Organization for Standardization (ISO) has been working on a series of blockchain and DLT standards ISO/TC 307[100], which will be released by 2021. The standards will include terminology and concepts, privacy and personally identifiable information, security risks and vulnerabilities, among others. According to the ISO, the demand for standards has been urgent. The aim of establishing standards is to support interoperability and data exchange between users, applications and systems. However, there are many challenges to developing these standards, including the significant regulations implemented globally (e.g. EU's GDPR) and the rapid progress and adoption of blockchain and DLT.

The World Economic Forum has also taken steps to formally establish a coherent international framework for governments to regulate the cryptocurrency industry. The

99 Allison, I. "Singapore Announces New AML Rules for Crypto Businesses," 27 January 2020. https://www.coindesk.com/singapore-announces-new-aml-rules-for-crypto-businesses

100 International Organization of Standardization (ISO), « Standards by ISO/TC 307. Blockchain and distributed ledger technologies ». https://www.iso.org/committee/6266604/x/catalogue/

'Global Consortium on Cryptocurrency Governance'[101], launched in 2020, will bring together a wide variety of state and non-state actors, including representatives from NGOs, academics, technical experts, national regulatory bodies and a mix of private and state-run banking institutions. The Consortium will focus on finding solutions for a fragmented regulatory system and on promoting public-private cooperation, with the overall aim to increase access to the financial system through innovative policy solutions that are inclusive and interoperable.

THE WAY FORWARD

Blockchain technologies have tremendous potential to benefit many industries, yet there are many legal and regulatory challenges that need to be addressed to advance the expansion of blockchain technologies and prevent their misuse for private gain or for facilitating criminal activities.

Many applications of DLT lack an appropriate legal and regulatory framework in which to operate. McKinlay et al (2018) highlight issues of complex jurisdictional issues, risk and liability in relation to malfunctioning blockchain services, the willingness of vendors to commit to performance assurances, intellectual property ownership, strategy and data privacy. If these issues are not addressed, the usefulness of blockchain may be limited or susceptible to abuse at the hands of a few, creating a new form of centralized political power.

"Widening digital divides - such as in the capabilities for harnessing digital data and frontier technologies - threaten to leave developing countries even further behind."

Moreover, the applicability and transferability of the instrument is limited for now. The adoption of blockchain technology by the developing world is unlikely to be realized on a large scale anytime soon, if there is a lack of digital infrastructure and lack of political commitment to invest and change existing systems[102]. Widening digital divides – such as in capabilities for harnessing digital data and frontier technologies – threaten to leave developing countries even further behind[103].

Importantly, it must be recognized that blockchain alone, like any other technology, has its limitations whether in combatting corruption or in enhancing transparency, accountability and integrity. Blockchain itself does not provide a mechanism for establishing strong and effective institutions, fundamentally necessary in preventing and tackling corruption. For example, Aggarwal and Floridi (2018) highlight that blockchain is more successful with strong institutions and infrastructure, such as the land registries in Georgia, where land is already documented and property registration processes are relatively streamlined and digitally enabled. Moreover, the use of blockchain in Georgia is driven by its tax benefits. As such, the effectiveness of blockchain technologies for integrity and anti-corruption still depend on the wider political economy context, in addition to the digital infrastructure, which power the blockchain.

Overall, blockchain is still far from being an easily applicable, scalable or transferable anti-corruption instrument[104]. A coordinated effort, bringing all stakeholders, including governments, private sector, civil society, technologists and academia together, will be needed to come up with feasible policy recommendations and guidelines to govern the use of blockchain technology.

101 World Economic Forum, "Governing the Coin: World Economic Forum Announces Global Consortium for Digital Currency Governance," 24 January 2020. https://www.weforum.org/press/2020/01/governing-the-coin-world-economic-forum-announces-global-consortium-for-digital-currency-governance/

102 K. Kim and T. Kang,"Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology", 2017. https://www.semanticscholar.org/paper/Does-Technology-Against-Corruption-Always-Lead-to-Kim-Kang/766de80c483ccfbd56936cc03ec82f58760284c0

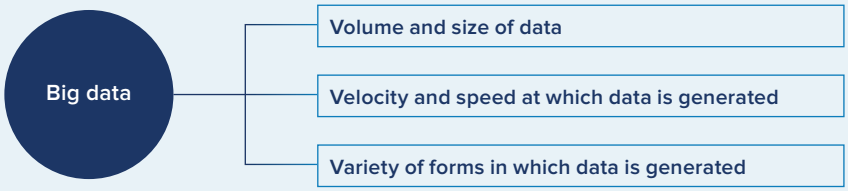
103 United Nations Conference on Trade and Development (UNCTAD) Digital Economy Report 2019 https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

104 Transparency International, Bitcoin, Blockchain and Corruption.

2.3 BIG DATA ANALYTICS

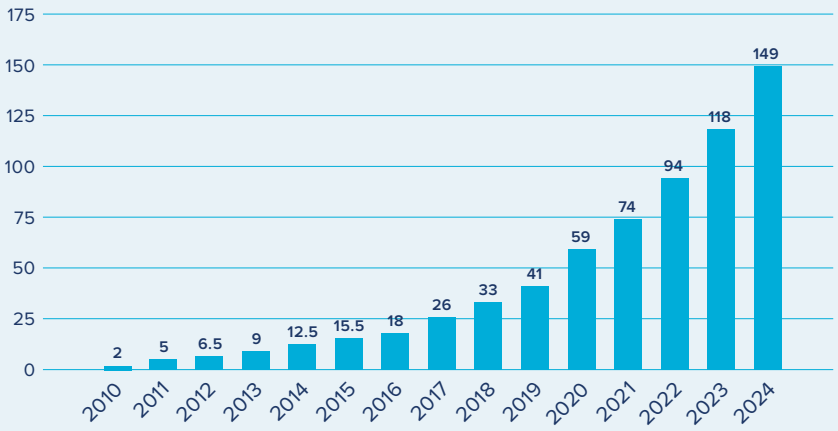
The term **'big data'** has existed for decades, but in recent years, the speed, efficiency and transformative power of big data has placed it in the spotlight. Big data refers to extremely large and complex data sets that may be analysed computationally to reveal patterns, trends and associations that cannot be dealt with by traditional data processing software. As presented in **Figure 2.9,** big data has three main characteristics: the volume and size of data; the velocity at which data is generated and processed; and the variety of forms in which the data is generated, ranging from photos to videos, transactions, text messages, location information, social media posts and others.[105]

Figure 2.9: Characteristics of big data



Source: United Nations Global Pulse[106]

Figure 2.10: Volume of data created worldwide from 2010 to 2024 (in zettabytes)



Source: Statista[107]

The volume of big data is growing at an unprecedented rate (Figure 2.10), and the billions of Internet-connected sensors and devices which represent the Internet of Things (IoT) are contributing significantly to the volume of big data collected. Techniques and analytical applications for analysing big data are also on the rise, with AI technologies, including machine learning and natural language processing, aiding the process of big data analytics. In addition, cloud computing services, which provide data storage and computing power on-demand, can help process, analyse and manage big data more efficiently in the cloud.

Using traditional data processing software, it is difficult to expose corruption due to the need to analyse large quantities and varieties of data. However, the rise of big data has led to new data management and data mining techniques to prevent fraud and abuse in the public sector.

105 D. Berliner and K. Dupuy, The promise and perils of data for anti-corruption efforts in international development work, Anti-Corruption Resource Centre, CMI Chr. Michelsen Institute, Norway, U4 Brief 2018:7. https://www.u4.no/publications/the-promise-and-perils-of-data-for-anti-corruption-efforts-in-international-development-work.pdf
106 United Nations Global Pulse, Big Data for Development: A primer, 2013. https://www.unglobalpulse.org/wp-content/uploads/2013/06/Primer-2013_FINAL-FOR-PRINT.pdf
107 Statista, "Volume of data/information created worldwide from 2010 to 2024", 2020. https://www.statista.com/statistics/871513/worldwide-data-created/

Figure 2.11: Big data analytics in anti-corruption work

Goals of analysis	Individual data entries	Analysis of full dataset	Cross-referencing multiple datasets
Identifying instances of corruption	Investigating specific individuals, firms, contracts, etc.	Identifying anomalous patterns or extreme values	Identifying instances of quid-pro-quo
Measuring prevalence of corruption	Combining multiple specific investigations	Measuring frequency of improper or suspicious values	Measuring frequency of improper or suspicious linkages
Comparison across entities or time		Comparing values across entities in order to produce rankings; or over time in order to assess trends	Comparing linkages across entities in order to produce rankings; or over time to assess trends
Evaluating impacts on corruption		Comparing values across treated/untreated units or before/after intervention	Comparing linkages across treated/untreated units or before/after intervention

Source: U4, 2018

Big data analytics in the area of anti-corruption, as summarised by U4 (2018), can be useful in identifying instances of corruption, measuring the prevalence of corruption, making comparisons across entities or time and evaluating the impacts on corruption **(Figure 2.11).**

The application of big data analytics promotes integrity and anti-corruption, broadly, in two main ways **(Figure 2.12):** first, in facilitating the detection, investigation, monitoring and audit of transactions and organizations[108]; and second, in informing and improving national, sectoral or local policies and outcomes by using predictive analysis and visualisations, thereby contributing to more efficient and improved decision-making. The ability of big data analytics to analyse and compare different sources of information is one of its biggest advantages, and these techniques have been employed for a range of areas, such as in taxation, procurement, smart cities, public services (e.g. improving diagnosis and clinical decisions in healthcare), evaluating performance and conducting oversight. Governments therefore can leverage big data analytics to improve the provision of public services.

Figure 2.12: Two main ways big data analytics promotes integrity and anti-corruption

This chapter will thus highlight the opportunities for integrity and anti-corruption using country examples, the corruption risks posed by big data analytics, the current regulatory mechanisms guiding the use of big data and analytics, and what needs to be done by a range of stakeholders to harness the benefits of big data analytics for integrity and anti-corruption.

BIG DATA ANALYTICS: OPPORTUNITIES FOR INTEGRITY, TRUST AND ANTI-CORRUPTION

Big data analytics can detect patterns of suspicious transactions in a wide range of areas and sectors, from healthcare to education, and from law enforcement to tax

108 See, for example, T. Malik, "Big data can shame grand corruption", The Express Tribune, Pakistan, 28 May 2016. https://tribune.com.pk/story/1112068/big-data-can-shame-grand-corruption

administration. With real time detection, agencies have been able to detect, stop and address fraudulent and corrupt activities, resulting in billions of dollars of potential cost savings. Big data analytics can also be useful in assessing corruption risks, which inform corruption risk mitigation actions. Decisions related to monitoring, audit and investigations concerning individual transactions and organizations can be facilitated by using big data analytics. Big data analytics have a huge potential to deter corruption given its effectiveness in identifying and analysing incidences of corruption, by using a vast quantity of data across different information sources to discover patterns that would otherwise have been impossible through regular audits and inspection.

APPLICATIONS OF BIG DATA ANALYTICS FOR ANTI-CORRUPTION ACROSS SECTORS

In the work of **investigative journalists,** big data analytics have proven to be useful in uncovering the biggest corruption scandals. The release of the **Panama Papers** by investigative journalists, for example, was aided by the use of big data tools to analyse and review over 11.5 million documents. Similarly, in **Brazil**, the Operation Car Wash scandal was investigated with the help of Lava JOTA, an innovative tool for analysing hundreds of thousands of official documentation of more than 1,100 lawsuits from Brazil's biggest corruption scandal, and uncovering hidden patterns of corruption, fraud, waste and abuse[109].

In **public procurement,** data mining is being used for audits to monitor bid issuance and to identify red flags, patterns of collusion and false information. It is also being used to identify 'corrupt intent' in payments or transactions through data visualization. Researchers at the Corruption Research Center Budapest[110] have examined huge volumes of data sets of public procurement procedures from **EU countries** by searching for abnormal patterns, such as exceptionally short bidding periods or unusual outcomes (e.g. no competition for the winning bid, or bids repeatedly won by the same company). In the **United Kingdom,** the Government Digital Service (GDS) is helping to tackle global corruption through the Global Digital Marketplace Programme[111], working with international governments to make their procurement data and processes more transparent and to boost their digital, data and technology sectors.

In assessing corruption and fraud risks in **infrastructure,** OECD supported the Airport Group of the City of Mexico (Grupo Aeroportuario de la Ciudad de México, or GACM) to link big data analytics to broader risk management objectives. It supported the GACM to develop data-driven risk assessments and its analytics capacity, which overall helped drive improvements in data governance while managing risks in large-scale infrastructure projects[112].

Anti-corruption software tools are also being designed specifically for detecting and responding to fraud in **public administration,** including the intelligent mining of data sets and administrative procedures. For example, the **European Commission (EC)** developed a data mining and data analytics software, ARACHNE[113], that cross-checks data from various public and private institutions. The purpose of this system is to respond to an increased demand for creating an adequate and accurate fraud prevention and detection strategy. It helps to identify projects susceptible to risks of fraud, conflict of interests or irregularities. The effective integration of these tools into the e-governance and e-procurement practices of the governments would not only enhance decision-making, but also bring greater transparency through the simplification of processes[114].

Big data analytics transform how government entities provide public services, evaluate performance and strengthen oversight and accountability. For example, the EC has used big data analytics for policy reform in public procurement, which plays a

109 F. Angelico, "Brazil: Open data just made investigating corruption easier". Transparency International. 12 May 2017. https://www.transparency.org/news/feature/brazil_open_data_just_made_investigating_corruption_easier
110 Corruption Research Center Budapest. https://www.crcb.eu/
111 Government of the United Kingdom, Digital Marketplace. https://www.digitalmarketplace.service.gov.uk/
112 OECD, Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments, 2019. https://www.oecd.org/gov/ethics/analytics-for-integrity.pdf
113 ARACHNE Risk Scoring Tool. https://ec.europa.eu/social/main.jsp?catId=325&intPageId=3587&langId=en
114 L. Silveira, "4 technologies helping us to fight corruption", World Economic Forum, 18 April 2016. https://www.weforum.org/agenda/2016/04/4-technologies-helping-us-to-fight-corruption/

Photo: Unsplash

crucial role in economic development and quality of government across the EU, accounting for about 13 percent of GDP. Big data analytics could inform, monitor and improve country- or sector-wide policy decisions on resource allocation, regulation requirements and other reforms, by integrating better quality information and evidence gathered from big data analytics into policymaking processes.

In the largest state of **India,** Madhya Pradesh, the implementation of several data-focused initiatives on e-governance and data analytics have led to widespread transparency and improved public service delivery. These include the Chief Minister's dashboard which integrates information from various sources (including real time information) to promote evidence-based decision-making, and the Chief Minister's Helpline, a unified gateway to register grievances related to all aspects of government functioning. Advance data analytics are used for monitoring and operations, to inform better decision-making regarding the services and schemes that citizens demand on the ground and to implement the reforms required for improvements in public service delivery[115].

GLOBAL PARTNERSHIP FOR SUSTAINABLE DEVELOPMENT DATA

The Global Partnership for Sustainable Development Data (GPSDD)[116] is a network of hundreds of members, including governments, the private sector, civil society, international organizations, academic institutions, foundations, statistical agencies and other data communities. It was established to help stakeholders across countries and sectors fully harness the data revolution for sustainable development, using this new knowledge to improve lives and protect the planet. Members of the GPSDD work together towards a world where data is being used more openly, effectively, and efficient, by governments to improve policymaking and service delivery, by citizens and civil society to hold leaders accountable for their actions and by private sector companies and businesses to build capacity and drive entrepreneurship and innovation.

The **European Investment Bank** (EIB) has used big data analytics for proactive integrity reviews in financing its projects across the EU, typically in the infrastructure sector. Providing over €50 billion of financing annually, there are thousands of procuring entities that manage these projects, leading to tens of thousands of contracts. To manage the many risks across such a large portfolio, from its management to ensuring transparency and accountability, every year the EIB screens and audits a handful of organizations receiving EIB loans. In this process, the Fraud Investigations Division of the EIB's Inspectorate General conducts 'proactive integrity reviews' with the aim of mitigating risks and avoiding large financial losses.

115 Grant Thornton, Public sector delivery mechanisms: Success story of Madhya Pradesh, 2019. https://www.grantthornton.sg/globalassets/1.-member-firms/india/assets/pdfs/public_sector_delivery_mechanism_mp.pdf
UN World Data Forum 2018, "Data for policy action: Using big data to drive development for all". https://unstats.un.org/unsd/undataforum/dubai-2018/sessions/ta3-07-data-for-policy-action-using-big-data-to-drive-development-for-all/
World Bank,"Madhya Pradesh Citizen Access to Responsive Services Project", 2016 (approval date). https://projects.worldbank.org/en/projects-operations/project-detail/P149182?lang=en

116 Global Partnership for Sustainable Development Data. http://www.data4sdgs.org/

BIG DATA AS A POWERFUL TOOL IN THE CRISIS MANAGEMENT AND RESPONSE TO THE COVID-19 PANDEMIC

Many countries have leveraged big data and advanced analytics to better manage the COVID-19 pandemic. In particular, big data-driven approaches to combatting COVID-19 have been useful in:

- **Predicting community and individual risk of infection** to better understand the risks involved and to develop mitigation/prevention strategies
- **Predicting treatment outcomes in patients** to make accurate treatment recommendations
- **Monitoring patients in health care facilities** to enable quick interventions and resource allocation
- **Predicting and forecasting the spread of outbreaks** to provide insights to better anticipate and manage the crisis

The near real-time COVID-19 trackers, for example, continuously collect big data from sources all around the world to help epidemiologists, policymakers, scientists and health professionals to make informed decisions in responding to COVID-19. Global sharing and collaboration of open data has reached unprecedented levels during these times of crisis.

Yet, unprecedented exceptional measures implemented during times of emergency or crisis bring data governance, personal data and privacy challenges. Without sufficient oversight mechanisms for checks and balances in governing the collection, use and sharing of data, there are risks of misuse of data for private gain, or of violation of rights and civil liberties.

OECD's policy response on 'Ensuring data privacy as we battle COVID-19'[117] builds on OECD data governance and privacy principles to guide data collection and sharing practices in COVID-19 responses. In particular,

- Governments need to promote the responsible use of personal data, ensuring that tools are implemented with full transparency, accountability and a commitment to cease exceptional uses of data when the crisis is over.
- Governments should work with oversight and accountability institutions to ensure sufficient checks and balances, as well as with privacy enforcement agencies to ensure appropriate safeguards are in place.
- Regulatory uncertainties regarding data protection and privacy frameworks should be addressed regarding the collection and sharing of personal data during the crisis.
- Governments should support national and international co-operation in collecting, processing and sharing personal health data for research, statistics and other health-related purposes in managing the COVID-19 crisis.
- Public engagement, participation and consultation of a wide range of stakeholders are necessary to build trust and ensure transparency and accountability.

117 OECD, "Ensuring data privacy as we battle COVID-19", 14 April 2020. https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19

BIG DATA FOR DEVELOPMENT, HUMANITARIAN ACTION AND PEACE

The United Nations Global Pulse is the UN Secretary-General's initiative on big data and artificial intelligence for development, humanitarian action and peace. UN Global Pulse works to foster global digital cooperation and realize the potential of digital technologies to advance human well-being and mitigate the risks of misuse of data and artificial intelligence, harnessed safely and responsibly for the public good.

The United Nations Development Group (UNDG) developed a **Guidance Note on Big Data for Achievement of the 2030 Agenda**[118] to address issues of data privacy, ethics and protection. This guide establishes nine common principles to support the operational use of big data for the achievement of the SDGs – including on open data, transparency and accountability. Specifically, the guidance note on big data recommends:

- Appropriate **governance and accountability mechanisms** to be established to monitor compliance with relevant laws (including privacy laws and the highest standards of confidentiality, moral and ethical conduct with regard to data use)
- **Transparency in data use** (e.g. publishing data sets or publishing an organization's data use practices or the use of algorithms)
- **Open data** as an important driver of innovation, transparency and accountability
- Conducting **risks, harms and benefits assessments** as one of the key accountability mechanisms for every use of data, to help determine the level of openness and transparency.

The guide also serves as a risk-management tool taking into account fundamental human rights and principles for obtaining, retention, use and quality control for data from the private sector.

CORRUPTION AND INTEGRITY RISKS IN BIG DATA ANALYTICS

A country's existing administrative and institutional laws, policies and processes form the foundation for data governance, management, collection, collaboration and sharing between government entities and sectors[119]. In addition, the capacity within government plays a role in how data is dealt with or used at all when looking at specific policy domains, including corruption and fraud risk management. These factors can influence the effectiveness and efficiency of big data analytics, and while they can enhance opportunities to inform anti-corruption and integrity efforts, they can also hinder these activities or even pose corruption risks, particularly in the misuse of power in data collection, privacy, protection, security, management and use. Importantly, these risks are especially significant when data pertains to individuals, with ramifications on human rights, or when analytic processing yields faulty or incorrectly interpreted results that may have wide-ranging negative consequences[120].

First, issues of data privacy, information misuse, cybersecurity threats and fraud pose huge risks in big data and data analytics. As a large amount of quality data is needed for data analytics to be meaningful, its value makes it potentially vulnerable to misuse, fraud and corruption. In particular, the public sector holds vast amounts of personal data, which is largely sensitive in nature, including data related to income and finances, health records, identification details and other political or economic information. The Cambridge Analytica scandal clearly showed us how easily personal data can be extracted and exploited for political gain.

A study[121] conducted by the Independent Broad-Based Anti-Corruption Commission in Australia (2020) found that unauthorised access and disclosure of information, or misuse of information (whether intentionally or unintentionally) by public officials, are key enablers

118 UNDG, Data privacy, ethics and protection: Guidance note on big data for the achievement of the 2030 Agenda, 2017. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf
119 OECD, Analytics for Integrity, Chapter 2.4.
120 K. Waterman and P. Bruening, "Big Data Analytics: Risks and Responsibilities". International Data Privacy Law, Volume 4, Issue 2, May 2014, Pages 89–95. https://academic.oup.com/idpl/article/4/2/89/734787
121 Independent Broad Based Anti-Corruption Commission, Victoria, Australia. Unauthorised access and disclosure of information held by the Victorian public sector, 2020. https://ibac.vic.gov.au/docs/default-source/research-documents/unauthorised-access-and-disclosure-of-information-held-by-the-victorian-public-sector.pdf?sfvrsn=d76fc48_6

of corrupt behaviour, yet they are often rated as low risk behaviours by agencies. In addition, the Association of Certified Fraud Examiners believes that 43 percent of fraud and corruption is detected by tip-offs and only 15 percent by internal audit[122].

It is vital that data privacy and the information that has been stored is properly secured and managed, as the increased reliance on technology for data collection and management also increases the risk of misuse. Moreover, once data is leaked, the source of misconduct is often challenging to identify and the data becomes impossible to retract, due to the speed at which information is disclosed and the quantity of this data. In the health sector, for example, there has been an increase in organized crime groups targeting health records and using health sector employees to leak official information, with data being used to access online banking or for other forms of extortion.

“ It is vital that data privacy and the information that has been stored is properly secured and managed, as the increased reliance on technology for data collection and management also increases the risk of misuse.”

Second, another significant risk area relates to the policy processes in which information from the data collected is used, the policy decisions made based on data analytics, and the regulatory frameworks directing data collection efforts and the sharing of information. In terms of the corruption risks associated with big data, the main issues do not lie only with the volume, velocity and variety of the generated data, but also with the analysis of the data using software and platforms to extract new and predictive knowledge for policymaking or decision-making processes[123]. Therefore, identifying and understanding the corruption risks in the processing of big data, from state capture to regulatory abuse, is necessary to mitigate the potential misuse and abuse that can occur in each of the areas. Moreover, big data analytics requires necessary analytical capabilities and skills, which many countries lack. Much of this data is also owned by private companies, limiting the potential for replication and verification.

INTERNET OF THINGS (IOT)

What is it?

The IoT is a system of interrelated and interconnected computing devices embedded in everyday objects, provided with unique identifiers and with the ability to transfer data over a network. Its applications are wide ranging, and are often categorized as consumer, commercial, industrial and infrastructure spaces. For example, a growing use of IoT devices are being created as consumer goods, including in the areas of home automation, wearable technology, health, connected vehicles and other appliances with remote monitoring capabilities.

What are some examples of corruption and fraud risks?

Since the key driver of IoT is data, the usefulness of IoT and its connecting devices is dependent on access, storage and the processing of data. Companies working on the IoT collect data from multiple sources and store it in their cloud network for further processing. Issues with **data privacy, security, ownership and protection** are thus a huge concern.

Cyberattacks are not uncommon. In fact, they are ‘accelerating at an unprecedented rate’[124], with huge implications for end-users. In 2019, a report by the cyber security and privacy company, F-Secure, ‘Attack Landscape H1 2019’[125], assessed that there had been a threefold increase in attack traffic to more than 2.9 billion events. Security researchers have attributed the increase in attacks to the increasing number of IoT devices deployed around the world. IoT devices often have weak security, making them prime targets for cybercriminals, including financially-motivated criminals[126].

122 Association of Certified Fraud Examiners, Report to the Nations. 2020. Global Study on Occupational Fraud and Abuse, 2020. https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

123 Council of Europe, “Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data”, 23 January 2017. https://rm.coe.int/16806ebe7a
A. Mantelero “Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework”, Computer Law and Security Review, Vol 33, Issue 5, October 2017, pp. 584-602. https://www.sciencedirect.com/science/article/pii/S0267364917301644

124 Z. Doffman, Cyberattacks On IOT Devices Surge 300% In 2019, “Measured In Billions”, Report Claims, 14 September 2019. https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#15c76f0c5892

125 M. Michael, “Attack Landscape H1 2019: IoT, SMB traffic abound”, F-Secure, 12 September 2019. https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

126 L. Greenemeier, “How Cryptojacking Can Corrupt the Internet of Things”. Scientific American, 31 July 2018. https://www.scientificamerican.com/article/how-cryptojacking-can-corrupt-the-internet-of-things/

CLOUD COMPUTING

What is it?

Cloud computing is the on-demand delivery of computing services and resources over the Internet (the "cloud"), including servers, storage, databases, networks, software, analytics and intelligence, without direct active management by the user. The main benefits of cloud computing are: reduced IT infrastructure costs, improved manageability and reliability, high speeds, increased productivity and efficiency and improved security from the centralization of data.

What are some examples of corruption and fraud risks?

In cloud computing, the back-end infrastructure is limited to the cloud vendor, who often decides on the management policies, and controls and manages the applications, data and services. Privacy and confidentiality remain huge concerns, especially regarding sensitive data that are non-encrypted.

Cloud computing could also be misused for fraud and corruption. An investigation by McAfee Labs and Guardian Analytics in 2012, 'Operation High Roller', revealed that cybercriminals built a sophisticated cloud-based fraud system that attempted to transfer possibly billions of dollars from targeted high-balance banking consumers and commercial accounts in banks located in Europe, Latin America and the United States. An estimated total of estimated US$78 million worth of transactions were successful[127].

REGULATORY MECHANISMS TO GOVERN THE USE OF DATA

The rapid accumulation of data in the public sector, businesses and on the internet has hugely increased risks related to personal data, human rights and accountability issues. Threats to data privacy, protection and security are of particular significance and they can jeopardize confidence and trust in new technologies. Yet, despite the increasing public distrust over issues, such as data privacy, protection and security, there is an increasing use of internet services – this is known as the privacy paradox. Online services and the Internet of Things have become such an integral part of our daily lives that even a low level of trust cannot prevent their use[128]. Thus there has been a continuously changing landscape in governing the use of data through regulation, laws and other mechanisms, both to prevent misuse and to build trust and to promote innovation in technologies that can be harnessed for the greater good.

In particular, the EU has taken significant steps in protecting consumer data with the GDPR, which requires companies to ensure they have a data consent management process. Transparency is an overarching obligation under the GDPR, requiring organizations to inform individuals about what personal data they collect and why, as well as what rights they have as data subjects. According to Zarksky (2017), the GDPR privacy regulations are trying to "balance between the ability to engage in big data analysis to its fullest extent and the protection of privacy interests and rights" (p. 1002). In addition, under the European Strategy for Data, the EU reiterates the importance of a strong legal framework – in terms of data protection, fundamental rights, safety and cyber security – both for promoting innovation and competition and for improving public services and ensuring transparency and accountable governance[129].

The GDPR has become an example for many national laws outside the EU, and many countries and states have data privacy laws similar in structure or provisions to the GDPR, such as South Korea's Personal Information Protection Act or the California Consumer Privacy Act (CCPA) in the United States. The CCPA, which went into effect in 2020, is one of the most comprehensive pieces of privacy legislation in the United States and gives residents unprecedented rights to control what information companies collect on them and how it is used. Like the GDPR, there is also a "right to delete" — with some exemptions — personal information on request.

With the growing opportunities for big data analytics, the expanding spectrum of big data and its applications, and in light of the evolution of technologies and their use, the regu-

128 EC, "Digital Transformation Monitor. Big data: a complex and evolving regulatory framework", January 2017. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Big%20Data%20v1_0.pdf

129 EC, A European strategy for data, Brussels, 19.2.20, COM(2020) 66 final. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

latory landscape will continue to evolve in the future. Governments and stakeholders will need to ensure that corruption and fraud risks are mitigated, alongside concerns over data management and use.

THE WAY FORWARD

It is important to note that for anti-corruption analytics to be meaningful and insightful in preventing and tackling corruption, several areas need to be taken into account: good quality data and analytical capabilities; relevant laws and regulations; and trust in data, systems and institutions.

First, good quality data and analytical capabilities underpin the benefits of big data analytics for anti-corruption efforts. Given that analytical platforms are designed to process data, the accuracy, relevance and usefulness of analytics depend on the quality and accuracy of the data. This underscores the importance of institutions responsible for collecting useful data, from official statistics to administrative registries, and for providing open data for appropriate use and analysis by technologists and policymakers. The risk of inaccurate data arising from its collection, aggregation, entry and management is inaccurate results, while the risk of inaccuracy within analytic processing is poor application.

Moreover, overall, government data remains concealed. According to the Global Open Data Index[130], fewer than 10 percent of government data are in an open format. Data on public contracting, which is particularly vulnerable to corruption, is especially opaque with fewer than 10 percent of the 120 countries surveyed by the Open Contracting Partnership providing quality and timely data on tenders and awards[131]. In this regard, entities such as the Open Government Partnership, help to 'ensure that governments do not become data monopolies' by pushing for open data policies and practices[132].

"Good quality data and analytical capabilities underpin the benefits of big data analytics for anti-corruption efforts."

Further, analytical capabilities and skills are necessary to harness the benefits of big data and analytical tools to identify suspicious transactions for audit or further investigation, or to inform policy decisions addressing particular corruption risks or improving resource allocation or regulations. According to the EC[133], big data and analytics are top of the list in terms of critical skills shortages. These have a significant impact on the quality of the analysis, with further implications on decision-making. As such, investments in such skills and analytics capabilities, such as within finance departments, audit institutions, regulatory bodies and anti-corruption agencies, are essential for maximizing the benefits of big data analytics in anti-corruption efforts.

Second, laws and regulations are important in governing and in promoting transparency, accountability and openness in the use of data, including its collection, storage, sharing, protection and security. With data being gathered in huge quantities at great speed due to an exponential growth in consumer and mobile technologies, the protection of data and fundamental rights are crucial in today's digital economy. For example, one of the core building blocks of the GDPR's enhanced rights for individuals is the requirement for greater transparency, where information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language[134]. In addition, accountability and data governance underpin the GDPR, requiring controllers to demonstrate and prove compliance with the data protection principles, and not just commit to those principles.

Third, there is a need to build public trust in data, systems and institutions. With threats of data breaches, identity theft, disinformation and other cybersecurity threats, the promise of new technologies and the data economy can be jeopardized by mistrust, as the downsides and risks of misuse of technologies come to prevail in society. This means that the responsible use of technology, underpinned by ethics, integrity and the protection of human rights will be crucial in building and maintaining trust in data, new technologies, systems and the institutions managing them.

130 Global Open Data Index. https://index.okfn.org/
131 G. Neumann, "Government contracts: Still a long way from open" (Blog on Open Contracting Partnership), 9 December 2015. https://www.open-contracting.org/2015/12/09/government_contracts_still_a_long_way_from_open/
132 Open Government Partnership, "A Guide to Open Government and the Coronavirus: Open Data", 4 May 2020. https://www.opengovpartnership.org/policy-area/open-data/
133 EC, A European strategy for data. https://ec.europa.eu/digital-single-market/en/european-strategy-data
134 DLA Piper, Data Protection Laws of the World. https://www.dlapiperdataprotection.com/index.html?t=world-map&c=CA

3.

RECOMMENDATIONS FOR KEY STAKEHOLDERS

In order to realize the full potential of new technologies in promoting integrity and in preventing corruption and other risks, it is important to recognize the key prerequisites for their success. These include the levels of digital infrastructure and progress made towards establishing a digital society – a tech-savvy population, with equal access and ownership of technology. Digital literacy, digitized public records, data and internet connectivity are just some of the conditions necessary to apply these technologies. For example, SDG 9.c, which states: "Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020", is particularly relevant to ensure that we 'leave no one behind'.

At the same time, legal and regulatory frameworks need to be established to prevent misuse and fraud, ensure data privacy and protection and build trust. This section lays out general and technology-specific recommendations for key stakeholders to create an enabling environment for the use and regulation of these new technologies in a way that supports integrity, trust and anti-corruption.

3.1 GENERAL RECOMMENDATIONS

Governments

1. Strengthen the capacity of law enforcement agencies and anti-corruption and oversight institutions to understand the opportunities and risks of new technologies in a national digital strategy. This strategy should have a clear implementation, coordination, regulatory, monitoring and evaluation framework and should promote innovation and inclusion, while minimizing potential risks of misuse or abuse. It should also be responsive to the changes and innovations in technology that are taking place with technological advancements.

2. Make sufficient investments:
   - Towards developing a digital knowledge society and strengthening the enabling environment, including facilitating affordable digital connectivity, ensuring adequate levels of digital interaction between government and society and reducing digital divides (including between the young and old, men and women and the rich and poor).
   - To build the digital infrastructure needed to enable AI tools, blockchain technology, big data analytics and other new technologies for anti-corruption work. Digitalization and data are prerequisites in enabling new technologies, but most developing countries do not have the level of digitalization and infrastructure necessary.
   - To develop the skills and analytical capabilities needed to deploy new technologies to detect, predict and analyse corruption data.

3. Develop guidance and procedures on the proper management and regulation of the use of data, including its collection, storage, sharing, privacy, security and protection. Provide support to institutions to standardize and collect data, from official statistics to administrative registries, to make them open for appropriate use, analysis and monitoring. Given that data underpins the benefits of new technologies, the accuracy, relevance and usefulness of analytics to strengthen anti-corruption efforts depend on the quality of the data.

4. Strengthen digital education and literacy within society so that the benefits of technologies can be harnessed for good, including strengthening equal access and ownership of technology within the population. A whole-of-government approach is necessary, where government institutions work with the private sector and also empower civil society and citizens with knowledge and information.

5. Work collaboratively with industries to ensure that regulatory compliance can be achieved, while still allowing new technologies to be used to maximum potential, including in continuous experimentation, innovation, adaptation and disruption.

Businesses

1. Set the tone at the top. Top management should ensure that ethics and integrity are built into products or processes, that collaboration is fostered in the design, development and deployment of responsible technologies and that transparency is built into technological processes.

2. Create business strategies and governance and management approaches that address ethical and rights-based standards and principles, including the responsible use of technology and data. This could include putting in place corporate business integrity policies, values, codes of ethics and guiding principles that are applied to new technologies.

3. Identify areas of business activity that could significantly benefit from the application of advanced technology and invest in them to realize their business integrity value. These might include a reduction in costs arising from fraud and supply chain corruption; reducing prosecution and reputational risks by detecting where bribery is being used with external parties; utilizing blockchain where fake goods, fraud and other supply chain risks can impact the business; and increasing revenue through enhanced customer trust, for example through environmentally-friendly product certification.

4. Strengthen transparency, accountability and integrity in business practices, which would contribute to a fair playing field for all businesses, and build a culture of ethics and integrity in the business environment.

5. Get involved in the creation of a regulatory framework to ensure that business interests are represented and to collaborate and partner with the government through public-private partnerships to pursue digital initiatives and goals. Given the knowledge and experience of industries, a close collaboration between government regulators, policymakers and the private sector is crucial in advancing the use of new technologies for integrity, trust and anti-corruption.

6. Establish industry-wide norms and standards on ethics and integrity in the use of new technologies, such as relating to steps in rolling out new technologies, starting from pilot testing to fully rolling out the application of such technologies, including continuous improvement in improving the technology, algorithms and its applications.

Civil society

1. Engage with private actors, technologists and policymakers in the development and implementation of new technologies to ensure that international human rights norms are considered and incorporated, and that the impact of these technologies on the human rights of beneficiaries are taken into account in their projects.

2. Promote the implementation of open government data initiatives, including open budgeting, open contracting and open procurement. This will promote monitoring, transparency, oversight and accountability.

3. Leverage technology in implementing civil society-led anti-corruption efforts, including crowdsourced issue reporting, corruption reporting and investigative journalism. This will encourage broad mobilization aimed at enhancing transparency in society.

4. Hold governments and technology firms accountable for practices relating to data management, collection and use, and for advocating in favour of non-discriminatory data practices, inclusion and representation of all sections of society, as well as of issues related to the privacy, protection and security of data. Civil society and communities can play an important role in advocating and implementing efforts to overcome the discriminatory biases or unethical practices embedded in data practices and in the technologies themselves.

International organizations and United Nations agencies

1. Shape global norms and standards that govern the ethical use of new technologies which supports integrity, trust and anti-corruption, including through knowledge sharing of good practices and lessons learned, building on the practices around the world. Currently, few global mechanisms are focused on tackling and minimizing the risks of misuse and abuse of new technologies, while maximizing their benefits.

2. Lead international efforts in promoting the harmonization of data, such as financial transactions, bids, contractual information, company registers, cross-border tax transfers, public spending and tax data, which will make the use of new technologies and data analytics more efficient and effective, particularly in promoting openness, transparency and accountability.

3. Foster digital cooperation among stakeholders, including by guiding them towards principles grounded in human rights and ethical values, including inclusiveness, integrity, transparency, openness, human-centredness and sustainability. Promote the responsible use of technology and data, including addressing challenges related to the misuse of data, consistent with the principles of transparency, accountability and openness.

UNDP/Shareef Sarhan

3.2 TECHNOLOGY-SPECIFIC RECOMMENDATIONS

Figure 3.1 Summary of findings and recommendations for each new technology

Opportunities	Risks and Limitations	Recommendations and Points to Note
Artificial intelligence technologies		
• Able to analyse large amounts of data to reveal complex relationships or patterns that are difficult for humans alone to identify • Allows authorities to take pre-emptive and preventive measures by picking up unusual patterns or 'red flags' and by predicting potential corrupt activities • Accelerates large amounts of data analysis that can allow humans to focus on scrutinizing potential corrupt activities and to follow up on unusual/ suspicious patterns	• Outcomes generated by AI and the usefulness of AI greatly depend on the design of the algorithm and the data used. • The complexity of 'black box' algorithms makes it impossible to explain exactly how the calculation resulting in a given output is performed. • AI-assisted procedures can also be used to facilitate corrupt activities (e.g. using AI techniques for fraud, manipulation and other illicit activities).	• Humans must first steer AI systems in the right direction when designing, developing and deploying them. Establishing strong governance and controls is critical to its safe and effective use. • Investments in good quality data are crucial to reap the benefits of AI. • Regulation is necessary to govern the responsible use of AI, including addressing issues of transparency, accountability, ethics, non-discrimination, integrity, access, inclusion and human rights.
Blockchain and distributed ledger technology		
• Able to create a transparent and accountable system where information can be verified. • Ensures a complete, public record of alterations, as transactions and documents stored on the blockchain cannot be changed or deleted, and are safe from manipulation and illegitimate changes. • Able to track the precise movement of money more accurately, and identify more easily exactly who has engaged in corrupt activities.	• Could also be misused for private gain, such as using cryptocurrency for money laundering, illegal transactions (e.g. black market) and tax evasion. • Data that is within the blockchain can hold sensitive information linked with an individual identity, which may be susceptible to cyberattacks and may also raise concerns about data privacy and the misuse of data.	• Many applications of DLT lack an appropriate legal and regulatory framework in which to operate, including a framework that deals with complex jurisdictional issues and risk and liability issues. These are barriers that governments and other stakeholders need to address. • Applicability and transferability of the instrument is limited for now, especially if there is a lack of digital infrastructure and processes to power the blockchain. Governments should make sufficient necessary investments to change existing systems and reap the benefits of blockchain.

Opportunities	Risks and Limitations	Recommendations and Points to Note
Big data analytics		
• Able to process large quantities and varieties of data to detect patterns of suspicious transactions in a wide range of areas and sectors. • Real time detection can help agencies to detect, stop and remediate fraudulent and corrupt activities. • Useful in assessing corruption risks, which would inform corruption risk mitigation actions. • Able to facilitate decisions related to monitoring, audit and investigations concerning individual transactions and organisations. • Able to transform how government entities provide public services, evaluate performance and strengthen oversight and accountability.	• Personal data can be extracted and exploited for private gain. • Vulnerabilities in the form of data privacy, information misuse, cybersecurity threats and fraud can jeopardize confidence and public trust. • Policy processes governing big data and data analytics can also be susceptible to abuse. These include the usage of data collected, policy decisions made based on data analytics, and the regulatory frameworks directing data collection efforts and the sharing of information.	• Good quality data and analytical capabilities underpin the benefits of big data analytics. The international community can play an important role in promoting open data, while governments should invest in good quality data collection, and ensure that responsible national institutions collect reliable and accurate data. • Analytical capabilities and skills are necessary to harness the benefits of big data and analytical tools. Governments and key stakeholders should invest in strengthening internal capacity and analytical skills to deploy new technologies. • Laws and regulation are important in governing and in promoting transparency, accountability and openness in the use of data, including its collection, storage, sharing, protection and security. • The responsible use of data, underpinned by ethics, integrity and the protection of human rights, will be critical in building and maintaining trust in data, new technologies, systems and the institutions managing them.

4.

CONCLUSION

In almost every domain and sector, technology has the ability to enhance efficiencies and to advance human progress and sustainable development. This study has outlined the ways in which new technologies can be used as effective tools to promote sustainable development from the perspective of integrity, trust and anti-corruption. However, these benefits can only be realized if we prevent the misuse of these technologies, mitigate the risks and challenges associated with their use and bridge the gaps that limit their effectiveness.

As demonstrated in this study, technology can be an important gamechanger in strengthening transparency, accountability and integrity. However, the complex nature of many emerging technologies may create risks and vulnerabilities, including the abuse or misuse of technologies for private gain, the lack of adequate safeguards for human rights and data protection and the widening digital divide.

"Digital infrastructure and effective digital governance, which promote accountability, ethics and integrity, are necessary to create a sustainable impact in this policy space, build trust and maximize the benefits for all, as we progress towards 2030."

What is essential is thus to recognize and address the risks, limitations and challenges that exist to effectively harness the benefits of new technologies for integrity and anti-corruption, and to accelerate efforts on sustainable development. In this regard, digital infrastructure and effective digital governance, which promote accountability, ethics and integrity, are necessary to create a sustainable impact in this policy space, build trust and maximize the benefits for all, as we progress towards 2030.

4.1 KEY TAKEAWAYS

The key takeaways of the study are therefore as follows:

- **Technology is an important tool in enhancing anti-corruption efforts,** not only in promoting increased transparency, accountability, openness, accessibility and citizen participation, but also in its potential to detect, analyse, predict, and therefore deter and prevent corruption. To harness its full potential, the application of technology for anti-corruption efforts should also take into account a major lesson learned: technology alone cannot solve corruption, which is also dependent on the wider political economy context and requires ethics and integrity to be embedded in systems, institutions and society.

- **Effective digital governance is necessary to ensure ethics and integrity in the use of new technologies,** including data-driven digital transformations and data quality management. The outcomes generated by technologies such as AI highly depend on the design and implementation of the algorithm and data used. These will generate outcomes that are inherently biased to some extent, whether systemic or random. In that regard, governments and policymakers need to work together with the systems and technologists and data scientists to produce data and services that ensure ethics and integrity are built in.

- **Along with the need to encourage innovation and the application of new technologies, there is an increasingly clear recognition that regulation is necessary to govern the responsible use of technologies and data.** This includes integrating the principles of transparency, accountability, non-discrimination, integrity, access, inclusion and human rights. Regulation is crucial to protect users and ensure security, but it should also create an environment that is conducive to continuous innovation. Without appropriate legal and regulatory frameworks in which technologies operate, the usefulness of technology may be limited or susceptible to abuse at the hands of those who design them. Therefore, through digital governance, governments have a crucial role to play in guiding technological change proactively alongside technologists and other stakeholders, a much different approach to traditional decision-making and policymaking processes.

Photo: Unsplash

- **While, on the one hand, digital technologies can play a key role in driving transparency, on the other hand, we need to build trust in the technology sector.** From the perspectives of integrity and trust, technology and anti-corruption measures have a mutually reinforcing relationship: technology for integrity and trust; and integrity and trust for technology. The ability of digital technologies to create platforms for data transparency and open information, which are useful for monitoring services, improving products and improving citizen engagement, can help build trust. Yet, privacy and security breaches, with wide-ranging implications for human rights and accountability, have led to declines in trust, not only in technology products but also in the technology sector.

- **Participatory approaches to digital governance, including public engagement, dialogue and consultation** of a wide range of stakeholders, particularly between technology and digital solution providers, regulators and oversight institutions and users of digital technologies, are necessary to build trust, safeguard human rights and ensure accountability. In addition, promoting a 'culture of openness' is important alongside promoting a 'culture of innovation'. Open resources, processes and standards can drive the internet ecosystem and promote continuous technology-based innovation globally.

- **Good quality data is necessary to provide meaningful insight, information and intelligence in any area of interest.** However, the wide-ranging opportunities and applications of data must be balanced with its ethical use, including measures to ensure data privacy and protection in its collection, storage, sharing and management. Addressing these issues would promote trust in digital systems and encourage innovation.

- **Investments in digital infrastructure need to be in place in order to reap the benefits of new technologies, accompanied by a strong political commitment to change existing systems and mechanisms.** To promote advancement in technologies, all technologies need to undergo experimentation, innovation, adaptation and a process of disruption. These require sustained and significant investments in order to turn disruptions into positive change.

- **Digital transformations should ensure inclusive, people-centred and human rights-based social contracts built on accountability and trust.** The widening digital divides between developed and developing countries, urban and rural areas, the rich and poor and men and women – such as in the capabilities for harnessing digital data and new technologies, or in the basic opportunities to participate in digital society – threaten to exacerbate inequalities and leave developing countries even further behind. Digital education and digital literacy are thus necessary, including strengthening equal access and ownership of technology within populations, so that no one is left behind.

REFERENCES

Aarvik, P. Blockchain as an anti-corruption tool: Case examples and introduction to the technology. Anti-Corruption Resource Centre, CMI Chr. Michelsen Institute, Norway. U4 Report 2020:7. https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf

------. Artificial Intelligence – a promising anti-corruption tool in development settings? Anti-Corruption Resource Centre, CMI Chr. Michelsen Institute, Norway. U4 Report 2019:1. https://www.u4.no/publications/artificial-intelligence-a-promising-anti-corruption-tool-in-development-settings.pdf

Adler, D. "Silk Road: The Dark Side of Cryptocurrency" (Blog). Fordham Journal of Corporate and Financial Law, 21 February 2018. https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/

Aggarwal, N. and Floridi, L. "The Opportunities and Challenges of Blockchain in the Fight against Government Corruption" (Feature Article in the 19th General Activity Report (2018) of the Council of Europe Group of States against Corruption (GRECO), adopted by GRECO 82 (18-22 March 2019)). Digital Ethics Lab, Oxford Internet Institute. https://www.oii.ox.ac.uk/wp-content/uploads/2019/06/Blockchain-and-Corruption-GRECO-article_AggarwalFloridi.pdf

Allison, I. "Singapore Announces New AML Rules for Crypto Businesses", Coindesk, 20 January 2020. https://www.coindesk.com/singapore-announces-new-aml-rules-for-crypto-businesses

Angelico, F. "Brazil: Open data just made investigating corruption easier". Transparency International. 12 May 2017. https://www.transparency.org/news/feature/brazil_open_data_just_made_investigating_corruption_easier

Angwin, J., Larson J., Mattu S., and Kirchner L. "Machine bias". Pro Publica, 23 May 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

ARTICLE 19. Blockchain and freedom of expression. London: ARTICLE 19, 2019. https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf

Artificial Intelligence Index Report 2019. Stanford University Human Centered Artificial Intelligence. https://hai.stanford.edu/research/ai-index-2019

Association of Certified Fraud Examiners. Report to the Nations 2020. Global Study on Occupational Fraud and Abuse. 2020. https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Bashir, I. "The growth of blockchain technology" in Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition. Birmingham, UK: Packt Publishing, March 2018. https://subscription.packtpub.com/book/big_data_and_business_intelligence/9781788839044/1/ch01lvl1sec10/the-growth-of-blockchain-technology

Berliner, D. and Dupuy, K. The promise and perils of data for anti-corruption efforts in international development work. Anti-Corruption Resource Centre. CMI Chr. Michelsen Institute, Norway. U4 Brief 2018:7. https://www.u4.no/publications/the-promise-and-perils-of-data-for-anti-corruption-efforts-in-international-development-work.pdf

Bitfury. "The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project". 2016. https://bitfury.com/content/downloads/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf

Busetto, B. and Timilsina, A. "The role of technology and anti-corruption measures in fighting COVID-19" (Blog) UNDP, 15 September 2020. https://www.undp.org/content/undp/en/home/blog/2020/the-role-of-technology-and-anti-corruption-measures-in-fighting-.html

Carson, B., Romanelli, G., Walsh, P. and Zhumaev, A. Blockchain beyond the hype: What is the strategic business value? McKinsey Digital, 19 June 2018. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Chen, S. “Is China’s corruption-busting AI system ‘Zero Trust’ being turned off for being too efficient?” South China Morning Post, Hong Kong, 4 February 2019. https://www.scmp.com/news/china/science/article/2184857/chinas-corruption-busting-ai-system-zero-trust-being-turned-being

Christian, J. “China built an AI to detect corruption and officials shut it down”. The Byte, 4 January 2019. https://futurism.com/the-byte/china-ai-corruption

ConsenSys. “Gartner: Blockchain Will Deliver $3.1 Trillion Dollars in Value by 2030”. 6 June 2019. https://media.consensys.net/gartner-blockchain-will-deliver-3-1-trillion-dollars-in-value-by-2030-d32b79c4c560

Copeland, M. “What’s the Difference Between Artificial Intelligence, Machine Learning and Deep Learning?” NVIDIA, 29 July 2016. https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/

Corruption Research Center Budapest https://www.crcb.eu/

Cosgrove, B. “8 ways to ensure your company’s AI is ethical”. World Economic Forum, The Davos Agenda, 16 January 2020. https://www.weforum.org/agenda/2020/01/8-ways-to-ensure-your-companys-ai-is-ethical/

Council of Europe. “Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data”. 23 January 2017. https://rm.coe.int/16806ebe7a

De Silva, M. “Bitcoin money laundering is a classically dumb crime”. Quartz, 5 December 2019. https://qz.com/1761343/bitcoin-money-laundering-is-a-classically-stupid-crime/

Deloitte. 5 Blockchain Trends for 2020. March 2020. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Consulting/Blockchain-Trends-2020-report.pdf

------. “AI ethics: A business imperative for boards and C-suites”. https://www2.deloitte.com/us/en/pages/regulatory/articles/ai-ethics-responsible-ai-governance.html

------. “Blockchain and GDPR: from practice to theory and back”. https://www2.deloitte.com/nl/nl/pages/legal/articles/blockchain-and-gdpr-from-practice-to-theory-and-back.html

------. Global Blockchain Survey 2019. https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

Dhameja, G. “UN World Food Programme uses Parity Ethereum to aid 100,000 refugees”. 18 February 2019. https://www.parity.io/un-world-food-programme-uses-parity-ethereum-to-aid-100-000-refugees/

DLA Piper. “Data Protection Laws of the World”. https://www.dlapiperdataprotection.com/index.html?t=world-map&c=CA

Doffman, Z. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data”. Forbes, 14 September 2019. https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#15c76f0c5892

Elliptic. “Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act)”. 18 September 2019. https://www.elliptic.co/our-thinking/bitcoin-money-laundering

European Commission. White Paper “On Artificial Intelligence – A European approach to excellence and trust”. Brussels. 19 February 2020, COM(2020) 65, Final https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

------. Shaping Europe's digital future. Ethics guidelines for trustworthy AI. 8 April 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

------. Communication from the Commission to the European Council, the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European strategy for data". 19 February 2020. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

_____. A European strategy for data, Brussels, 19.2.20, COM(2020) 66 final. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

------. "Digital Transformation Monitor. Big data: a complex and evolving regulatory framework". January 2017. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Big%20Data%20v1_0.pdf

------. Shaping Europe's digital future. "High-Level Expert Group on Artificial Intelligence (AI HLEG". 18 November 2020. https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

------. Finland AI Strategy Report. 2020. https://ec.europa.eu/knowledge4policy/ai-watch/finland-ai-strategy-report_en#aistrategy

European Union. Elements of AI, Finland. https://www.elementsofai.com/eu2019fi

Fanning, B. "The Future of Work is Coming. FS leaders admit they are no ready". Accenture, 2 April 2019. https://talentorganizationblog.accenture.com/financialservices/the-future-of-work-is-coming-fs-leaders-admit-they-are-not-ready

Foley, S., Karlsen, J. and Putnins, T. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?" The Review of Financial Studies, Volume 32, Issue 5, May 2019, Pages 1798–1853. https://academic.oup.com/rfs/article/32/5/1798/5427781

GIZ.The potential of distributed ledger technologies in the fight against corruption, April 2020. https://www.giz.de/en/downloads/Blockchain_Anticorruption-2020.pdf

------. "Blockchain for Sustainable Development: Promising use cases for the 2030 Agenda". 2019. https://www.giz.de/en/downloads/giz2019-EN-Blockchain-Promising-Use-Cases.pdf

------. "Concept Note. Land registries on a distributed ledger". 2019 https://www.giz.de/en/downloads/giz2019-en-distributed-land-registry.pdf

------. Embracing Digitalization: How to use ICT to strengthen Anti-Corruption. March 2018. https://www.giz.de/de/downloads/giz2018-eng_ICT-to-strengthen-Anti-Corruption.pdf

Government of Singapore. Compendium of Use Cases: Practical Illustrations of the Model AI Governance Framework. 2020. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGAIGovUseCases.pdf

------. Personal Data Protection Commission. "Model AI Governance Framework". 2019. https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework
------. Infocom Media Development Authority. Personal Data Protection Commission. Model Artificial Intelligence Governance Framework. Second Edition. 21 January 2020. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGov-Framework2.pdf

------. Smart Nation Singapore. National Artificial Intelligence Strategy. Advancing our Smart Nation Journey. November 2019. https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4

Global Open Data Index. Tracking the State of Open Government Data. https://index.okfn.org/

Global Partnership for Sustainable Development Data. http://www.data4sdgs.org/

Granickas, K. "Learning insights: The latest impacts emerging from Ukraine's Prozorro reforms". Open Contracting Partnership, 12 January 2018. https://www.open-contracting.org/2018/01/12/learning-insights-latest-impacts-emerging-ukraines-prozorro-reforms/

Grant Thornton India LLP. Public sector delivery mechanisms: Success story of Madhya Pradesh. https://www.grantthornton.sg/globalassets/1.-member-firms/india/assets/pdfs/public_sector_delivery_mechanism_mp.pdf

Greenemeier, L. “How Cryptojacking Can Corrupt the Internet of Things”. Scientific American, 31 July 2018. https://www.scientificamerican.com/article/how-cryptojacking-can-corrupt-the-internet-of-things/

Greenman, S. “Governments must build trust in AI to fight COVID-19 – Here’s how they can do it”. World Economic Forum. 21 April 2020 https://www.weforum.org/agenda/2020/04/governments-must-build-trust-in-ai-to-fight-covid-19-here-s-how-they-can-do-it

Group of Twenty (G20). Ministerial Statement on Trade and Digital Economy. https://www.mofa.go.jp/files/000486596.pdf

Handforth, C. “What Singapore can teach about an effective coronavirus response” (Blog). UNDP, 25 March 2020. https://www.undp.org/content/undp/en/home/blog/2020/what-singapore-can-teach-about-an-effective-coronavirus-response.html

Hileman, G. and Rauchs, M. Global Blockchain Benchmarking Study. Cambridge Centre for Alternative Finance. University of Cambridge Judge Business School. 2017. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-global-blockchain-benchmarking-study-2017.pdf

IBM. Fighting financial crime with AI. 2019. https://www.ibm.com/downloads/cas/WKLQKD3W

Independent Broad Based Anti-Corruption Commission, Victoria, Australia. Unauthorized access and disclosure of information held by the Victorian public sector. February 2020. https://ibac.vic.gov.au/docs/default-source/research-documents/unauthorised-access-and-disclosure-of-information-held-by-the-victorian-public-sector.pdf?sfvrsn=d76fc48_6

Joshi, N. “Why regulatory compliance can be complicated and how AI can simplify it”. Forbes. 22 July 2019. https://www.forbes.com/sites/cognitiveworld/2019/07/22/why-regulatory-compliance-can-be-complicated-and-how-ai-can-simplify-it/#400cc55e377e

Kenyon, H. “Privacy ‘poisoning’ poses threat to companies using blockchain”. PhysOrg, 10 April 2019. https://phys.org/news/2019-04-privacy-poisoning-poses-threat-companies.html#:~:text=Known%20as%20privacy%20%22poisoning%2C%22,in%20conflict%20with%20local%20laws.

KfW Development Bank. “Blockchain creates more transparency in development cooperation.” 17 December 2018. https://www.kfw.de/KfW-Group/Newsroom/Latest-News/Pressemitteilungen-Details_500800.html

------. “TruBudget Project Information”. 2018. https://www.kfw-entwicklungsbank.de/PDF/Entwicklungsfinanzierung/Themen-NEU/Digitalisierung/2018_TruBudget.pdf

------. TruBudget. https://openkfw.github.io/trubudget-website/

Kim, K. and Kang T. “Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology” https://www.semanticscholar.org/paper/Does-Technology-Against-Corruption-Always-Lead-to-Kim-Kang/766de80c483ccfbd56936cc03ec82f58760284c0

Lopez-Iturriaga, F. and Pastor-Sanz, I. “Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces”. SSRN. 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075828

Malik, T. “Big data can shame grand corruption”. The Express Tribune, Pakistan. 28 May 2016. https://tribune.com.pk/story/1112068/big-data-can-shame-grand-corruption

Malta Chamber. “Employers In Malta Will Soon Be Able To Verify Skills And Credentials Through Blockchain”. 21 February 2019. https://www.maltachamber.org.mt/en/employers-in-malta-will-soon-be-able-to-verify-skills-and-credentials-through-blockchain

Mantelero, A. “Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework”. Computer Law and Security Review, Vol. 33, Issue 5, October 2017, pp. 584-602. https://www.sciencedirect.com/science/article/pii/S0267364917301644

Mazrekaj, D., Schiltz, F. and Titl, V. “Identifying politically connected firms: a machine learning approach”. 2019 OECD Global Anti-Corruption and Integrity Forum, 20-21 March 2019. https://www.oecd.org/corruption/integrity-forum/academic-papers/Mazkeraj-Machine-Learning.pdf

McKinlay, J., Pithouse, D., McGonagle, J. and Sanders, J. “Blockchain: background, challenges and legal issues”. DLA Piper, 2 February 2018. https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/

McKinsey Global AI Survey 2019.
https://www.mckinsey.com/featured-insights/artificial-intelligence/global-ai-survey-ai-proves-its-worth-but-few-scale-impact

Micallef, K. “Malta begins multiyear roll out of Blockcerts”. AIBC Europe, 26 February 2019.
https://maltablockchainsummit.com/news/malta-begins-multiyear-roll-out-of-blockcerts/

Michael, M. “Attack Landscape H1 2019: IoT, SMB traffic abound”. F-Secure, 12 September 2019.
https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

Nelson, D. “Crypto Criminals Have Already Stolen $1.4B in 2020, Says CipherTrace”. COINDESK, 2 June 2020. https://www.coindesk.com/crypto-criminals-have-already-stolen-1-4b-in-2020-says-ciphertrace

Neumann, G. “Government contracts: Still a long way from open” (Blog on Open Contracting Partnership). 9 December 2015. https://www.open-contracting.org/2015/12/09/government_contracts_still_a_long_way_from_open/

Open Government Partnership. “A Guide to Open Government and the Coronavirus: Open Data”. 4 May 2020. https://www.opengovpartnership.org/policy-area/open-data/

Organisation for Economic Co-operation and Development (OECD). “Ensuring data privacy as we battle COVID-19”. 14 April 2020. https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g-82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19

------. “Forty-two countries adopt new OECD Principles on Artificial Intelligence” 22 May 2019.
https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

------. Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments. OECD, 2019. https://www.oecd.org/gov/ethics/analytics-for-integrity.pdf

------. The Policy Environment for Blockchain Innovation and Adoption. 2019 OECD Global Blockchain Policy Forum Summary Report. OECD, 2019. http://www.oecd.org/finance/2019-OECD-Global-Blockchain-Policy-Forum-Summary-Report.pdf

------. “OECD Open Government, DoZorro Case Study,” 2018. https://oecd-opsi.org/innovations/dozorro/

------. Blockchain Technology and Corporate Governance (DAF/CA/CG/RD(2018)1/REV1). Directorate for Financial and Enterprise Affairs, Corporate Finance Committee, 6 June 2018.
https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/CA/CG/RD(2018)1/REV1&docLanguage=En

------. “What are the OECD Principles on AI?” https://www.oecd.org/going-digital/ai/principles/

Petheram, A. and Asare, I. “From open data to artificial intelligence: the next frontier in anti-corruption”. Oxford Insights. 27 July 2018. https://www.oxfordinsights.com/insights/aiforanticorruption

Oprunenco, A. and Akmeemana, C. “Using blockchain to make land registry more reliable in India” (Blog). UNDP, 1 May 2018. https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html

PricewaterhouseCoopers. “Gaining National Competitive Advantage through Artificial Intelligence (AI)”. 2019. https://www.pwc.lu/en/advisory/digital-tech-impact/technology/gaining-national-competitive-advantage-through-ai.html

Privacy International and ARTICLE 19. Privacy and Freedom of Expression In the Age of Artificial Intelligence. April 2018. https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf

Salmon, J. and Myers, G. “Blockchain and Associated Legal Issues for Emerging Markets”. International Finance Corporation. EM Compass Emerging Markets. Note 63, JAN 2019. https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F

Sanburn, J. “How Exactly Do Cyber Criminals Steal $78 Million?” Time, 3 July 2012. https://business.time.com/2012/07/03/how-exactly-do-cyber-criminals-steal-78-million/

Sayers, S. Code to Integrity. Ministry of Foreign Affairs of Denmark, 2018. https://um.dk/~/media/UM/English-site/Documents/News/Code%20to%20Integrity_EnkeItsider_Web.pdf?la=en

Schwab, K. “The Fourth Industrial Revolution: what it means, how to respond”. World Economic Forum. 14 January 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Shield FC. “Moving Compliance Forward”. https://www.shieldfc.com/

Skeet, A. and Guszcza, J. “How businesses can create an ethical culture in the age of tech”. World Economic Forum. 7 January 2020. https://www.weforum.org/agenda/2020/01/how-businesses-can-create-an-ethical-culture-in-the-age-of-tech

Smith, A. “How the World Food Programme uses blockchain to better serve refugees” ITU News, 11 April 2019. https://news.itu.int/how-the-world-food-programme-uses-blockchain-to-better-serve-refugees/

Smith, J., Robert, N. and Bitro P. “Automation is the future of fraud risk management”. Deloitte. https://www2.deloitte.com/in/en/pages/finance/articles/automation-is-the-future-of-fraud-risk-management.html

Sookman, B. “COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic”. 14 April 2020. https://www.mccarthy.ca/en/insights/blogs/techlex/covid-19-and-privacy-artificial-intelligence-and-contact-tracing-combatting-pandemic#page=1

Statista. “Volume of data/information created worldwide from 2010 to 2024”. 2020. https://www.statista.com/statistics/871513/worldwide-data-created/#statisticContainer

Tan, T. “Tapping AI to battle Covid-19” .The Straits Times, Singapore, 29 April 2020. https://www.straitstimes.com/tech/tapping-ai-to-battle-covid-19

The Partnership on AI. https://www.partnershiponai.org/

Transparency International. Bitcoin, Blockchain and Corruption: An overview. 2018. https://knowledgehub.transparency.org/helpdesk/bitcoin-blockchain-and-corruption-an-overview
Transparency International Ukraine. “DoZorro artificial intelligence to find violations in ProZorro: How it works”. 2018. https://ti-ukraine.org/en/news/dozorro-artificial-intelligence-to-find-violations-in-prozorro-how-it-works/

U-Hopper. “3 mega trends driving the Digital Transformation”. https://blog.u-hopper.com/2020/01/10/mega-trends-digital-transformation/

United Nations Conference on Trade and Development (UNCTAD). Digital Economy Report 2019. https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

United Nations Development Programme (UNDP). Beyond Recovery: Towards 2030. 2020. https://www.undp.org/content/undp/en/home/librarypage/hiv-aids/beyond-recovery--towards-2030.html

------. Recovering from COVID-19: Lessons from past disasters in Asia and the Pacific. 2020. https://www.undp.org/content/undp/en/home/librarypage/crisis-prevention-and-recovery/recovering-from-COVID-19-lessons-from-past-disasters-in-asia-pacific.html

------. Transparency, Accountability and Anti-Corruption Service Offer for COVID-19 Response and Recovery. 2020. https://www.undp.org/content/undp/en/home/librarypage/democratic-governance/anti-corruption/transparency--accountability-and-anti-corruption-service-offer-f.html

------. Integrating Transparency, Accountability and Anti-Corruption in Socio-Economic Impact Analyses, Needs Assessment and Response to the COVID-19 Pandemic. 2020. https://www.undp.org/content/undp/en/home/librarypage/democratic-governance/anti-corruption/integrating-transparency--accountability-and-anti-corruption-in-.html

------. Corruption and Development: A Primer. 2008. http://www.undp.org/content/undp/en/home/librarypage/democratic-governance/anti-corruption/corruption.html

------. “Beyond bitcoin: Using blockchain to advance the SDGs”. https://feature.undp.org/beyond-bitcoin/

------. “UNDP Digital Strategy”. https://digitalstrategy.undp.org

------. “UNDP Innovation Facility”. https://www.undp.org/content/undp/en/home/2030-agenda-for-sustainable-development/partnerships/sdg-finance--private-sector/innovation.html

------. UNDP Strategic Plan 2018-2021. https://strategicplan.undp.org/

UNDP Malawi. “Promoting E-payment systems as a COVID-19 Preventative Strategy”. UNDP Digital Responses to COVID-19. https://airtable.com/shrGXLJECotnZa1Ou/tblwPhDJfiisTMNg6/viwRoWh6lu99wyzz7/rec1n5BVkcc5iiU3O?blocks=bipVDslkfppjON6Dh

UNDP Seoul Policy Centre for Knowledge Exchange through SDG Partnerships, “Public Information Disclosure on COVID-19”. 22 April 2020. https://www.undp.org/content/seoul_policy_center/en/home/presscenter/articles/2019/Collection_of_Examples_from_the_Republic_of_Korea/covid-public-information-disclosure.html

UNDP Serbia. “How is UNDP helping Serbia fight the coronavirus epidemic”, 31 March 2020. https://www.rs.undp.org/content/serbia/en/home/presscenter/articles/2020/kako-undp-poma_e-srbiji-u-borbi-sa-epidemijom-korona-virusa.html

United Kingdom Government Digital Service (GDS). Government Digital Marketplace Programme. https://www.digitalmarketplace.service.gov.uk/

United Nations Educational, Scientific and Cultural Organization (UNESCO). Ad Hoc Expert Group (AHEG) for the Preparation of a Draft text of a Recommendation the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000373434

United Nations Secretary-General’s Task Force on Digital Financing of the Sustainable Development Goals. People’s Money: Harnessing Digitalization to Finance a Sustainable Future (Final Report). August 2020. https://unsdg.un.org/sites/default/files/2020-08/DF-Task-Force-Full-Report-Aug-2020-1.pdf

United Nations. United Nations Activities on Artificial Intelligence (AI). 2019. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2019-1-PDF-E.pdf

------. The Age of Digital Interdependence. Report of the UN Secretary-General’s High-level Panel on Digital Cooperation. 2019. https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf

United Nations Office on Drugs and Crime (UNODC). United Nations Convention against Corruption (UNCAC). https://www.unodc.org/unodc/en/corruption/uncac.html

U.S. Congress, H.R.2231. “The Algorithmic Accountability Act of 2019”. 116th Congress, First Session, 10 April 2019. https://www.congress.gov/bill/116th-congress/house-bill/2231/text

U.S. National Science and Technology Council. “National Artificial Intelligence Research and Development Strategic Plan: 2019 Update”. June 2019. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

United Nations Development Group. Data privacy, ethics and protection: Guidance note on big data for the achievement of the 2030 Agenda. 2017. https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

United Nations Secretary-General’s Special Advocate for Inclusive Finance for Development. (UNSGSA) FinTech Working Group and Cambridge Centre for Alternative Finance. Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes and RegTech. 2019.

https://responsiblefinanceforum.org/publications/early-lessons-regulatory-innovations-enable-inclusive-fintech-innovation-offces-regulatory-sandboxes-regtech/

United Nations World Data Forum 2018. “Data for policy action: Using big data to drive development for all”. https://unstats.un.org/unsd/undataforum/dubai-2018/sessions/ta3-07-data-for-policy-action-using-big-data-to-drive-development-for-all/

Visser, C. and Hanich, Q. (2018) “How blockchain is strengthening tuna traceability to combat illegal fishing” 201 (2018) 22 January, The Conversation 1-4, University of Wollongong, Australia. https://theconversation.com/how-blockchain-is-strengthening-tuna-traceability-to-combat-illegal-fishing-89965

Waterman, K. and Bruening, P. “Big Data Analytics: Risks and Responsibilities”. International Data Privacy Law, Volume 4, Issue 2, May 2014, Pages 89–95. https://academic.oup.com/idpl/article/4/2/89/734787

Watson, G. “Malta first to introduce Blockcerts for academic credentials”. Newsbook, 21 February 2019. https://newsbook.com.mt/en/malta-first-to-introduce-blockcerts-for-academic-credentials/

Wellers, D. “Is this the future of the Internet of Things”. World Economic Forum. 27 November 2015. https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things/?utm_content=buffer10b03&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Whitelaw, S., Mamas, M., Topol, E. and Van Spall, H. “Applications of digital technology in COVID-19 pandemic planning and response”. The Lancet. 29 June 2020. https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30142-4/fulltext

Whiting, K. “Blockchain could police the fishing industry - here’s how”. World Economic Forum. 12 February 2020. https://www.weforum.org/agenda/2020/02/blockchain-tuna-sustainability-fisheries-food-security/

World Bank. “Madhya Pradesh Citizen Access to Responsive Services Project”. 2016 (approval date). https://projects.worldbank.org/en/projects-operations/project-detail/P149182?lang=en

World Economic Forum. Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption. 17 June 2020. https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption

------. Companion to the Model AI Governance Framework – Implementation and Self-Assessment Guide for Organizations (Prepared in collaboration with the Info-communications Media Development Authority of Singapore). January 2020. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf

------. White Paper. A Framework for Developing a National Artificial Intelligence Strategy. Centre for Fourth Industrial Revolution. August 2019. http://www3.weforum.org/docs/WEF_National_AI_Strategy.pdf

------. “Governing the Coin: World Economic Forum Announces Global Consortium for Digital Currency Governance”. 24 January 2020. https://www.weforum.org/press/2020/01/governing-the-coin-world-economic-forum-announces-global-consortium-for-digital-currency-governance/

World Food Programme. Innovation Accelerator. “Building Blocks: Blockchain for Zero Hunger”. https://innovation.wfp.org/project/building-blocks

World Wildlife Fund (WWF). “New blockchain project has potential to revolutionise seafood industry”. 8 January 2018. https://wwf.panda.org/?320232/New-Blockchain-Project-has-Potential-to-Revolutionise-Seafood-Industry

WWF-New Zealand. “Blockchain Tuna Project”. https://www.wwf.org.nz/what_we_do/marine/blockchain_tuna_project/

United Nations Development Programme
One United Nations Plaza
New York, NY 10017

www.undp.org