STUDY

Requested by the CONT Committee

The future of digitalisation in budgetary control

Policy Department for Budgetary Affairs
Directorate-General for Internal Policies
PE 759.623 – February 2024

EN

The future of digitalisation in budgetary control

Abstract

This study, commissioned by the European Parliament's Committee on Budgetary Control, explores new technological developments that are being or could be applied in the field of budgetary control and how these could be used to enhance the prevention of fraud and corruption and ensure sound financial management of EU funds. New technological developments covered by the study include big data analytics, artificial intelligence, digital platforms, robotic process automation, distributed ledger technologies (blockchain) and satellite imagery.

This document was requested by the European Parliament's Committee on Budgetary Control.

AUTHORS

James RAMPTON, Centre for Strategy & Evaluation Services LLP (CSES)
Marta DIMAURO, Centre for Strategy & Evaluation Services LLP (CSES)
Christine STEDTNITZ, Centre for Strategy & Evaluation Services LLP (CSES)
Jana VENCOVSKÁ, Centre for Strategy & Evaluation Services LLP (CSES)
Laura GRANITO, Centre for Strategy & Evaluation Services LLP (CSES)
Vítezslav TITL, Utrecht University School of Economics

ADMINISTRATORS RESPONSIBLE

Alexandra POUWELS, András SCHWARCZ

EDITORIAL ASSISTANT

Adrienn BORKA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Budgetary Affairs
European Parliament
B-1047 Brussels
Email: Poldep-Budg@ep.europa.eu

Manuscript completed in February 2024

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

AFCOS	Anti-fraud coordination service
AI	Artificial Intelligence
BIEP	Benchmarking Information Exchange Project
BUDG	European Parliament Committee on Budgets
CAFS	European Commission's Anti-Fraud Strategy
CAP	Common Agricultural Policy
CONT	European Parliament Committee on Budgetary Control
CPR	Common Provisions Regulation
CSO	Civil society organisation
DG AGRI	European Commission Directorate-General for Agiculture
DG BUDG	European Commission Directorate-General for Budget
DG ECFIN	European Commission Directorate-General for Economic and Financial Affairs
DG EMPL	European Commission Directorate-General for Employment, Social Affairs and Inclusion
DG REGIO	European Commission Directorate-General for Regional and Urban Policy
DL	Deep Learning
ECA	European Court of Auditors
ECOFIN	Economic and Financial Affairs Council configuration
EDES	Early Detection and Exclusion System
EMPL	European Commission Directorate-General for Employment, Social Affairs and Inclusion
EPPO	European Public Prosecutor's Office
ERDF	European Regional Development Fund
ESF	Department for Work and Pensions for European Social Fund
ESIF	European Structural and Investment Funds
EU	European Union

FPDNet	Fraud Prevention and Detection Network
GDP	Gross Domestic Product
IA	Intelligent Automation
IMS	Integrated Management System
IT	Information technologies
LLM	Large Language Model
MA	Managing Authority
ML	Machine Learning
MOOC	Massive Open Online Course
NGO	Non-governmental organisation
NLP	Natural Language Processing
OCR	Optical Character Recognition
OLAF	European Anti-Fraud Office
RPA	Robotic Process Automation
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
USA	United States of America
VAT	Value Added Tax

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Introduction

This study has explored recent new technological developments in budgetary control, what new developments can be expected and how these could be used to protect the EU's budget by preventing fraud and ensuring sound financial management. New technologies include AI-powered systems, machine learning, large language models, big data, and robotic process automation. The study has assessed the advantages and limitations of these technologies, as well as factors (including data privacy, legal requirements, technical and cost issues) that facilitate or hinder their uptake and successful use for EU funds under different management modes.

The findings in this study draw on evidence from a review of literature and websites, interviews of EU bodies (European Commission, European Anti-Fraud Office, European Public Prosecutor's Office), a survey of public budgetary authorities which attracted 75 responses, and interviews of 39 national and regional authorities, universities and NGOs. The study particularly focused on technologies used at EU level and in a sample of eight EU Member States (Czechia, Germany, Hungary, Italy, Poland, Portugal, Romania, Sweden) and two non-EU countries (UK, USA).

Context for digitalisation in budgetary control

The misuse of EU funds remains a serious problem, with Member States reporting a total of 12,455 irregularities, amounting to EUR 1.77 billion, in 2022.[1] In this context, budgetary authorities have increasingly used new digital technologies to protect the EU budget. For example, digital tools operated by the European Commission help identify risks of irregularities:

- Arachne is a risk-scoring tool used by managing authorities (MAs) on a voluntary basis to detect risks of fraud and irregularities in the use of European Structural and Investment Funds. By combining data from MAs with data about companies, politically exposed persons and sanction lists, Arachne computes risks such as bankruptcy, criminal convictions or conflicts of interest. However, Arachne is limited by low awareness of the tool, privacy concerns, a high administrative burden, limited accessibility, inaccurate risk scores, and a high number of false positives.
- The Early Detection and Exclusion System (EDES) is a database allowing EU bodies to flag financial risks posed by (potential) recipients of EU funds. The EDES currently has limited reach, given that it does not apply to funds under shared management. However, the proposed new Financial Regulation includes a targeted extension to all management modes from 2028. In addition, a new web service would allow for fast checks of any economic operator.
- The Irregularity Management System (IMS) is a database within which Member States report irregularities in the management of EU funds. The IMS is valued by those MAs that use it but its utility is limited by the substantial variation in reporting practices across Member States.

New technologies currently used in budgetary control

New technologies currently used to improve budgetary control practices include big data analytics, artificial intelligence (AI), machine learning (ML), natural language processing (NLP), deep learning (DL), large language models (LLMs), robotic process automation (RPA), blockchain, and satellite imagery. Many of these technologies are inter-connected.

[1] OLAF PIF Report 2022, section 4.1.

Some of the most important technological developments in budgetary control are in the field of AI. AI is a broad term that refers to the science of teaching machines to mimic human intelligence and perform human cognitive functions like problem-solving and learning. Machine learning, natural language processing, deep learning and large language models technologies are subfields of AI that leverage and build upon each other.

- ML is a core subfield of AI and is referred to as predictive modelling. Its purpose is to teach machines to learn from data, to describe data, to identify patterns and to make predictions based on data. ML is dependent on human intervention to teach a computer to perform tasks.
- DL is a powerful subset of ML and requires less human intervention. It uses neural networks, inspired by the human brain, to learn from data and improve the accuracy of their predictions.
- NLP is another subfield of AI that teaches computers to process language, 'understand', and generate human language. NLP uses different statistical, ML and DL models.
- LLMs are large DL neural networks that can perform a variety of tasks, including NLP tasks, such as translating text from one language to another, or answering questions.

AI-powered tools are used to protect public funds and help auditors and public procurement officers manage large volumes of data effectively, and can reduce the risk of manual errors and allow budgetary authorities to focus on higher-value tasks. On the other hand, developing AI-powered tools takes time and is costly. In addition, they may not be able to capture new indicators of fraud that have not been defined based on auditors' experience, and may generate false positives.

The main applications of AI technologies are in information management and risk-scoring.

AI-powered information management tools can help managing and audit authorities save time by outsourcing text processing tasks to computers. Platforms using LLMs allow organisations to process large bodies of complex data and text and to retrieve relevant information instantly, without investing staff time in undertaking such tasks manually.

AI-powered risk scoring tools can help protect public funds by detecting risks of fraud and alerting relevant authorities to contracts that may contain irregularities. In fact, in recent years, civil society organisations (CSOs) and non-governmental organisations (NGOs) in Central and Eastern Europe have developed tools that use machine learning technologies to uncover corruption in public procurement. Risk-scoring tools in EU audit institutions are still in development; however, they have great potential. For instance, auditors in Belgium, Norway, Portugal, Spain and Sweden are developing tools that will use ML technology to find indications of fraud in large documents of audit data and explore ways to potentially move away from a sample-based auditing process to a 100% AI check. Evidence from the United States confirms this potential. In two state-level audit institutions consulted for this project – Massachusetts and New York – AI-powered risk scoring tools are already in use.

RPA is another new technology used to increase the efficiency of budgetary control. Contrary to AI based technologies, RPA is not used for predictive analytics and insight generation (i.e. to uncover irregularities and fraud). The aim of RPA is to automate tasks that are repetitive, rule-based and require a high degree of accuracy, thus allowing the audit teams to focus on higher-value or more complex tasks. Leveraging RPA technology can help institutions within the public sector to make rapid and effective improvements without a complete system overhaul, and to meet strict deadlines and respond more quickly.

RPA and AI sub-fields are complementary technologies that can work together to improve operational efficiency and enhance the quality of data-driven budgetary control. AI can help RPA automate tasks more fully, handle more complex data, and find patterns in data or extract meaning from images, text or speech. In turn, RPA can enable AI insights to be actioned faster without having to wait for manual implementations.

Both AI technologies and RPA can significantly enhance the capabilities, efficiency, and user experience of digital platforms.

Digital platforms are an effective and efficient tool for information and knowledge sharing, development of joint initiatives, and harmonised approaches to auditing and control, which can enhance the efficiency, speed, accuracy, and quality of budgetary control, as well as fraud detection activities. However, the recent uptake of digital platforms raises concerns about data privacy, especially in light of the European Court of Justice case law of 22 November 2022,[2] which emphasises the need to balance transparency in processing personal data in financial dealings with the protection of individual (i.e. beneficial owner) privacy rights.

Blockchain is a distributed ledger or a record of encrypted data and transactions that is duplicated and shared across a network of computers. In some ways, blockchain and digital platforms serve the same purpose, namely storing information. The main differences concern the number of places the data is stored, the number of entities involved in verifying it, and the way new data is entered. Data on digital platforms is generally stored in one place (disregarding backup sites), whereas data stored in a blockchain is stored in many places. The data on a digital platform is generally verified by one entity (aside from auditors), whereas the data in a blockchain is verified by all entities that are part of the network. While blockchain is not yet widely used in budgetary control, there are pilot projects to curb corruption in public procurement, e.g. in Brazil, Columbia, Nigeria, Peru, Rwanda and South Africa.

Satellite imagery is widely used in budgetary control. The EU's Copernicus Sentinel satellites support budgetary control through the provision of frequent and high-resolution images and data to paying agencies within the Common Agricultural Policy (CAP). The Sentinel images and data allow them to identify specific crops and monitor action such as harvesting with very high levels of precision. The continual evolution of satellite imaging together with the use of AI have the potential to transform multiple EU monitoring and budgetary control systems.

Possible future developments

Looking ahead, two technological developments offer particular promise for budgetary control.

Blockchain: the EU could develop a private and permissioned grant management and/or public procurement system based on blockchain technology. Such a system would record every procurement or grant transaction in multiple places, making it very difficult for any one operator to use EU funds in ways that are not intended, thus increasing transparency, accountability, efficiency in contract management, and trust in the process. At the national level, national authorities could use blockchain to back up citizens' digital tax files, thus making taxable transactions and ownership of assets transparent and traceable. However, the wider application of blockchain technologies in budgetary control would have to overcome challenges including high set-up costs, data protection concerns and high energy consumption.

AI: AI could be used to simplify public procurement processes, for example through new contract management tools. ML algorithms could be used to calculate risk scores in large sets of data and could include an internal chatbot allowing auditors to ask questions about any audit files and be pointed to the relevant file, enabling them to fact-check the chatbot's answer in a matter of minutes. However,

---

[2] Vistra (2023),"ECJ ruling on access to beneficial ownership information: Balancing transparency and privacy"

wider application of AI in budgetary control will have to overcome the risk of high levels of inaccuracy in the output of LLMs, high energy consumption and limited scalability.

Potential applications of new technologies

Evidence from the research carried out for this study suggests potential ways in which big data and new technologies can improve the management, control and auditing of EU expenditure and strengthen the prevention and detection of fraud and misuse of EU funds.

- Big data analytics and data mining: can facilitate access to data, risk-scoring, interoperability between institutions and harmonised data collection, verification and analysis.
- Machine learning: can enhance risk-scoring, strengthen prevention and detection of irregularities, identify weaknesses in control systems, and increase understanding of factors causing anomalies.
- Generative AI/LLMs: can allow for the summarising of large datasets, automatically correct, standardise and organised data, allow cross-referencing against other sources, and generate written reports.
- Robotic process automation: can enable web-scraping for data extraction, verification and reporting, and automate repetitive or time-consuming tasks.
- Digital Platforms: can facilitate the sharing of knowledge and verification of results between authorities.
- Blockchain: can enable the traceability and identification of transactions, streamline data collection and storage, and facilitate efforts to combat tax fraud (including cross-border).
- Satellite imagery can verify the quantity and quality of agricultural output funded by the CAP funds and detect anomalies.

Conclusions and recommendations

The misuse of EU funds poses a serious threat to the EU's ability to advance its strategic priorities and maintain public confidence in the EU. To address this, digitalisation is at the heart of the strategic vision of the European Commission and other bodies responsible for management and control of EU expenditure. EU-level IT tools, such as Arachne, EDES and IMS, are helping to protect the EU budget, but there is scope for further application of digital technologies.

Recommendation 1: Continue to enhance existing EU tools for budgetary control. This includes expanding Arachne to all management modes, integrating advanced technologies, ensuring interoperability with other tools, addressing privacy concerns, and enabling faster checking of operators against more up-to-date and comprehensive data cases. The IMS could be improved by introducing consistent thresholds for reporting cases of fraud and providing more up-to-date information.

Recommendation 2: Promote awareness of and training in the use of existing EU tools for budgetary control. For Arachne, this would relate to how the tool works, how to use it and how to use all the different functionalities, i.e. going beyond conflicts of interest and fraud red flags. For the IMS, this might include training in thresholds for reporting cases of 'suspected' and 'established' fraud.

Recommendation 3: Consider making the use of EU tools mandatory. In the case of Arachne, the Parliament, the Council and the Commission have committed to examining and re-discussing the compulsory use of the tool during the post-2027 multiannual financial framework.

New data-driven technologies such as data-mining, machine learning, robotic process automation and artificial intelligence could increase the efficiency and quality of budgetary control. AI and machine learning algorithms are proving accurate in detecting potential risk or cases of fraudulent spending and corruption. Machine learning can also be used to automate checks on operations in public procurement and for real-time monitoring of spending.

Recommendation 4: The EU and its Member States could consider pilot projects to explore the possibilities for applying new data-driven technologies to budgetary control. Such projects might be best developed on a transnational basis from the outset to ensure their applicability to different national contexts and to ensure a degree of consistency in the use of EU funds across the EU-27. Where appropriate, there may be possibilities for such pilots to be co-financed by relevant EU funding programmes.

To date, there has not been a broad and consistent deployment of data-driven technologies in budgetary control across the EU due to differences in national control strategies and systems, regulatory frameworks, investment capacity, digital competences and political priorities between Member States.

Recommendation 5: Support mutual learning, the sharing of good practices and exchanges of information between relevant authorities. Widening knowledge of good practice might help and inspire budgetary authorities to adopt new tools or configure themselves in such a way as to best exploit new technologies. More consistent adoption of new data-driven technologies might also support the harmonisation of control practices and standardisation of reporting methods.

Challenges in the use of new technologies include the need for uniform data collection, interoperability of data and systems, cost, privacy regulation compliance, ethical concerns relating to biases embedded in AI systems and a high number of false positives.

Recommendation 6: The EU could consider defining common standards for the use of new technologies in budgetary control accompanied by a code of conduct for the proper and 'fair' deployment of these technologies for budgetary control.

Recommendation 7: Assess the costs and benefits before deploying new technologies. In some cases, the deployment of new technologies can be expensive and the benefits uncertain, particularly where error rates are already low. Budgetary authorities should thus carefully assess the potential benefits of deploying new technologies relative to their cost. In some cases, it might be appropriate for ex ante impact assessment (including cost-benefit analysis) to be undertaken at EU level in respect of the possible deployment of new technologies at EU level (or across all Member States). Mutual learning and exchange of experience could inform this process.

Recommendation 8: Carry out regular "horizon scanning" to identify potential new technological developments suited for application to budgetary control and share information about such developments with budgetary authorities at EU level and in the Member States.

1. INTRODUCTION

1.1. Study objectives

The digitalisation process and the development of information technologies (IT) in recent years have unveiled new possibilities in different fields. In the field of budgetary control, these innovative technologies contribute to strengthening the prevention and detection of irregularities, including cases of fraud, corruption and the misuse of funds and thus, reinforce the protection of European Union (EU) financial interests. It is therefore of utmost importance to explore these new frontiers.

In this context, this study has explored:

- new technologies currently used in the field of budgetary control;
- new developments can be expected in the field of budgetary control; and,
- how these could be used to protect the budget of the Union in general, including but not limited to the prevention of fraud and corruption, the sound financial management of EU funds and the protection of the Union's budget in the implementation of EU sanctions.

The study focuses on the use (or potential use) **of IT technologies, tools and systems in the management, control and audit of public expenditure** at both the EU and national levels. In this study, IT technologies refer to emerging technologies such as AI-powered systems, machine learning, large language models (LLM), big data, robotic process automation and others with the potential for application in budgetary control. The study also assesses the advantages and limitations of these technologies as well as factors (including but not limited to data privacy, legal requirements, technical and cost issues) that could facilitate or hinder their uptake and successful use across the EU, and on EU funds under different management modes. Possible combinations of different tools and their potential in the fight against fraud and corruption are examined.

1.2. Summary of the methodology

The findings presented in this report draw on evidence gathered from multiple sources, namely:

- **desk research**, reviewing literature and websites on the use of new technologies in budgetary control at the EU level and in a sample of eight EU Member States (Czechia, Germany, Hungary, Italy, Poland, Portugal, Romania, Sweden) and two non-EU countries (UK, USA).
- **review of secondary sources**, including information provided by EU agencies on EU-funded programmes and projects, publications of national governments, academic journal articles, and reports or information provided by private sector companies.
- **EU-level interviews**, including European Commission Directorates-General (AGRI, BUDG, DIGIT, ECFIN, EMPL, REGIO.DAC), European Anti-Fraud Office (OLAF), European Public Prosecutor's Office (EPPO).
- **Survey of other public authorities responsible for budgetary control** which attracted responses from 75 relevant authorities in the Member States.
- **Interviews of other stakeholders**, namely 39 representatives of national and regional authorities, universities and NGOs across the sample of Member States, as well as the UK and the US.

Both the survey and the interviews aimed to identify new tools and technologies that are used in the digitalisation of budgetary control, to solicit views on how well those new tools work and, if they were not yet used, gauging interest in using them in the future. Respondents were also asked for their views on tools that are already available at the EU level (Arachne, the EDES, and IMS), and their general views on the use of new technologies in budgetary control.

1.3. Structure of the report

The subsequent sections of the report provide the following content:

- **Section 2 Context:** summarises the problem of misuse of EU funds, the current EU policy framework to address such misuse, EU technological tools to help address the problem, and other relevant developments at EU level;
- **Section 3 New technological developments currently available in the field of budgetary control**: explores the most important new technological developments and explains how they improve control practices and their associated advantages and disadvantages.
- **Section 4: Expected new technological developments**: describes technological developments that experts expect to unfold in the next five to ten years but that are not yet widely applied to budgetary control.
- **Section 5: Potential applications of new technologies**: assesses the possible benefits and costs associated with the deployment and implementation of expected new technologies in the budgetary control process and the potential implications for specific types of EU funds.
- **Section 6: Conclusions and Recommendations**: summarises the findings presented in the previous sections and offers findings for the EU and its Member States.

2. CONTEXT FOR DIGITALISATION IN BUDGETARY CONTROL

This section describes the problem of fraud, irregularities and misuse of funds in the EU, outlining key challenges the EU is currently facing. It also presents the EU policy framework, emphasising the efforts made to promote the digitalisation of budgetary control practices in response to these challenges. The section also provides a brief overview of the different tools available at EU level and addresses their strengths and weaknesses, including current reservations and concerns from Member States regarding the use of these tools.

2.1. The problem of misuse of EU funds

The misuse of EU funds is a serious problem that significantly affects the capacity of the EU to pursue its strategic priorities and undermines public trust in the EU and its institutions. According to the European Anti-Fraud Office's (OLAF) 2022 annual report on the protection of the EU's financial interests (the "PIF Report"), a total of 12,455 irregularities,[3] amounting to EUR 1.77 billion were reported by Member States through the Irregularity Management System (IMS) in 2022.[4] The total number of irregularities reported by Member States through the IMS increased by 7% in 2022 compared to 2021 but the related amounts have decreased overall (-13%). The PIF Report distinguishes between irregularities that are fraudulent (i.e. those that arise through deliberate intent') and those that are not. This distinction is necessary because irregularities can be the result of genuine errors, such as the failure to upload a required document; and do not always have a negative impact on the financial interests of the Union.[5] According to the PIF report, the number of reported fraudulent irregularities remained reasonably stable during 2018-2022 (e.g. only increasing by 2% in 2022 compared with 2021), although the financial amounts linked to those cases varied more, due to a limited number of individual cases with high financial impacts.

Cohesion policy funds feature a higher level of fraud on the expenditure side of the EU budget, compared with other areas of EU policy.[6] A total of 206 fraudulent irregularities in Cohesion funds were reported in 2022 in the EU 27. These accounted for EUR 169.1 million. In agriculture, the number of fraudulent irregularities increased during the programming period of 2014-2020 but, according to OLAF, less than expected. Here, too, OLAF points to rising detection rates to explain the rising numbers. The detection of fraudulent cases was higher in rural areas and concentrated in a few Member States, and frequently related to the manipulation of aid requests or supporting documentation.[7]

The available evidence suggests that there have been improvements in the identification of fraud risks and detection of cases by national authorities and bodies thanks to the use of the Commission's IT tools.[8] OLAF noted improvements concerning the coherence of anti-fraud legislation across the EU, thanks to the correction of problems in the transposition of EU rules into national

---

3 OLAF PIF Report 2022, section 4.1. And 'irregularity' means any' infringement of a provision of Community law resulting from an act or omission by an economic operator, which has, or would have, the effect of prejudicing the general budget of the Communities or budgets managed by them, either by reducing or losing revenue accruing from own resources collected directly on behalf of the Communities, or by an unjustified item of expenditure.' Article 1(2) of Regulation (EC, Euratom) No 2988/95.

4 IMS is an IT database developed by the European Commission, accessible through the portal called "AFIS", which allows Member States to draw up and submit irregularity reports to OLAF. The tool is widely used for statistical purposes and analysis of the reported irregularities. The annual PIF Reports are based on the information provided in IMS.

5 Anti-Fraud Knowledge Centre. 'What is an irregularity?'

6 The Cohesion Policy funds are: the European Regional Development Fund (ERDF), the Cohesion Fund (CF), the European Social Fund (ESF) and the Just Transition Fund (JTF). Taken together, these funds account for almost one third of the total MFF budget 2021 – 2027 (i.e. EUR 1.211 trillion).

7 OLAF PIF Report 2022, section 4.3.1.

8 Sources include the ECA's special reports and audits, OLAF's investigations and annual reports, the European Parliament's annual resolutions on the protection of the financial interests of the EU.

systems.[9] Altogether, 24 Member States have adopted or are about to adopt a strategy to enhance the safeguarding of the EU's financial interests.[10]

However, there are still **shortcomings in the national management and control systems which increase the likelihood of fraud vulnerabilities**. Measures used to identify fraud such as on-the-spot checks and audits, internal fraud reporting mechanisms and the monitoring of indicators are mainly reactive in their nature. Potentially more effective methods for the proactive detection of fraud such as checks on collusion in public procurement, semantic analysis of bids, and identification of irregular bidding patterns, have not been broadly implemented. Moreover, not all Member States make systematic use of tools such as the Arachne (which is used on a voluntary basis by the Member States) and the Irregularity Management System (IMS), although some have developed their own fraud prevention systems.[11] A comprehensive uptake and use of these EU-level fraud prevention tools has not yet been achieved today (see section 2.3).

The true scale of fraud against EU finances is thought to be significant under-estimated. For example, the European Court of Auditors (ECA) has acknowledged that the Commission lacks comprehensive information on the scale, nature and causes of fraud in EU spending.[12] The ECA argued that the Commission's statistics on detected fraud are incomplete and that there is no assessment of undetected fraud and no detailed analysis on the causes and incentives which lead beneficiaries to defraud the EU's finances. The ECA also indicated that fraud is often hidden because it is only detected once ex-ante and ex-post checks have been performed. Official statistics on fraud can be composed of cases that are detected, reported, investigated, prosecuted and established by court procedures, but there is still a large amount of fraud that likely remains undetected.

Furthermore, the **trend in cross-border online e-fraud continues to affect the EU's financial interests**. During the COVID-19 pandemic, citizens increasingly carried out financial activities on-line, as did fraudsters. This trend has continued since the end of COVID restrictions and poses new challenges for competent authorities such as monitoring expenditure and working across borders to reconstruct a bigger picture of the fraudulent activity.

As emphasised in an interview conducted for this study, there is a 'single market for fraud in the EU' but no common and integrated system for management and control of funds. In particular, there are **290 different reporting systems for reporting project spending and beneficiaries** affecting EU funding programmes under shared management.[13] The situation is even more complicated if funds under other management modes are also considered. The fragmentation in the reporting systems across the EU limits data comparability and prevents the use of new technologies and big data sets and systems for the monitoring and controlling the funds.[14] Against this background, **there is scope for EU action to promote digitalisation, help address current gaps and barriers** in Member States, when expending EU funds, and thus reap the benefits of the digital transformation in budgetary control.

---

9 OLAF PIF Report 2022.

10 Ibid.

11 For instance, the 'PREVENT' system in Romania and the 'SALER' IT system in Valencia, Spain.

12 ECA (2019). Special report No 01/2019: Fighting fraud in EU spending: action needed. See: https://www.eca.europa.eu/Lists/ECADocuments/SR22_14/SR_CAP_Fraud_EN.pdf.

13 European Parliament (2021). Digitalisation of European reporting, monitoring and audit. p. 3.

14 Ibid.

2.2. EU policy framework

Growing attention has been paid in recent years to possible ways in which the EU could support the digitalisation of budgetary control and thus help increase the effectiveness and efficiency of controls on EU expenditure. For example, the European Parliament has called on the Commission to propose a regulation for the establishment of an interoperable IT system allowing for uniform and standardised reporting in a timely manner by Member States' authorities in the area of shared management. In the Parliament's view, such a system would help avoid systematic problems, such as misuse, fraud, conflict of interest and double funding, and would bring more efficiency in the monitoring and control of the use of EU funds, allowing the use of AI and big data sets and systems.[15] The Committee on Budgetary Control also organised a public hearing to better understand the technical support provided to Member States in the areas of better administration, digitalisation and EU fund implementation.[16]

Several EU policy initiatives and measures have promoted the digitalisation of information, use of databases and novel technologies in the field of budgetary control. The underlying assumption is that the benefits of the digital transformation will outweigh the costs of implementing and using these tools and systems.

As regards cohesion policy, an **e-cohesion approach** was embedded in the 2014-2020 Common Provisions Regulation (CPR)[17] and has now been made compulsory for all programmes in the 2021-2027 CPR. The new regulation has increased the volume and type of data that Member States should make available through their IT systems, in particular in relation to beneficiaries and underlying recipients of umbrella schemes.

In 2019, the Commission updated its 2011 'Anti-Fraud Strategy' (CAFS) with a Communication to protect the EU's financial interests from fraud, corruption and other intentional irregularities and address the risk of serious wrongdoing inside the EU's institutions and bodies.[18] This revision strengthened the EU's fraud prevention and detection capacity both on the expenditure and revenue side (e.g. by preventing tax fraud and tackling smuggling)[19] and adopted **a more centralised system of oversight for its anti-fraud action**. In particular, the first objective of the CAFS was to improve the understanding of fraud patterns, fraudsters' profiles and systemic vulnerabilities relating to fraud affecting the EU budget. Accurate data collection and analysis are key to achieving this objective. As indicated in the CAFS, the Commission 'is committed to **improving the quality and completeness of the data retrieved**, and the analysis of the nature or methods of detected fraud in general (through continued development of the analysis of IMS data and the use of other data available) and in relation to specific sectors and/or Member States' through in-depth analysis and tailored data collection. The Commission also emphasised the importance of better and more comparable data on fraud patterns. A new intelligence scanning function for the overall process was integrated in the 2019 CAFS to proactively explore the anti-fraud landscape for emerging cross-cutting or sector-specific fraud risks.

In 2021, the Commission adopted a new CAFS and revised action plan to **strengthen all phases of the anti-fraud cycle (prevention, detection, investigation and correction).** The new strategy promotes

---

15 European Parliament (2021). 2019 discharge: EU general budget - Commission and executive agencies.

16 European Parliament (2022), Instruments and Tools at EU Level and Developed at Member State Level to Prevent and Tackle Fraud - ARACHNE.

17 Regulation (EU) No 1303/2013 of the European Parliament and of the Council of 17 December 2013. p.320. This Regulation lays down common provisions for all ESI funds. However, it applies only partially to the EAFRD which is managed differently. The management system for the EAFRD is described in Section 2.3 of this report, under the CAP.

18 Commission Anti-Fraud Strategy. COM/2019/196 final and SWD(2019) 170 final.

19 As also indicated in the Report from the Commission to the European Parliament and the Council; Annual Report to the Discharge Authority on internal audits carried out in 2016, COM(2017) 497 final of 15 September 2017.

more effective action against fraud on the EU budget through 44 actions grouped in seven themes that reflect the EU's priorities. **A key priority is to foster digitalisation and the use of IT tools to fight fraud** to further strengthen the existing IT tools and systems and incorporate solutions to make the fight against fraud more effective.[20] Another priority is to **reinforce the EU anti-fraud architecture and anti-fraud governance** by facilitating cooperation and coordination across organisational boundaries of all players involved in the anti-fraud architecture and through the Fraud Prevention and Detection Network (FPDNet).

The new CAFS complements other key policy initiatives including the proposal for an interinstitutional Ethics Body,[21] the Anti-corruption package,[22] the recast of the Financial Regulation,[23] the Rule of Law mechanism[24] and the Conditionality mechanism[25] which sets out a regime of conditionality for the protection of the Union budget. All these policy documents acknowledge the potential of digital technologies to improve budgetary control.

In the proposal for a recast of the Financial Regulation, **the Commission indicated the need to increase the efficiency and quality of controls and audits with the help of digitalisation and emerging technologies such as machine learning, robotic process automation and artificial intelligence**. The provisional agreement between the Council and the European Parliament also stressed the need to protect data in the process of digitalisation.[26] Adoption of the new Regulation is foreseen for the first half of 2024. Digitalising the fight against fraud is also a topic for the revision of the action plan accompanying the CAFS. The proposed new Financial Regulation seeks to enhance transparency in the use of EU funds, digitise efforts against fraud, and improve fraud risk management whilst maintain human oversight.[27] The aim of these measures is to reduce the administrative burden for applicants and recipients of EU funds, without creating additional risks for the sound financial management of the EU budget. The recast also aims to improve the quality and interoperability of data on recipients of funding, including through the use of a single integrated IT system for data-mining and risk-scoring (see section 2.3.1).

An effective anti-fraud action across the EU also requires dedicated efforts from the competent national authorities. In accordance with Article 325 of the TFEU, the EU and its Member States counter fraud and any other illegal activities affecting the financial interests of the Union. Member States are also required to take the same measures to counter fraud affecting the EU's financial interest as they take to counter fraud affecting their own financial interest.[28]

Effective action on fraud also requires the development of better tools at EU level and the wider use of such tools, for example, as evidenced by the survey of Managing Authorities (MAs) undertaken for this study. The use of existing tools was reported to be hindered by limited knowledge of the tools (22/59 MAs), issues with quality and interoperability of data (14/59), the use of alternative national tools (11/59), national rules on data confidentiality and protection (10/59) and the non-mandatory nature of

[20] Commission Anti-Fraud Strategy Action Plan - 2023 revision. COM(2023) 405 final and SWD(2023) 245 final.
[21] COM(2023) 311 final.
[22] COM(2023) 234 final / 2023/0135(COD).
[23] COM(2022) 223 final, 16.5.2022.
[24] COM(2019) 163 final, COM(2019) 343 final.
[25] Regulation (EU, Euratom) 2020/2092. This Regulation establishes the rules necessary for the protection of the Union budget in the case of breaches of the principles of the rule of law in the Member States, including suspension of support.
[26] European Council (2023), [Financial Regulation: Council and Parliament reach an agreement](https://).
[27] Ibid.
[28] Article 325 of TFEU.

some tools (10/59). [29] The ECA has also stated a view that there is more scope for the Commission to exploit new technologies in respect of addressing fraud within CAP spending. For example, the ECA notes the significant potential of AI to enable the detection of patterns among billions of data points and the potential of data-mining tools to make monitoring systems more efficient and to detect fraud and mismanagement.[30]

In order to promote innovation in the development of digital tools (including but not limited to budgetary control), the EU Digital Finance Platform creates a collaborative space, specifically for innovative financial firms and national supervisors. The platform was set up in 2020 as part of the European Commission's Digital Finance Strategy, which promotes a more competitive and innovative European financial sector. It includes a Data Hub with the potential to support the AI technologies discussed in Section 3, as it provides datasets of synthetic supervisory data to participating companies, academics and researchers, which can be used to test new solutions and train AI/ML models. [31]

2.3. EU tools

2.3.1. Arachne Risk-scoring Tool

Arachne is a risk-scoring tool that helps MAs detect risks of fraud and irregularities in the disbursement of European Structural and Investment Funds (ESIF). Developed by the Commission and operational since 2013, Arachne is used on a voluntary basis by some but not all MAs in their administrative controls and management checks. For example, Germany, Sweden, Finland, Denmark, Poland, Greece and Cyprus did not use Arachne for the 2014-2020 programming period.[32]

MAs upload project data from their own IT systems in an XML format.[33] Arachne then enriches the project data with data from three other sources:

- ORBIS[34] provides data on almost all companies worldwide (address, turnover, shareholders, subsidiaries, key staff, etc.).
- WorldCompliance[35] provides lists of 'politically exposed persons' across the world [36], as well as sanctions lists[37] (e.g. the World Bank Debarred Parties List), enforcement lists (e.g. EU Terrorism List, Interpol's Most Wanted lists, Federal Bureau of Intelligence in the USA) as well as of lists companies or individuals linked with illicit activities in the news ('adverse media lists').[38]
- Vies[39] provides VAT numbers of companies.

Using this data, Arachne computes various risk indicators, such as risks of bankruptcy in the next 12-18 months, risks of criminal convictions and risks of conflicts of interest. Risks are automatically recalculated every week, helping MAs to detect risks of fraud and irregularities.[40]

---

29 European Parliament (2022), Instruments and Tools at EU Level and Developed at Member State Level to Prevent and Tackle Fraud - ARACHNE.
30 European Court of Auditors (2022), The Commission's response to fraud in the Common Agricultural Policy.
31 EU Digital Finance Platform
32 Answer given by Mr Schmit on behalf of the European Commission to the Parliamentary question - E-001007/2022(ASW): https://www.europarl.europa.eu/doceo/document/E-9-2022-001007-ASW_EN.html
33 Extensible Markup Language (XML) is a markup language and file format, which can be used to store and transmit data in a way that allows reading by humans or machines.
34 Bureau van Dijk (2023) "Orbis".
35 Lexis Nexis (n.d.) "LexisNexis® WorldCompliance™ Online Search Tool"
36 Lexis Nexis (n.d.) "Politically Exposed Persons List"
37 Lexis Nexis (n.d.) "Sanctions List Screening"
38 Lexis Nexis (n.d.) "Adverse Media Monitoring"
39 European Commission (n.d.) "VIES VAT number validation"
40 Molemans (2018) "Arachne risk scoring tool – Identifying and monitoring of risky projects."

MAs with experience of using Arachne tend to offer a positive view. Of the 35 MAs who answered the relevant question in the survey for this study, most (21) reported that it was effective in detecting and tackling fraud corruption and irregularities to a great (5) or reasonable (16) extent. Another 7 reported that it was effective to a slight extent, whilst only 7 reported that it was not effective at all. The reported benefits include: the vast data that can be processed, allowing MAs to focus on cases flagged by Arachne; wide geographical scope, allowing MAs to assess risks beyond their own country; data visualisation tools, allowing MAs to see, for instance, networks of applicants they would otherwise miss.

At the same time, a number of drawbacks have been identified, namely:

- **Low awareness and thus low take-up**. For example, 24 of the 59 MAs that responded to the survey for this study were unable to provide a view on the effectiveness of Arachne. In a 2018 study, MAs for seven operational programmes pointed to a lack of awareness or a need for training, mainly related to how Arachne works, how to use it (and how to use all the different functionalities, i.e. going beyond conflicts of interest and fraud red flags, which are most commonly used), how to interpret the results, and how to identify fraud based on Arachne's risk scores.[41] Several MAs consulted for this study also mentioned low awareness as a problem, although some also mentioned that they changed their views on Arachne after using it and seeing the benefits. The European Commission's 2022 survey of Arachne users also highlighted that some authorities were unsure of how the tool should be used, e.g. the consequences of red flags.
- **Privacy concerns** were reported by some of the MAs consulted for this study (notably in Germany) as a reason for not using Arachne. Challenges around compliance with data protection regulations were also highlighted by the Commission's survey of users.
- **Administrative burden** of entering a substantial amount of information for Arachne to provide reliable estimates were also reported by some of the MAs consulted for this study. Where MAs use Arachne in addition to national risk-scoring tools or procedures, they have to input data into two systems. Concerns about the administrative burden were also highlighted by users responding to the Commission's user survey. To address this, some MAs have suggested making it easier to use alongside national tools[42] and to make it possible to download Arachne data in an Excel format, which national systems tend to use.
- **Accessibility issues**. Some users responding to the Commission's survey reported language barriers and technical limitations, which raised a need for multilingual support and user-friendly interfaces.
- **Accuracy of the risk scores**. Because Arachne is not used by all MAs, it lacks information on contractors and beneficiaries in some Member States.[43] In addition, MAs upload data at different times, some more often than others, meaning that the weekly risk scores are not always based on the latest data available at national level. In the 2018 study, it was found that 8 out of 45 MAs mentioned the incompleteness of the database as a reason not to use Arachne, six mentioned outdated data.[44]

[41] European Commission (2018) "Preventing fraud and corruption in the European Structural and Investment Funds – taking stock of practices in the EU Member States", Study commissioned by DG REGIO, p.20.
[42] European Parliament (2022) "Preventing fraud and corruption in the European Structural and Investment Funds", p.20.
[43] European Court of Auditors (2023). Digitalising the management of EU funds.
[44] European Commission (2018) "Preventing fraud and corruption in the European Structural and Investment Funds – taking stock of practices in the EU Member States", Study commissioned by DG REGIO, p.19

- **High number of false positives**, i.e. cases Arachne identifies as potentially fraudulent but which are not in fact fraudulent, which can happened particularly often for small companies. This was mentioned by some MA interviewed for the 2018 study.[45]
- **Being configured only to be used for the ESF and the ERDF**. In other words, Member States cannot use Arachne as a 'one size fits all' fraud prevention tool.[46]

In response to these challenges, the Commission is looking to expand the functionalities or policy areas covered by Arachne, integrate advanced technologies such as machine learning and artificial intelligence to enhance data analysis capabilities and decision-making processes, and optimise user interfaces for improved accessibility and usability. The Commission is also developing interoperability between Arachne and other tools, such as EDES (see section 2.3.2) and SUMMA (the Commission's next generation corporate financial platform), so as to facilitate seamless data exchange and collaboration across various platforms, while enhancing data quality and security and reducing the administrative burden for users.

Furthermore, Article 36 of the Financial Regulation recast, agreed by the co-legislators in December 2023, will provide for an extension of the scope of Arachne to all management modes as from 2028, including the compulsory feeding of data into Arachne. [47] The potential compulsory use of the risk-scoring provided by Arachne may be rediscussed after a Commission assessment of the readiness of the system by 2027. In a draft joint statement, the Parliament, the Council and the Commission agreed on the need to further develop the tool taking into account established approved systems in Member States and committed to examining and rediscussing the compulsory use of the tool during the post-2027 multiannual financial framework.[48]

2.3.2. Early Detection and Exclusion System (EDES)

The EDES is a database blacklisting (or excluding) untrustworthy counterparties such as those involved in fraud, corruption, professional misconduct, money laundering, or non-payment of taxes. According to the 2023 ECA report, the EDES has a broad scope of application, i.e. a broad range of exclusion situations, and a robust exclusion procedure.[49] Exclusion can even happen before judicial proceedings against the concerned actors have been finalised.[50] Set up by the Commission 2016, it allows the Commission and other EU bodies to flag up financial risks posed by (potential) recipients of EU funds and to exclude unreliable ones from EU funding in direct and indirect management.[51] The Commission operates the EDES for funds it manages directly, and for funds it manages indirectly through implementing partners. In this way, the EDES centralises the exclusion process for all EU bodies.

The evidence suggests that several limits to the usefulness of EDES as a digitalisation tool for budgetary control. For example, only 8 of the 59 MAs that responded to the survey for this study reported that EDES was effective to a great (4) or reasonable (4) extent, whilst 8 reported it to be effective only to a slight extent and 4 reported that it was not effective at all.

---

45 Ibid p.20.
46 European Commission (n.d.) "Arachne risk scoring tool".
47 European Commission (2022) "Proposal for a Regulation of the European Parliament and of the Council on the financial rules applicable to the general budget of the Union".
48 Draft joint statement of the European Parliament, the Council and the Commission on the single data-mining and risk-scoring tool provided for in Article 36 of the Financial Regulation; December 2023.
49 European Court of Auditors (2023) "Protecting the EU budget Better use of blacklisting needed", p. 4.
50 European Parliament (2021), The Impact of Organised Crime on the EU's Financial Interests. Study for the European Parliament's Committee on Budgetary Control.
51 European Commission (11 July 2023) "Commission Anti-Fraud Strategy Action Plan - 2023 revision"

The limits to the EDES include:

- **Low awareness**. For example, 39 of the 59 MAs that responded to the survey for this study were unable to provide a view on the effectiveness of EDES. The Commission's Internal Audit Service (IAS) has noted a "general lack of awareness about EDES across the Commission".[52]
- **Low number of recommendations**. For example, in 2022, the panel responsible for assessing cases issued only nine recommendations to exclude entities (as well as ten recommendations not to exclude entities). As a result, the ECA concluded in 2023 that "exclusion is not being used effectively to protect EU funds from untrustworthy counterparties."[53] However, a July 2023 European Commission report to the Parliament suggests that recent awareness-raising activities have increased the number of cases authorising officers are referring to EDES and, thereby, the number of exclusions.[54]
- **Difficulties in accessing Member State data on exclusion situations**, such as business registers and criminal records. There are no EU-wide registers or records. Even where EU-level data exists (e.g. relating to fraud investigations) the data is not always used or usable. Authorising officers deal with companies from a wide range of Member States and other countries and rely on publicly available data sources. Some sources of information are hidden behind paywalls or only accessible in the relevant national language. According to the above-mentioned ECA report, "In practice, the Commission places a high degree of reliance on declarations on honour from EU counterparties regarding the absence of an exclusion situation."[55] There are also legal restrictions: criminal records cannot always be accessed and may require authorisation from Member State authorities or even the person concerned.[56]
- **Limited scope of the entries on the EDES website**, which do not always include all the necessary identifier information making difficult to identify excluded persons or entities.

The EDES currently has limited reach, given that it does not apply to funds under shared management. However, the proposed new Financial Regulation includes a targeted extension of the EDES to all management modes from 2028. In addition, a new web service would allow a fast checking of any economic operator in the database against the up-to-date list of exclusion or early detection cases. The first service requester of the EDES web service will be e-procurement. However the service may be useful to other applications in the Commission, for example e-grant or even the Arachne application. The same solution could be provided to Member States' managing authorities to make a query in the EDES database via their own national IT systems (e.g. grant management database). As noted earlier, the Commission is also developing interoperability between EDES and other tools, such as Arachne and SUMMA.

2.3.3. Irregularity Management System (IMS)

The IMS is a database within which Member States are required to report irregularities detected in the management of EU funds. It was set up to help Member States and countries benefiting from pre-accession assistance to meet their legal requirement to report irregularities, including suspected and

[52] IAS audit report: IAS.B4-2017-BUDG-001 of 25 January 2019, cited in European Court of Auditors (Nov 2023) "Protecting the EU budget Better use of blacklisting needed", p. 22. In response to a 2019 report by the Commission's Internal Audit Service (IAS) pointing to these issues the Commission has been carrying out training and awareness activities.
[53] European Court of Auditors (2023) "Protecting the EU budget Better use of blacklisting needed", p. 4
[54] European Commission, "34th Annual Report," p.9, p.13
[55] European Court of Auditors, "Protecting the EU Budget," p. 5.
[56] Ibid. p. 25.

established fraud in areas where the EU provides financial support. (Under EU law, Member States must report such irregularities in revenue and expenditure to the Commission).[57] The IMS is managed by OLAF and used by 3,000 individuals from 700 reporting organisations in 35 countries.[58]

IMS is a preventive measure to support proactive risk analysis in Member States; second, it allows the Commission to monitor action taken by Member States.[59] All Commission departments have access to information reported through the IMS on a need-to-know basis. They use this information for a variety of purposes, including for analysis and reporting, e.g. informing the annex to the PIF Report, to support policy initiatives, to OLAF in its case selection process, to prepare for audits, and to reply to questions from the European Parliament.[60] The IMS allows Member States to classify the irregularity they report as 'suspected fraud' or 'established fraud' or simply as an 'irregularity'.[61] The IMS is valued by those MAs that use it.[62] For example, of 31 MAs who answered the relevant question in the survey for this study, most (19) reported that it was effective in detecting and tackling fraud corruption and irregularities to a great (5) or reasonable (14) extent. Another 10 reported that it was effective to a slight extent, whilst only 2 reported that it was not effective at all.

One benefit of the IMS as a digitalisation tool for budgetary control is the possibility to regularly update information. For example, authorities can immediately delete all data records if the administrative or judicial procedure finds that the action did not in fact constitute an irregularity.[63]

Another benefit is that Member States can specify the stage that any case of suspected fraud is at. For instance, Member States may report that an administrative decision has been taken (i.e. the Member State has established, based on the type of irregularity they found, that this is a case of suspected fraud), or that they have forwarded information about the case to the prosecution service to determine if it constitutes an infringement of EU or national provisions to the detriment of the EU's financial interests. Member States may also report that they have opened criminal investigations, or that they request the indictment of a person in relation to an infringement of provisions to the EU's financial interests.[64]

The main limitation of the IMS is the substantial variation in reporting practices across Member States with some reporting many more irregularities than others.[65] This may reflect different thresholds for reporting a case of different interpretations of 'suspected' and 'established' fraud.[66] There is also a lack of coordination between national authorities, which means that the database is not always up to date.[67] Perhaps reflecting this, 28 of 59 MAs responding to the survey for this study were unable to provide a view on the effectiveness of the IMS.

---

57 European Anti-Fraud Office "Sharing data and expertise".
58 European Anti-Fraud Office "Union Programme – IMS component".
59 European Anti-Fraud Office (2017) "Handbook on Reporting of irregularities in shared management" p.9.
60 European Anti-Fraud Office (n.d.)"Sharing data and expertise".
61 Ibid, p.22.
62 European Parliament (2022), Identifying Patterns of Fraud with EU Funds under Shared Management - Similarities and Differences between Member States. Study for the European Parliament's Committee on Budgetary Control.
63 Article 3(1) of Commission Delegated Regulations (EU) No 2015/1970, 2015/1971, 2015/1972 and 2015/1973, quoted in European Anti-Fraud Office (2017) "Handbook on Reporting of irregularities in shared management", p.72
64 OLAF (2017) "Handbook on Reporting of irregularities in shared management", p.23
65 Consultations for this study, November 2023; see also European Court of Auditors (2023) "Digitalising the management of EU funds", p.43, see also Kuhl (2020), "Implementation of Effective Measures against Fraud and Illegal Activities in Cohesion Policies".
66 OLAF (2017) "Handbook on Reporting of irregularities in shared management, p.4-5.
67 European Parliament (2022), Identifying Patterns of Fraud with EU Funds under Shared Management - Similarities and Differences between Member States. Study for the European Parliament's Committee on Budgetary Control.

2.4. Other developments at the EU level

The European Commission DG BUDG is overseeing the implementation of a new financial corporate system SUMMA, which will replace the previous system (ABAC). Amongst other things, SUMMA will increase the use of new technologies. For example, it will improve (smart) reporting expertise using artificial intelligence, increase the use of automation and support simplified corporate models and procedures building on the progressive development of e-grants, e-procurement.

The concept of "**e-Cohesion**" was introduced within Cohesion Policy funds in the 2014-2020 period. By the end of 2015 Member States were required to establish an electronic data exchange system which allows the secure exchange of natively digital documents or scanned documents from system to system via standardised interfaces between the Managing, Certifying and Audit Authorities as well as Intermediate Bodies, on the one hand, and the beneficiaries, on the other hand.[68] The requirement was strengthened in the CPR for all programmes in the 2021-2027 period. The new regulation has increased the volume and type of data that Member States should make available through their IT systems, in particular in relation to beneficiaries and underlying recipients of umbrella schemes.

The ECA has expanded its use of digitalisation, for example, using digital audit techniques for the first time for the financial audit of the EU agencies in 2020, which confirmed the potential to enhance the quality and efficiency of the audits.[69] In its Annual Activity report, the ECA also described its commitment to enhance the integration and interoperability of its audit tools, to automate processes, to use advanced data analytics, and to identify technologies that can be used to innovate and support audit work. For instance, ECA has integrated its tool for sharing documents and data with the auditees, **ECAFiles**, with two other tools: **ASSYST**, its main audit management system, and **CLEAR**, its system managing the clearance process. Integrating these tools saves both parties time: it has made it easier for ECA and the institutions it audits to communicate. ECA has also found an alternative to manually downloading, saving, and checking documents from the databases of the auditees in cases where programmatic access to those databases was not possible: a robotic process automation service.[70]

In 2021, ECA established a **D.A.T.A. (Data and Technology for Audit) team** to work closely with the audit teams to understand their work processes and needs and explore ways in which the IT systems could be improved, including through assessing the feasibility of a new semantic search engine for ECA. In addition, ECA has put in place a 'data science infrastructure' to make it easier for auditors to process and analyse big and unstructured datasets, using advanced analytics and visualising data. Another innovation is ECA's new "data warehouse as a service", launched in 2022, which makes it easier for auditors to process and analyse structured data, allowing them to get predefined reports, or even to create ad hoc reports and data visualisations.[71]

The European Public Prosecutor's Office (EPPO) is currently implementing the IT Autonomy Programme, which will offer a complete catalogue of administrative IT services that are fully managed internally. In 2022, the team began to design the systems needed to run IT operations autonomously. Since then, the team have introduced the EPPO Intranet platform, concluded the first version of the EPPO Business Continuity and Disaster Recovery plan, and started working on the EPPO Records and Document Management System.[72] In parallel, the EPPO's **Case Management System (CMS) Programme** is increasing digitalisation for example through the integration of a digital signature

---

68 Terri Thomas: e-Governance / e-Cohesion in the EU Context.
69 European Court of Auditors (2020). "Our Activities in 2020".
70 European Court of Auditors (2022) "Our Activities in 2022".
71 Ibid.
72 European Public Prosecutors Office (2022) "2022 Report".

within the CMS, based on EU Sign services, as well as improved machine translation functionalities, with new translation engines and additional use cases for new document types. In addition, the eCodex pilot project has developed a structured and more effective document management approach in the CMS.[73]

OLAF has developed an approach to data mining which uses a machine learning model to detect suspicious language in files.[74] OLAF has also been involved in the European Commission Joint Research Centre's Contraffic research project[75] This project curbs the transport of counterfeit and other illegal and potentially harmful goods through the use of complex algorithms to track the ports-of-call of containers and the ships used in their transport. In this way, customs officials can spot unusual itineraries, which may be attempts to circumvent duties or to smuggle goods. OLAF also supports the use of AI and big data for ex-post fraud detection. For example, the Hercule component of the Union Anti-Fraud Programme strengthens the capacity of EU Member States to investigate activities detrimental to the EU budget through the purchase of technical equipment and tools, such as investigation and surveillance equipment, forensic tools, and tools to analyse data.[76] For example, the programme has supported a project implemented by the Special Investigation Service of the Republic of Lithuania, which is enabling speedier, more efficient and better quality analysis and visualisation of large amounts of data in different formats.[77] The Service's computer system will be complemented by software for visual-association, geographic (spatial) and textual analysis, and hardware for displaying and saving big data.

[73] European Public Prosecutors Office (2022) "2022 Report".
[74] European Parliament (2021) "Proceedings of the workshop on Use of big data and AI in fighting corruption and misuse of public funds - good practice, ways forward and how to integrate new technology into contemporary control framework".
[75] European Commission (2006), JRC develops risk analysis system to fight maritime fraud.
[76] OLAF (2023): Union Anti-Fraud Programme - Hercule component
[77] Special Investigation Service of the Republic of Lithuania (2019), Strengthening analytical skills in order to protect EU financial interests.

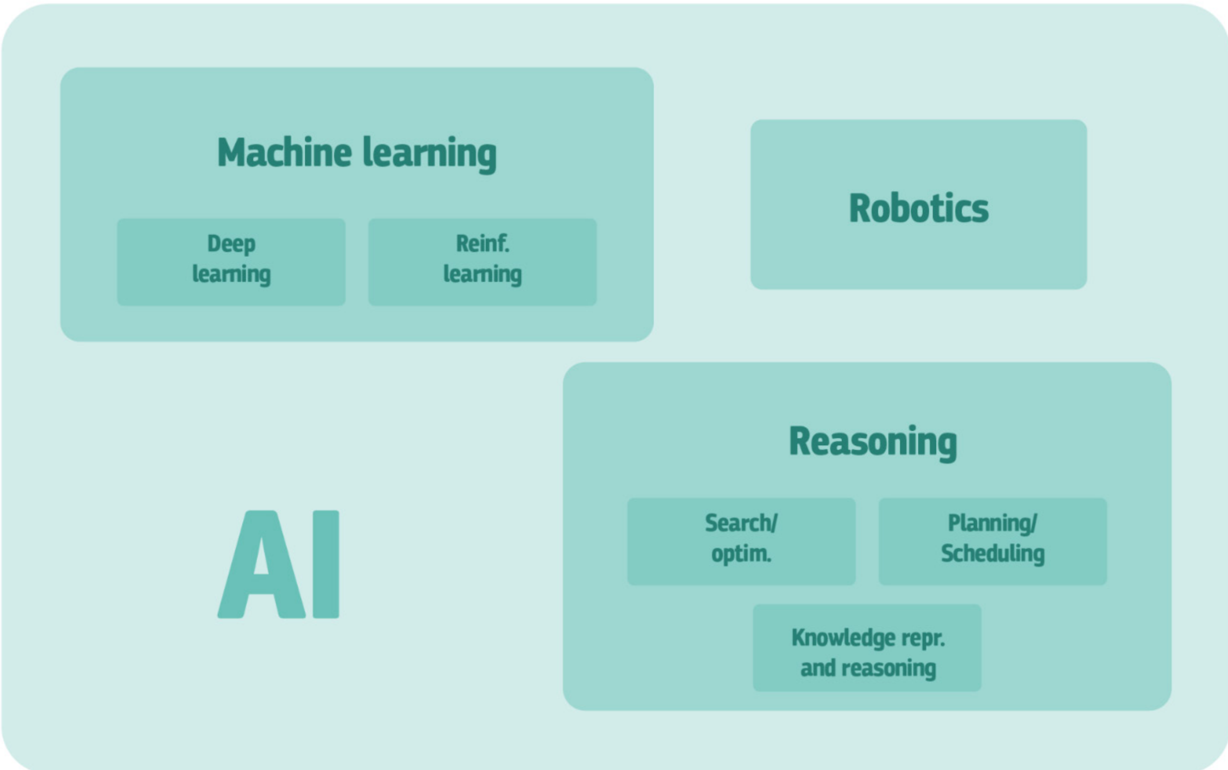
3. NEW TECHNOLOGIES CURRENTLY USED IN BUDGETARY CONTROL

3.1. Overview

This section explores the application of new technological developments in the field of budgetary control within the EU and elsewhere. It explains how such technologies improve current control practices and the associated advantages and disadvantages in their application. The technologies include big data analytics, artificial intelligence (AI), natural language processing (NLP) and large language models (LLMs), deep learning (DL), machine learning (ML), blockchain, robotic process automation, and satellite imagery. Many of these technologies are inter-connected. For instance, as shown in Figure 3.1, machine learning, robotics, and reasoning technologies are all subfields of artificial intelligence. What all of these technologies have in common, however, is their use of large amounts of data.

The following sub-sections provide a brief definition of the relevant technologies and then present ways in which they are applied to budgetary control. A more in-depth definition is provided in the glossary in appendix D and in the respective case studies in Appendix A.

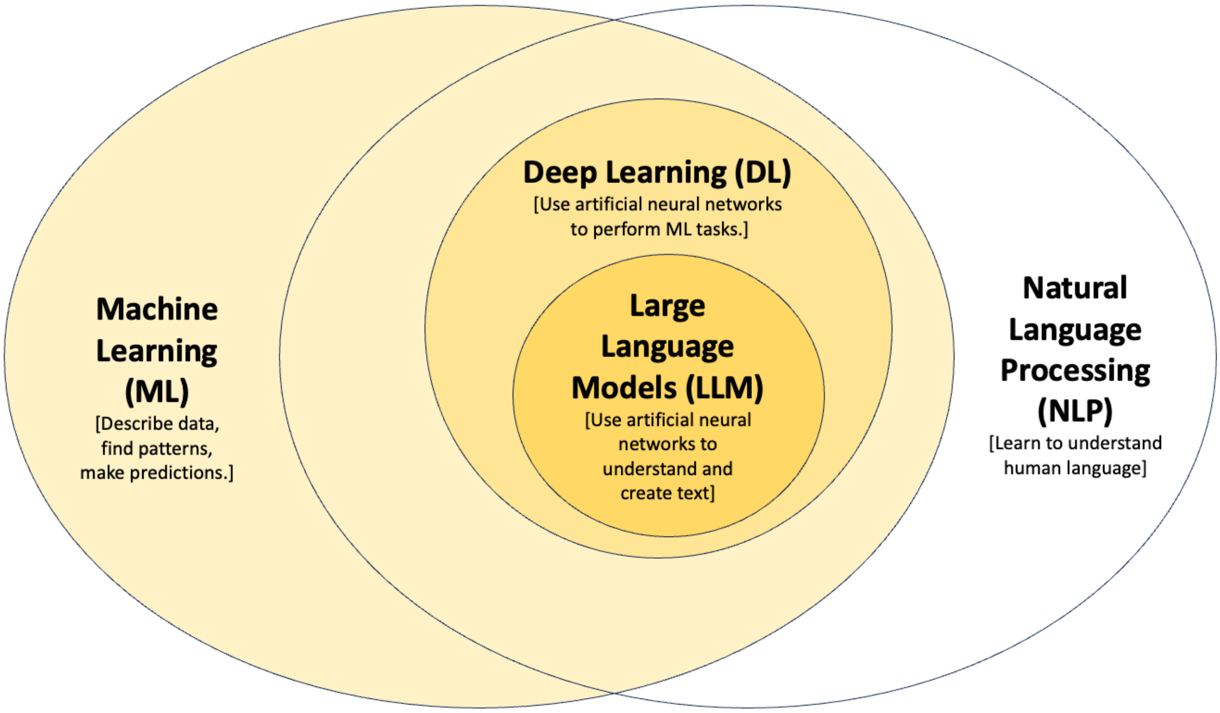
Figure 3.1: AI's sub-disciplines and their relationship



Source: European Commission High-Level Expert Group on Artificial Intelligence (2018), A definition of AI: Main capabilities and scientific discipline

3.2. Big data analytics and AI in budgetary control

Figure 3.2: Machine Learning (ML), Natural Language Processing (NLP), Deep Learning (DL) and Large Language Models (LLMs)



Source: Author's own elaboration.

Some of the most important technological developments in budgetary control are in AI and ML. AI, in its broadest sense, refers to the science of teaching machines to mimic human intelligence and perform human cognitive functions like problem-solving and learning. According to the European Commission's High-Level Expert Group on AI, "AI refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions.[78] Figure 3.2 illustrates the subfields of AI that are relevant to the field of budgetary control: ML, NLP, DL, and LLM. As illustrated by the connecting circles, these technologies intersect, and build on each other. For instance, LLMs, shown in the inner-most circle, are specific types of DL algorithms, which, in turn, are specific types of ML algorithms. LLMs are built to perform NLP tasks. While ML is a common (and more modern) approach to NLP there are also other approaches (rule-based approaches).

Machine learning in its broadest terms, refers the science of teaching machines to learn from data, to describe data, to identify patterns, and to make predictions based on data. ML can also be referred to as 'predictive analytics, or 'predictive modelling'. Traditional machine learning depends on human intervention to teach a computer to perform tasks.[79] A particularly powerful variant of ML is DL, which requires less human intervention to teach the computer to learn. It uses neural networks,

---

[78] The European Commission's High-Level Expert Group on Artificial Intelligence (2018, Dec 18th). "[A definition of AI: Main capabilities and scientific disciplines]." See also IBM Data and AI Team (2023, July 6th). "[AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?]"

[79] IBM Data and AI Team (2023, July 6th). "[AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?]"

inspired by the human brain, to learn from data and improve the accuracy of their predictions. Deep learning models that can generate high-quality content such as text, images, software codes, molecules etc. based on the data they were trained on are also known as generative AI. The modern machine learning applications that will be presented in this chapter are built on decades of research in natural language processing (NLP).

The sub-sections that follow show how AI-powered tools are used to protect public funds. We start with applications of AI (specifically, large language models) that help auditors and public procurement officers manage large volumes of data effectively. Next, we present applications of AI (specifically, machine learning) that help civil society organisations and auditors flag risks of corruption in public procurement. All these applications streamline work processes, increase efficiency, reduce the risk of manual errors and allow budgetary authorities to focus on higher-value tasks.

3.2.1. AI-powered information management tools

Recent advances in research and development of large language models have opened up new possibilities to outsource text processing tasks to AI. Chatbots are computer programmes that simulate human conversations with an end user.[80] They can perform a variety of NLP tasks. NLP is the branch of AI concerned with giving computers the ability to understand and generate human language. While computers have conducted NLP tasks for decades, the development of LLMs has changed the landscape. LLMs are trained on vast amounts of data and have shown exceptional performance at NLP tasks such as classifying text, summarising it, answering questions, and even generating text or performing coding tasks. While commercial LLMs such as OpenAI's ChatGPT, Google's Bard, or Meta's LLaMA are gaining in popularity they are not suitable for public authorities processing sensitive data. However, LLMs can be adapted to the needs of individual organisations. Recent years have a trend toward these 'chat with your docs' applications.

Some audit authorities are piloting the use of large language models. One example of an audit office using LLMs to manage internal documents is the Swedish National Audit Office's new document recommender. 'DocRec' helps auditors at the very beginning of the audit process by recommending documents they should read for any specific case. It is trained on internal data, as well as data from the Swedish parliament and provides users with a tailored reading list in response to key words or questions. The tool is currently being trialled in the Swedish Audit Office and is reported to be gaining in popularity.[81] Other institutions are developing chatbots for external use, i.e. chatbots designed to provide the citizens with information about their work. For example, the US Government Accountability Office (GAO), an independent, non-partisan agency that examines expenditures of the United States Congress, is developing a chatbot to allow citizens to ask questions about its work. Once developed, the chatbot will answer questions about any topics GAO has investigated, summarising findings and recommendations, and pointing citizens to the respective reports.[82]

Large language models also offer the potential for improved budgetary control through improved contract management. Box 3.1 offers an example of an AI-powered contract management tool used by public procurement bodies in Czechia and Slovakia. Slovakian public procurement officials consulted for this project reported a significant improvement in their workflow after switching to Cequence, in particular, when managing large numbers of tenders. While the stakeholders were unable

80 IBM (2024). What is a chatbot?

81 CSES Consultations. See also Maameri, Sami (2023, May 20). Building a Multi-Document Reader and Chatbot With LangChain and ChatGPT

82 US Government Accountability Office (2024, Jan 30). Artificial Intelligence: GAO's Work to Leverage Technology and Ensure Responsible Use

to provide a specific estimate of how much time the tool has saved them, they reported being able to manage contracts in a fraction of the time it took them using previous tools, such as Excel. Similarly, while the stakeholders could not estimate the extent to which the tool improved compliance, they felt that suppliers were more likely to supply their work or goods on time, and according to the terms and conditions agreed upon.

Box 3.1: AI in Public Procurement: Slovakia

One new tool that is gaining in popularity among public procurement officials in Slovakia and in Czechia is an AI-powered automated contract management tool called Cequence. It was first developed by a team of computer scientists and lawyers in Slovakia in 2018. Their vision was to use modern technology to manage contracts more efficiently, i.e. to make it easier for the different parties of a contract to collaborate and agree on the terms and conditions, to speed up process of writing and signing the contracts, to simplify searches for specific information within the signed contracts later on, and to move the entire process online. Hence, they developed a tool that combines all steps of contract management, from the first draft to the signed document on one online platform.

Cequence uses optical character recognition, natural language processing, machine learning and generative AI to read the contracts, extract key pieces of information, summarise them and answer questions about them. The workflow is simple. Users log on and either drag and drop their draft contracts or start with a template. In a matter of seconds, the tool converts PDFs to word documents, scans the text, extracts the important information, and summarises it. Users then scroll through a popup window, check the input and add any additional information. Next, they create a 'new project', drag it to the right place, and add a few important pieces of information such as the type of contract (e.g. an NDA), and the names of the individuals involved. Then, they can edit the contract, for instance, using an in-built document editor like Word Online, and they can use a chat function to communicate with each other. Once agreed, both parties sign the contract virtually using their preferred e-signature tool which is also integrated in the platform.

Crucially, Cequence then saves all those contracts in an easy-to-find fashion, allowing users to log back on at any time, find the contract, and ask any questions they may have. The LLM-powered search engine allows users to ask any questions they may have about the contract in everyday language, answers it, and points them to the right section in the contract that contains the answer to the question. Cequence is used in public procurement bodies across Slovakia and Czechia, who have found it to be much easier and quicker than their previous systems, as well as by private sector clients including Dell, who, based on an internal audit, found that Cequence halved the time needed to execute a contract, and increased compliance with contractual obligations by 62 per cent. The tool is easily scalable to any industry or public body managing any contracts.

Overall, managing and audit authorities can save time by outsourcing text processing tasks to computers. Given the volume and complexity of the information they process, platforms using LLMs to manage reports, contract or any other types of text data allow organisations to process much larger bodies of text than individuals could on their own and to retrieve relevant information instantly, without investing staff time in undertaking such tasks manually.

3.2.2. AI-powered risk-scoring tools

Another way in which AI can help protect public funds is by detecting risks of fraud. Public authorities and civil societies alike are increasingly relying on risk-scoring tools, or applications that alert them to contracts that may contain irregularities.

In the last few years, civil society organisations (CSOs) and non-governmental organisations (NGOs) in Central and Eastern Europe have developed tools that use machine learning technologies to uncover corruption in public procurement. These 'Red flagging' tools like Czechia's zIndex and Hungary's Red Flags Project (see below) use machine learning techniques to analyse large sets of public procurement data and identify patterns indicative of fraudulent or corrupt activities. For instance, they would flag a contract if the cost of the winning bid is much higher than average, or if there are political ties between the supplier and the procurement authority, suggesting a potential conflict of interests. As such, they serve as a national-level complement to Arachne, and have helped uncover many cases of fraud and corruption. They also shed light on failures to implement sanctions. For instance, in April 2023, the Czech think-tank Datlab found that between February 2022 and April 2023 public tenders worth EUR 2.5bn were awarded to companies tied to Russia.

Box 3.2: Examples of risk-scoring tools developed by CSOs

The Hungarian Red Flags tool was developed by Transparency International Hungary, K-Monitor, and PetaByte in 2015, with funding from the European Commission. It aims to enhance transparency by allowing citizens to monitor the public procurement process. The Red Flags tool is a database that contains high-value procurement documents from various sources, including the EU's Tenders Electronic Daily (TED) and public sources in Hungary such as the Hungarian Competition Authority and the Public Procurement Authority. Its algorithm reviews these contracts and flags those with a higher risk of corruption. It differentiates between "red flags", indicating specific risks or legal breaches, and "pink flags", suggesting potential risks based on broader information or market history. The tool is free to use; anyone can create an account, log on, and use a filter function to see contracts in any areas of interest. It lists all contracts in the respective area, along with a description and, if applicable, a flag.[83]

The Czech risk-scoring tool zIndex was developed by the Czech think thank Datlab in 2011 and launched in 2014. Its goes beyond merely flagging of corruption risks: zIndex by seeking to evaluate all public contractors, rewarding those who follow good practices, and showing others where and how they can improve. zIndex combines procurement data with data from publicly-available sources, such as the Czech business register, the insolvency register, or data on political party donations to assess the extent to which contractors follow best practices. A low zIndex indicates a deviation from good practice as defined by, for example, the Czech Ministry for Regional Development and the European Commission. It does not guarantee to identify fraud but does indicate risks of wastefulness or corruption. For full disclosure, the website allows contractors to leave comments under their results, explaining, for instance, why they may have scored lower. Zindex assesses performance on nine indicators covering three broad areas: openness (whether jobs are available to suppliers), competition (whether there is a genuine competition among several suppliers) and control (whether the public, and public authorities are able to monitor progress of public contracts.)[84]

Risk-scoring tools are used in audit. Auditors in Belgium, Norway, Portugal, Spain and Sweden are currently developing tools that will use artificial intelligence, in particular, machine learning, to find indications of fraud in large documents of audit data. For example, in 2023, auditors at the Swedish

83 RedFlags.eu (2024). About the Project.
84 Datlab (2024). ZIndex.

National Audit Office started exploring ways to use machine learning to analyse general ledger transactional data. The goal of the project is not to replace any audit work but to provide auditors with an additional source of information to help direct their attention to cases that merit closer attention. The Swedish auditors are in contact with their counterparts in the UK and in Norway, who are working on similar projects, and are sharing experiences as part of an informal network. Examples of projects that are further along in their development are in Portugal (see Box 3.3), and in Flanders, Belgium (see Box 3.4).

In Portugal, auditors at the Portuguese Court of Auditors are planning to use NLP tools to process large numbers of public tenders, awards and contracts that are already collected in a national database named BASE. Next, they plan to deploy ML algorithms to find patterns and predict risks of irregularities in those public tenders, awards, and contracts. Similar to Czechia's zIndex and Hungary's Red Flags, the Portuguese tool starts with human-defined risk indicators. The project is halfway through its two-year development process. If successful, it will become operational by 2025.

Box 3.3: AI in Audit: Portugal

Automating Public Procurement Risk Analysis – A Machine Learning-driven project in the Portuguese Court of Auditors, in cooperation with OECD and NOVA Information Management School.

The Portuguese Court of Auditors is currently developing a new approach to audit, using machine learning tools to predict risks of irregularities in public procurement data. The goal of the EU-funded '22PT01' project is to automate risk assessment by predicting risks of irregularities in all public procurement data in Portugal. The auditors benefit from a Portuguese law by which all public procurement data has to be made publicly available: the Institute of Public Markets, Real Estate and Construction (IMPIC), maintains a complete, openly accessible, and continuously updated dataset of all public procurement data in Portugal. This will be the most important source of data for the 22PT01 project. The new tool aims to automatically scan this public procurement data and search for both common and unusual patterns.

Over the course of the last year, the team have compiled a list of risk indicators, or signs of irregularities. These indicators were devised in close collaboration with auditors across the Portuguese Court of Auditors, as well as the Brazilian Court of Auditors who have developed a similar tool. In the next stage, the team will calculate these risks. The auditors expect some indicators to be more challenging to calculate than others. For instance, high value contracts are easily extracted from procurement data. In contrast, determining whether the price of any specific public procurement contract was significantly above average, given the sector and the relevant context, will require more advanced data mining and machine learning modelling. The final phase of the project – developing the risk model – most likely, a mix of supervised and unsupervised learning – will be led by AI experts at Lisbon's NOVA University Information Management School (NOVA IMS).

The project is managed by the OECD on behalf of (and financed by) the European Commission (DG REFORM). As the project's executing body, OECD partnered with NOVA IMS to develop the project on behalf of Portugal's Court of Auditors. The project is led by two of the Court's Judges and implemented by the Court's Innovation and Technology Lab. To assure the project's future continuity, the Court of Auditors will store and update the procurement data on its own servers, thus enabling the Court to use it to check risks on a daily basis, as necessary. As of early 2024, the team are half-way through the two-year project time frame.

In Belgium, the Flemish Audit Authority is currently redesigning the entire audit process based on AI. Moving away from a sample-based auditing process, the Authority is exploring the use of AI to allow a 100% check. The auditors plan to combine various AI technologies with a risk model to assess signs of irregularities in all incoming audit files and, in a second step, direct auditors to investigate cases that exhibit a higher risk of irregularities. The project was initiated in 2020 and is intended to become operational by 2026.

Box 3.4: AI in Audit: Belgium

Flanders spearheading the use of AI in Audit - the CATE project

The Flemish Audit Authority for European Structural Funds (Vlaamse Auditautoriteit van de Europese Structuurfondsen, VAA), is currently developing the CATE (Continuous Auditing based on Techn(olog)ical Evolution and Data Mining) project, which aims to replace sample-based auditing with an approach based on the use of AI to check all incoming data. This new approach is intended to address three problems: the limited number of cases auditors can check (AI could allow a 100% check), the burden of checking those cases (AI could automate repetitive tasks), and the timing of the checks (AI could allow continuous auditing rather than auditing long after the end of a project).

With funding from the Flemish Government, the Authority is working with consultants from Deloitte and AI-specialists from the Ghent-based Artificial Intelligence and Machine Learning Company ML6 to develop the new approach. After six months, they found that some aspects of the audit process could already be automated. For instance, Robotic Process Automation (RPA) and Machine Learning (ML) technologies could already be used to check whether documents were complete and to extract data from structured documents. Other aspects of the audit process could not yet be automated. At the time of launching, in mid-2020, the state of the art in the development of machine learning and, in particular, natural language processing did not allow full interpret free text and risks could not be assessed automatically. However, recent technological developments may allow the team to develop a full, AI-powered audit architecture.

The auditors imagine the new AI-driven process to work as follows. First, the system will automatically extract the relevant information out of the documents the auditors receive; for instance, it will pull out information on the supplier, the price, and a description of an expenditure from an invoice. It will store this information neatly in a full data model. Next, the system will compute various correlators to detect errors, possibly with the help of large language models. For instance, the system will compute various probabilities around each purchase (e.g. wrong cost category, not eligible for subsidy, not according to the cost plan, declared twice, wrong timing etc.), around each project partner, (e.g. that they are in financial difficulty) and around paid work (e.g. the incorrect hourly rate of a contractor, incorrect number of declared hours). Based on these risk scores the system will then compute three overarching risk models for the three levels: the overall probability of errors at the cost item level, the project level, and the project partner level. In a final step, those risk models are used to determine whether a case needs to be audited, or not.

While the risk-scoring tools in European audit institutions are still in development, their potential is great. If successful, they promise to reduce manual errors, enhance efficiency, and help prevent fraud and corruption in various EU funds. According to tests conducted in Flanders in late 2023, the new process the auditors envision would save 80% of the time it currently takes to conduct an audit, while investigating not just a small sample, but all cases. The fact that this new system relies only on the documents auditors already receive (not on any national-level databases) it is easily scalable, and could be used in any other EU Member State.

Evidence from the United States confirms this potential. In two state-level audit institutions consulted for this project – Massachusetts and New York – AI-powered risk scoring tools are already in use. The Office of the New York State Comptroller, for example, uses a point-and-click software (Esri ARCGIS geographic information system) to visualise large sets of different types of data, including location data, and to identify risks of fraud. To identify these indicators, the Office conducts periodic audit planning sessions where all auditors come together to brainstorm and identify patterns indicative of fraud. They also search the web for inspiration from other countries: an in-house application using natural language processing allows auditors to enter keywords and search for audit work across the world. The New York auditors also use continuous audit approaches: They have developed computer logic, and built it into some auditees' billing systems in order to flag potentially improper payments in real time. This also allows them to catch human mistakes in filling forms. If, for instance, a person accidentally enters a calendar date in a payment field, the continuous audit system notices the unusual entry right away, saving the auditors costly and time-consuming visits later on.

Table 3.1: Benefits and limitations of using risk-scoring tools to detect irregularities

Benefits	Limitations
Saving time. Because risk-scoring tools can check almost infinite amounts of data for patterns or indicators of risk they save auditors time, **Allowing a 100% check.** Risk-scoring tools may allow auditors to check not just a random sample, but all cases. **Minimising human errors.** Automating manual searches reduces human errors, and increases the chances of finding any cases of fraud and corruption. **Deterrent effect.** The increased transparency offered, in particular, by public risk-scoring tools could have a deterrent effect.	**Time and cost to develop the system.** Developing indicators, finding appropriate data, and developing risk-scoring tools to mine that data is a time and resource-intensive process. **May not capture new indicators of fraud.** Most risk-scoring tools are based on the indicators auditors defined based on their own experience. New ways to commit fraud may not be detected. This may be an issue in fast-paced environments where types of irregularities change over time. **False positives.** Not every case that is 'flagged' is fraudulent. Working with risk scores requires a level of digital literacy. While risk scores are designed to point auditors to cases to examine in more detail there is a danger that auditors may automatically see them as 'fraudulent'. [85]

3.3. Digital platforms and robotic process automation

3.3.1. Overview

In general, digital platforms are defined as '*digital services that facilitate interactions via the internet between two or more distinct but interdependent sets of users*' whether they are companies or individuals.[86] Digital platforms are used in a wide range of sectors and include, inter alia, search engines, online marketplaces, app stores, social media, mobile banking applications as well as other platforms for the collaborative economy.[87] As regards their application in financial management and control,

[85] Advantages and disadvantages are based on data from CSES Consultations.
[86] EBA (2021), "Report on the use of Digital Platforms in the EU Banking and Payments Sector"
[87] EP (2020), "Online platforms: Economic and societal effects"

digital platforms are seen as particularly useful as they can facilitate better collaboration between different stakeholders and can also create further added value by encouraging innovation.

Digital platforms can support more efficient information sharing, development of joint initiatives and harmonised approaches to auditing and control. However, the limitations should be carefully considered and addressed, especially if these platforms are used to share information that is not normally publicly available between different stakeholders.[88]

The benefits and limitations of the use of digital platforms in budgetary control are summarised in the table below.

Table 3.2: Benefits and limitations of the use of digital platforms for collaboration between institutions in budgetary control

Benefits	Limitations
Enhanced efficiency: digital platforms streamline workflow by allowing effective communication and information sharing between different teams and institutions. This can increase the efficiency of an investigation and prosecution activities, where timely provision of good quality data plays a vital role. The platforms can also enable automation of manual tasks, which saves time and reduces errors. **Real-time collaboration** and interactions among audit teams can be facilitated by digital platforms, regardless of their physical location. Audit team members can also feel more motivated as they actively participate in decision-making and problem solving, which can further encourage innovation. **Single repositories of data** facilitate smoother audits as all parties have access to the same information. This can reduce confusion caused by multiple versions of documents. **Document version control and tracing** can be enabled by digital platforms, including an audit trail of revisions.	**Cybersecurity and data privacy concerns:** the uptake in the use of digital platforms raises concerns about data protection and vulnerability to cyber-attacks. Ensuring robust cybersecurity measures is crucial. Furthermore, clear data ownership arrangements between financial institutions should be made before starting the audit process.[89] **Adequate skills and training are necessary** for successful implementation of digital platforms. **Unforeseen technological limitations**: the full range of capabilities and limitations of digital platforms and other digital technologies is not yet fully understood. Moreover, advancements in technology might not always keep pace with the needs of the audit process. **Interoperability challenges** might arise if financial institutions use different digital platforms. Collaboration and seamless data exchange between multiple platforms might be hindered, especially where data formats are inconsistent. Multilingual data collected from various sources must be standardised so that it can be integrated into a single platform. This requires advanced translation software that can handle technical and financial terminology accurately.

[88] Examples of information and data commonly shared between different financial institutions and/or departments during an audit process, which require careful handling and confidentiality due to their sensitive nature, include financial records, internal controls documentation, HR data, business plans and strategies, tax records and IT security data.

[89] This is particularly important in light of the European Court of Justice case law (22 November 2022, cases C-37/20 and C-601/20), which has set precedents on the limitations of processing personal data of beneficial owners. More specifically, the Court's ruling emphasises the need to balance transparency in financial dealings with the protection of individual privacy rights. More information about the Court's ruling is available at Vistra (2023),"ECJ ruling on access to beneficial ownership information: Balancing transparency and privacy"

Progress tracking: digital platforms facilitate tracking progress, milestones and tasks within budgetary control. Continuous monitoring of progress can help in ensuring timely completion of the audits.	**Legal and regulatory compliance** with data protection laws and audit standards needs to be ensured; institutions collaborating across borders could face legal complexities. **Resistance to change:** institutions may be accustomed to traditional audit methods and resist implementing digital platforms.

Source 1: Lois, P. et al. (2020), "Internal audits in the digital era: opportunities risks and challenges"
Source 2: EC (2021), "Online platforms: Economic and societal effects"
Source 3: Wegner, D., da Silveira, A.B., Marconatto, D. et al. (2023), "A systematic review of collaborative digital platforms: structuring the domain and research agenda"

The above summary highlights the need for strategic implementation and continuous development of both technology and human resources as well as the need for standardisation of data formats in order to reap the benefits of digital platforms in budgetary control.

The following sub-sections present examples of digital platforms used specifically in the fields of budgetary control and public procurement.

3.3.2. Digital platforms in budgetary control including fraud prevention, detection and investigation

The use of digital collaboration and information-sharing platforms can enhance the efficiency, speed, accuracy, and quality of budgetary control as well as fraud detection activities. This increases efficiency of the investigation and prosecution activities, where timely provision of good quality data plays a vital role. The application of new IT technologies, including digital platforms, is currently less widely-used in fraud investigation and prosecution than in fraud prevention and detection.[90] However, information shared via digital platforms can serve as an essential source of evidence and support the investigation process. Examples of digital collaboration and information-sharing platforms used in budgetary control including fraud prevention, detection and investigation in EU Member States are presented in the box below.

Box 3.5: Examples of digital platforms used in budgetary control (including fraud detection and investigation)

INFOFRAUD is an online communication channel established in 2017 by the Spanish National Anti-Fraud Coordination Service (SNCA).[91] The channel facilitates the reporting of any actions that may constitute fraud or irregularities in relation to projects or operations financed by EU funds to the relevant public authorities and thereby prompts them to investigate. SNCA analyses the information received and determines the appropriate course of action. The identities of individuals reporting information via INFOFRAUD are kept confidential, except under specific circumstances, such as legal requirements or judicial proceedings. All identities are omitted in all communications and verification activities.

MySMIS2021/SMIS2021+[92] is an integrated information system developed by the Ministry of Investments and European Projects in Romania. It entails the management of non-reimbursable external funds, and provides transparent, simplified, and easy access to EU funds.

[90] European Commission, Commission Staff Working Document, 2023.
[91] IGAE (2023), INFOFRAUD by SNCA
[92] Resurse MySMIS 2021

MySMIS2021/SMIS2021+ is able to interact efficiently with the European Commission's IT system - SFC 2021 and facilitates an electronic data exchange platform between beneficiaries and programme authorities.

BIEP (Benchmarking Information Exchange Project)[93] was initiated by the Supreme Audit Office of the Czech Republic in 2016 and offers a platform for cooperation among supreme audit institutions and encourages auditors to share ideas and experience. More than 36 institutions from the EUROSAI organisation and more than 500 SAI employees from 47 countries are active participants in the project. The data and information exchange on this platform is based on the 3C principles - communication, cooperation and comparison. BIEP contributes to saving time and audit costs. It allows users to access publicly available audit reports, analytical information or other relevant documents. There is also a non-public area with more materials such as methodologies, questionnaires and other documents as well as discussion forums.

An online platform set up by Lursoft[94] (an IT company based in Latvia), assists legal entities and individuals by providing access to a range of databases in one place, such as Latvian public and private databases, information on companies in Lithuania, Estonia, Great Britain and other European countries. Users can log in with Latvian Internet banking or e-signature to obtain information from various databases as well as gain access to a wide range of analytical services[95] for private and business needs, which help companies to develop their activities more successfully.

The Integrated Anti-Fraud Platform (PIAF)[96] is based on and complementary to Arachne. It aims to prevent fraud to the EU budget by combining data from national and EU-level sources, e.g. from the Italian Ministry of Economy and Finance, the Italian Ministry of Justice (for information on court cases), the Italian Court of Auditors (for information on cases that led to damage to the Italian national budget), the Italian Business Register (on the history of companies, and their shareholders), as well as the European Commission's IMS (for information on companies that committed fraud in other Member States), and the list of beneficiaries of EU contracts. The platform is being developed by the Italian Finance Ministry and the National Committee aimed at countering fraud against the European Union budge (Comitato nazionale per la repressione delle frodi nei confronti dell'Unione Europea, COLAF), in cooperation with five other Member States (Bulgaria, Latvia, Lithuania, Romania and Slovenia). Once fully operational, it will allow these countries to assess the activities of regional and national administrations managing EU funds, to flag risks, and to easily exchange information with anti-fraud coordination services (AFCOs) and other Member States.

3.3.3. Digital platforms in public procurement

Digital platforms facilitating collaboration and information-sharing are widely used by individual Member States for public procurement. Budgetary authorities are moving from procurement portals to digital platforms with enhanced features, such as automatic order generation, digital contract management, simplified or automated payments (e.g. for recurring purchases), enhanced account management and product and vendor reviews.

93 Benchmarking Information Exchange Project.
94 More information about the online platform set up by Lursoft can be accessed at: https://www.lursoft.lv/en
95 Analytical services include inter alia: **Financial ratios of industries**: provides financial ratios and statistical indices of different industries; **financial analysis**: review company's liquidity, activity, capital structure etc.; **relationship graph**: a data visualization tool that graphically shows relations between multiple legal or natural persons in Latvia; and **insolvency statistics**.
96 European Commission Anti-Fraud Knowledge Centre (n.d.) "PIAF (Integrated Anti-Fraud Platform)".

Examples of digital platforms used for public procurement in Germany and Czechia are presented below.

Box 3.6: Examples of digital information-sharing platforms for public procurement

The Competition Register for Public Procurement ("Wettbewerbsregister") is a new national database of criminal offenses committed by companies operating in Europe. It includes convictions, penalties, and fines related to economic offenses such as corruption, bribery, and tax evasion, as well as human trafficking. Contractors use an online portal to check whether a company is listed and, therefore, whether it can or must be excluded from an award procedure according to German law (Sections 123 or 124 of the Act Against Restraints of Competition).[97] The portal requires them to enter information about the company they wish to grant a contract to, including its VAT identification number as well as commercial register data (data contractors are encouraged to ask for during the tender process).[98] Only public contractors, sector contracting entities, and concession granters are allowed to register on the portal and check the database against any company they wish to award a contract.[99]

The Register is widely recognised to have streamlined the verification process. Before its adoption in 2022, only 9 out of 16 federal states had a 'corruption register'. In general, they only included companies that had committed offenses in the respective federal state, and only required public contractors from those states to use the register.[100] This meant that contracting authorities relied to a large extent on information applicants submitted themselves to assess whether they were eligible to receive public contracts. The new register allows contractors to check companies across the 16 states. The overall goal is to ensure fair competition and to prevent economic crime in public procurement.[101]

PROEBIZ platform[102] was set up by PROEBIZ, a company based in Ostrava, Czech Republic and specialising in digitalisation of procurement processes. The platform offers software solutions for procurements processes and activities.[103] Each solution can work independently or in conjunction with one another, having the ability to share features and data. A unified data structure ensures data compatibility and the capability to connect with other software systems. Notably PROEBIZ JOSEPHINE is a platform for the digitalisation of the procurement process. The software is designed in accordance with the European public procurement directive, so that, with the help of adjustable templates, it can meet all legislative requirements of EU Member States.[104] Currently, the tool is used in the Czech Republic, Slovakia and Poland. The system is customisable for different national electronic signatures and authentication processes.

AI sub-fields (e.g. ML and LLMs) as well as robotic process automation (RPA) are used in conjunction with digital platforms to enhance their features and to enable further automation and digitalisation in the management and control of public expenditure. ML and LLMs have been discussed in more detail

---

97 Wieler, Anne-Christine. Überblick zum Wettbewerbsregister. Lutz Label. 7 April 2023.
98 Bundeskartellamt 2023. Abfrage des Wettbewerbsregisters. Accessed 10 Noc 2023.
99 Heidland Werres Diederichs 2023. Das Wettbewerbsregister beim Bundeskartellamt
100 Jungermann, Sebastian. 2023. Das zentrale Wettbewerbsregister beim Bundeskartellamt. Deutscher AnwaltSpiegel 28 June 2017.
101 OLAF 2023. Anti-Fraud Knowledge Centre.
102 Proebiz platform
103 E.g. PROEBIZ TENDERBOX – tenders and auctions, JOSEPHINE – public tenders, WENDY – purchase request management, MARQUET – indoor catalogue and BASE – shared supplier catalogue
104 Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance

Sections 3.2 and 3.3, respectively. The following sub-section describes the RPA technology and associated benefits and limitations of its use and gives an overview of the tasks and processes that can be automated using this technology.

3.3.4. Robotic Process Automation (RPA)

RPA is a no-code or low-code software tool that can replicate and automate repetitive tasks while improving process accuracy and speed. Low-code tools require very little or very simple coding to make them work. The no-code approach requires no coding skills at all, which makes it accessible for non-technical users, as it enables them to automate processes using visual interfaces with drag-and-drop features. RPA is delivered via software robots, also known as bots. The word 'robot' in this case does not mean a physical machine, but rather a computer coded software, programmes that replace humans performing repetitive rules-based tasks and/or cross-functional and cross-application macros.[105]

The most frequent applications of RPA technology in financial control, management and auditing are the following:

- **Data extraction and consolidation:** RPA bots can extract financial data from various sources (for example invoices, grant applications, receipts etc.) and consolidate the data into a central system for further analysis.
- **Reconciliation processes**: automated bots can perform information reconciliations by matching data from different sources, such as financial statements to ledger entries, to ensure accuracy in financial records.
- **Report generation:** creation of financial reports can be automated, such as budget summaries, by gathering and formatting data into predefined report templates.
- **Audit-trail creation**: RPA software bots can track and record changes made to financial documents, creating a transparent and reliable audit trail.
- **Compliance checks:** RPA can automate the process of checking transactions and records against current compliance rules and regulations.
- **Budget monitoring:** bots can continuously monitor budget allocations against expenditures and issue an alert when there are deviations from the planned budget.

In summary, leveraging RPA technology can help institutions within the public sector to make rapid and effective improvements without a complete system overhaul and to meet strict deadlines and respond quicker. More specifically, the benefits and limitations related to the use of RPA in budgetary control are summarised in the table below.

[105] Deloitte (2017). "The new machinery of government Robotic Process Automation in the Public Sector"

Table 3.3: Benefits and limitations of the use of Robotic Process Automation (RPA) in budgetary control

Benefits	Limitations
Improved operational efficiency and resource optimisation by reducing the time and effort to complete repetitive tasks, thus allowing the audit teams, to focus on more complex issues related to audit findings. **Reduction of costs** in the long term after the initial investment to implement the technology by reducing the need for human labour or enabling staff to focus on higher-value or more complex tasks. In addition, RPA software can perform the automated tasks round the clock. **Improved compliance and data security:** automation can ensure that processes are carried out in compliance with current regulations and in a consistent manner. In addition, the risk of data breaches or unauthorised access can be reduced through automation of data encryption and access control. **Boosted accuracy** of data entry and processing by reducing the risk of errors. RPA can provide an audit trail, which makes it easier to monitor progress and resolve issues more quickly. **Easy integration** with existing legacy systems within an organisation, as well as relatively straightforward implementation process. Moreover, RPA does not necessarily require a developer to configure, which makes it ideal in cases where resources are too scarce to develop deep integrations.	**Shift in organisational culture:** as RPA deployment requires a focus on more complex tasks, the adaptability of staff is an important factor for successful outcomes in automation and digital transformation projects. Teams can be trained to adapt to the shifts in priorities. **Unable to automate more complex tasks** that require advanced decision-making as only processes with well-defined rules can be automated. **Can be difficult to scale up:** the limited ability to handle large volumes of data may hinder RPA adoption. **Unable to learn from past experiences** and needs human intervention to learn from data and to adapt to new situations.

Source 1: Dataconomy.com (2023), "Difference between robotic process automation and machine learning"
Source 2: Shinde, B. (2021), "Artificial Intelligence Adoption in Internal Audit Processes"
Source 3: IBM (2023), 'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM

3.3.5. Differences between using RPA and AI technology for finance management and budgetary control

RPA is often mistaken for AI when in fact the two technologies are different, however, can complement each other well (their complementarity is discussed in more detail in Section 3.6).Generally speaking, AI simulates human intelligence, while RPA replicates human-directed tasks.[106] The paragraphs below discuss the difference between RPA and AI technologies and explore how these technologies complement each other as well as the benefits of combining the use RPA and AI, highlighting the

[106] IBM (2023), 'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM

specific applications of these two technologies when it comes to aiding the audit process and ensuring sound financial management.

RPA and AI technologies can both make processes more efficient by automating certain tasks. However, there are differences in how these results are achieved, in terms of the type of input data that can be handled by these technologies, the level of human intervention that is required and their adaptability and scalability within an organisation.

RPA uses software applications to automate tasks that are repetitive, rule-based and require high degree of accuracy (e.g. transferring data from funding application or an invoice into an organisation's financial management system; cleaning and formatting data; expense tracking; reporting). RPA is not used for predictive analytics and insight generation (i.e. to uncover irregularities and fraud). Instead, RPA limits the need for human intervention in performing repetitive tasks. RPA can work independently without any intervention, although some level of human oversight may be required to ensure the accuracy and quality of the output. The technology can be easily integrated within existing legacy systems that are used within an organisation.[107] Users that have some experience with digital tools and/or for instance regularly use functions in spreadsheets can introduce an RPA software into their workflow relatively easily as well as build simple RPA after a couple of weeks of RPA training.[108]

Sub-fields of AI that have been discussed in more detail in sections 3.2 and 3.3 (e.g. machine learning and natural language processing) enable continuous learning from data and thereby improving the performance of systems and gradually making them more accurate at performing complex tasks (e.g. fraud detection; identification of other patterns and anomalies in large datasets; classification of data into categories, making predictions based on historical data etc.). As opposed to RPA, AI technologies often require a significant amount of data preparation (data labelling, model selection, tuning etc.) and training before they can be deployed. [109]

3.4. Distributed ledger technologies: Blockchain

3.4.1. Overview

A blockchain is a distributed ledger or a record of encrypted data and transactions that is duplicated and shared across a network of computers. The blocks in a blockchain can be thought of as a page in a ledger, or a folder in a filing cabinet. These pages or files can record different types of information such as assets or contracts. Unlike a traditional ledger or a filing cabinet, however, a blockchain does not sit in a single location. It is distributed across a network of computers (called 'nodes') which makes it highly secure and resistant to manipulation or forgery. Once a piece of data is recorded inside a blockchain it is almost impossible to modify.

Blockchain was first invented by two researchers, Stuart Haber and W. Scott Stornetta in 1991 as a way to timestamp digital documents to make it impossible to backdate them – much like a digital notary or a digital audit log. The technology went largely unnoticed until a researcher under the pseudonym of Satoshi Nakamoto used it in 2009 to create the digital cryptocurrency Bitcoin.[110] While cryptocurrencies

[107] Dataconomy.com (2023), "Difference between robotic process automation and machine learning"

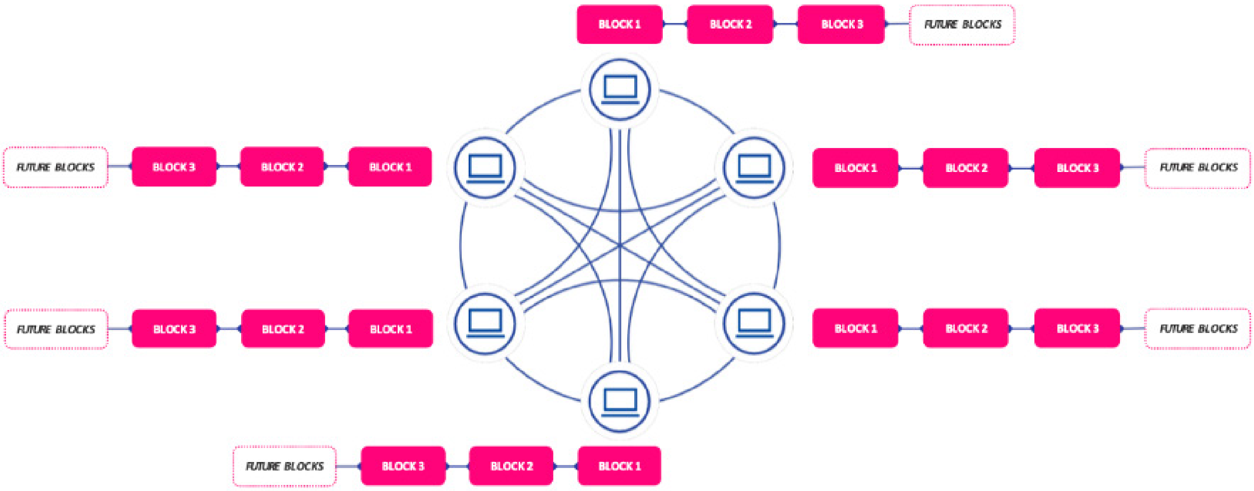
[108] 'However, when it comes to complex business processes or automating at scale, someone with an IT background and past experience developing automation software is essential', see IBM (2020), "Seven perspectives on what's required to ensure business users can easily and effectively build software robots.", Fact vs. Fiction: Business Users Can Easily Build Software Robots Using RPA Tools - IBM Blog

[109] Dataconomy.com (2023), "Difference between robotic process automation and machine learning"

[110] Williams-Elegbe, S. (2019). Public Procurement, Corruption and Blockchain Technology in South Africa: A Preliminary Legal Inquiry. SSRN Electronic Journal.

are perhaps the most well-known application of blockchain, the technology can be used to record many other types of transactions, including tax transactions, real estate transactions, or even vaccinations.[111]

Figure 3.3: Blockchains



Source: European Blockchain Services Infrastructure (2024). [Blockchain, a resilient source of truth]

The figure above illustrates how a decentralised ledger works. In this example, the data is distributed across six computers, or nodes in a network. Each computer contains an exact replica of the whole chain of transactions, stored in chronological order. Here, the chain contains three blocks. Each block stores information on some data or transaction and a reference to the previous block in the chain. For instance, in a blockchain of financial transactions Block 1 might contain information about the amount of money an official managing public funds has received from a public authority; Block 2 might contain information about a payment they made to a beneficiary, and Block 3 might contain information about a payment the beneficiary made. In addition to the actual data (e.g. the record of who sent what to whom), each block contains a unique fingerprint – called a hash – which is derived from the data it stores. That hash might include the index (i.e. the position of the block in the chain, e.g. whether it is the first transaction, Block 1, the second, third etc.), the fingerprint of the previous block (or the previous hash), and a timestamp (e.g. the date of the transfer).

The distribution of records across a network of computers makes it highly secure and resistant to any attempts to modify data retrospectively. New blocks are added to the chain by consensus (i.e. all computers in the network check whether the data matches up). Once added to the chain, a record cannot be modified. If someone tried to modify it, for instance, if a beneficiary tried to pretend to have paid more for goods than they did, the hash of the block that records that transaction would change, and it would no longer match the fingerprint that had been recorded by the following block. Moreover, it would no longer match the record stored by the other five computers in the network. Whenever someone new joins the network they receive the full copy of the blockchain, including all hashes, and previous hashes.

Blockchain networks have rules about who can join and participate. There are three main types of blockchain networks: 'public', 'private, and 'consortium' networks.

- Public blockchains are mainly used for exchanging cryptocurrencies. They are permissionless and non-restrictive. Anyone can join, anyone can add and verify transactions and, once recorded, view

[111] European Blockchain Services Infrastructure (2024). [Blockchain, a resilient source of truth]

all the transactions recorded in the blockchain. Public blockchains operate on a decentralised network of nodes, making them resistant to control by a single authority. As all transactions are visible to anyone in the network, they offer the highest levels of transparency.

- Private blockchains are best suited for organisations that wish to use blockchain for internal purposes, since they are permissioned and restrictive. Because private blockchains restrict access to authorised individuals they are able to maintain confidentiality. They also allow greater control over the rules of the network.
- 'Consortium networks' (or federated Blockchains) works well for a group or consortium of entities (e.g. financial institutions, insurance companies, or healthcare institutions) wishing to exchange sensitive, or confidential information. Unlike a private blockchain, consortium blockchains are decentralised; there is more than one authority in charge. Yet like private blockchains, network members have a degree of control over who can join the network. Typically, each member of the consortium will run at least one note. Each node can read and write transactions. New blocks (i.e. new data, or new transactions) have to be approved by each node.[112]

Blockchain technologies also enable smart, or self-executing contracts. Smart contracts are agreements that are automatically enforced once the predefined conditions are met. A smart contract requires no trust between the parties; both parties know that the money will be paid if the condition is met. Because contracts are automatically executed there is no need for intermediaries such lawyers to verify ownership of an asset or to ensure that both parties comply with the terms of the contract. For example, the Swedish land registry uses smart contracts to register real estate transactions, which is said to have reduced transaction times by over 90%.[113]

Estonia offers an example of an EU Member State that has applied blockchain across a range of government functions including budgetary control: Estonia's KSI ('Keyless Signature Infrastructure') Blockchain technology is used to secure digital identities (e-Residency), and to protect sensitive digital data in health: Estonia maintains an e-Health Record and a e-Prescription database, which keeps health information secure and accessible to authorised individuals, and to prevent damage to a person's health by, for instance, giving them the wrong medicine or dose. Estonia also uses blockchain in law (e-Law and e-Court systems), in policing (e-Police data), in banking (e-Banking), business (e-Business Register), in land registration (e-Land Registry), and in defence (to prevent the manipulation of defence data or smart war machines).[114] Many other countries are in the process of developing and testing blockchain solutions, as illustrated by the examples presented in the table below.

[112] Blockchain Council (2023, Nov 14). Types of Blockchains Explained- Public Vs. Private Vs. Consortium, see also Medium (2022, Jan 5). Types of Blockchain.
[113] Modin, J. (2021, February 8). Balancing Blockchain and AI: ChromaWay and the Swedish Land Registry Submit Findings for Government Report. Chromia, see also Pandey, A. (2022, November 6). How governments can harness the potential of blockchain. McKinsey Digital.
[114] E-Estonia. (2024). KSI Blockchain Stack: Zero Trust Applications. Digiexpo.e-Estonia.Com. https://digiexpo.e-estonia.com/cyber-security/ksi-blockchain-stack-zero-trust-applications/ , see also E-Estonia. (2024). Frequently Asked Questions. Estonian Blockchain Technology.

Box 3.7: Blockchain applications in public administration

- **Finance.** Blockchain technology is used to ensure transparency in financial transactions, for cross-border payments, digital currencies, micropayments, and payment tracking. Countries, including the Bahamas, Jamaica, and Nigeria have introduced central bank digital currencies.[115]
- **Identity verification or digital credentials.** Blockchain technology is used to back up digital identities, e.g. in Australia, or in Estonia[116] which make it easier for customers to prove their identity, for instance, to access online banking or online public services (including online voting in Estonia), or to prove their age (e.g. to buy alcoholic beverages). Digital identities also reduce the risk of identity theft.
- **Tax collection.** Blockchain technology is used to collect taxes, e.g. in Denmark or Estonia. Blockchain technologies can replace the traditional tax system where individuals and businesses send their financial records to the tax authorities at the end of the tax year, with a system where they have real-time access to financial data. Blockchain-powered tax systems allow tax authorities to detect tax evasion as it happens. In addition, it prevents the errors, omissions, and disputes that come with manually reporting taxes.[117]
- **Healthcare.** Blockchain technology is used to store patient records, e.g. in Estonia. It was also used during the COVID-19 pandemic, when the World Health Organisation, various government agencies and private-sector companies including IBM and Oracle Microsoft collaborated in building a blockchain-based open data hub called MiPasa to detect infection hotspots and COVID-19 carriers across the world, and to share this information with hospitals and public health institutions .[118]
- **Education**. Blockchain technology is used to store and verify academic credentials or certificates for mobile workers. Malta, which has branded itself the 'Blockchain Island' implemented the world's first pilot project for a nationwide project for issuing academic credentials to a blockchain in 2017.[119] Other institutions using blockchain to verify credentials are in Singapore,[120] Spain (Universidad Carlos III de Madrid[121]), and the US (e.g. MIT)[122]. This reduces verification costs for non-citizens and improves trust in their diplomas.
- **Voting systems.** Blockchain technology is used to enhance the security of electronic voting systems and reduce election fraud, e.g. in Estonia, Denmark, Switzerland, or in West Virginia, USA.
- **Trade and supply chain management.** Blockchain technology is used to track and trace products in supply chain, e.g. in China, Singapore, Switzerland and the US, and by large companies such as Amazon, British Airways, Coca-Cola, FedEx, Ford, Maersk, UPS, and Walmart.[123]
- **Property and land registration.** Blockchain technology is used to create timestamped and immutable records for land and property ownership, real estate transactions, and other legal

---

115 Kumar, A., Chhangani, A., Brownstein, G., & Meng, P. (2024). Central Bank Digital Currency Tracker. Atlantic Council. see also Adrian, T., Dong, H., Mancini-Griffoli, T., & Sun, T. (2023, November 20). Central Bank Digital Currency Development Enters the Next Phase. IMF Blog, Jones, M. (2023, June 29). Study shows 130 countries exploring central bank digital currencies. Reuters.

116 Dock. (2024, January 10). Blockchain Identity Management: Complete Guide 2024. Dock.Io.

117 Funmilayo, Mebude (2023, Nov 2nd). Enhancing tax transparency with blockchain technology.

118 Van Hoek, Remko & Lacity, Mary (2020, April 27). How the pandemic is pushing blockchain forward. Harvard Business Review. See also Singh, G., & Levi, J. (2020, May 27). MiPasa project and IBM Blockchain team on open data platform to support Covid-19 response. IBM Blog.

119 Cocks, P. (2017), Malta first to launch education blockchain certification, Malta Today

120 Smartnation.gov.sg. Graduate with a Digital Academic Certificate.

121 Unviersidad Carlos III de Madrid (2018), Acreditaciones de Competencias Utilizando la Tecnología Blockchain en Cursos Spocs.

122 Durant, Elizabeth (2027, Oct 17). Digital Diploma debuts at MIT.

123 Freeman, O. J. (2023, March 8). 10 Companies Using Blockchain Technology for Sustainable Supply Chain. Medium. Krauth, O. (2022, September 16). Five companies using blockchain to drive their supply chain. Tech Republic.

records, e.g. in Canada, Georgia[124], Nigeria[125], Russia, South Korea or Sweden.[126] Blockchain systems streamline the lengthy process of buying property and protect property rights, fuelling business activity. Blockchain land registration systems are particularly appealing for environments in which acquiring property requires paying officials bribes and in which land ownership is frequently contested (for instance, because fraudsters with friends in land registration agencies sell a piece of land which they may not even need to own to multiple buyers.) With blockchain, sellers can prove the property is theirs, buyers do not need to pay bribes, and have certainty that they will receive the land after they have paid the price. For those reasons, governments, NGOs, and tech startups across the world, including, for instance, in Kenya, are investigating blockchain solutions for land registration.[127]

3.4.2. Blockchain in public procurement

Some national governments are testing the use of blockchain in public procurement. For example, Peru is cooperating with the blockchain startup Stamping.io to create a fraud-resistant, blockchain-based verification system for government contracts.[128] Preliminary findings from South Africa, which is trialling a new, blockchain-powered open tender process show that the new system has reduced corruption and increased operational activities.[129] Similarly, a project in Ghana using blockchain to track subsidies for farmers purchasing fertiliser has increased transparency and reduced corruption in the distribution of these subsidies.[130] A project in Kenya using blockchain to track the delivery of medical supplies to hospitals has reduced theft and diversion, making sure that supplies intended for hospitals reach hospitals.[131] The textbox below describes an example of blockchain in public procurement in Colombia in more detail.

Box 3.8: Blockchain in Public Procurement: An example from Colombia

Colombia is trialling the use of blockchain in public procurement. After a number of high-profile cases of corruption around school lunches, involving suppliers either not supplying food at all, or supplying it at inflated costs (e.g. selling chicken breasts at four times the price of local supermarkets) Colombia's Office of the Inspector General teamed up with experts from the Inter-American Development Bank and the World Economic Forum to investigate, design, and trial the use of blockchain in public procurement. The initial project will focus on the phase with the highest risk of corruption: the selection of contractors.[132]

The goal is to make the bidding process more transparent, fairer, and more competitive. Once the system is operational, bidders will submit encrypted proposals which will be stored on computers across the blockchain network. Once a bid is submitted, it cannot be modified or manipulated. The software will then automatically evaluate those bids and eliminate those that do not meet the requirements, and publish the results of those that do. Third, a winner is selected. Depending on the nature of the selection process, the procurers can either choose to let the system choose the winner

[124] Shang, Q., & Price, A. (2019). A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. Innovations: Technology, Governance, Globalization, 12(3–4), 72–78.
[125] Burola, Thomas (2023, Aug 9th). Public Procurement: Blockchain.
[126] Berryhill, J., T. Bourgery and A. Hanson (2018), "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", OECD Working Papers on Public Governance, No. 28, OECD Publishing, Paris.
[127] F6S (2024, Feb 8th). 38 top Blockchain companies and startups in Kenya in 2024.
[128] Stamping.io. APIConnector to decentralized services of #web3.
[129] Faal, E. (2023, September 27). Blockchain could revolutionise public procurement and combat corruption in Africa. LSE Blogs.
[130] Burola, Thomas (2023, Aug 9). Public Procurement: Blockchain.
[131] Ibid, see also Orisakwe, Jennifer (2023, Apr 26). East Africa keenly explores blockchain technology in healthcare. Omnia Health.
[132] Kshetri, Nir (2022, Nov-Dec). Blockchain's Role in Fighting Corruption and Improving Public Sector Efficiency in Developing Countries.

automatically or they can do so manually. Whatever approach is taken, a record of the assessment, and of any interventions actions or decisions remains recorded in the system.[133]

The experience of Colombia suggests that political will is essential to the successful adoption of any solution. For example, adopting a new, decentralised ledger for public procurement bids requires public policies, and a solid regulatory framework. Given that there are other opportunities for corruption outside the bidding process and beyond the reach of the blockchain, the success of the project will also depend on the commitment of public authorities to fight corruption.

Using blockchain to record transactions in public procurement can eliminate corruption at various points in the process. First, it forces tenderers to publicly commit to contract terms and selection criteria before they elicit bids.[134] Having an immutable record of the selection criteria eliminates the risk that a tenderer tailors the selection criteria to a favoured contractor after the tender is published. It can also increase the possibility that an outsider can win. Having an immutable record of the submitted bids prevents contractors from changing their bids after they learn new information about competing bids.

Shifting to blockchain should also increase trust that the process is fair. That trust, in turn, ought to attract more bids, increasing competitiveness and leading to cost-effective winning bids. Finally, because all actions and decisions are automatically recorded, and permanently, and publicly viewable, the procurement process is easier to monitor from the outside. Monitoring can happen in two ways: First, it is possible to include a user interface allowing the public to monitor actions and decisions and to flag risks in real time. Second, the records are auditable; audit authorities have immediate access to the entire history of the procurement process.[135]

In some ways, blockchain and digital platforms serve the same purpose, namely storing information. The main differences concern the number of places the data is stored, the number of entities involved in verifying it, and the way new data is entered. Digital platforms are generally stored in one place (disregarding backup sites) whereas data stored in a blockchain is stored in many places. The data in a digital platform is generally verified by one entity (aside from auditors), whereas the data in a blockchain is verified by all entities that are part of the network.

Table 3.4: Benefits and limitations of using blockchain in public procurement

Benefits	Limitations
Transparent: Data stored in a blockchain is permanently recorded on all computers in the network. It is traceable and auditable. **Tamper-proof:** Members of the network can add to a blockchain but cannot change records that are already recorded, meaning that data stored in a blockchain is tamper-proof and immutable.	**Requires advanced IT infrastructure**: Blockchain networks require stable electricity, secure internet connections, and large data storage capacities. **Cost**: Building and maintaining blockchain networks is more expensive than traditional databases.[138] **Interoperability:** Blockchains cannot easily be linked with other databases.

133 Rodriguez, Daniel & Gutierrez, Paula Andrea (n.n.) Implementation of blockchain in public procurement to reduce corruption risks.
134 It is worth noting that this is already the norm for EU contracts. All EU contracts are published online and cannot be altered. However, at a national level, there remain risks of corruption in the pre-tendering and the tendering phase, see OECD 2016. Preventing Corruption in Public Procurement.
135 Kshetri, Nir (2022, Nov-Dec). Blockchain's Role in Fighting Corruption and Improving Public Sector Efficiency in Developing Countries.
138 Budhi, Veera (2022, Oct 20). Advantages and disadvantages of blockchain technology.

Private: While public blockchains show transaction data, private and consortium blockchains restrict access to all data a closed network, ensuring high levels of confidentiality.[136] **Guarantees regulatory compliance:** Smart contracts promise to guarantee compliance. **Public blockchains require no trust:** they do not require intermediaries or central authorities to process or approve transactions, making them a useful technology for low-trust environments.[137]	**Data protection:** There are some concerns around storing personal data, the 'right to be forgotten' in Article 17(1) GDPR, and not having a 'data controller' who could be held accountable. **Immature smart contracts:** Results from a first generation of self-executing contracts have been promising but not 100% reliable.[139] **Energy usage:** certain types of public blockchains, in particular, Bitcoin, consume a large amount of energy, raising questions about environmental sustainability.[140] **Speed, performance, and scalability:** public blockchains are much slower than traditional databases, and can face challenges handling large numbers of transactions simultaneously, storing data, an increasing the number of nodes running the network efficiently.[141] **Privacy:** While the data is encrypted identity, transactions on public blockchains are visible to all.[142] **Risk of a '51% attack':** Theoretically, a group of miners controlling more than half of its computational power would allow the controlling parties to alter the blockchain. Due to the high cost of acquiring that level of computing power, 51% attacks are generally limited to smaller cryptocurrency networks.[143]

3.5. Satellite imagery for budgetary control

The use of satellite imagery in public administration is well-established, including in the field of budgetary control. Satellite imagery show photographs of the Earth captured by satellites orbiting the planet. These satellites are fitted with diverse sensors designed to detect visible light, infrared light, microwave radiation, and other wavelengths, enabling the creation of high-resolution images of the Earth's surface. The images are used to monitor developments in climate, geography, and human-

[136] Louw, Liz (2022, Feb 22). How public and private blockchain compete on data privacy and throughput; Hayes, Adam (2023, Dec 15). Learn what these digital public ledgers are capable of.

[137] Sharma, Toshendra Kumar (2023, Nov 14). Types of Blockchains Explained – Public vs. private vs. consortium. Blockchain Council.

[139] Zaazaa, Oualid, El Bakkali, Hanan El (2023, Dec 1). Unveiling the Landscape of Smart Contract Vulnerabilities: A Detailed Examination and Codification of Vulnerabilities in Prominent Blockchains. Cornell University.

[140] This relates mainly to bitcoin because bitcoin uses a very specific process to add new blocks to a chain: In order to validate a new block, members of the network compete to solve a puzzle (and earn a reward) that require significant computing power. This validation process, called 'proof of work', requires extremely high levels of energy. Researchers estimate that bitcoin alone consumes more than 127 TWh per year – an amount that is equivalent to the annual electricity consumption of many countries, including the Netherlands, or Norway. See Huestis, Samuel (2023, Jan 30). Cryptocurrency's Energy Consumption Problem. RMI. This point is discussed in more detail in the case study in Appendix A.

[141] Finextra (2023, Sep 26). Blockchain and the scalability challenge: solving the blockchain trilemma.

[142] Louw, Liz (2022, Feb 22). How public and private blockchain compete on data privacy and throughput; Hayes, Adam (2023, Dec 15). Learn what these digital public ledgers are capable of.

[143] Frankenfeld, Jake, Rasure, Erika, Kvilhaug, Suzanne (2023, June 7). 51% Attack: Definition, who is at risk, example, and cost. Note that there are a few examples of 51% attacks on larger currencies: In May 2018, Bitcoin Gold experienced a 51% attack worth USD 18m of BTG; two years later, in August 2020, Ethereum Classic experienced an attack worth USD 5.6m. Bartosz (2023, June 29). 51% Attack: The Concept, Risks, and Prevention, Hacken.

made structures in real time.[144] Satellite imagery is used in various sectors across government including defence, communication, agriculture, forestry, disaster management, urban planning, and many others. The European Space Agency and Copernicus, uses satellite imagery for environmental monitoring and climate research.[145]

The EU's Copernicus Sentinel satellites support budgetary control through the provision of frequent and high-resolution images and data to paying agencies for the Common Agricultural Policy (CAP). The CAP has allowed the use of aerial photographs and satellite images to check its area-based support since 1992. Such images and data can be processed automatically without human intervention, which helps the agencies to monitor agricultural practices and check aid applications for some schemes (so-called "checks by monitoring"). However, take-up of Sentinel data and digital cloud services has been limited to date.[146]

A 2003 CAP reform required Member States to create a computerised geographic information system, recording all their agricultural parcels. This system came to be known as the Land Parcel Identification System (LPIS). LPIS data is comprised of georeferenced parcels (or blocks) of agricultural areas which are potentially eligible for EU support. A 2013 CAP reform then made it compulsory to use the LPIS system. In 2015, CAP introduced another tool to enhance checks of aid applications: the Geospatial Aid Application (GSAA). GSAA data is comprised of georeferenced parcels of agricultural areas which are in agricultural use and for which individuals have applied for aid.[147] The high resolution of LPIS photographs (around 25-50cm per pixel) make it possible for paying agencies to use the LPIS for cross-checks on all area-aid applications to verify that funds are only paid for agricultural land that is eligible and that it is only paid once for every area of land. However, due to the low frequency of updates to LPIS images, they cannot be used to verify activities that take place on the respective parcels during the year (i.e. planting, harvesting, mowing, etc.).[148] Here, remote sensing comes in handy. Since 1992, the Commission has used satellite images from commercial providers (e.g. SPOT, WorldView, and PlanetScope) to check the parcels throughout the year ('checks with remote sensing'). Nowadays, around 80% of field inspections use remote sensing. The paying agency will only come for 'rapid field visit' if the images are unclear. To apply for CAP funding, farmers can now submit the geo-location of their declared agricultural parcels along with their applications, allowing the paying agencies' IT systems to link geospatial information to agricultural parcels.

A major achievement in the European satellite infrastructure was the Copernicus Programme and the launch of the EU-owned Sentinel satellites 1 and 2 in 2015. The new satellite images offer very high spatial resolution (10 metres spatial resolution per pixel) every 5 days (more frequently even than the US satellite Landsat every 16 days). Time series Sentinel data allows agencies to identify specific crops and monitor action such as harvesting with very high levels of precision. In May 2017, EU paying agencies endorsed the "Malta Declaration," urging the Commission to use new technologies to simplify its Integrated Administration and Control System (IACS), the database set up and operated in each Member State to manage CAP payments. A month later, the Commission proposed legislative changes to allow 'checks by monitory' as of 2018. Since then, Member States can automate their checks

---

[144] Mapbox. (2024). What is Satellite Imagery? Exploring the full picture. Mapbox.

[145] European Commission, D. C. (2015). "Copernicus. Europe's Eyes on Earth"

[146] European Court of Auditors (2020) "Using new imaging technologies to monitor the Common Agricultural Policy: steady progress overall, but slower for climate and environment monitoring"

[147] Euro Data Cube Consortium. (2024). IACS - LPIS/GSAA data - Easy access to publicly available georeferenced agricultural parcels in EU Member States. Eurodatacube.Com. https://eurodatacube.com/marketplace/data-products/lpis

[148] Owen, P. W., Roberts, G., Bortnowschi, R., Prigent, O., Hardy, R., Dolezal, J., Brems, E., Braz, P., Ruiz, A. C., Chaudry, A., Konstantopoulos, M., Poulsen, A., Scheckenbach, B., & Ulander, P. (2020). Special Report 04/2020: Using new imaging technologies to monitor the Common Agricultural Policy: steady progress overall, but slower for climate and environment monitoring. In Luxembourg: Publications Office of the European Union., p.8.

using Copernicus Sentinel data. Member States are also free to use other new technologies, such as drones and geotagged images or data captured by other satellites as supplementary evidence for compliance checks under the CAP.

Sentinel data has been a gamechanger in the management and control of the CAP. Paying authorities can now use machine learning algorithms to process large quantities of photographs, and obtain accurate information on crop types and agricultural activities on each parcel, and throughout the year. The checks by monitoring approach have simplified checks for paying authorities and for farmers. Traditionally, paying authorities had to select small samples of farmers to check and then visit the farms to check the parcel area and the crops grown against the information the farmer had provided in their aid claim. Satellite imagery has made it possible to replace this costly, time-consuming check of just a few farms with a cheaper, quicker check of all farms. Under the new approach, paying agencies can monitor all agricultural parcels in their region and limit field visits to cases where the images are inconclusive or where non-compliance would have a particularly high financial impact.

The uptake of Satellite imagery differs depending on the Member State. Some paying authorities use it more systematically to check aid requirements, whilst others choose not to. The textboxes below offer three examples of paying agencies who have successfully integrated satellite data into their workflow.

Box 3.9: Sentinel Data in Spain (Castile and Leon), Belgium (Flanders), and Estonia

Flanders, Belgium: Sentinel data is used to monitor the eligibility requirements for three agricultural schemes. Under these schemes, farmers are required to demonstrate the use of their land for agricultural activities. To achieve this, a machine learning algorithm has been developed and trained using a time series of Sentinel 1 and 2 images alongside information provided in farmers' declarations. This algorithm predicts the probability that each parcel belongs to one of five classes: arable land, grassland, leguminous crops, fallow, and non-eligible. Parcels where the algorithm's prediction contradicts the farmer's declaration are flagged with a red marker, prompting a follow-up field visit. Parcels with inconclusive outcomes are marked with a yellow flag and are further monitored on screen, with field visits conducted if necessary. Notably, in 2019, permanent crops were excluded from this process, as they are verified using an update of the LPIS (Land Parcel Identification System). This integration of Sentinel data represents a significant advancement in budgetary control of agricultural subsidies in Belgium, facilitating more accurate assessments of land use and eligibility for agricultural schemes.

Castile and Leon, Spain: the paying agency is leveraging Sentinel data from satellite imaging to monitor agricultural schemes across nine categories. While basic schemes require simple verification of land use—whether it's arable land, grassland, or for permanent crops—more detailed crop identification is necessary for greening and voluntary coupled support. To achieve this, Spain employs a machine-learning algorithm trained on farmers' declarations for crop classes and uses additional data sources to identify non-crop classes. This classification process involves 26 crop classes and 9 non-crop classes, with time series of Sentinel 2 images serving as the primary data source. These images are complemented with climate data, as well as information on elevation, aspect, and slope. Furthermore, various markers have been developed, including those related to specific crop types or to detect certain events such as land preparation for cultivation. Parcels that are inconclusive or potentially non-compliant are flagged with a yellow marker. Parcels exceeding a certain financial threshold undergo further scrutiny in the office and, if still inconclusive, prompt a field visit. This integration of Sentinel data has transformed the budgetary control of agricultural subsidies in Spain, enabling more accurate and efficient assessment of land use and compliance with agricultural schemes.[149]

Estonia: the Agricultural Registers and Information Board (ARIB) has adopted satellite imaging technology to automate the monitoring of grassland activities. The SATIKAS system, sourcing data from the European Copernicus Programme, employs AI to monitor mowing activities across Estonian grasslands. This system uses deep learning methods and convolutional neural network approaches to analyse the satellite data from the European COPERNICUS programme to automatically detect whether mowing has taken place on the Estonian grasslands As labour costs escalate, traditional field inspections have become more expensive, prompting the need for a more efficient method to ensure compliance with subsidy requirements. The goal of the project was to automate the EU's agricultural subsidy checks to help to reduce the need for inspectors' field visits.[150] SATIKAS emerged from collaborative efforts between ARIB, CGI, and the Tartu Observatory. It is powered by deep learning methodologies such as recurrent and convolutional neural networks, SATIKAS analyses data from Sentinel-1 radar and Sentinel-2 optical satellite images. Supported by funding from the European Regional Development Fund, SATIKAS utilised diverse resources and expertise from various organisations, including the University of Tartu's Institute of Computer Science and the Software Technology and Applications Competence Centre. As the project expanded, technological infrastructure adapted to accommodate the increasing data volumes, transitioning to the Environmental Agency of the State Service's infrastructure. Ultimately, SATIKAS demonstrated its value as concerns regarding job displacement among field inspectors proved unwarranted. Stakeholder acknowledged the system's effectiveness, highlighting Estonia's commitment to harnessing technological innovation for budgetary control in relation to agricultural subsidies.[151]

The continual evolution of satellite imaging together with the use of AI are likely to transform multiple EU monitoring and budgetary control systems. At the EU level, this can be used to ensure that funds allocated for such projects are being used effectively and that projects progresses as planned. Especially, in the fields of agriculture, resource monitoring, disaster response and infrastructure monitoring such developments have the potential to enhance the efficiency, transparency and efficacy of the current EU monitoring systems.

3.6. Possible synergies between RPA and AI

RPA and AI specific sub-fields (ML and OCR) are complementary technologies that can work together to improve operational efficiency and enhance the quality of data-driven budgetary control. More specifically, AI can help RPA automate tasks more fully, handle more complex data as well as find patterns in data or extract meaning from images, text or speech.[152] In turn, RPA can enable AI insights to be actioned faster without having to wait on manual implementations.[153]

Intelligent automation (IA) is a term that describes the combination of RPA, AI and other related automation technologies. One example of the application of IA technologies in practice is the

---

149 Owen, P. W., Roberts, G., Bortnowschi, R., Prigent, O., Hardy, R., Dolezal, J., Brems, E., Braz, P., Ruiz, A. C., Chaudry, A., Konstantopoulos, M., Poulsen, A., Scheckenbach, B., & Ulander, P. (2020). Special Report 04/2020: Using new imaging technologies to monitor the Common Agricultural Policy: steady progress overall, but slower for climate and environment monitoring. In Luxembourg: Publications Office of the European Union, p.32

150 Tartu Observatory. (2019, January 24). Information system SATIKAS helps to detect mowing by using satellite data. University of Tartu. https://kosmos.ut.ee/en/content/information-system-satikas-helps-detect-mowing-using-satellite-data

151 Van Noordt and Misuraca, "Exploratory Insights on Artificial Intelligence for Government in Europe."

152 Deloitte (2019), "Automation with intelligence Reimagining the organisation in the 'Age of With'", dt-Automation-with-intelligence.pdf (deloitte.com)

153 IBM (2023), 'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM

Intelligent Document Processing (IDP), which uses IA to extract, process and validate data from images and other files where data often appears in an unstructured format.

In order to decide which technology or combination of technologies would be most efficient in automating organisation's processes, it is necessary to start with determining exactly which tasks should be automated and the associated level of complexity – would it be a simple and repetitive task such as pulling data out of a spreadsheet, classifying information or making more complex decisions? The complexity of tasks will give an idea of the type of technology/combinations of technologies needed to perform the tasks and, secondly, how much expertise will be required to deploy the technologies, i.e. in case of automating complex business processes using IA or automating at scale, it is essential to involve someone with an IT background and experience in developing automation software.[154] As noted in Deloitte (2019), which surveyed organisations piloting, implementing or scaling up IA technologies, it was forecasted that IA would provide an average cost reduction of 22% and an increase in revenue of 11% over the next three years from the date of IA implementation.[155]

3.7. E-learning and knowledge sharing supporting budgetary control

E-learning and knowledge sharing services are an increasingly popular way of enhancing the knowledge of individuals involved in public procurement or other aspects of budgetary control. E-learning can be delivered in a web-based Massive Open Online Course (MOOC) format or via online streaming. The goal of e-learning and knowledge sharing services is to streamline the public procurement process while ensuring that it is efficient and transparent. Generally, the success of training and e-learning programmes relies on the capacity and knowledge of the experts sharing the good practices. The content of the programmes should be based on national needs and the regulatory framework and tailored to the specific needs of learners. Some examples are summarised in the box below.

E-learning and knowledge sharing services could be used to strengthen the capacity of the competent authorities in the field of budgetary control. In particular, they could help staff members gain a better understanding of the rules applicable to the management and control of funds and thus ensure better compliance with legislation. They would also help retain relevant information on the interpretation of irregularities and cases of misuse of funds at the institutional level thus contributing to more effective controls.

Box 3.10: E-learning and knowledge sharing services supporting budgetary control

ePROCUREMENT.TV - Knowledge sharing and e-learning tool set up by PROEBIZ (based in Ostrava, Czech Republic). ePROCUREMENT.TV is a shared streaming channel for corporate and public procurement. The channel was set up in 2020 during the Covid-19 pandemic and currently broadcasts in four languages: Czech, Slovak, Polish, and English. The individual broadcasts cover a wide range of private and public procurement topics from many different perspectives of different producers. Most broadcasts are between 25-30 minutes long and presented by procurement specialists, prominent industry figures and providers of electronic tools who share their knowledge on legislative issues, copyright, HR and modern technology in public and private procurement.[156]

[154] IBM (2020), "Seven perspectives on what's required to ensure business users can easily and effectively build software robots.", Fact vs. Fiction: Business Users Can Easily Build Software Robots Using RPA Tools - IBM Blog

[155] Deloitte (2019), "Automation with intelligence - Reimagining the organisation in the 'Age of With'", dt-Automation-with-intelligence.pdf (deloitte.com)

[156] ePROCUREMENT.TV, available at: https://eprocurement.tv/ (explanatory text on the website is currently only accessible in Czech language, however, broadcasts are available in four languages: EN, CZ, PL and SK)

Certificate Program in Public Procurement (CPPP) is a distance learning programme offered by The Governance – Global Practice of the World Bank and the partner institutions of Charter for Public Procurement Studies (CPPS) that can be accessed free of charge by users online. The CPPP is offered in a MOOC format and delivers e-learning courses for procurement professionals who want to update their knowledge, non-procurement professionals, employees of private sector bidding in public procurement as well as others interested in public procurement.[157]

C.A.T.O.N.E. project ("Cooperation Agreements and Training on Objectives and New Experiences")[158] was set up by the Commission's DG for International Partnerships in partnership with the Italian Court of Auditors. It supports the collaboration and exchange of good practices between the Court of Auditors and accounting and criminal prosecution offices in Portugal, Spain, France and Greece, as well as EU stakeholders (OLAF, EPPO, EU Court of Justice, EU Court of Auditors, AFCOS). The project includes training sessions and focuses on how to enhance the IT systems for reporting irregularities related to EU funds. It aims to enhance cooperation and share knowledge among the Member States to effectively combat fraud and ensure the proper use of EU financial resources. The project entailed an international training event held online via videoconference by the prosecutor general of the Italian Court of Auditors and the National Committee aimed at countering fraud against the European Union budget (COLAF). The training programme covered different topics including the protection of EU financial resources and the improvement of effective procedures for the recovery of fraudulent or unduly received resources.

157 Procurement learning.com (2023), "Certificate Program in Public Procurement (CPPP)"
158 Corte dei Conti, C.A.T.O.N.E. project

4. POSSIBLE FUTURE DEVELOPMENTS

This section describes two technological developments that experts expect to offer particular promise in global efforts to safeguard public funds and fight fraud and corruption. One, blockchain, is preventative; promising to fight fraud before it happens; the other, AI, is corrective, promising to fight fraud after it happens. Blockchain has the power to transform the management of public funds; AI has the power to transform the audit of public funds. We first present these developments and then assess the potential benefits and challenges associated with their potential applications in the field of budgetary control.

4.1. Possible future developments in blockchain technologies

Blockchain technologies are still in a development stage. Both the technology and its use in the public and private sectors are still emerging, and much more research remains to be undertaken to further develop this new technology and to fully understand the areas in which shifting to blockchain is worth the cost of setting up and maintaining the blockchain infrastructure. However, the possibilities seem endless, and both public and private sector investment raise expectations. After a slow adoption rate in the 1990s and early 2010s, the rise of cryptocurrencies like bitcoin and, more recently, the pandemic, and the new digital strategies have fuelled interest in the idea of recording transactions immutably on multiple servers. As of early 2024, an end of what journalists and tech experts have termed the 'blockchain hype' is not in sight.[159] According to a report by Fortune Business Insights, the global blockchain market is likely to grow from USD 7.18 billion in 2022 to USD 163.83 billion by 2029.[160] While researchers and developers will be fine-tuning the technology, governments will be exploring ways to leverage the benefits of it. Within the next five to ten years, results from the many pilot tests described in section 3 are expected to become available, allowing those managing and auditing public funds to assess the costs and benefits of adopting blockchain technologies more widely in this area.

The potential that experts see in blockchain as a tool to protect public funds can hardly be overstated. It could upend the institutional set-up that allows fraud and corruption. For instance, Ebrima Faal, a corruption scholar at the London School of Economics states that "Blockchain could very well mark a watershed moment in the fight against corruption, ushering in a new era of transparency, efficiency, and public accountability. While it might not be a silver bullet for every procurement challenge, it undeniably holds significant promise in redefining public procurement and reinstating public trust in administrative processes."[161]

4.1.1. Application of blockchain technology in the EU

The groundwork for a wider use of blockchain in Europe has been laid. In 2018, the EU Member States, Norway, and Liechtenstein joined forces to create the European Blockchain Partnership (EBSI). EBSI will consist of a peer-to-peer network of interconnected nodes. Each country in the network will run at least one node. Once established the new blockchain network will allow public administrations to develop applications that use the infrastructure. Plans are under way to use it for notarisation (i.e. creating digital audit trains and automating compliance checks), diplomas (i.e. managing education

---

159 Litan, A. (2022, August 30). Metaverse, Web3 and Crypto: Separating Blockchain Hype from Reality. Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-08-30-metaverse-web3-and-crypto-separating-blockchain-hype-from-reality

160 Fortune Business Insights. (2023, May). Market Research Report. Blockchain Technology Market Size, Share and Growth. https://www.fortunebusinessinsights.com/industry-reports/blockchain-market-100072

161 Faal, E. (2023, September 27). Blockchain could revolutionise public procurement and combat corruption in Africa. LSE Blogs. https://blogs.lse.ac.uk/africaatlse/2023/09/27/blockchain-could-revolutionise-public-procurement-and-combat-corruption-in-africa/

credentials to reduce verification costs and increase trust in diplomas from other countries in the network), a European digital identity (allowing citizens to create their own identity across borders without relying on national authorities), and data sharing (securely sharing data amongst EU authorities, starting with the Import One-Stop-Shop (IOSS) number to combat VAT fraud). The new infrastructure will allow a simpler, safer, and more transparent way of keeping records and exchanging information across countries in the network.[162] All of these projects promise to save EU citizens and institutions time, effort, and money.

At the national level, blockchain technology could facilitate effort of tax administrations to combat tax fraud. Asking (or allowing) citizens to file their taxes digitally, and backing them up using blockchain will make taxable transactions and ownership of assets transparent and traceable. This will reduce options to evade taxes, for instance, through cross-border transactions.[163] As recognised in a motion for a European Parliament Resolution on the impact of crypto and blockchain on taxation (2021/2201(INI)), blockchain technology promises to play a significant role in protecting public budgets. It will allow members to set up more efficient tax and administrative procedures, and it will increase the visibility and traceability of taxable transactions and ownership of assets. This is particularly important in a context of increasing cross-border transactions. Overall, this will create opportunities for "better and more fairly designed tax systems to tax both mobile taxpayers and assets".

At the EU level, blockchain technology could contribute to the protection of the EU budget by making EU funds and EU public procurement procedures corruption-proof. Similar to the examples described in section 4 (e.g. in Colombia or Peru) the EU could develop a private and permissioned grant management and/or public procurement system based on blockchain technology. A blockchain-based public procurement system would keep records of every procurement transaction – from the publication of the tender to the last payment to the supplier – in multiple places. A blockchain-based grant management system would keep records of every grant transaction – from the application to the last payment to the beneficiary – in multiple places. Such systems would make it very difficult for any one individual or organisation to use public funds in ways that are not intended. Recording procurement and grant transactions on a blockchain would increase transparency, accountability, efficiency in contract management, and trust in the process.[164]

Whether such a system is cost-effective needs to be carefully assessed. Stakeholders consulted for this project expressed reservations about spending public funds on new IT systems if the existing IT systems work; and on spending public funds to fight fraud and corruption in funds or in regions where fraud and corruption rarely happens. The European Blockchain Services Infrastructure (EBSI) recommends using blockchain if the following conditions are met:

- There are multiple organisations contributing to a record.
- There is a risk of contention over control of the data.
- There is a need to store historical records.
- There is a need to prevent tampering with those records.
- There is a need to store those records permanently.
- There is a need to store those records in multiple places.

---

[162] EBSI (2024). Experience cross-border services with EBSI. [The first public sector blockchain services in Europe](#).

[163] This is recognized in a motion for a European Parliament Resolution on the impact of crypto and blockchain on taxation (2021/2201(INI))

[164] Burola, Thomas (2023, Aug 9th). [Public Procurement: Blockchain.](#)

These conditions are not always met. If, for instance, there is no need to store historical data then e-mails or spreadsheets might be sufficient. If just one organisation is involved in the data sharing process, or if multiple organisations are involved but there is no risk of contention over the data, a centralised database might be a better choice. To assess the necessity of using blockchain technologies to manage EU funds, further research is needed to estimate the amounts lost to fraud in each fund, and to compare that cost with the cost of setting up and maintaining a blockchain infrastructure. As the technology is evolving rapidly, the cost of the latter can be expected to go down in the next five to ten years. Until then, progress in those countries that are using blockchain already, such as Estonia and Sweden, ought to be monitored carefully in order to identity the lessons learnt there.[165]

4.1.2. Challenges associated with using blockchain in budgetary control

The main challenge in the development of blockchain solutions is the high initial setup costs. Many of the pilot projects described in section 3 started a few years ago but are not yet complete and remain to be evaluated. Successful development of blockchain takes time and requires technical expertise. Setting up and maintaining a blockchain infrastructure requires tech experts at every node of the network, and an advanced IT infrastructure with stable internet connections, a reliable energy supply, and high storage and computing capabilities. In addition, there are concerns about high energy consumption – however, new research on low-energy variants is under way and promises to bring down energy usage significantly.

There are also legal challenges, in particular, around data protection policies in the EU. At present, there is no consensus on whether encrypted data on a blockchain is to be seen as 'personal data' and, if so, how that can be squared with the 'right to be forgotten' in Article 17(1) GDPR. Relatedly, there are issues around accountability. Data protection policy implicitly assumes that there is a natural or legal person who manages data, the 'data controller', who can be contacted in order to enforce citizens' rights under EU data protection law. This is an issue for public, open blockchains, where anyone can host a node and anyone can view and add blocks. A possible solution – and one that frequently adopted in the public sector – is to rely on private, permissioned blockchains, where running nodes, viewing, adding, and validating data is restricted to authorised parties, thereby allowing at least some level of accountability, albeit with a lower level of transparency.

4.2. Possible future developments in AI

Developments in machine learning – in particular, the exponential growth of large language models in the last few years – raise high expectations for the future use of AI in budgetary control. Frontier AI companies such as OpenAI, DeepMind, and Anthropic are attracting significant investments. For instance, Google has pledged to invest USD 2 billion in the AI safety and research start-up Anthropic,[166] OpenAI is on track to hit USD 2 billion revenue,[167] and Mistral has attracted EUR 358 million of investment and been valued at €2 billion.[168] Across Europe, 150 start-ups are working on generative AI.[169] Most innovation is expected to occur in the field of generative AI and, specifically, large language models. Aside from the more traditional applications (e.g. synthesis, information extraction, narrative generation), LLMs are expected to play a significant role in the future of scientific discovery. Recent research suggests that using AI to solve scientific problems can accelerate the rate of discovery

[165] Brothwell, R. (2023, June 5). "Six countries using blockchain right now."
[166] Forbes (2023, Oct 31st). "Google invests in anthropic for USD 2bn as AI race heats up"
[167] Reuters (2024, Feb 9th). "OpenAI hits USD 2bn revenue milestone."
[168] New York Times (2023), Mistral, French A.I. Start-Up, Is Valued at $2 Billion in Funding Round.
[169] Smith, Tim (2023, Sep 22nd). "Europe's generative AI startups, mapped."

by a factor of ten, or even a hundred in certain domains.[170] Another strand of research looks into multimodal training, training AI systems to process and produce not only text files but also other types of data such as images, audio, video, code, and other sensory data. Moreover, models are likely become more interconnected and gain access to the Internet in real time, which may improve the relevance and accuracy of their outcome.

The benefits of using machine learning tools and, in particular, LLMs are tangible. They allow the processing of vast amounts of data (such as, in budgetary control, audit files or public procurement documentation), recognise patterns (such as risks of corruption), and even assist with text generation, such as writing e-mails, reports, or contracts. Using LLMs saves time, frees up capacities for high-level tasks and, ultimately, saves staff costs. This makes them a valuable technology for the future of digitalisation in budgetary control.

4.2.1. Application of machine learning and LLMs technology in the EU

One possible application of machine learning tools in the field of EU budgetary control could be to simplify public procurement processes. Procurement institutions across the EU and its Member States would benefit from contract management tools such as the one developed by the Slovakian start-up Cequence described in section 3. Another way in which ML could help protect the EU budget is to simplify audit processes.

Perhaps because of the large bodies of text they process, audit institutions have been at the forefront of research and innovation into new, AI-powered ways to audit. While the machine-learning based risk-scoring tools described in section 3 remain in development, their potential to help uncover fraud and corruption is enormous. The example from Flanders described in section 3 is a case in point. At present, the auditors can neither guarantee whether this project will be successful, nor when. Yet if it is successful, it has the potential to revolutionise auditing. According to tests conducted in late 2023, the new process the auditors envision would save eighty percent of the time it currently takes to conduct an audit, while investigating not just a small sample, but all cases. The fact that this new system relies only on the documents auditors already receive (not, like the project at the Portuguese Court of Auditors described in section 3) makes the new system easily scalable. If successful, it could be adapted to be used by audit institutions in any other EU Member State.

Early success stories from the Massachusetts State Auditor's Office (USA) point to a great potential. In January 2024, the Massachusetts' auditors shifted to a new, AI-powered audit workflow that uses machine learning algorithms to calculate risk scores in large sets of data and that includes an internal chatbot allowing auditors to ask questions about any audit files. The chatbot not only answers those questions but, conveniently, points users to the relevant file, allowing them to fact-check the chatbot's answer in a matter of minutes.[171] Similar approaches applying large language model to internal data, in particular, open source LLMs that give the owners full control over their data and allow them to keep sensitive information on their own cloud or server will help streamline processes in and beyond audit.

4.2.2. Challenges associated with using machine learning and LLMs

One of the main limitations of LLMs is the accuracy of their output. The output of a large language model – such as, for instance, the answer GPTs might provide to a question – depends on the data they

[170] Dean, Jeff (2023, Dec 22nd). "2023: A Year of Groundbreaking Advances in AI and Computing"
[171] CSES Consultations

were trained on.[172] LLMs that are trained on incomplete, inaccurate or contradictory data can 'hallucinate', or predict words that are factually incorrect, nonsensical, or do not fit the context. According to a recent study, GPTs hallucinate about 3 per cent of the time.[173] Another issue occurs if training data is unrepresentative in gender, ethnic, or other terms. Unrepresentative training data can lead to bias. Moreover, in the context of fraud detection, training data can only contain discovered fraud data. For developers, finding large sets of complete, accurate, consistent, and representative training data remains a challenge – in particular, as owners of large datasets are beginning to restrict access due to privacy concerns. However, experts expect major advances in bias detection, and in the generation of high-quality synthetic data to counter data scarcity caused by privacy restrictions, low quality or inaccessible data.

Another limiting factor is scalability, or the availability of computing power. Over the past decade, the computing power that has been used to train LLMs worldwide has risen by a factor of 55 million.[174] Training data usage has been growing at over 50 per cent per year. On the one hand, these ever-rising levels of computing power that are needed to develop LLMs raise concerns about scalability. On the other hand, they raise ethical and environmental concerns about energy consumption. A final limiting factor is the cost of developing LLMs.

172 Generative pre-trained transformers (GPT) are a type of large language model developed by OpenAI, a research organisation based in the USA.

173 Hughes, Simon (2023, Nov 6th). "Cut the Bull… Detecting Hallucinations in Large Language Models."

174 EpochAI (2022, Feb 16th). "Computing trends across three eras of Machine Learning."

5. POTENTIAL APPLICATIONS OF NEW TECHNOLOGIES

This section presents how the new technological developments described in the previous sections could be applied to the field of budgetary control. It assesses the possible benefits and costs associated with the deployment and implementation of these technologies in the budgetary control process and the potential implications for specific types of EU funds. The section draws on evidence from secondary sources and feedback from the survey and interview programme.

5.1. Potential application of new technologies in budgetary control

The EU has developed a range of IT tools to support the management and control of EU expenditure (Section 2). Some Member States are more active than others in using the available EU IT tools for budgetary control including Arachne, the data-mining and risk-scoring tool developed by the Commission. However, these tools are not uniformly used across the EU and could be further enhanced by integrating some technologies and features. As noted in section 2.3.1, the Parliament, the Council and the Commission have committed to examining and rediscussing the compulsory use of the tool during the post-2027 multiannual financial framework.

The study has identified some practical examples of application of AI, machine learning, robotic process automation, and other big data technologies for public procurement and budgetary control in Member States (Section 3 and 4). The identified solutions are currently being tested or implemented by national or regional authorities responsible for the management, control, and audit of public funds, as well as for the prevention and detection of irregularities, and risks of fraud, corruption, and misuse of funds, more broadly. Most of these applications have been developed either by the public administration using own resources, or by public bodies in collaboration with academics, NGOs and experts from the private sector.

Due to the limited adoption of these new technologies across the EU, it is not possible to clearly assess the benefits and costs associated with their deployment and implementation at the EU level. However, evidence from the research in the Member States and the consultation carried out for this study suggests that there are many potential ways in which big data and new technologies can improve the management, control and auditing of EU expenditure and strengthen the prevention and detection of fraud and misuse of EU funds.

The potential advantages and disadvantages derived from specific technologies have been described in section 3. Table 5-1 summarises how new and emerging technologies can be applied to enhance the management and control of EU expenditure.

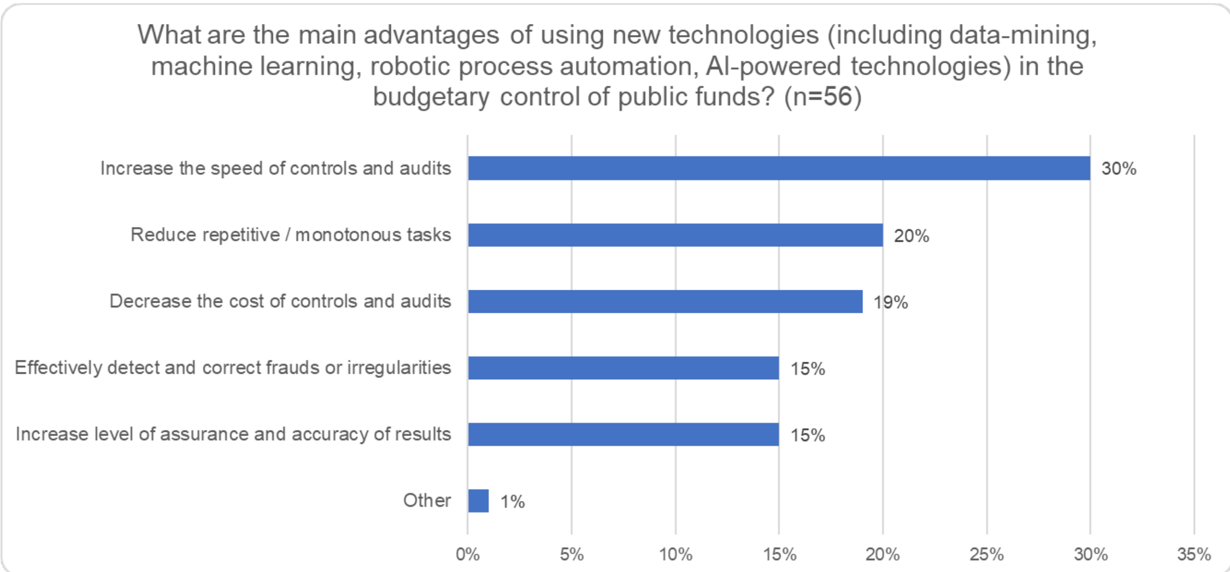
Table 5.1: Application of new technologies in budgetary control

Technologies	Benefits of new technologies in budgetary control
Big data analytics and data mining	• Easier and quicker access to important data during verifications • Enhanced risk-scoring and thus detection of irregularities/fraud • Cross-border organisation/institutional interoperability • Harmonisation of data collection, verification and analysis • Streamlining the audit process and improvement of the audit trail.
Machine learning	• Enhanced risk-scoring, accuracy of red flags and identification of patterns • Stronger prevention and detection of irregularities/fraud/corruption in the EU expenditure • Identification of weaknesses in the national control systems for EU funded programmes

Technologies	Benefits of new technologies in budgetary control
	• Better understanding of the explanatory factors leading to a situation/anomalies
Generative AI/ LLMs	• Possibility to summarise large amount of data and information • LLMs can be used to automatically correct spelling errors, standardise formats, and organise data into structured formats like tables or spreadsheets. • LLMs can be used to cross-reference data against other sources to verify accuracy and reliability. • LLMs excel in generating written content - can automate the creation of reports, summaries, and documentation by structuring collected data into coherent narratives, following specified templates or guidelines.
Robotic process automation	• Web-scraping tools or external APIs can be used for data extraction, verification and reporting thereby streamlining the entire control and assurance process. • Automate repetitive and time-consuming tasks to allow authorities to focus on strategic tasks.
Digital Platforms	• Sharing of knowledge by Member States in the use of effective IT tools • More effective sharing of management verification results • Reduce gold-plating due to the introduction of unnecessary national / regional rules.
Blockchain	• Traceability and identification of operations and transactions • Capacity to streamline data collection and to store immutable and reliable data • Facilitate tax administrations' efforts to deter and combat tax fraud (including cross-border).
Satellite imagery	• Deep learning image classification algorithms on high-definition satellite imagery to monitor the quantity as well as the quality of crop yield and to check applications for EU funds • Can be leveraged for budgetary control purposes to verify the quantity and quality of agricultural output funded by the CAP funds and detect anomalies.

These benefits were also confirmed in the study survey where several respondents indicated that new technologies would increase the speed of controls and audits (30%, 16), reduce repetitive and monotonous tasks (20%, 11) and decrease the costs of controls and audits (19%,10).

Figure 5.1: Budgetary authorities' views of new technologies



Source: Study survey

The deployment of new technologies will also improve the quality and accuracy of management verifications and audits, facilitate data collection, cleaning, verification, and reporting, thus streamlining the control process. This will in turn contribute to the sound financial management of EU funds and to strengthening the protection of the Union's budget.

Experience from audit authorities in the United States where many of these new technologies are already in use shows that, given the pace of change, audit authorities can make best use of new technologies if they dedicate teams to exploring them. For instance, at the Office of the New York State Comptroller, innovation has been driven by a dedicated innovation unit, a team of comptrollers who continually assess new, innovative approaches and high-end technologies. The team pilot new ideas within the unit. If successful, they undergo a cost-benefit analysis before they are deployed across the organisation. Similarly, the United States Government Accountability Office has an innovation lab to test the use of cutting-edge technologies like AI or distributed ledger technology in a 'sandbox' testing environment. To be able to scale up the use of these cutting-edge technologies, both organisations have benefitted from a workforce with diverse skills, including not only applicants with an accounting background but, increasingly, graduates who have specialised in computer science, maths, technology and engineering.

5.2. Implications for specific EU funds and programmes

The study explored the potential implications of the deployment of these technologies on specific EU funds and programmes. Particular attention was paid to the following funding instruments:

- **Next Generation EU (NGEU)** - a temporary recovery instrument aiming to help countries mitigate the economic and social impacts of the COVID-19 pandemic. NGEU will make EUR 723.8 billion available to the Member States through loans and grants. At the heart of NGEU, there is the Recovery and Resilience Facility (RRF) which supports national reforms and public investments set out in national plans to be implemented by 2026.
- **Cohesion policy funds** - including the European Regional Development Fund (ERDF), the Cohesion Fund (CF), the European Social Fund Plus (ESF+), and the Just Transition Fund (JTF). A total of EUR 392 billion have been allocated to cohesion policy for 2021-27 to support the social and economic development of all EU regions, reduce regional disparities, support investments in environment and transports, and the creation of jobs in the EU.[175]
- **Common agricultural policy (CAP) funds** - including the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD). With a budget of EUR 387 billion in 2021-27, the CAP aims to strengthen the social, environmental, and economic sustainability in agriculture and rural areas by providing income support to farmers, measures for rural development and to address difficult market situations.[176]
- **Horizon Europe** - the EU funding programme for research and innovation. With a total budget of EUR 95.5 billion, the programme supports collaboration for research and innovation, the development of the European Research Area and the consolidation of a single market for research, innovation, and technology in the EU whilst tackling global challenges.[177]

[175] European Commission (2024). Available budget of Cohesion Policy 2021-2027. Available at: https://ec.europa.eu/regional_policy/funding/available-budget_en. (Accessed: 19 February 2024).

[176] European Commission (2024). Common agricultural policy funds. Available at: https://agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-funds_en. (Accessed: 19 February 2024).

[177] European Commission (2024). Horizon Europe. Available at: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en. (Accessed: 19 February 2024).

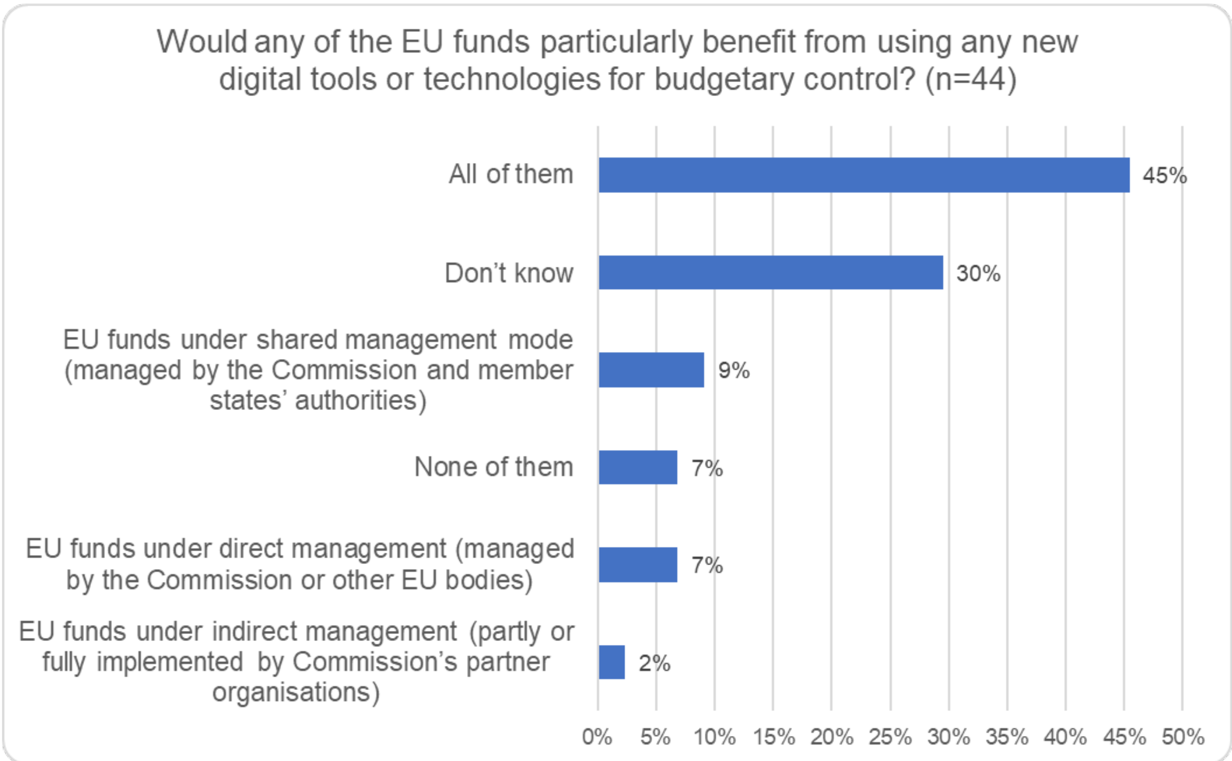
Around 70% of the EU programmes is implemented in shared management mode. In shared management, the Commission and the Member States share the responsibility of implementing and controlling specific programmes supported by the funds. In direct management, the EU funding is managed directly by the Commission whereas in indirect management, other partner organisations and authorities inside/outside the EU are involved.[178]

Looking at the funds in scope, the cohesion funds and most of the CAP budget are implemented under shared management. A large share of the NGEU funds, notably the RRF, is implemented in direct management mode. NGEU funds are disbursed directly to the Member States as they make progress in their reform and investment plans. Horizon Europe is also implemented in direct management mode.

The survey undertaken for this study asked budgetary authorities to indicate **which specific EU funds, if any, would particularly benefit from using new digital tools or technologies**. Almost half of the respondents to this question (46%, 24) indicated that all EU funds would equally benefit from these technologies. Several respondents (29%, 13) did not have a strong opinion on this matter and only two indicated that none of the funds would derive advantages from these technologies.

Considering the implementation mode, a few respondents to this survey question argued that EU funds implemented under shared management would benefit more from new technologies (9%, 4) compared to funds directly managed by the Commission (7%, 3) or indirectly managed through other entities (2%, 1). Given the limited number of respondents, it is not possible to draw some conclusions on these differences.

Figure 5.2: Budgetary authorities' views of using new tools/technologies within EU funds



Source: Study survey

[178] European Commission (2024). Funding by management mode. Available at: https://commission.europa.eu/funding-tenders/find-funding/funding-management-mode_en.

The study also gathered views on the potential implications of the use of new technologies for EU funds under different management modes through the interview programme. The feedback gathered can be summarised as follows:

- In cohesion funds, the use of data-driven technologies (e.g. ML, RPA) can facilitate the standardisation and collection of data provided by beneficiaries for the purpose of administrative verifications and the audit trail (i.e. step-by-step record of supporting data and documentation which can be used to verify operations). It could also help direct on-the-spot verifications to riskier operations, thus making the sampling strategy more effective. The availability of large amount of data on past cases and irregularities (also from other countries) could also help the audit authority in the formulation of its opinion on the accounts and on the legality and regularity of expenditure. This would in turn favour the application of the single audit approach and avoid the duplication of controls on beneficiaries.
- In CAP funds, the deployment of data-driven technologies is likely to bring many potential benefits. The 2020 reform paved the way for a performance-based CAP and a simplification and reduction of the administrative burden.[179] The use of satellite imagery has already provided various benefits (see section 3.6). Data mining and machine learning could offer more accurate risk analysis, thus reducing the need for on-the-spot controls on farms and in turn helping to reduce the burden associated with compliance. The uptake of technologies and digitalisation could contribute to the reinforcement of the assurance framework for CAP expenditure overall.
- Due to its very unique characteristics, the RRF is also subject to a lot of scrutiny from different players. Feedback from the interviews with relevant stakeholders suggests that there this has resulted in an increased workload for the competent authorities. AI solutions are currently being tested and will be probably implemented in the next ten months. The expected benefits include a higher accuracy of controls, better quality data, a reduction of the burden on competent staff and thus the possibility to allocate staff members to higher-value activities. In parallel, it will be important to ensure that AI is used properly. Therefore, training and the compliance with data protection legislation as well as the Commission’s guidelines on the use of AI[180] will be key.

Overall, there is a broad consensus among relevant stakeholders regarding the potential benefits of using big data and new technologies to improve the management and control of public expenditure.[181] However, it is necessary to ensure the proper and 'fair' use of these technologies. Stakeholders contributing to this study expressed reservations regarding the possibility of deploying any data-driven solutions for decision-making and to implement sanctions due to their shortcomings and possible failure. Therefore, new and emerging technologies will be used by competent authorities to support and facilitate their control and audit functions, rather than as substitutes. The human factor will remain key.

179 European Commission, The common agricultural policy: 2023-27.
180 European Commission (2024). COMMUNICATION ‘Artificial Intelligence in the European Commission (AI@EC)’. C(2024) 380 final.
181 Feedback from interviews conducted for this study.

6. CONCLUSIONS AND RECOMMENDATIONS

Based on the findings presented in the previous sections, this section offer conclusions as well as recommendations for the EU and its Member States.

The misuse of EU funds poses a serious threat to the EU's ability to advance its strategic priorities and maintain public confidence in the EU. Despite progress made at both the EU and national level in preventing, detecting, and prosecuting fraud and irregularities, the overall number of cases has remained relatively stable over the last five years. A notable gap persists in obtaining comprehensive information regarding the scale, nature, and underlying causes of fraud in EU expenditure. The lack of a thorough assessment of undetected fraud and a detailed analysis of the motivations behind fraudulent activities pose challenges in effectively addressing this issue. There remains a need for more effective efforts to protect the EU budget.

Digitalisation is at the heart of the strategic vision of the European Commission and other bodies responsible for management and control of EU expenditure. Efforts to support digitalisation in budgetary control have been promoted through various EU initiatives, including the 2019 and 2021 revisions of the Anti-Fraud Strategy and the proposal for a recast of the Financial Regulation. These support the Commission's commitment to be 'digital by default' and encouraged the digitalisation of control practices in Member States.

EU-level IT tools, such as Arachne, EDES and IMS, are helping to protect the EU budget, but there is scope for further application of existing and new digital technologies. Arachne is not universally adopted by all relevant authorities in Member States, low awareness, national data privacy rules, administrative burden associated with data input, limited accuracy of risk scores, high number of false positives and the availability of alternative tools at national level. The EDES is not currently applicable to shared management, although the Commission has proposed a targeted extension in the post-2027 period. The mandatory and consistent use of these digital tools across the EU could contribute to ensuring sound financial management and improve the interoperability of national systems.

Recommendation 1: Continue to enhance existing EU tools for budgetary control. This can include continuing the Commission's current efforts to expand the capability of Arachne to cover all management modes, integrate advanced technologies (e.g. ML, AI), ensure interoperability with other tools and address privacy concerns. It can also include enabling faster checking of operators against more up-to-date and comprehensive Member State data on exclusion or early detection cases. The quality of information within the IMS could be improved by introducing consistent thresholds for reporting cases of fraud and through the provision of more up-to-date information by national authorities.

Recommendation 2: Promote awareness of and training in the use of existing EU tools for budgetary control. Whilst Arachne is mostly appreciated by those budgetary authorities that use it, its effectiveness is limited by modest take-up. Raising awareness of the IMS would lead not only to greater use but also a higher volume and quality of information provided by national authorities. Greater and more effective use could also be encouraged by the provision of training for national authorities. For Arachne, this would relate to how the tool works, how to use it and how to use all the different functionalities, i.e. going beyond conflicts of interest and fraud red flags. For the IMS, this might include training in thresholds for reporting cases of 'suspected' and 'established' fraud.

Recommendation 3: Consider making the use of EU tools mandatory. In the case of Arachne, the Parliament, the Council and the Commission have committed to examining and rediscussing the compulsory use of the tool during the post-2027 multiannual financial framework. Making use of the tool mandatory would increase the volume and quality of information on contractors and beneficiaries in some Member States, thus increasing the tool's effectiveness in helping to combat fraud and misuse of EU funds.

New data-driven technologies such as data-mining, machine learning, robotic process automation and artificial intelligence could increase the efficiency and quality of budgetary controls and audits. AI and machine learning algorithms are proving accurate in detecting potential risk or cases of fraudulent spending and corruption. Machine learning can also be used to automate checks on operations in public procurement and for real-time monitoring of spending. The use of these technologies could also lead to efficiency gains reducing the burden on managing bodies and beneficiaries. The potential benefits brought by these technologies extend throughout the fraud risk management cycle.

Recommendation 4: The EU and its Member States could consider pilot projects to explore the possibilities for applying new data-driven technologies to budgetary control. Such projects might be best developed on a transnational basis from the outset, so ensure their applicability to different national contexts and also to ensure a degree of consistency in the use of EU funds across EU-27. Where appropriate, there may be possibilities for such pilots to be co-financed by relevant EU funding programmes.

To date, there has not been a broad and consistent deployment of data-driven technologies in budgetary control across the EU. The reasons for this include differences in national control strategies and systems, varying regulatory frameworks, differences in investment capacity and digital competences within the public administration as well as in the political priorities between Member States. Some countries have been more at the forefront of this transition than others. Experience from the USA suggests that budgetary authorities can configure themselves in such a way as to foster innovation effectively, for example, through units dedicated to identifying, testing and rolling out innovations and comprised of individuals with different training backgrounds (i.e. not only accounting but also computer science, maths and engineering).

Recommendation 5: Support mutual learning, the sharing of good practices and exchanges of information between relevant authorities. As shown in this report, there are pockets of innovation and good practice in applying new data-driven technologies to the budgetary control of public funds. Widening knowledge of such examples might help and inspire budgetary authorities either to adopt the same tools or develop similar ones or configure themselves in such a way as to best exploit new technologies. More consistent adoption of new data-driven technologies might also in support the harmonisation of control practices and standardisation of reporting methods.

Challenges in the use of these technologies persist and will need to be considered. This includes the need for uniform data collection, interoperability of data and systems, the cost of implementing these technologies, privacy regulations compliance and ethical concerns relating to biases embedded in AI-systems. False positives remain a concern, necessitating case-by-case checks. Furthermore there will be a need to improve the EU legal framework in order to allow a proper development and application of these technologies and prevent any misuse. A concerted effort to overcome these challenges and create a mature legal framework for AI will be essential to reap all the benefits of digitalisation.

Recommendation 6: The EU could consider defining common standards for the proper use of certain new technologies in the budgetary control of EU funds. This could be accompanied by a code of conduct for the proper and 'fair' deployment of these technologies for budgetary control. Evidence from experience shows that the potential benefits applying new technologies to budgetary control risk being undermined by inconsistent or inappropriate deployment within and between Member States and budgetary authorities therein. Common standards and a code of conduct might increase consistency and reliability.

Recommendation 7: Assess the costs and benefits before deploying new technologies. In some cases, the deployment of new technologies can be expensive and the benefits uncertain, particularly where error rates are already low. Budgetary authorities should thus carefully assess the potential benefits of deploying new technologies relative to their cost. In some cases, it might be appropriate for ex ante impact assessment (including cost-benefit analysis) to be undertaken at EU level in respect of the possible deployment of new technologies at EU level (or across all Member States). Mutual learning and exchange of experience could inform this process.

Recommendation 8: Carry out regular "horizon scanning" to monitor emerging trends and developments with a potential positive impact on budgetary control. Given the fast pace of technological development, new possibilities will continue to emerge that offer potential benefits and risks for budgetary control. The provision and sharing of information at EU level about emerging developments and their possible application could support successful effective assessment and successful deployment by budgetary authorities at EU level and in the Member States.

APPENDIX A: CASE STUDIES

Natural Language Processing and Large Language Models

1. Introduction- Overview of the technology

Natural Language Processing (NLP) is the branch of AI concerned with giving computers the ability to understand and generate human language. Research in the field started in the 1950s with attempts to automatically translate Russian and Chinese language into English, using complex hand-written rules.[182] In the 1980s, researchers started feeding computers bodies of text that were available in multiple languages, for instance, legal documents from the Canadian government, and the EU, using statistical approaches to teach the computers to process and translate those texts. The next big development was the rise of the internet in the 2000s, which made it possible to use data mining, web scraping and machine learning methods on an ever-growing body of data. Meanwhile, computational power rose exponentially, allowing computers to execute complex mathematical computations faster than ever before. Between 1975 and 2009, the computational capacity of computers doubled every 1.5 years.[183] This rise in computation powers allowed researchers to return to a machine learning approach that was first invented by Warren McCullough and Walter Pitts, two researchers at the University of Chicago in 1944: artificial neural networks, a process inspired by data processing in the human brain, in which a computer learns to perform tasks by analysing labelled training data. Today, neural networks (or deep learning methods) are used in many fields, such as image recognition, natural language processing (e.g. machine translation, image recognition, large language models), speech recognition, and autonomous driving.[184]

In the 2010s, researchers started using recurrent neural network approaches to try to generate text. Back then, the approach was focused on the sentence structure, i.e. the models attempted to predict the next word in a text sequence. Despite some early successes, the text predicted using these recurrent neural networks was nowhere close to the sophistication of the text generated by large language models today. The defining moment in the development of today's large language models was the invention of transformer models and Google's seminal 2017 paper "Attention is all you need".[185] Contrary to recurrent neural networks, the new attention mechanism examines the entire sentence, or even paragraph, rather than one word at a time (as recurrent neural networks did), providing the transformer model with a much better understanding of the context of a word. Today's state-of-the-art large language models such as OpenAI's ChatGPT, Google's Bard, or Meta's LLaMA are based on these transformers.[186]

Large language models have shown exceptional performance mimicking human speech patterns. They can conduct a wide range of NLP tasks such as classifying text, extracting information out of text (e.g. named entity recognition, NER), finding hidden topics within text ('topic modelling'), understanding emotions within text ('sentiment analysis'), translating text, summarising text, answering questions, and even performing coding tasks. A great advantage of foundational models is that they can carry out multiple tasks at once, rather than, for instance, only classifying text, or only finding a hidden topic (hence why they are called 'foundational'). They are excellent at combining text data with different styles and tones.

---

182 John Hutchins, "The Georgetown-IBM Experiment Demonstrated in January 1954."

183 Roser, Max; Ritchie, Hannah, Mathieu, Edouard (2023, March 28). What is Moore's Law? Our World in Data.

184 Wolfewicz, A. (2023). Deep Learning vs. Machine Learning – What's The Difference? Levity. https://levity.ai/blog/difference-machine-learning-deep-learning

185 Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 2017-December.

186 Tam, Adrian (2023, July 20). What are Large Language Models? Machine Learning Mastery; Stöffelbauer, Andreas (2023, Oct 24). How Large Language Models work. From zero to ChatGPT. Medium.com

2. State of play - Use in the field of budgetary control

In the field of budgetary control, NLP applications are currently used in two broad fields. The first field is custom-built chatbots, which allow auditors or public procurement officials to 'chat with their docs', i.e. sift through large bodies of internal data and find relevant information. The second field is in risk scoring. Here, NLP is used in combination with machine learning techniques to detect signs of irregularities, or patterns that indicate risks of fraud in large bodies of text (in this case, audit files.). Both types of uses save auditors time, allowing them to process much larger volumes of data. They can also improve the quality of their work, by pointing auditors to relevant information they may have missed without the help of AI.

This case study focuses on chatbots. We start with an overview of public-facing chatbots in public administrations; while these are not yet used in the field of budgetary control, they help those managing and auditing public funds communicate with citizens in the future (see section 5 of this case study). Next, we move on to internal chatbots, which are currently piloted in a few audit institutions in the US and in Europe.

Public-facing chatbots

Chatbots are computer programs that simulate human conversations with an end user.[187] While chatbots are most prominently used by private sector customer services, they have, since the mid-2010s, made their way into public administrations. Here, the goal is to provide either the public or internal employees with quick answers to common questions. For instance, one early adopter of a public-facing chatbot was the U.S. Citizenship and Immigration Services whose chatbot 'Emma' answers questions about services offered by the department (e.g. immigration services, green cards, passport services, etc.) in English and Spanish. Another example is the Mississippi State's government's chatbot 'Missi' who answers any questions about the state, for instance, directing citizens to the right state agency, or sending links the applications forms[188], or the Australian Taxation Office's chatbot 'Alex' who helps with any questions around tax and income. Some of these chatbots, such as Mississippi's 'Missi', Los Angeles' 'L.A.City', and Dubai's 'RAMMAS', work with virtual assistants such as Amazon's Alexa, allowing users to ask their questions out loud.[189]

First-generation chatbots used a rules-based approach, where pre-defined decision trees dictated responses to queries. That approach had limitations. On the one hand, developers had to anticipate the different ways in which users might word the same question to program chatbots to respond to different wordings. On the other hand, users who were not using the pre-defined words were not receiving the correct answer. More complex questions, or questions the chatbots were not trained to answer, could not be answered. The emergence of LLMs has radically changed the landscape. The first government chatbots have started to migrate over to LLM-powered engines in order to provide more helpful, and more accurate responses.[190] Given the prohibitively high cost of developing large language models from scratch, and the need to retain access over sensitive data, government agencies typically buy access to existing LLMs, bring them in-house, and train and fine-tune them on their own data. In practice, these applications, often referred to as 'chat with your docs' or 'chat with your data' allow users to ask simple questions, just like Google or ChatGPT. They then search through the internal documents, find the most semantically similar pieces of text, and feed those bits, along with the initial question, back into an LLM which will produce a coherent answer.[191] A good example of an LLM-powered chatbot that will facilitate communication with citizens is Estonia's Bürokratt.

---

187 IBM (2024). What is a chatbot?
188 US Citizenship and Immigration Services. (2018, April 13). Meet Emma, Our Virtual Assistant. Uscis.Gov.
189 VSoft Consulting (n.d.) 12 Global Government Agencies that use Chatbots.
190 Hirdaramani, Y. (2023, September 14). Is it time to say goodbye to 'Ask Jamie'? Inside GovTech's refresh of government chatbots. Govinsider.Asia.
191 CSES Consultations.

Estonia is currently developing a chatbot that will allow citizens to get all the answers they need from the state in one place, free of charge, 24/7. Bürokratt is managed by the Estonian Information System Authority (RIA) within the administrative area of the Ministry of Economic Affairs and Communication. The idea is to make communication with the state as easy as possible by allowing users to obtain any information they need through their preferred communication channel: in a chat window, by SMS, email, phone, or by voice assistant. In a first instance, BÜROKRATT will help citizens with issues such as applying for various permits, applying for family benefits, renewing their identity card, borrowing books from public libraries, registering vaccinations, or identifying mushrooms. Eventually, developers plan to expand the topics the chatbot can help with, until almost all public services are available through BÜROKRATT.

While public-facing chatbots are not widely used in the field of budgetary control they are currently trialled at the United States Government Accountability Office (GAO). GAO, often called the 'congressional watchdog', is an independent, non-partisan agency that works for the United States Congress. It examines how Congress spends taxpayer dollars and provides recommendations to protect public funds.[192] GAO publishes information, such as reports, recommendations, videos, podcasts, or blogposts on a wide range of issues, for instance, public spending or ways to save taxpayer money in particular areas.[193] To provide citizens with easier access to their findings and recommendations, GAO is currently developing an early-stages prototype of a chatbot that will respond to citizens' questions on any published GAO work. Once operational, this chatbot will point citizens to GAO's work on any given topic and will summarise the main findings.[194]

Chatbots can also be used within businesses, or public administrations. Here, common goals are to simplify access to internal data, to increase efficiency and reduce manual processes.

Internal chatbots (and other uses of LLMs in budgetary control)

Audit and public procurement offices in Europe and the US are trialling the use of internal chatbots. For instance, the Swedish National Audit Office are currently trialling the use of LLMs to assist with text-related audit tasks such as reading and summarising large bodies of text, finding important pieces of information in text, comparing information from different sources, or writing reports. One of their very early-stages projects aims to automate comparisons between steering documents. The auditors plan to use LLMs to find out how documents have changed over time. A more advanced project – one that is fully developed and currently being tested – points auditors to documents worth reading.

'Doc-Rec', the new document recommender at the Swedish National Audit Office, works like a customised search engine. It speeds up the information gathering stage at the very beginning of the audit process. Doc-Rec allows auditors to ask questions or simply enter keywords and provides them with recommendations for relevant official documents, mainly from the Swedish Parliament, that auditors ought to read. Whilst classic search engines like Google serve a similar purpose, Doc-Rec is an improvement in two ways. First, it only contains official documentation, while a Google search will yield many other types of information that are not relevant to an auditor. Second, it conducts semantic (not just lexical) searches, meaning that it searches not only for documents that contain the exact keywords but also for documents that contain similarities in terms of meaning. In this way, Doc-Rec provides auditors with a much more

192 US Government Accountability Office (n.d.). About.
193 US Government Accountability Office (n.d.). View Topics.
194 US Government Accountability Office (2024, Jan 30). Artificial Intelligence: GAO's Work to Leverage Technology and Ensure Responsible Use

targeted list of recommendations than any general-purpose search engine could. The tool has been introduced and, while it is not yet used by all auditors, is gaining in popularity.[195]

Customised search engines are also used in public procurement. Here, a prominent example is a contract management tool developed by a Slovakian start-up. Cequence, which is used by managing authorities in Slovakia and Czechia, allows users to upload draft contracts onto an online platform, to edit them in collaboration with other users, and to sign them electronically. All contracts are stored on the platform; a customised search engine lets users ask any questions about the contracts, for instance, providing information about the terms and conditions.

3. Possible future developments relating to this type of technology

Recent advances in research on LLMs and, more broadly, generative AI, the success of these applications, and the size of investments in the industry suggest a nearly unlimited potential for growth. Frontier AI companies such as OpenAI, DeepMind, Anthropic and Mistral, who are producing highly capable general-purpose AI are attracting significant investments: Google has pledged to invest USD 2 bn in Anthropic - the AI safety and research start-up besides Claude, while[196] OpenAI is on track to hit USD 2bn revenue milestone,[197] and Mistral has attracted EUR 358 million and been valued at €2 billion.[198] Across Europe, there are already more than 150 start-ups working on generative AI.[199] According to experts in the field, models are likely to increase in intelligence and situational awareness. However, their progress is contingent upon three key factors: data, computing power, and improvements in the underlying algorithmic structure.[200]

First, the progress of LLMs will depend on access to large volumes of high-quality training data. For instance, insiders estimate that ChatGPT was trained on around 300 billion words or 570GB of data, mainly scraped from the web.[201] However, access to high-quality training data is becoming more and more challenging. According to recent estimates, developers will exhaust publicly available high-quality data sources (e.g. books, newspaper articles, scientific articles, and open-source repositories) within the next three years. This technical challenge is amplified by an ethical challenge around consent to data being used for training purposes, which has already led to increasing restrictions on web-scraping activities.[202] After that, developers will have to either resort to lower quality sources (e.g. social media) or find new ways to use smaller bodies of text more efficiently. One way to do so may be to use LLMs to generate high-quality synthetic data.[203]

Second, the progress of LLMs will depend on access to specialised computing hardware, computing power and energy. GPT-3, for instance, with its 175bn parameters, consumed 284,000kWh of energy.[204] That leads to high costs – the development of currently deployed LLMs such as ChatGPT is estimated to have cost between USD 300m-600m. Moreover, costs are rising: larger models require more computational power, i.e. more expensive processors, and longer training times (several months to reach optimal performance). The next generation of large language models is expected to pass USD 1bn within the next few years.[205] This has led to a trend to customise existing models rather than build new ones from scratch.

195 CSES Consultations. See also Maameri, Sami (2023, May 20). Building a Multi-Document Reader and Chatbot With LangChain and ChatGPT
196 Forbes (2023, Oct 23). Google invests in anthropic for USD 2bn as AI race heats up.
197 Financial Times (2024, Feb 8). OpenAI on track to hit USD 2b revenue milestone as growth rockets.
198 New York Times (2023), Mistral, French A.I. Start-Up, Is Valued at $2 Billion in Funding Round.
199 Smith, Tim (2023, Sep 22). Europe's generative AI startups, mapped. Sifted.eu
200 CSES Consultations.
201 Nolan, Beatrice (2023, Dec 4). Google researchers say they got OpenAI's ChatGPT to reveal some of its training data with just one word.
202 Stokel-Walker (2023, Jan 6). AI chatbots could hit a ceiling after 2026 as training data runs dry. New Scientist
203 UK Parliament (2023, March). House of Lords Communication and Digital Select Committee Inquiry: Large Language Models.
204 AI (2023, March 4). Power
205 Smith, Craig S. (2023, Sep 8). What Large Language Models cost you – There is no free AI lunch. Forbes.

Third, the progress of LLMs will depend on improvements in the models themselves. Experts expect improvements in LLM performance, both in text generation (writing and reasoning skills) and in the generation of other types of output such as video, music, or code. Key research areas include finding solutions for current issues such as LLMs hallucinating (or filling in factually incorrect or nonsensical information), exhibiting bias (learned from the training data), or revealing confidential information.[206]

In addition, a few notable developments are expected to improve both the quality and the popularity of LLMs. One is the trend towards open-access models. This is driven in part by the falling costs of customising LLMs to fit one's own needs and the growing ease and familiarity with these models in the machine learning community. By lowering entry barriers to coders around the world, open source LLMs will speed up research reducing biases and increasing the accuracy of LLMs.[207] Another development is a trend toward multimodal LLMs. The first generation of LLMs was focused on textual data, meaning that current LLMs are useful assistants for text processing tasks such as finding information in text, writing reports, or even coding. Multimodal language models are trained on different kinds of data, i.e. not just text, but also images, or video or audio files. That will help improve language tasks and accomplish new tasks such as describing images or videos, and generating prompts for robots.[208] Moreover, new models will likely gain access to the internet in real time, which may improve the relevance and accuracy of their outcome.[209] Finally, LLMs, and more broadly, foundational models, will likely play a significant role in the future of scientific discovery. Using AI in science can accelerate the rate of discovery in certain domains by a factor of ten, or even one hundred.[210]

The goal of LLM research is to create models that are helpful, honest, and harmless. The so-called 'HHH framing', coined by Askell et al (2021) prescribes that LLMs need to be helpful, i.e. follow instructions, perform tasks, and answer questions (and, if the intention of the question was unclear, they need to follow up and ask clarification questions). They also need to be honest, i.e. provide factually accurate information and acknowledge the limitation of their own knowledge. Finally, they need to be harmless, for instance, avoiding offensive or hurtful responses and refusing to assist with any harmful activities.[211]

4. Potential applications of new technologies

In the future, NLP applications could help those managing and auditing funds in various ways. 'Chat with your docs' applications can help those dealing with large bodies of data find relevant information quickly. For instance, public procurement officials in Czechia and Slovakia report saving time by using Cequence (see above) to manage large numbers of contracts. Instead of searching through e-mails to find information about any particular contract they now ask the chatbot. The transparency and the ease of access also increases compliance, meaning that goods and services are delivered on time, and according to the terms and conditions agreed on in the contract. Tools such as Cequence are easily scalable and facilitate the protection of public funds by making contract management more cost-effective.

LLM-powered chatbots could also be used to bridge information gaps about any EU funds. While the development of large-scale, citizen-facing chatbots takes years, it may be worth considering a chatbot, perhaps modelled on Estonia's 'one-stop-shop' chatbot (Bürokratt, see above) for all EU funds. A chatbot that would allow EU citizens to ask what funding is available for their own,

206 Department for Science, Innovation and Technology (2023, Oct). AI Safety Summit. Capabilities and risks from frontier AI. A discussion paper on the need for further research into AI risk.
207 Canales Luna, Javier (2023, Nov). 8 top open-source LLMs for 2024 and their uses. DataCamp.
208 Dickson, Ben (2023, March 13). What you need to know about multimodal language models. Tech Talks.
209 CSES Consultations
210 Google DeepMind (2023, Dec 22). 2023. A Year of Groundbreaking Advances in AI and Computing.
211 Askell, A., Bai, Y., Chen, A., Drain, D., Ganguli, D., Henighan, T., Jones, A., Joseph, N., Mann, B., DasSarma, N., Elhage, N., Hatfield-Dodds, Z., Hernandez, D., Kernion, J., Ndousse, K., Olsson, C., Amodei, D., Brown, T., Clark, Jack, McCandlish, S., Olah, C., Kaplan, J. (2021). A General Language Assistant as a Laboratory for Alignment.

specific needs, and that could provide step-by-step instructions on how to apply, including pointing them to the relevant forms and up-to-date deadlines could solve an issue highlighted by many managing authorities interviewed for this study: the burden of applying. Many organisations, in particular, smaller organisations and those with lower budgets often forego opportunities to apply for available funding simply because they do not have the time or the resources to find out about the funding, and to submit an application. It could also save managing and paying authorities time as clear instructions will help beneficiaries submit all relevant pieces of information in a timely manner.

Machine Learning and Big Data Analytics for Risk Scoring

Introduction- Overview of the technology

In the field of budgetary control, the last ten years have seen significant advances in research detecting risks of corruption. This research is largely based on data mining and machine learning tools.

Data mining is the process of identifying or extracting patterns from large datasets.[212] Typically, researchers collect data from different sources, often, they will visualise it, for instance creating graphs to show relationships between variables, trends, or networks visually, they classify or group data, they identify outliers (extreme cases) to better understand it and, then, they analyse it using different methods. In corruption research, researchers use various types of machine learning tools to find patterns and underlying trends in large datasets.

Machine learning is a technology that allows a system to learn how to solve problems without describing the exact path to solution or whose solution method cannot be described by symbolic reasoning rules, but by providing input-output examples from which the system learns on its own.[213] Differently from data mining, machine learning uses algorithms that can 'learn' from data and use this output to predict the future. The most wide-spread approaches to machine learning are supervised learning, unsupervised learning, and reinforcement learning.

Supervised learning is a type of machine learning in which the machine is taught by example. An operator feeds the machine learning algorithm with a labelled dataset that includes the desired inputs and the desired outputs. For instance, a public procurement dataset might include variables denoting the size of a contract, the timing, and companies involved (i.e. inputs), as well as a variable showing whether each contract was found to be fraudulent (yes/no). A supervised learning algorithm will learn from the old observations and make predictions about new observations. In a feedback process the operator (who knows, in this case, which contracts were fraudulent and which were not) corrects the algorithm's predictions, improving the accuracy of its predictions over time. One type of supervised learning that is often used to predict fraud and corruption is **regression analysis**. Regression methods are used to predict an outcome variable (or a 'dependent variable') based on one or more predictor variables (or 'independent variables'). For instance, in the area of fraud detection, a regression model might predict the likelihood of any particular contract containing evidence of fraud based on factors such as the value of the contract, or the number of suppliers bidding for it. Another type of supervised learning that is often used to predict fraud and corruption is **random forest models**. These models create a 'forest' of decision trees trained on random subsets of the training data, and then combine the opinions of these trees, or individual models, to improve the accuracy of the prediction.[214]

[212] Han, Jiawei; Kamber, Micheline (2001). Data mining: concepts and techniques. Morgan Kaufmann. p. 5. ISBN 978-1-55860-489-6.
[213] European Commission's HLEG on artificial intelligence: A definition of AI.
[214] Lima, M. S. M., & Delen, D. (2020). Predicting and explaining corruption across countries: A machine learning approach. Government Information Quarterly, 37(1), 101407; Decarolis, F., Giorgiantonio, C. Corruption red flags in public procurement: new evidence from Italian calls for tenders. EPJ Data Science. 11, 16 (2022). For a simple explanation of random forest models, see Sruthi E R (2024, Jan 3). Understand Random Forest Algorithms With Examples. Analytics Vidhya.

Reinforcement learning is a more dynamic type of machine learning in which a computer (or AI system, or agent) uses trial and error to achieve its goal. That goal is often to maximise its cumulative reward. There is no answer key, and no training dataset. The computer decides what to do to perform its task; and receives feedback (positive or negative) from its action. Reinforcement learning methods include Monte Carlo, state-action-reward-state-action (SARSA) and Q-learning methods.[215]

State of play - Use in the field of budgetary control

In the context of budgetary control, machine learning technologies are used to detect cases of fraud and corruption in public procurement. In the last ten years, both NGOs, CSOs, and government agencies have started using machine learning technologies to build 'red flagging' tools. In this context, red flags are indicators of fraud in subsidies and/or public procurement contracts. For instance, a red flagging tool might flag a contract if the costs of a winning bid is significantly higher than the average cost of a winning contract in the sector. It might also flag a contract if there are political or family ties between the procurement official and the supplier, or if any stakeholder has been linked with fraud, corruption, or the misuse of public resources in the past.

Most red flagging tools use manually defined indicators. To define those indicators, researchers, auditors or NGOs examine past cases of identify patterns of fraud. For instance, if fraudulent contracts in the past tended to exclude information on, for instance, evaluation methods, or if they tended to be renewed many times then these observations will inform the indicators used in red-flagging tools. At the EU level, a prominent example of a red-flagging tool is Arachne (see section 1). At the Member State level, examples of red-flagging tools developed by NGOs include the **Czech zIndex**, and the **Hungarian Red Flags** Project; examples of red-flagging tools developed by auditors include the **Portuguese 22PT01 project** (all described in detail in section 3).

A new approach currently discussed in the academic literature is to use machine learning tools to define red flags. Instead of starting with clearly defined rules the algorithm looks for, these new approaches use unsupervised machine learning algorithms to learn which patterns are associated with higher risks of fraud and corruption.[216]

Possible future developments relating to this type of technology

The increasing availability of large public procurement datasets, and other sources of data on companies, in combination with advances machine learning technology itself leads experts to expect the accuracy of risk-scoring tools to improve significantly over the next five to ten years.[217] Risk-scoring tools can help automate audit processes, reducing manual errors and facilitating more robust and effective control mechanisms.

However, these technological advancements come with challenges. One concern public authorities consulted for this study have raised was about data protection and privacy. Another concern is the cases flagged as potentially fraudulent. An algorithm can flag a case but it cannot explain why. Not every flagged case is indeed fraudulent and there is a risk of discrimination, in particular, if certain societal groups or geographical locations were overrepresented in training data.[218] Hence, training those who work with risk scoring data will be crucial.

In addition, the successful application of data mining and machine learning hinges on the availability of data, for instance, procurement data, and the interoperability of such data, i.e. allowing for the combination of data from multiple sources, for example, through the use of unique identifiers.

Security is another significant concern. However, it is important to note that data can be

[215] Brooks, "What Is Reinforcement Learning? - University of York."
[216] Titl, V., Mazrekaj, D. and Schiltz, F. (2024), Identifying Politically Connected Firms: A Machine Learning Approach*. Oxford Bulletin of Economics and Statistics, 86: 137-155. https://doi.org/10.1111/obes.12586
[217] CSES Consultations.
[218] European Union Agency for Fundamental Rights, Bias in algorithms - Artificial intelligence and discrimination.

pseudonymized for algorithm training and many machine learning applications. This involves processing the data in a way that makes it impossible to link it back to any specific individual while still keeping it suitable for analysis. For instance, this can involve replacing unique identifiers and names with reference numbers to ensure that a data record cannot be traced back to an individual.

Potential applications of new technologies

EU and national-level risk-scoring tools using machine learning will be key components of the fraud prevention and detection strategy in the future. These technologies have proven their potential to improve fraud detection rates, to recover costs, and to protect national and EU budgets.

In the future, Member States that are currently not using Arachne will need more support to catch up. Providing up-to-date and easy-to-understand guidance on how Arachne works, how it protects data and, most importantly, how to use it, will be crucial. Meanwhile, Member States that already use their own risk-flagging tools are expected to continue to use and further develop those tools. As such, national-level tools can complement Arachne and the outcomes from Arachne would ideally be made integrated in the national tools. I.e., officers working with national tools would be able to see projects and beneficiaries flagged as susceptible to risks of fraud, conflict of interest and irregularities by Arachne in the national tools. Integrated systems will be particularly helpful as they will cover contracts at all levels, allowing wider searches and closing loopholes for fraudsters operating at both national and EU level. Member States considering setting up their own red-flagging system could use public procurement data from Tender Electronics Daily and their own business registries as core components of a national-level risk-scoring tools.

Challenges in developing national-level risk-scoring tools will depend on the situation in the Member States especially regarding data availability and data interoperability. For instance, the public procurement risk scoring tools in Czechia (zIndex) and Hungary (Red Flags Project) still need to be evaluated on real conviction or irregularities data. The same holds for any Member State that would like to develop a similar system. One source of information on irregularities is the EU-wide dataset of irregularities stored in the Irregularity and Management System (IMS). Any red flagging tool using machine learning in any Member State could be then trained using the IMS data. The more this tool is used, and the more information it contains, the more valuable it will be as a source of data for EU-wide risk scoring tools.

Robotic process automation (RPA)

1. Introduction - Overview of the technology

Robotic Process Automation (RPA), also known as software robotics, is a no-code or low-code software tool that can replicate and automate repetitive tasks while improving process accuracy and speed. Low-code tools require very little or very simple coding to make them work. No-code approach requires no coding skills at all, which makes it accessible for non-technical users as it enables them to automate processes using visual interfaces with for instance drag-and-drop features.

RPA is delivered via software robots, also known as bots. The word ‘robot’ in this case does not denote a tangible mechanical device, but rather a computer coded software, programmes that replace humans performing repetitive rules-based tasks and/or cross-functional and cross-application macros.[219]

In general, RPA automates repetitive time-consuming office tasks such as opening emails and attachments, moving files and folders, copying and pasting, filling in forms, collecting social media

[219] Deloitte (2017). “The new machinery of government Robotic Process Automation in the Public Sector”

statistics, extracting structured data from documents, making calculations and scraping data from web.[220]

It is important to note that RPA is often mistaken for Artificial Intelligence (AI) when in fact the two technologies are different. Generally speaking, AI simulates human intelligence, while RPA replicates human-directed tasks.[221]

RPA and AI technologies can both make processes more efficient by automating certain tasks. However, there are differences in how these results are achieved, in terms of the type of input data that can be handled by these technologies, the level of human intervention that is required and their adaptability and scalability within an organisation.

RPA uses software applications to automate tasks that are repetitive, rule-based and require high degree of accuracy (e.g. transferring data from funding application or an invoice into an organisation's financial management system; cleaning and formatting data; expense tracking; reporting). RPA is not used for predictive analytics and insight generation, for instance to uncover irregularities and fraud. Instead, RPA limits the need for human intervention in performing repetitive tasks. RPA can work independently without any intervention, although some level of human oversight may be required to ensure the accuracy and quality of the output. The technology can be easily integrated within existing legacy systems that are used within an organisation.[222]

Low code solutions have become increasingly popular as they enable users to create and deploy RPA solutions with minimal coding knowledge. Users that have some experience with digital tools and/or for instance regularly use functions in spreadsheets can introduce an RPA software into their workflow relatively easily as well as build simple RPA after a couple of weeks of RPA training. However, when it comes to complex business processes or automating at scale, someone with an IT background and past experience developing automation software is essential'[223]

2. State of play - Use in the field of budgetary control

In the context of budgetary control, RPA technology is used to automate the following tasks:

- **Data extraction and consolidation:** RPA bots can extract financial data from various sources (for example invoices, grant applications, receipts etc.) and consolidate the data into a central system for further analysis.
- **Reconciliation processes:** Automated bots can perform information reconciliations by matching data from different sources, such as financial statements to ledger entries, to ensure accuracy in financial records.
- **Report generation:** Creation of financial reports can be automated, such as budget summaries, by gathering and formatting data into predefined report templates.
- **Audit-trail creation**: RPA software bots can track and record changes made to financial documents, creating a transparent and reliable audit trail.

[220] Dataconomy.com (2023), "Difference between robotic process automation and machine learning"
[221] IBM (2023), 'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM
[222] Dataconomy.com (2023), "Difference between robotic process automation and machine learning"
[223] IBM (2020), "Seven perspectives on what's required to ensure business users can easily and effectively build software robots.", Fact vs. Fiction: Business Users Can Easily Build Software Robots Using RPA Tools - IBM Blog

- **Compliance checks:** RPA can automate the process of checking transactions and records against current compliance rules and regulations.
- **Budget monitoring:** Bots can continuously monitor budget allocations against expenditures and issue an alert when there are deviations from the planned budget.

The aim of RPA is to automate tasks that are repetitive, rule-based and require high degree of accuracy thus allowing the audit teams to focus on higher value or more complex tasks - for instance related to audit findings. Furthermore, leveraging RPA technology can help institutions within the public sector to make rapid and effective improvements without a complete system overhaul and to meet strict deadlines and respond quicker.[224] Automation can also ensure that processes are carried out in compliance with current regulations and in a consistent manner. The risk of data breaches or unauthorised access can be reduced through automation of data encryption and access control.[225]

Implementing RPA technology does not require large upfront investment and over the long term, it leads to further cost savings by diminishing the reliance on human labour or allowing employees to concentrate on tasks of higher value or complexity. Moreover, RPA software has the capability to execute automated tasks continuously, 24 hours per day. This constant operation not only accelerates process completion but also enhances productivity, as the software can work outside of regular business hours.

The use of RPA in the field of budgetary control is limited by its inability to automate more complex tasks that require advanced decision-making as well as necessary shift in organisational culture. This shift involves retraining teams to adapt to new priorities, focusing on more complex tasks that cannot be handled by RPA. Additionally, unlike more advanced AI systems, RPA cannot learn from past experiences or adapt to new situations without human intervention.

3. Possible future developments relating to this type of technology

Main developments in RPA technology include its combinations with AI specific sub-fields, such as Machine Learning (ML), Natural Language Processing (NLP), and Optical Character Recognition (OCR). **AI and RPA are complementary technologies that can work together to improve operational efficiency and enhance the quality of data-driven budgetary control.**

More specifically, AI can help RPA automate tasks more fully, handle more complex data as well as find patterns in data or extract meaning from images, text or speech.[226] In turn, RPA can enable AI insights to be actioned faster without having to wait on manual implementations.[227]

Intelligent automation (IA) is a term that describes the combination of RPA, AI and other related automation technologies. IA technology can analyse data, learn from patterns, make decisions based on historical data, and perform tasks that traditionally required some level of human judgment or intervention. One example of the application of IA technologies in practice is the Intelligent Document Processing (IDP), which uses IA to extract, process and validate data from images and other files where data often appears in an unstructured format. For instance, IDP can be used to automatically extract and process data from invoices and purchase orders.

---

224 IBM (2023), 'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM
225 Shinde, B. (2021), "Artificial Intelligence Adoption in Internal Audit Processes"
226 Deloitte (2019), "Automation with intelligence Reimagining the organisation in the 'Age of With'", dt-Automation-with-intelligence.pdf (deloitte.com)
227 IBM (2023), 'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM

Hyperautomation of complex business processes that involve both structured and unstructured data has emerged as a significant trend in recent years. The term 'hyperautomation' describes the evolution or extension of IA, taking it to a more advanced level of application.[228] It aims to extend automation capabilities across a wider range of organisational processes with the aim of creating an interconnected and automated workflow across the organisation.

Both IA and hyperautomation find applications across a wide range of sectors including healthcare, banking, retail operations and supply chain and finance. Within the supply chain and finance industries, IA and hyperautomation are capable of streamlining numerous procedures, including procurement and payment processes. By handling repetitive tasks such as processing invoices, managing orders, and tracking shipments, these advanced technologies substantially improve both operational efficiency and accuracy. [229]

Moreover, AI sub-fields as well as robotic process automation (RPA) can be used in conjunction with digital platforms to enhance their features and to enable further automation and digitalisation in the management and control of public expenditure.[230]

4. Potential applications of new technologies

IA and hyperautomation technologies can significantly contribute to a more effective, efficient management and control of EU funds under all three management modes leading to better resource utilization, reduced administrative burden and enhanced service delivery. It is important to note that the field of digital process automation, organizations may gravitate towards low-code/no-code tools such as RPA as these solutions empower non-technical users to implement process improvements swiftly.[231] This is especially likely in case of audit institution, which are in general accustomed to traditional audit methods and resist implementing more advanced solutions.[232]

Due to their complex and decentralised nature, EU funds under the shared management mode can particularly benefit from the adoption of RPA technologies.[233]

The following processes can be enhanced within the management and control of EU funds:

- **Enhanced Efficiency in Performing Administrative Tasks** - RPA can automate routine, repetitive tasks such as data entry, processing of applications, and document management.
- **Improved Data Analysis and Reporting -** RPA can facilitate better data management and analysis. It can automatically gather and consolidate data from various sources, making it easier to generate reports, conduct audits, and perform analytics, which are essential for transparent and effective fund management.
- **Enhanced Fraud Detection** - RPA, combined with other AI technologies can be used to enhance the detection of irregularities and potential fraud. Automated systems can monitor transactions and flag anomalies more efficiently than manual checks.

[228] Consultation for this study.
[229] SageIT (2023). "Hyperautomation vs Intelligent Automation: The Key Differences Explained"
[230] OECD (2019), "An Introduction to Online Platforms and Their Role in the Digital Transformation"
[231] SageIT (2023). "Hyperautomation vs Intelligent Automation: The Key Differences Explained"
[232] Consultation for this study.
[233] Consultation for this study.

- **Enhanced Communication** - Sending automated updates or responses to frequently asked questions can be automated, thereby improving the stakeholder engagement and inter-institutional communication.
- **Faster Processing of Payments and Claims** - RPA technologies can speed up the processing of payments and claims related to EU funds. Faster processing not only improves efficiency but also can enhance satisfaction among beneficiaries.
- **Accuracy and Compliance with Regulatory Requirements** - Since EU funds come with strict regulatory requirements, RPA can ensure that the processing of funds adheres to these regulations consistently, thereby reducing the risk of errors and non-compliance.

Digital platforms

1. Introduction - Overview of the technology

Digital platforms are defined as '*digital services that facilitate interactions via the internet between two or more distinct but interdependent sets of users*' whether they are companies or individuals.[234] **Digital platforms are utilized across a wide array of sectors, reflecting their versatility.** They vary widely in their specific features and purposes and include, inter alia, search engines, online marketplaces, app stores, social media, mobile banking applications as well as other platforms for the collaborative economy.[235]

Sectors that make extensive use of digital platforms include the following:

- **E-commerce and Retail** - online shopping and transactions.
- **Entertainment and Media** - streaming music, movies, TV shows, and other media content.
- **Healthcare** - patient management, telemedicine, electronic health records, and health information exchange.
- **Education** - online learning and virtual classrooms.
- **Financial Services** - online banking, trading, financial planning, and fintech services.
- **Real Estate** - property listings, virtual tours, and online transactions.
- **Travel and Hospitality** - booking platforms for flights, hotels, etc.
- **Information Technology and Services** - IT services, including cloud computing and software development.
- **Manufacturing and Supply Chain** - supply chain management and inventory control.
- **Marketing and Advertising** - targeted advertising, social media marketing and analytics.
- **Government Services** - public service delivery.
- **Transportation and Logistics** - routing, fleet management and logistics planning.

Digital platforms support a wide range of activities, from facilitating transactions and communication to enhancing project management and document collaboration. In fact, they are designed to enable real-time collaboration, where multiple users can work on the same document simultaneously. This is a particularly useful when it comes to activities like editing and reviewing documents.

---

[234] EBA (2021), "Report on the use of Digital Platforms in the EU Banking and Payments Sector"
[235] EP (2020), "Online platforms: Economic and societal effects"

With the rise of remote working, digital collaboration and information sharing platforms have become essential for teams spread across different locations. They allow employees to communicate, share files, and work on projects together as if they were in the same office.[236]

2. State of play - Use in the field of budgetary control

In the context of budgetary control, digital platforms are seen as particularly useful as they can facilitate better collaboration between different stakeholders and can create further added value by encouraging innovation - for instance, audit team members can feel more motivated as they actively participate in decision-making and problem solving. Moreover, digital platforms can support more efficient information sharing, development of joint initiatives and harmonised approaches to auditing and control. [237] **They are instrumental in enhancing the efficiency, transparency, and effectiveness of budgetary control practices.**

Digital platforms act as centralized budgetary information and data repositories, making the data readily available to relevant stakeholders. The centralization ensures that everyone is working with the same data, which can reduce discrepancies. This can increase the efficiency of fraud investigation and prosecution activities, where timely provision of good quality data plays a vital role.

Furthermore, digital platforms allow for real-time updates, ensuring that all parties involved in budgetary control have access to the most up-to-date financial data. Transparency and access to real-time data is crucial for accurate budget tracking and forecasting.[238] Continuous monitoring of progress, milestones and individual tasks within the budgetary control process can aid in ensuring timely completion of the audits.[239]

By incorporating new AI based technologies and/or Robotic Process Automation, the platforms can enable automation of manual tasks, which can help audit teams save time and reduce errors.

The use of digital platforms for information sharing purposes presents both opportunities and challenges.

As mentioned above, these platforms can significantly enhance efficiency, transparency, and real-time decision-making. **However, they also bring issues related to data security, privacy, and interoperability, especially in a multilingual and multi-jurisdictional context like the European Union**.[240] Especially institutions collaborating across borders face legal complexities as they need to ensure legal and regulatory compliance with national data protection laws as well as audit standards.

Both EU and national institutions often store and share data on digital platforms, which require careful handling and confidentiality due to their sensitive nature. This includes financial records, internal controls documentation, HR data, business plans and strategies, tax records, IT security data and other information and other data typically shared during an audit process. Since 2020, under a provision of the EU Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT)

---

[236] OECD (2019), "An Introduction to Online Platforms and Their Role in the Digital Transformation"
[237] EP (2020), "Online platforms: Economic and societal effects"
[238] Lois, P. et al. (2020), "Internal audits in the digital era: opportunities risks and challenges"
[239] Wegner, D., da Silveira, A.B., Marconatto, D. et al. (2023), "A systematic review of collaborative digital platforms: structuring the domain and research agenda"
[240] Consultation for this study.

legal framework[241], businesses were required to register a considerable amount of information about beneficial owners into beneficial ownership registers. This included the following details about the beneficial owners: full name, nationality, date and place of birth, country of residence, complete private/company address, identification number, and nature of beneficial interest. The information in these registers is publicly accessible. The recent European Court of Justice case law (from 22 November 2022, cases C-37/20 and C-601/20)[242] struck down this provision and emphasized the need to balance transparency in financial dealings with the protection of individual privacy rights.[243]

Strategic implementation and continuous development of both technology and human resources as well as the standardisation of data formats and language play are fundamental in order to reap the benefits of digital platforms in budgetary control. It has been emphasized during the consultation for this study that adequate skills and training of staff are necessary for successful implementation of digital platforms.

3. Possible future developments relating to this type of technology

Digital platforms facilitating collaboration and information-sharing are widely used by individual Member States for public procurement, however, the degree of digitalisation of these platforms varies across Member States. It is possible that the traditional public procurement models with minimal digitalisation may eventually progress into highly digitalised models with more advanced futures.

More specifically, there are four main possible levels of digitalisation in the public procurement (and the government commercial payments) sector[244]:

- **Traditional models** are predominantly dependent on extensive paperwork, face-to-face interactions, and manual processes. These methods are generally viewed as expensive, inefficient, and slow. Most specifications and contracts are prepared in paper format, and data is often stored across various Excel spreadsheets or Word documents. This makes the evaluation process not only complicated but also susceptible to mistakes. Despite its drawbacks, traditional procurement remains the most common approach globally.[245]
- **Procurement portals** are online platforms where government bodies post tender notices and make related documents available for interested parties to access. These portals digitise the procurement process by integrating a vendor portal with internal procurement software. The vendor portal facilitates efficient online interaction with bidders and suppliers. Meanwhile, the procurement software automates approval processes and analyses historical tenders and cost savings. In this system, government commercial transactions are conducted digitally. Procurement portals allow for centralised management of various aspects of commercial payments, including invoicing, payments, dispute resolution, refunds, accounting.
- **E-Procurement platforms** transition the process of vendor selection and awarding to an online environment and encompass the following modules: e-tendering, e-auctioning, and e-catalogs. Inbuilt management systems can automatically create orders from approved purchase requests. The entire framework, including payments, contract management, monitoring, auditing, and analytics, is digitalised. In fact, OECD countries are progressively connecting their e-procurement systems with other governmental IT infrastructures - for example with

[241] EU Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) legal framework. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843

[242] Eur-LEX (2022), "Judgment of the Court (Grand Chamber) of 22 November 2022"

[243] Brewcynska, M. (2022). "Privacy and data protection vs public access to entrepreneurs' personal data. Score 2:0".

[244] Kearney (2022), "Digitalizing Government Commercial Payments"

[245] World Bank Group (2017). "Benchmarking Public Procurement"

budgeting tools, business and tax registries, social security databases, and public finance systems. E-procurement platforms put a strong focus on speedy, easy, and seamless payment transactions. In case of card payments, card information can be stored in the system, facilitating one-click authentication and payment processing.

- **E-Marketplaces** add an extra layer of sophistication and automation to e-procurement platforms, transforming government procurement into a contactless, paperless, and cashless process. E-marketplaces offer features that enable users to search and compare based on specific criteria as well as access product or vendor reviews. They facilitate centralised management of spending, vendors, and accounts across multiple government departments. Additionally, these platforms provide automated approval workflows, graphical representations, and analytical tools, enhancing oversight and control over public expenditures. A notable aspect of e-marketplaces is the use of smart contracts. Based on blockchain technology, these contracts are self-executing, self-verifying, tamper-proof, and offer several advantages in public procurement, including decentralisation, transparency and accurate representation of agreements.

Future possible evolution of digital platforms involves further integration of existing AI, RPA and blockchain technologies in order to enhance their capabilities, efficiency as well as user experience.

Any future developments relating to digital platforms will have to comply with relevant EU legislation on digital platforms - the Digital Markets Act (DMA) and Digital Services Act (DSA) both adopted by the Council and the European Parliament in 2022.[246]

DMA focuses on promoting fair and contestable markets within the digital sector. This act specifically targets large digital platforms, designated as "gatekeepers", which provide core services like search engines, app stores, and messaging services. The DMA imposes certain obligations and prohibitions on these gatekeepers to prevent unfair practices and ensure a level playing field for all market participants. For instance, gatekeepers are required to allow third-party interoperability with their services in specific situations and provide business users access to data generated on their platforms. Conversely, they are prohibited from self-preferencing their services or products and tracking users for targeted advertising without explicit consent. This act is a pioneering regulatory tool aimed at regulating the power of major digital companies and complements existing EU competition rules.[247]

In conjunction with the DMA, the DSA has been proposed to regulate the liability of platforms and impose new obligations regarding content moderation, due diligence for illegal content, and transparency of advertising. The DSA, along with DMA, fits into the broader European Digital Strategy. This strategy aims to create a single market for data, ensuring Europe's global competitiveness and data sovereignty. The strategy emphasizes the free flow of data within the EU, respecting EU rules and values, including competition law and data protection. As of 17 February 2024, all platforms must comply with rules under the DSA. Before then, these rules had already applied to Very Large Online Platforms (VLOPs) or Very Large Online Search Engines (VLOSEs) with more than 45 million users in the EU (i.e. reaching more than 10 percent of the EU's population).[248]

[246] Also known as 'The Digital Services Act Package', available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[247] EC (2022). "The Digital Markets Act: ensuring fair and open digital markets"
[248] EC (2022), "Digital Services Act Overview"

4. Potential applications of new technologies

Ongoing efforts to ensure compliance with evolving data privacy regulations and cybersecurity standards will remain crucial to maintaining the integrity and trustworthiness of digital collaboration and information sharing platforms.[249]

Expected technological developments of digital platforms include increasing the level of digitalisation of public procurement platforms, as well as continuous integration of AI, RPA and blockchain technologies within the existing platforms. These developments have the potential to further enhance the management and distribution of EU funds in the following ways:

- **Enhanced Collaboration and Coordination** by supporting mutual learning, the sharing of good practices and exchanges of information between relevant authorities involved in fund management, including EU institutions, national and local authorities, and beneficiaries.
- **More Robust Monitoring and Evaluation** by enabling real-time monitoring and evaluation of fund usage, tracking progress, measuring impact, and identifying areas needing improvement, ensuring that funds are achieving their intended outcomes.
- **Streamlined Administrative Processes** – more advanced digital platforms can automate routine administrative tasks using RPA technology, reducing manual effort and the potential for human error. This includes processes like application submission, data entry, and reporting, leading to more efficient fund management.
- **Data-Driven Decision Making** – digital platforms with integrated data analytics tools can process vast amounts of data to provide insights and forecasts. This data-driven approach can aid in strategic planning and risk management.
- **Enhanced Security and Fraud Detection** - advanced digital platforms can incorporate security measures and fraud detection algorithms.

The insights of EU level institutions shared as part of consultation for this study confirm that leveraging the strengths of both new and existing technologies can lead to synergies that address a wider range of challenges and requirements within budget management and control processes. The aim is to connect disparate tools and platforms to create a unified ecosystem that supports the entire lifecycle of budget management, from planning and allocation to execution and reporting.

Management and control of funds falling under the shared management mode is complex due to the decentralised nature and requires robust monitoring and oversight mechanisms to ensure compliance and accountability across various stakeholders and implementing entities. Hence, they are likely to benefit most from the advances in development of digital platforms.

[249] Consultation for this study.

Blockchain Technologies

1. Introduction- Overview of the technology

Blockchain is a distributed ledger or a shared record of accounting transactions over time. The technology was first invented by a group of researchers in 1991 as a way to timestamp digital documents to make it impossible to backdate them. Functionally, a blockchain is like a digital notary: Once an entry is made it cannot be edited. The technology went largely unnoticed until an individual or a group of individuals under the pseudonym of Satoshi Nakamoto (whose identity remains unknown) picked it up again in 2009 to create the digital cryptocurrency Bitcoin (BTC).[250] Since then, a range of other cryptocurrencies have emerged, including Ethereum (ETH), Ripple (XRP), Litecoin (LTC) and others. These cryptocurrencies use blockchain technology to collect and store information on when individuals buy, sell or exchange cryptocurrency. This information is recorded in different locations and not controlled by any banks or central governments.

While the primary use of blockchain technology remains in cryptocurrency, it is being applied in other domains where information needs to be stored and shared securely. A prominent use is in supply chain management: Logistics companies such as Maersk or Fr8 use blockchain to increase transparency, tracking their goods through each stage of the manufacturing process and across borders and to reduce bottlenecks caused by paperwork and mislabelled goods.[251] Blockchain is also used, or trialled in government, for instance, for land registration, tax collection, storing healthcare records or education certificates, for digital identities, or electronic voting.[252] Leading countries in blockchain technology are the US, China, Switzerland, Singapore, the UK, Germany, Japan, South Korea, El Salvador, and Canada.[253]

A blockchain consists of a chain of connected blocks. Each block stores a piece of data or a transaction. Typically, a block contains four main pieces of information: an index, the data, a unique hash, and the hash of the previous block (unless, of course, it is the first block in the chain, the 'genesis' block). The blocks are linked in chronological order; the index shows where on the chain a block sits. (The first transaction will be stored in a block with the index 1, the second transaction will be stored in a block with the index 2 etc.). The data in a block depends on the type of the blockchain. A bitcoin chain, for instance, includes information on the amount of money (say, 1 bitcoin) that was sent, the sender, and the receiver. A hash is a long string of letters and numbers that identifies the block, or acts as a fingerprint for all the data stored in that block. It includes the index, the previous hash, and the timestamp. The previous hash is the hash of the block that comes before the respective block in the chronological chain. In other words, each block contains not just its own fingerprint, but also the fingerprint of the previous block. (Except, of course, for the first block, or the 'genesis block' which starts the chain, so cannot contain any information on a previous block.)[254]

Any attempts to tamper with the data stored in a block are immediately noticed. If an individual were to change the data in block 1, for instance, increasing the amount of bitcoins to enrich themselves, the hash of that block would change. Because the next block in the chain contains the hash of the previous chain, those hashes would no longer match up. Block 2, and all following blocks would become invalid, making it evident that data has been tampered with. Unlike

---

250 Williams-Elegbe, S. (2019). Public Procurement, Corruption and Blockchain Technology in South Africa: A Preliminary Legal Inquiry. SSRN Electronic Journal. https://doi.org/10.2139/SSRN.3458877
251 Stanford Online (n.d.) Popular blockchain use cases across industries.
252 IBM (2024). How blockchain can bring value to government.
253 Kumar Sharma, Toshendra (2023, Oct 26). Top 10 Countries Leading Blockchain Technology in the World. Blockchain Council.
254 Simply Explained. (2017, November 13). How does a blockchain work? YouTube. https://www.youtube.com/watch?v=SSo_EIwHSd4

traditional accounting systems, blockchain systems are not just stored in one location, where one individual or organisation can see the data but in many locations, where many can see the data. Every node (or host) has a full copy of the entire dataset on their local computer or server. If someone new joins a network, they receive a full copy of the data. This transparency makes it virtually impossible for individuals to tamper with any information stored in a blockchain unnoticed.[255]

One reason why businesses and public authorities have started to use blockchain technology is that they allow them to use smart, or self-executing contracts. Smart contracts are contracts that are automatically enforced once the predefined terms and conditions are met. As such, they allow business to operate in low or no-trust environments. Smart contracts are often likened to vending machines: One does not need to trust the vending machine. Once the item is selected and the money is paid the machine is automatically programmed to release the item. Hence, having a smart contract can make it easier, quicker, and more efficient to execute a contract. For instance, the Swedish land registry (Lantmäteriet) has shifted from notaries to smart contracts, which has reduced transaction times by over 90%.[256] They remove the need for intermediaries, such as lawyers, to ensure that both parties complied with the terms of the contract or to verify ownership of an asset.

There are three main types of blockchain networks: public, private, and consortium blockchains. In a public blockchain networks, anyone can join and participate, i.e. read, write and audit all activities. Public blockchain networks are primarily used for cryptocurrencies where transparency is key. Private blockchain networks, such as those operated by IBM[257], R3 Corda[258], or the open-source blockchain framework Hyperledger Fabric,[259] restrict access to authorised participants. Private blockchain networks are often used by businesses and organisations dealing with sensitive data. They are not decentralised but maintained by a single authority. Finally, consortium (or 'permissioned', 'private and permissioned') blockchain networks are a mix between public and private networks. They allow anyone to join after an identity verification process but place restrictions on certain activities.[260]

2. State of play - Use in the field of budgetary control (Ref. DFR Section 3)

While blockchain is not yet widely used in the field of budgetary control, there are a few pilot projects intended to curb corruption in public procurement. One example is from Colombia. In 2019, after a string of corruption cases surrounding school lunches, which led to the partial or non-fulfilment of contracts, and, in some cases, schools not receiving food that had been paid for, the Office of the Inspector General of Colombia started collaborating with the Inter-American Development Bank and the World Economic to use blockchain to stop corruption in public procurement.[261] In the same year, the Peruvian government announced a partnership with a blockchain startup called Stamping.io in order to create more transparent, corruption-proof contract procurement system.[262] In a similar effort, in 2021, Brazil launched a government blockchain network, the Brazilian Blockchain Network (RBB) which will be used in public institutions

255 Simply Explained. (2017, July 18). Creating a blockchain with JavaScript (Blockchain, part 1). YouTube.
256 Modin, J. (2021, February 8). Balancing Blockchain and AI: ChromaWay and the Swedish Land Registry Submit Findings for Government Report. Chromia, see also Pandey, A. (2022, November 6). How governments can harness the potential of blockchain. McKinsey Digital.
257 IBM (2024). IBM Blockchain.
258 R3 Corda (2024). Open, Permissioned Distributed Platform.
259 Hyperledger (2024). Hyperledger Fabric Docs.
260 Seth, Shobhit (2023, August 24). Public, Private, Permissioned Blockchains Compared.
261 World Economic Forum (2019, May 17). Here's how blockchain could stop corrupt officials from stealing school lunches.
262 Castro Giraldo, Sebastian (2019, May 27). Peru's government looks to blockchain to fight corruption.

to allow citizens to trace public expenditures.[263] Other countries, such as South Africa, Nigeria and Rwanda, are exploring the use of blockchain technologies in public procurement.[264]

The main advantage of using bitcoin in government, and in public procurement, is the transparency it offers. All blockchain transactions are permanently recorded, visible to everyone in the network, and almost impossible to tamper with. By eliminating intermediaries, blockchain technology offers the potential to eliminate opportunities for corruption. As such, blockchains are a key technology for the future of digitalisation in budgetary control.[265]

Notwithstanding the vast opportunities, there are a number of limitations in using blockchain technologies, namely:

- **Energy use**. The main concern – and the reason why blockchain has come under severe criticism – is its high energy use, raising environmental concerns. However, this mainly applies to Bitcoin and other cryptocurrencies, not the blockchains used in the field of public procurement. This point is discussed in more detail below.
- **Infrastructure**. Countries need a reliable technology infrastructure including stable electricity, secure internet connections, data storage and processing capacities, as well as technological expertise in order to set up new nodes, or even participate in existing networks.
- **Scalability**. Demands to handle a growing number of transactions, store growing volumes of data, and increase the number of nodes running in a blockchain network can affect processing speed. Processing more and more transactions quickly and effectively to meet the increasing demand is a challenge for many blockchain networks.[266]
- **Privacy**. While private and permissioned networks tend to guarantee high levels of privacy many public blockchains do not and, instead, reveal data, or metadata publicly and permanently.[267]
- **Interoperability**. As a young technology, blockchains are rarely compatible with other data storage systems.
- **Smart contracts**. Programming code for smart contracts is a challenge. Once the code is stored on a blockchain, it can no longer be edited. A smart contract that is badly designed, or contains a bug, cannot be fixed. Coding bug-free contracts is extremely challenging.[268]
- **Accuracy**. Blockchain systems guarantee that entries are not changed but they do not guarantee that entries are truthful in the first place.
- **Unauthorised access**. There are concerns around how to prevent malicious actors from entering a blockchain.

3. Possible future developments relating to this type of technology

Experts expect two key developments in the development and deployment of blockchain technology in the next ten years. The first is about fine-tuning the technology itself; the second is about creating the legal and technical infrastructure to scale up its use.

[263] Tribunal de Contas Da União (2022, May 25). TCU e BNDES lançam Rede Blockchain Brasil
[264] Faal, E. (2023, September 27). Blockchain could revolutionise public procurement and combat corruption in Africa. LSE Blogs.
[265] Aarvik, Per (2020). Blockchain as an anti-corruption tool. U4 Anti-Corruption Resource Centre.
[266] De Meijer, Carlo R.W. (2023, Sep 26). Blockchain and the scalability challenge. Solving the blockchain trilemma. FinExtra.
[267] Finck, M. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? https://doi.org/10.2861/535
[268] GIZ (2020). Blockchain in Africa. Opportunities and Challenges for the next Decade, p.10-11.

Blockchain research is advancing at a fast pace. Universities, research centres, private sector businesses and even governments across the world are heavily investing in research to overcome the technological obstacles facing blockchain technology. For instance, researchers are working on ways to increase the speed with which blockchains can process transactions, fine-tuning the technology behind smart contracts, and, in particular, working on ways to reduce energy consumption. Given the size of the problem and its effect on public acceptance of the technology it merits a closer description.[269]

Bitcoin alone consumes more than 100 TWh per year – an amount that is equivalent to the annual electricity consumption of the Netherlands.[270] These high levels of energy consumption are due to a design choice, specifically, Bitcoin's 'proof of work' mechanism, or the way bitcoin inventors envisioned the validation of new blocks. In any blockchain, new blocks (or transactions) are not simply added to the chain but need to be validated first. In a bitcoin blockchain, this validation process is a competition where individuals ('miners') compete to solve complex mathematical problems to validate new blocks. As a reward for their work they receive bitcoins – for many, this is a lucrative job. The puzzles are difficult to solve but easy to check. As soon as someone solves a puzzle, they send the solution to the rest of the networks who can easily check if the solution is correct. If it is, the block is added to every copy of the bitcoin chain, and miners can start solving the puzzle for the next block. The computing power required to solve these puzzles, and the large number of miners attempting to solve them across the world at the same time leads to extreme levels of energy consumption. Recent advances in research have shown that moving away from the competition can dramatically reduce the energy consumption.

Ethereum, the world's second-largest cryptocurrency, has solved the energy issue by moving to a less competitive validation mechanism in 2022.[271] Under the new 'proof of stake' system, miners lodge money with the network in order to gain the right to receive rewards by validating transactions. That transition has curbed Ethereum's energy usage by over 99 per cent (down to about 6.6 gigawatt hours of electricity per year, about as much as 2,000 homes[272]). As of early 2024, it is unclear whether Bitcoin and other proof-of-work-based cryptocurrencies will follow suit.[273] Research on reducing the environmental impact of blockchain, for instance, by exploring alternative consensus algorithms, developing more efficient mining techniques, and optimising blockchain protocols to minimise energy consumption is ongoing.[274] In this context, the problem of very high energy consumption only applies to Bitcoin (and, to a lesser degree, other proof-of-work cryptocurrencies) but not to blockchain technology itself. For instance, human operators in private networks or automated approval methods like a smart contract use much less energy to validate transactions. Overall, experts expect the technological obstacles to be overcome soon. According to Andrew Lewis-Pye, blockchain expert at the London School of Economics, "the technological issues are either solved of completely solvable".[275] What is more difficult to predict, Lewis-Pye maintains, is the public's appetite for blockchain technology and its regulation. "If the appetite is there, then the technology will deliver", Lewis-Pye maintains.

---

269 Lewis-Pye, Andrew (2003, Sep 26). Building better blockchains. LSE.
270 Coroamă, V. (2021). Blockchain energy consumption. An exploratory study. www.bfe.admin.ch
271 Nevil, S. (2023, May 27). What Is Proof of Work (PoW) in Blockchain? Investopedia.
272 Huestis, Samuel (2023, January 30). Cryptocurrency's Energy Consumption Problem. RMI; Sparkes (2023, April 26). Cryptocurrency Ethereum has slashed its energy use by 99.99 per cent. New Scientist.
273 Castor, Amy (2023, Feb 28). Ethereum moved to proof of stake. Why can't Bitcoin? MIT Technology Review.
274 Clarke, Anthony (2023, May 30). The Environmental Impact of Blockchain Technology. Nasday.com; Schletz, Marco (2021, Aug 25). Blockchain energy consumption: Debunking the misperceptions of Bitcoin's and blockchain's climate impact. Data Driven Envirolab.
275 Lewis-Pye, Andrew (2003, Sep 26). Building better blockchains. LSE.

Creating a legal framework and, in a second step, the technical infrastructure to use blockchain more widely, including in government, is another challenge. One challenge governments are facing at the moment is how to apply data protection regulations to blockchain technologies.[276] Blockchain technology challenges some of the underlying assumptions of data protection policies. For instance, the EU's data protections policies implicitly assume that there is a natural or legal person who manages data, the 'data controller', who can be contacted in order to enforce citizens' rights under EU data protection law. Public blockchains, however, are designed to replace the data manager with many different players, meaning that, at least in a public blockchain, there is no one person or organisation to contact, or hold accountable. Another concern, and one that applies to all types of blockchains, is the implicit assumption of data protection policies that data *can* be modified or erased, i.e. the 'right to be forgotten' in Article 17(1) GDPR. Blockchains are designed to make it impossible to edit any data. If data that is stored on blockchains is seen as 'personal data' then blockchains cannot enforce the right to be forgotten.[277] Here, too, it is important to note that many of the privacy concerns only apply to public blockchains. Accountability, for instance, is less of an issue in private or consortium blockchains which do have an operator who allows individuals to join and execute functions.[278]

4. Potential applications of new technologies

The EU has taken steps to support the development and the use of blockchain technologies. These include the introduction of the European Blockchain Services Infrastructure (EBSI) in 2018 and the European Commission's decision to license the EBSI software as open-source in 2022.[279] EBSI is a joint effort of the 27 Member States, Norway, Liechtenstein, and the Commission to build a permissioned blockchain infrastructure to facilitate the development and use of blockchain in public (and, eventually, private) organisations across Europe. EBSI's nodes are hosted by node operators who are approved by the European Blockchain Partnership and must adhere to security standards. Initial pilot projects are using the network in a few areas such as identity verification (fighting identity theft), product verification (fighting counterfeit products), or education certificates.[280] In the future, the network could be used to track and record payments in any EU fund. Doing so would reduce opportunities for intermediaries to divert payments or for beneficiaries to use payments in any unintended ways. As such, blockchain technology has the potential to play a pivotal role in fighting fraud and corruption in EU funds, and in safeguarding the EU budget.

---

276 Hallak, Issam and Salén, Rasmus (2023, Sep). European Parliament Briefing. Non-EU countries' regulations on crypto-assets and their potential implications for the EU. European Parliamentary Research Service.

277 Finck, M. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? https://doi.org/10.2861/535

278 Finck, M. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? https://doi.org/10.2861/535

279 Regulation (EU) 2023/114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 , Decentralized Identity (2024). European Blockchain Services Infrastructure (EBSI) and the eSSIF.

280 EBSI (2024). EBSI Projects.

Satellite Imagery

Introduction- Overview of the technology

Satellite images are photographs of the Earth captured by satellites orbiting the planet. These satellites are fitted with diverse sensors designed to detect visible light, infrared light, microwave radiation, and other wavelengths, enabling the creation of high-resolution images. Satellite images monitor developments in climate, geography, and human-made structures in real time. There are different types of images:

- Visible imagery captures surface features akin to traditional photos;
- Infrared imagery detects temperature emissions, which help, for instance, track fire spread and assess soil moisture;
- Water vapor imagery measures atmospheric water content using microwave sensors, crucial for weather forecasting and climate studies.

Governments use satellites data in many ways, for instance, in defence and communication (to inform military operations, surveillance, and intelligence gathering), in urban planning (to manage infrastructure, and to detect changes in land cover), in law enforcement (to analyse crime scenes), or in disaster management (to track areas hit by floods, earthquakes, or wildfires in real time). In agriculture and forestry, satellite imagery is used to monitor fields and crops, to predict yield, and to assess damages.[281]

The EU has a set of dedicated satellites (the Sentinel family) and contributing missions (existing commercial and public satellites) serving Copernicus, the Earth Observation component of the EU's Space programme. The first of the eight Sentinel satellites in orbit today was launched in 2014. Since June 2015, Sentinel 1 and 2 have been sending freely available high-resolution satellite data. The Sentinel-1 satellites (1A and 1B) send out microwave images to the Earth and measure the signal that bounces back, while the Sentinel-2 satellites (2A and 2B) measure visible and infrared light reflected from the Earth.[282]

Since 2017, Sentinel images offer an even higher resolution and send new images with 10 metres spatial resolution every 5 days. Both the resolution and the frequency surpass even the capacity of the United States' equivalent satellite: Landsat, the US satellite Earth observation programme sends a 30 metres resolution image every 16 days. The Sentinel satellite data, which is fully, and freely available, along with sensors on the ground, in the air and below sea, provide citizens, public authorities, and international organisations with a rich data source. By 2023, the EU plans to complete the constellation of around 20 satellites.[283]

State of play - Use in the field of budgetary control

The main use of satellite imagery for EU budgetary control is in the Common Agricultural Policy. Because almost 80% of EU funding for agriculture and rural development is area-based the CAP has a long history of using satellite data to verify farmer's aid claims.

The cornerstone of paying agencies' control systems for area-based CAP schemes is the Land Parcel Identification System (LPIS), an IT system based on high-resolution aerial photographs and satellite

281 Mapbox (2024). What Is Satellite Imagery? Exploring the Full Picture.
282 EUSpace (2024). Copernicus: Europe's Eyes on Earth, p.11
283 EUSpace (2024). Copernicus: Europe's Eyes on Earth, p.10

images of agricultural parcels that are used to check payments made under the Common Agricultural Policy (CAP).[284] Paying agencies use the LPIS to verify that CAP payments are only paid for eligible agricultural land and only once for any parcel of land. Because the LPIS grids are only updated every three years they cannot be used to verify activities taking place on the land during the year, for instance, to check whether farmers grow the crops they reported growing in their aid forms. Therefore, paying agencies continue to carry out field inspections for a small sample of around 5% of farmers.[285] However, field visits are expensive and time-consuming and only provide a record of the situation on the field on one particular day. Satellite imagery, in contrast, provide paying agencies with evidence on the activities on every farm they are responsible for. They can save time, costs, and provide a continuous record of agricultural activity.

The 1992 CAP reform first allowed paying agencies to use satellite images for 'checks with remote sensing'**.** Since then, paying agencies can use satellite images from commercial providers (e.g. SPOT, WorldView, PlanetScope), provided a few times a year, to inspect parcels. According to estimates, around 80% of field inspections are now performed using remote sensing. Paying agencies only carry out a 'rapid field visit' if they cannot draw a conclusion based on the satellite images.

While remote sensing is already a significant improvement to the traditional approach relying on field visits, the new Sentinel-2 satellites data opens up even more opportunities. Since 2018, the EU allows paying agencies to conduct 'checks by monitoring', i.e. to monitor farming activity using Copernicus Sentinel data instead of conducting field visits. This change was made possible because of the high quality and the frequency of the images: The satellite images are clear enough to allow paying agencies to distinguish between different crops and monitor activities such as tilling or mowing. The fact that they are sent out every five days allow paying agencies to monitor agricultural activity throughout the growing season. [286]

A 2022 audit by the European Court of Auditors found that both the Commission and some Member States had started using Sentinel data in the management of CAP funds. The first paying agency that switched to 'checks by monitoring' was the Italian province of Foggia, in Puglia. By 2019, following a number of conferences and workshops as well as bilateral support by the Commission, 15 out of 66 paying agencies (in Belgium, Denmark, Italy, Malta and Spain) were relying on Sentinel data to check aid applications for some schemes and some groups of beneficiaries.[287]

The new 'checks by monitoring' approach combines satellite data with the information provided by farmers. The paying agencies use big data analytics and machine learning algorithms to assess the type of crop and the activities on each declared parcel for each aid scheme. Then, they visualise compliance on digital maps of the respective fields, divided into small parcels. Any parcels the machine learning algorithm assesses as compliant are coloured in green. Any parcels it assesses as non-compliant are coloured in red. Parcels that require further processing (for instance, because there are indications of potential non-compliance or because results are inconclusive) are coloured in yellow.[288]

The new checks are automated and continuous: paying agencies monitor agricultural activity throughout the year and check them against the information they receive from the farmers. For

[284] European Court of Auditors (2016). The Land Parcel Identification System A useful tool to determine the eligibility of agricultural land – but its management could be further improved. Special report No 25, 2016

[285] European Court of Auditors, "Using New Imaging Technologies to Monitor the Common Agricultural Policy: Steady Progress Overall, but Slower for Climate and Environment Monitoring.", p.9

[286] Ibid, p.18

[287] Ibid, p.12

[288] Ibid, p.13

instance, grassland parcels that will need to be mowed by a certain deadline are coloured in yellow until the deadline passes. At that point, if the new data shows that they have indeed been mowed, they switch to red.

The new system offers benefits to paying agencies and farmers. It allows paying agencies to monitor not just a small sample of farms, but all agricultural parcels in the respective region. (Under the 'checks by monitoring system' paying agencies only carry out field visits if the satellite-based monitoring process is inconclusive and if the financial impact of non-compliance exceeds a certain threshold.) This can reduce the number of field visits, saving farmers and paying agencies time and money. The checks by monitoring system also gives paying agencies more leeway to warn farmers in the case of non-compliance. For instance, if a field is not mowed by a deadline, they can give the farmers the opportunity to take corrective action instead of penalising them right away.[289] Finally, it provides farmers with data they can use to increase the productivity of their farm. For instance, farmers receive data about the content of nitrogen in the soil, or on drought stress, which can help them decide where and when to irrigate fields and apply fertiliser. This, in turn, can increase the quality and the quantity of their produce, providing a material benefit for all parties involved.

Possible future developments relating to this type of technology

Earth observation activities are expected to continue expanding in the next 5-10 years. The global satellite communication (SATCOM) market, estimated at USD 77bn in 2022, is expected to grow at over 9% until 2030. This is driven by a growing demand for new High-throughput Satellite Systems (HTS) which enable faster data transmission that are used for bandwidth-intensive applications such as video streaming, remote sensing, and smart product connectivity.[290] Progress in sensor technology and platform miniaturization are enhancing data resolution and coverage, leading to a substantial increase in data volume.[291]

Lower expenses have spurred the emergence of new start-ups and motivated established aerospace firms to pursue innovative opportunities previously deemed too costly or complex. Heavy launch costs to low-Earth orbit (LEO) have plummeted from USD 65,000 per kilogram to USD 1,500 per kilogram (in 2021 dollars) - a reduction of over 95%. These technological strides have also captured the interest of investors, resulting in a surge of funding for space ventures over the past five years.[292]

Experts have great expectations for the forthcoming project "FutureEO" by EESA, with its focus on pioneering research satellite missions aimed at tackling contemporary and future societal challenges. These endeavours encompass a wide array of areas, ranging from elucidating atmospheric dynamics and ice melt in the climate system to addressing critical issues like food security and freshwater resources, ultimately aiming to deliver scientific excellence.[293]

Further development examples also include the new NASA service called terraView, an online platform designed for tracking tree cover, deforestation, and related metrics. Offering the highest resolution available globally, this service effectively detects and monitors forest changes on a comprehensive scale.[294]

[289] European Court of Auditors, "Using New Imaging Technologies to Monitor the Common Agricultural Policy: Steady Progress Overall, but Slower for Climate and Environment Monitoring.", p.18
[290] Grand View Research (2022). Satellite Communication (SATCOM) Market Size, Share & Trends Analysis Report.
[291] Lynnes, Christopher; Huang, Thomas (2019). Future of Big Earth Analytics.
[292] Brukhardt, Ryan (2022, November 28). How will the space economy change the world? McKinsey Quarterly
[293] European Space Agency (n.d.). Introducing FutureEO
[294] NASA (2023, April 20). Taking the Pulse of Earth

Earth Observations are expected to continue expanding rapidly. Moreover, NASA's EOSDIS is projected to experience a tenfold increase, surpassing 200 PB of data within the next six years due to the launch of SWOT and the NASA-Indian Space Research Organization Synthetic Aperture Radar Mission (NISAR).[295]

Potential applications of new technologies

In recent years, the CAP has witnessed significant technological developments aimed at enhancing the efficiency, sustainability, and competitiveness of the agricultural sector. These advancements reflect a broader commitment to modernise farming practices and address climate change, resource scarcity, and the need for increased food production.

Notably, the adoption of digital farming practices, including precision agriculture techniques, has gained momentum. These new farming practices are made possible through the technological innovations of the past few decades, including the satellite-based Global Positioning System (GPS) which can precisely locate individuals or items anywhere on the Earth's surface, and the GPS-based sensors that can be installed in fields, on farming equipment, or in stables to measure data such as air quality, temperature, or humidity, or to track movements.

Geospatial data services provide real-time, location-specific insights, enabling farmers to make informed decisions. In particular, they help farmers monitor the health of their crops and detect the outbreak of diseases early on. In addition, with geospatial data, farmers can precisely apply inputs, such as fertilizers and pesticides, only where they are needed.[296]

The main application of satellite data in the EU is the new 'checks by monitoring' approach described above. While a few paying agencies have switched to the continuous, satellite-based monitoring system the overall take-up by paying agencies is still low. The 2022 ECA audit provided the Commission with a set of recommendations to increase take-up. In particular, the auditor recommend providing incentives for Member States to use checks by monitoring. The auditors also recommend making better use of Sentinel data to monitor environmental and climate requirements.[297]

295 Lynnes, Christopher; Huang, Thomas (2019). Future of Big Earth Data Analytics
296 Utilities One (2023, Jul 18). Understanding the role of geospatial data services in precision farming
297 European Court of Auditors, "Using New Imaging Technologies to Monitor the Common Agricultural Policy: Steady Progress Overall, but Slower for Climate and Environment Monitoring.", p.5

APPENDIX B: BIBLIOGRAPHY

- Aarvik, P. (2020). "Blockchain as an Anti-Corruption Tool". *U4 Anti-Corruption Resource Centre.* Available at: https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption

- Adrian, T., Dong, H., Mancini-Griffoli, T., & Sun, T. (2023). "Central Bank Digital Currency Development Enters the Next Phase". IMF Blog. Available at: https://www.imf.org/en/Blogs/Articles/2023/11/20/central-bank-digital-currency-development-enters-the-next-phase

- Anti-Fraud Knowledge Centre. "What Is an Irregularity?". Available at: https://antifraud-knowledge-centre.ec.europa.eu/guidance-legislation/faq_en

- Article 325 of TFEU. Available at: https://www.legislation.gov.uk/eut/teec/article/325

- Askell, A., Bai, Y., Chen, A., Drain, D., Ganguli, D., Henighan, T., Jones, A., Joseph, N., Mann, B., DasSarma, N., Elhage, N., Hatfield-Dodds, Z., Hernandez, D., Kernion, J., Ndousse, K., Olsson, C., Amodei, D., Brown, T., Clark, Jack, McCandlish, S., Olah, C., Kaplan, J. (2021). "A General Language Assistant as a Laboratory for Alignment". Available at: https://arxiv.org/abs/2112.00861v3

- Bartosz (2023). "51% Attack: The Concept, Risks, and Prevention, Hacken". Available at: https://hacken.io/discover/51-percent-attack/

- Ben Cottier (2023). "Trends in the Dollar Training Cost of Machine Learning Systems". Published online at epochai.org. Available at: https://epochai.org/blog/trends-in-the-dollar-training-cost-of-machine-learning-systems

- Berryhill, J., T. Bourgery and A. Hanson (2018). "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", *OECD Working Papers on Public Governance, No. 28*, OECD Publishing, Paris. Available at: https://doi.org/10.1787/3c32c429-en

- BIEP platforms. Available at: https://biep.nku.cz/

- Blockchain Council (2023). "Types of Blockchains Explained- Public Vs. Private Vs. Consortium". Available at: https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/

- Brewcynska, M. (2022). "Privacy and data protection vs public access to entrepreneurs' personal data. Score 2:0". Available at: https://europeanlawblog.eu/2022/12/15/privacy-and-data-protection-vs-public-access-to-entrepreneurs-personal-data-score-20/

- Brooks, R. (2021). "What Is Reinforcement Learning? - University of York". Available at: https://online.york.ac.uk/what-is-reinforcement-learning/

- Brothwell, R. (2023). "Six Countries Using Blockchain Right Now". Available at: https://www.bsvblockchain.org/news/6-countries-using-blockchain-right-now

- Budhi, Veera (2022). "Advantages and Disadvantages of Blockchain Technology". Available at: https://www.forbes.com/sites/forbestechcouncil/2022/10/20/advantages-and-disadvantages-of-blockchain-technology/?sh=401b133b3453

- Bundeskartellamt (2023). "Abfrage des Wettbewerbsregisters". Available at: https://www.bundeskartellamt.de/DE/Wettbewerbsregister/WettbewReg_node.html

- Bureau van Dijk (2023) "Orbis". Available at: https://www.moodys.com/web/en/us/capabilities/company-reference-data/orbis.html
- Burola, T. (2023). "Public Procurement: Blockchain". Available at: https://medium.com/@tburola/public-procurement-blockchain-eb99c0549327
- Canales L., Javier (2023). "8 Top Open-Source LLMs for 2024 and Their Uses". *DataCamp*. Available at: https://www.datacamp.com/blog/top-open-source-llms
- Castor, A. (2023). "Ethereum Moved to Proof of Stake. Why Can't Bitcoin?". *MIT Technology Review*. Available at: https://www.technologyreview.com/2023/02/28/1069190/ethereum-moved-to-proof-of-stake-why-cant-bitcoin/
- Castro Giraldo, S. (2019). "Peru's Government Looks to Blockchain to Fight Corruption". Available at: https://www.perureports.com/perus-government-looks-to-blockchain-to-fight-corruption/9045
- Clarke, A. (2023). "The Environmental Impact of Blockchain Technology". Available at: https://www.nasdaq.com/articles/the-environmental-impact-of-blockchain-technology
- Cocks, P. (2017). "Malta First to Launch Education Blockchain Certification". *Malta Today*. Available at: https://www.bloomberg.com/news/articles/2018-09-10/blockchain-island-dream-is-calculated-risk-says-malta-leader
- Cointelegraph. (n.d.). "Permissioned Blockchain vs. Permissionless Blockchain: Key Differences". *Cointelegraph.Com*. Available at: https://cointelegraph.com/learn/permissioned-blockchain-vs-permissionless-blockchain-key-differences
- COM (2017) 497 final. "Annual Report to the Discharge Authority on Internal Audits Carried Out in 2016". Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52017DC0497
- COM (2019) 163 final, "Further Strengthening the Rule of Law within the Union State of Play and Possible Next Steps". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0163
- COM (2019) 343 final. "Strengthening the Rule of Law within the Union A blueprint for Action". Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2019%3A343%3AFIN
- COM (2022) 223 final. "Proposal for a Regulation of the European Parliament and of the Council on the Financial Rules Applicable to the General Budget of the Union (Recast)". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0223
- COM (2023) 234 final. "Proposal for a Directive of the European Parliament and of the Council on Combating Corruption". Available at: https://eur-lex.europa.eu/procedure/EN/2023_135
- COM (2023) 311 final. "Proposal for an Interinstitutional Ethics Body". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023DC0405
- COM (2023) 405 final and SWD (2023) 245 final. "Commission Anti-Fraud Strategy Action Plan - 2023 Revision". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023DC0405
- Commission Anti-Fraud Strategy (2019). "COM/2019/196 final and SWD (2019) 170 final". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0196
- Coroamă, V. (2021). "Blockchain Energy Consumption. An Exploratory Study". www.bfe.admin.ch

- Corte dei Conti. (2021). "C.A.T.O.N.E. Project". Available at: https://www.corteconti.it/HOME/StampaMedia/Notizie/DettaglioNotizia?Id=5b0a6ded-eda7-4b52-8f04-a3b8cc56112f
- Dataconomy.com (2023), "Difference Between Robotic Process Automation and Machine Learning". Available at: https://dataconomy.com/2023/03/27/robotic-process-automation-vs-machine-learning/
- Datlab (2024). "ZIndex". Available at: https://zindex.cz/about_us/
- De Meijer, Carlo R.W. (2023). "Blockchain and the Scalability Challenge. Solving the Blockchain Trilemma". *FinExtra*. Available at: https://www.finextra.com/blogposting/24941/blockchain-and-the-scalability-challenge-solving-the-blockchain-trilemma
- Dean, J. (2023). "2023: A Year of Groundbreaking Advances in AI and Computing". Available at: https://deepmind.google/discover/blog/2023-a-year-of-groundbreaking-advances-in-ai-and-computing/
- Decarolis, F., Giorgiantonio, C. (2022). "Corruption Red Flags in Public Procurement: New Evidence from Italian Calls for Tenders". *EPJ Data Science. 11, 16 (2022).* Available at: https://doi.org/10.1140/epjds/s13688-022-00325-x
- Decentralized Identity (2024). "European Blockchain Services Infrastructure (EBSI) and the eSSIF". Available at: https://decentralized-id.com/government/europe/eu/ebsi-essif/
- Deloitte (2017). "The New Machinery of Government Robotic Process Automation in the Public Sector". Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-innovation-the-new-machinery-of-govt.pdf
- Deloitte (2019). "Automation with Intelligence Reimagining the Organisation in the 'Age of With'", Available at: https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/rpa/dt-Automation-with-intelligence.pdf
- Department for Science, Innovation and Technology (2023). "AI Safety Summit. Capabilities and Risks from Frontier AI. A Discussion Paper on the Need for Further Research into AI Risk". Available at: https://assets.publishing.service.gov.uk/media/65395abae6c968000daa9b25/frontier-ai-capabilities-risks-report.pdf
- Dickson, B. (2023). "What You Need to Know About Multimodal Language Models". *Tech Talks.* Available at: https://bdtechtalks.com/2023/03/13/multimodal-large-language-models/
- Dock. (2024). "Blockchain Identity Management: Complete Guide 2024. Dock.Io." Availabe at: https://www.dock.io/post/blockchain-identity-management
- Durant, Elizabeth (2027). „Digital Diploma Debuts at MIT". Availalbe at: https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017
- EBA (2021), "Report on the Use of Digital Platforms in the EU Banking and Payments Sector". Available at: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1019865/EBA%20Digital%20platforms%20report%20-%20210921.pdf

- EC (2014). "Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC Text with EEA Relevance". Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024
- E-Estonia. (2024). "KSI Blockchain Stack: Zero Trust Applications. Digiexpo.e-Estonia.Com". Available at: https://digiexpo.e-estonia.com/cyber-security/ksi-blockchain-stack-zero-trust-applications/
- EpochAI (2022). "Computing Trends across Three Eras of Machine Learning". Available at: https://epochai.org/blog/compute-trends
- ePROCUREMENT.TV. Available at: https://eprocurement.tv/
- EU Digital Finance Platform. Available at: https://digital-finance-platform.ec.europa.eu/
- Euro Data Cube Consortium. (2024). "IACS - LPIS/GSAA Data - Easy Access to Publicly Available Georeferenced Agricultural Parcels in EU Member States". *Eurodatacube.Com*. Available at: https://eurodatacube.com/marketplace/data-products/lpis
- European Anti-Fraud Office (2017) "Handbook on Reporting of Irregularities in Shared Management". Available at: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp/union-anti-fraud-programme-ims-component_en
- European Anti-Fraud Office "Sharing Data and Expertise" (n.d.). Available at: https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/sharing-data-and-expertise_en
- European Anti-Fraud Office "Union Programme – IMS Component" (n.d.). Available at: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp/union-anti-fraud-programme-ims-component_en
- European Blockchain Services Infrastructure (2024). "Blockchain, a Resilient Source of Truth". Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Explained+Series
- European Blockchain Services Infrastructure (2024). "Experience Cross-Border Services with EBSI. The First Public Sector Blockchain Services in Europe". Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home
- European Commission (2006). "JRC Develops Risk Analysis System to Fight Maritime Fraud". Available at: https://cordis.europa.eu/article/id/26644-jrc-develops-risk-analysis-system-to-fight-maritime-fraud
- European Commission (2022), "34th Annual Report; PIF Report". Available at: https://anti-fraud.ec.europa.eu/system/files/2023-07/pif-report-2022_en_0.pdf
- European Commission (2022). "Digital Services Act Overview". Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
- European Commission (2022). "The Digital Markets Act: ensuring fair and open digital markets". Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en
- European Commission (2023) "Commission Anti-Fraud Strategy Action Plan - 2023 revision". Available at: https://anti-fraud.ec.europa.eu/system/files/2023-07/cafs-action-plan-2023-rev_en_0.pdf

- European Commission (2024) 380 final. "Communication: 'Artificial Intelligence in the European Commission (AI@EC)'". Available at: https://commission.europa.eu/system/files/2024-01/EN%20Artificial%20Intelligence%20in%20the%20European%20Commission.PDF
- European Commission (2024). "Available Budget of Cohesion Policy 2021-2027". Available at: https://ec.europa.eu/regional_policy/funding/available-budget_en
- European Commission (2024). "Common Agricultural Policy Funds". Available at: https://agriculture.ec.europa.eu/common-agricultural-policy/financing-cap/cap-funds_en
- European Commission (2024). "Funding by Management Mode". Available at: https://commission.europa.eu/funding-tenders/find-funding/funding-management-mode_en
- European Commission (2024). "Horizon Europe". Available at: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
- European Commission (n.d.) "2014-2020 European structural and investment funds".
- European Commission (n.d.) "Arachne Risk Scoring Tool". Available at: https://ec.europa.eu/social/main.jsp?catId=325&intPageId=3587&langId=en
- European Commission (n.d.) "VIES VAT Number Validation". Available at: https://ec.europa.eu/taxation_customs/vies/#/vat-validation
- European Commission Anti-Fraud Knowledge Centre (n.d.) "PIAF (Integrated Anti-Fraud Platform)". Available at: https://antifraud-knowledge-centre.ec.europa.eu/library-good-practices-and-case-studies/good-practices/piaf-integrated-anti-fraud-platform_en
- European Commission, D. C. (2015). "Copernicus. Europe's Eyes on Earth". Available at: https://doi.org/10.2873/93104
- European Commission's HLEG on Artificial Intelligence: A Definition of AI (2018). Available at: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf
- European Council (2023). "Financial Regulation: Council and Parliament Reach an Agreement". Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/12/08/financial-regulation-council-and-parliament-reach-an-agreement/
- European Court of Auditors (2019). "Special Report No 01/2019: Fighting Fraud in EU Spending: Action Needed". Available at: https://www.eca.europa.eu/Lists/ECADocuments/SR22_14/SR_CAP_Fraud_EN.pdf
- European Court of Auditors (2020) "Using New Imaging Technologies to Monitor the Common Agricultural Policy: Steady Progress Overall, but Slower for Climate and Environment Monitoring". Available at: https://www.eca.europa.eu/ga/publications?did=52913
- European Court of Auditors (2020). "Our Activities in 2020". Available at: https://www.eca.europa.eu/Lists/ECADocuments/AAR20/AAR2020_EN.pdf
- European Court of Auditors (2022) "Protecting the EU Budget Better Use of Blacklisting Needed". Available at: https://www.eca.europa.eu/en/publications?did=61175
- European Court of Auditors (2022). "Our Activities in 2022". Available at: https://www.eca.europa.eu/ECAPublications/AAR-2022/AAR-2022_EN.pdf

- European Court of Auditors (2022). "The Commission's Response to Fraud in the Common Agricultural Policy". Available at: https://op.europa.eu/webpub/eca/special-reports/fraud-in-cap-14-2022/en/
- European Court of Auditors (2023). "Digitalising the Management of EU Funds". Available at: https://www.eca.europa.eu/ECAPublications/RV-2023-04/RV-2023-04_EN.pdf
- European Parliament (2018) "Preventing Fraud and Corruption in the European Structural and Investment Funds", Study commissioned by DG REGIO. Available at: https://ec.europa.eu/sfc/sites/default/files/study-_implem_article125_en-final.pdf
- European Parliament (2020). "Online Platforms: Economic and Societal Effects". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf
- European Parliament (2021). "2019 Discharge: EU General Budget - Commission and Executive Agencies". Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0164_EN.html
- European Parliament (2021). "Digitalisation of European Reporting, Monitoring and Audit". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694229/EPRS_STU(2021)694229_EN.pdf
- European Parliament (2021). "Proceedings of the Workshop on Use of Big Data and AI in Fighting Corruption and Misuse of Public Funds - Good Practice, Ways Forward and How to Integrate New Technology into Contemporary Control Framework". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/691722/IPOL_STU(2021)691722_EN.pdf
- European Parliament (2021). "The Impact of Organised Crime on the EU's Financial Interests. Study for the European Parliament's Committee on Budgetary Control". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697019/IPOL_STU(2021)697019_EN.pdf
- European Parliament (2022), E-001007/2022(ASW)). "Parliamentary Question - E-001007/2022(ASW)". Available at: https://www.europarl.europa.eu/doceo/document/E-9-2022-001007-ASW_EN.html
- European Parliament (2022). "Identifying Patterns of Fraud with EU Funds under Shared Management - Similarities and Differences between Member States. Study for the European Parliament's Committee on Budgetary Control". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/702671/IPOL_STU(2022)702671_EN.pdf
- European Parliament (2022). "Instruments and Tools at EU Level and Developed at Member State Level to Prevent and Tackle Fraud – ARACHNE". Available at: https://www.europarl.europa.eu/cmsdata/259102/ARACHNE%20Briefing.pdf
- European Public Prosecutors Office (2022) "2022 Report". Available at: https://www.eppo.europa.eu/sites/default/files/2023-02/EPPO_2022_Annual_Report_EN_WEB.pdf
- F6S (2024). "38 Top Blockchain Companies and Startups in Kenya in 2024". Available at: https://www.f6s.com/companies/blockchain/kenya/co

- Faal, E. (2023). "Blockchain Could Revolutionise Public Procurement and Combat Corruption in Africa". *LSE Blogs*. https://blogs.lse.ac.uk/africaatlse/2023/09/27/blockchain-could-revolutionise-public-procurement-and-combat-corruption-in-africa/
- Finck, M. (2019). "Blockchain and the General Data Protection Regulation. Can Distributed Ledgers be Squared with European Data Protection Law?" Available at: https://doi.org/10.2861/535
- Finextra (2023). "Blockchain and the Scalability Challenge: Solving the Blockchain Trilemma". Available at: https://www.finextra.com/blogposting/24941/blockchain-and-the-scalability-challenge-solving-the-blockchain-trilemma
- Forbes (2023). "Google Invests in Anthropic for USD 2bn as AI Race Heats Up". Available at: https://www.forbes.com/sites/qai/2023/10/31/google-invests-in-anthropic-for-2-billion-as-ai-race-heats-up/?sh=2868f8fe664e
- Fortune Business Insights. (2023). "Market Research Report. Blockchain Technology Market Size, Share and Growth". Available at: https://www.fortunebusinessinsights.com/industry-reports/blockchain-market-100072
- FRA (2022). "Bias in algorithms - Artificial Intelligence and Discrimination". Available at: https://fra.europa.eu/en/publication/2022/bias-algorithm.
- Frankenfeld, Jake, Rasure, Erika, Kvilhaug, Suzanne (2023). "51% Attack: Definition, who is at risk, example, and cost". Available at: https://www.investopedia.com/terms/1/51-attack.asp
- Freeman, O. J. (2023). "Ten Companies Using Blockchain Technology for Sustainable Supply Chain. Medium". Available at: https://medium.com/@OjFRSA/10-companies-using-blockchain-technology-for-sustainable-supply-chain-6d17ca8cca25
- Funmilayo, M. (2023). "Enhancing Tax Transparency With Blockchain Technology". Available at: https://punchng.com/enhancing-tax-transparency-with-blockchain-technology
- GIZ (2020). "Blockchain in Africa. Opportunities and Challenges for the Next Decade". Available at: https://www.giz.de/expertise/downloads/Blockchain%20in%20Africa.pdf
- Google DeepMind (2023). "2023. A Year of Groundbreaking Advances in AI and Computing". Available at: https://deepmind.google/discover/blog/2023-a-year-of-groundbreaking-advances-in-ai-and-computing/
- Grand View Research (2022). "Satellite Communication (SATCOM) Market Size, Share & Trends Analysis Report". Available at: https://www.grandviewresearch.com/industry-analysis/satellite-communication-market
- Hallak, I. and Salén, R. (2023). "European Parliament Briefing. Non-EU Countries' Regulations on Crypto-Assets and Their Potential Implications for the EU". *European Parliamentary Research Service.* Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/753930/EPRS_BRI(2023)753930_EN.pdf
- Han, J.; Kamber, M. (2001). "Data Mining: Concepts and Techniques", Available at: https://mitmecsept.files.wordpress.com/2017/04/data-mining-concepts-and-techniques-2nd-edition-impressao.pdf
- Hayes, A. (2023). "Learn What These Digital Public Ledgers Are Capable Of". Available at: https://www.investopedia.com/terms/b/blockchain.asp

- Heidland Werres Diederichs (2023). „Das Wettbewerbsregister beim Bundeskartellamt". Available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/21_12_2023_Jahresrueckblick.html
- Hirdaramani, Y. (2023). "Is It Time to Say Goodbye to 'Ask Jamie'?. Inside GovTech's Refresh of Government Chatbots". Govinsider.Asia. Available at: https://govinsider.asia/intl-en/article/is-it-time-to-say-goodbye-to-ask-jamie-inside-govtechs-refresh-of-government-chatbots
- Huestis, S. (2023). "Cryptocurrency's Energy Consumption Problem". Available at: https://rmi.org/cryptocurrencys-energy-consumption-problem/
- Hughes, S. (2023). "Cut the Bull - Detecting Hallucinations in Large Language Models". Available at: https://vectara.com/blog/cut-the-bull-detecting-hallucinations-in-large-language-models/
- Hutchins, J. (2004). "The Georgetown-IBM Experiment Demonstrated in January 1954." Available at: https://link.springer.com/chapter/10.1007/978-3-540-30194-3_12
- Hyperledger (2024). "Hyperledger Fabric Docs". Available at: https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html
- IBM (2020), "Seven Perspectives on What's Required to Ensure Business Users Can Easily and Effectively Build Software Robots.", Fact vs. Fiction: Business Users Can Easily Build Software Robots Using RPA Tools - IBM Blog. Available at: https://www.ibm.com/blog/fact-vs-fiction-business-users-can-easily-build-software-robots-using-rpa-tools/
- IBM (2023), "'What is Robotic Process Automation', What is Robotic Process Automation (RPA)? | IBM". Available at: https://www.ibm.com/topics/rpa
- IBM (2024). "How Blockchain Can Bring Value to Government". Available at: https://www.ibm.com/blockchain/industries/government
- IBM (2024). "What is a Chatbot?". Available at: https://www.ibm.com/topics/chatbots
- IBM Data and AI Team (2023). "AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?". Available at: https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/
- IGAE (2023). "INFOFRAUD by SNCA". Available at: https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/Paginas/inicio.aspx
- Interacly AI. (2023). "LLMs and Chatbots: A Match Made in Tech Heaven". Interacly AI. Available at: https://medium.com/@interacly/llms-and-chatbots-a-match-made-in-tech-heaven-dc548583146c
- Jones, M. (2023). "Study Shows 130 Countries Exploring Central Bank Digital Currencies". *Reuters*. https://www.reuters.com/markets/currencies/study-shows-130-countries-exploring-central-bank-digital-currencies-2023-06-28/
- Jungermann, Sebastian (2023). "Das Zentrale Wettbewerbsregister beim Bundeskartellamt. Deutscher Anwalt". Available at: https://www.deutscheranwaltspiegel.de/anwaltspiegel/archiv/das-zentrale-wettbewerbsregister-beim-bundeskartellamt/

- Kearney (2022). "Digitalizing Government Commercial Payments". Available at: https://www.globalgovernmentforum.com/wp-content/uploads/visa-kearney-digitalizing-government-commercial-payments.pdf
- Krauth, O. (2022). "Five Companies Using Blockchain to Drive Their Supply Chain | TechRepublic. Tech Republic". Available at: https://www.techrepublic.com/article/5-companies-using-blockchain-to-drive-their-supply-chain/
- Kshetri, N. (2022). "Blockchain's Role in Fighting Corruption and Improving Public Sector Efficiency in Developing Countries". Available at: https://www.computer.org/csdl/magazine/it/2022/06/10017403/1JYZDoOjX1e
- Kumar Sharma, T. (2023). "Top 10 Countries Leading Blockchain Technology in the World. Blockchain Council". Available at: https://www.blockchain-council.org/blockchain/top-10-countries-leading-blockchain-technology-in-the-world/
- Kumar, A., Chhangani, A., Brownstein, G., & Meng, P. (2024). „Central Bank Digital Currency Tracker. Atlantic Council". Available at: https://www.atlanticcouncil.org/cbdctracker/
- Lewis-Pye, A. (2003). "Building Better Blockchains". *LSE.* Available at: https://www.lse.ac.uk/research/research-for-the-world/society/building-better-blockchains
- Lexis Nexis (n.d.) "Adverse Media Monitoring". Available at: https://internationalsales.lexisnexis.com/glossary/data-as-a-service/adverse-media-monitoring
- Lexis Nexis (n.d.) "LexisNexis® WorldCompliance™ Online Search Tool. Available at: https://risk.lexisnexis.com/products/worldcompliance-online-search-tool
- Lexis Nexis (n.d.) "Politically Exposed Persons List". Available at: Politically Expose Persons List
- Lexis Nexis (n.d.) "Sanctions List Screening". Available at: https://risk.lexisnexis.co.uk/corporations-and-non-profits/financial-crime-compliance/watchlist-screening/sanctions-list-screening
- Lima, M. S. M., & Delen, D. (2020). "Predicting and Explaining Corruption across Countries: A Machine Learning Approach". *Government Information Quarterly, 37(1), 101407.* Available at: https://www.sciencedirect.com/science/article/abs/pii/S0740624X19302473
- Litan, A. (2022). "Metaverse, Web3 and Crypto: Separating Blockchain Hype from Reality. Gartner". Available at: https://www.gartner.com/en/newsroom/press-releases/2022-08-30-metaverse-web3-and-crypto-separating-blockchain-hype-from-reality.
- Lois, P. et al. (2020), "Internal Audits in the Digital Era: Opportunities Risks and Challenges". Available at: https://www.emerald.com/insight/content/doi/10.1108/EMJB-07-2019-0097/full/html
- Louw, Liz (2022). "How Public and Private Blockchain Compete on Data Privacy and Throughput". Available at: https://www.bsvblockchain.org/news/how-public-and-private-blockchain-compete-on-data-privacy-and-throughput
- Lursoft online platform, Available at: https://www.lursoft.lv/en
- Lynnes, Ch.; Huang, T. (2019). "Future of Big Earth Analytics". Available at: https://ntrs.nasa.gov/api/citations/20190000507/downloads/20190000507.pdf

- Maameri, Sami (2023). "Building a Multi-Document Reader and Chatbot With LangChain and ChatGPT". Available at: https://betterprogramming.pub/building-a-multi-document-reader-and-chatbot-with-langchain-and-chatgpt-d1864d47e339
- Mapbox. (2024). "What is Satellite Imagery? Exploring the Full Picture". *Mapbox.* Available at: https://www.mapbox.com/insights/satellite-imagery
- Medium (2022). "Types of Blockchain". Availalbe at: https://medium.com/techskill-brew/types-of-blockchain-part-4-blockchain-basics-c0b2e40c1780
- Modin, J. (2021). "Balancing Blockchain and AI: ChromaWay and the Swedish Land Registry Submit Findings for Government Report. Chromia". Available at: https://blog.chromia.com/balancing-blockchain-and-ai-chromaway-and-the-swedish-land-registry-submit-findings-for-government-report/
- Molemans, L. (2018) "Arachne Risk Scoring tool – Identifying and Monitoring of Risky Projects.", *Video tutorial.* Available at: https://www.youtube.com/watch?v=lIJBc-ImcOQ
- Molemans, L. (2018) "Arachne Risk Scoring Tool – Identifying and Monitoring of Risky Projects," PowerPoint Presentation. Available at: https://slideplayer.com/slide/14283052/
- MySMIS2021/SMIS2021+ Platform. Available at: https://resurse.mysmis2021.gov.ro/ords/repo_bo/r/mysmis-2021/home
- Nevil, S. (2023)." What Is Proof of Work (PoW) in Blockchain?". *Investopedia*. Available at: https://www.investopedia.com/terms/p/proof-work.asp
- New York Times (2023). "Mistral, French A.I. Start-Up, Is Valued at $2 Billion in Funding Round". Available at: https://www.nytimes.com/2023/12/10/technology/mistral-ai-funding.html
- Nolan, Beatrice (2023). "Google Researchers Say They Got OpenAI's ChatGPT to Reveal Some of Its Training Data with Just One Word". Available at: https://www.businessinsider.com/google-researchers-openai-chatgpt-to-reveal-its-training-data-study-2023-12?r=US&IR=T
- Okta. (n.d.). Practical Thoughts on Blockchain and Identity. Okta.Com. Available at: https://www.okta.com/resources/whitepaper/practical-thoughts-on-blockchain-and-identity/
- OLAF (2017) "Handbook on Reporting of Irregularities in Shared Management". Available at: Available at: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp/union-anti-fraud-programme-ims-component_en
- OLAF (2022). "PIF Report". Available at: https://op.europa.eu/webpub/olaf/pif-report-2022/en/#chapter4
- OLAF (2023). "Anti-Fraud Knowledge Centre. Competition Register". Available at: https://antifraud-knowledge-centre.ec.europa.eu/index_en [Accessed 9 Nov 2023].
- OLAF (2023). "Union Anti-Fraud Programme - Hercule component". Available at: https://anti-fraud.ec.europa.eu/policy/union-anti-fraud-programme-uafp/union-anti-fraud-programme-hercule-component_en
- Orisakwe, Jennifer (2023). "East Africa Keenly Explores Blockchain Technology in Healthcare". *Omnia Health*. Available at: https://insights.omnia-health.com/technology/east-africa-keenly-explores-blockchain-technology-healthcare

- Owen, P. W., Roberts, G., Bortnowschi, R., Prigent, O., Hardy, R., Dolezal, J., Brems, E., Braz, P., Ruiz, A. C., Chaudry, A., Konstantopoulos, M., Poulsen, A., Scheckenbach, B., & Ulander, P. (2020). "Special Report 04/2020: Using New Imaging Technologies to Monitor the Common Agricultural Policy: Steady Progress Overall, but Slower for Climate and Environment Monitoring. In Luxembourg: Publications Office of the European Union". Available at: https://www.eca.europa.eu/Lists/ECADocuments/SR20_04/SR_New_technologies_in_agri-monitoring_EN.pdf
- Pandey, A. (2022). "How Governments Can Harness the Potential of Blockchain. McKinsey Digital". Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/how-governments-can-harness-the-potential-of-blockchain
- Procurement learning.com (2023), "Certificate Program in Public Procurement (CPPP)". Available at: https://www.procurementlearning.org/certificate-program-public-procurement-cppp/
- Proebiz platform. Available at: http://www.proebiz.com/en
- Propopulus (2019). "France Will Monitor Poplar Plantations Using New Remote Sensing Images from Satellites.". Available at: https://propopulus.eu/en/france-will-monitor-popular-plantations-using-new-remote-sensing-images-from-satellites/
- R3 Corda (2024). "Open, Permissioned Distributed Platform". Available at: https://r3.com/products/corda/
- RedFlags.eu (2024). "About the Project". Availalbe at: https://www.redflags.eu/
- Regulation (EU) 2023/114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/753930/EPRS_BRI(2023)753930_EN.pdf
- Regulation (EU) No 1303/2013 of the European Parliament and of the Council of 17 December 2013. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex%3A32013R1303
- Regulation (EU, Euratom) 2020/2092. "On a General Regime of Conditionality for the Protection of the Union Budget". Available at: https://eur-lex.europa.eu/eli/reg/2020/2092/oj
- Reuters (2024). "OpenAI Hits USD 2bn Revenue Milestone". Available at: https://www.reuters.com/technology/openai-hits-2-bln-revenue-milestone-ft-2024-02-09/
- Rodriguez, Daniel & Gutierrez, Paula Andrea (n.n.). "Implementation of Blockchain in Public Procurement to Reduce Corruption Risks". Available at: https://cms.law/en/col/publication/implementation-of-blockchain-in-public-procurement-to-reduce-corruption-risk
- Roser, M.; Ritchie, H., Mathieu, E. (2023). "What is Moore's Law?". *Our World in Data*. Available at: https://ourworldindata.org/moores-law
- Schletz, M. (2021). "Blockchain Energy Consumption: Debunking the Misperceptions of Bitcoin's and Blockchain's Climate Impact". *Data Driven Envirolab*. Available at: https://datadrivenlab.org/climate/blockchain-energy-consumption-debunking-the-misperceptions-of-bitcoins-and-blockchains-climate-impact/

- Shang, Q., & Price, A. (2019). "A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. Innovations: Technology, Governance, Globalization", 12(3–4), 72–78. Available at: https://doi.org/10.1162/INOV_A_00276
- Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2022). Blockchain technology and its applications to combat COVID-19 pandemic. Research on Biomedical Engineering, 38(1), 173. https://doi.org/10.1007/S42600-020-00106-3
- Shinde, B. (2021). "Artificial Intelligence Adoption in Internal Audit Processes" Available at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-40/artificial-intelligence-adoption-in-internal-audit-processes
- Shobhit, S. (2023). "Public, Private, Permissioned Blockchains Compared". Available at: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/
- Simply Explained. (2017). "Creating a Blockchain with JavaScript (Blockchain, part 1)". *YouTube*. Available at: https://www.youtube.com/watch?v=zVqczFZr124
- Simply Explained. (2017). "How Does a Blockchain Work?". *YouTube*. https://www.youtube.com/watch?v=SSo_EIwHSd4
- Singh, G., & Levi, J. (2020). "MiPasa Project and IBM Blockchain Team on Open Data Platform to Support Covid-19 Response". *IBM Blog*. https://www.ibm.com/blog/mipasa-project-and-ibm-blockchain-team-on-open-data-platform-to-support-covid-19-response/
- Smartnation.gov.sg. "Graduate with a Digital Academic Certificate". Available at: https://www.smartnation.gov.sg/initiatives/digital-government-services/opencerts/
- Smith, C., S. (2023). "What Large Language Models Cost You – There is No Free AI Lunch." *Forbes*. Available at: https://www.forbes.com/sites/craigsmith/2023/09/08/what-large-models-cost-you--there-is-no-free-ai-lunch/?sh=76f6ecc04af7
- Smith, T. (2023). "Europe's Generative AI Startups, Mapped". Available at: https://sifted.eu/articles/europe-generative-ai-startups
- Sparkes (2023). Cryptocurrency Ethereum Has Slashed its Energy Use by 99.99 Per Cent". *New Scientist*. Available at: https://www.newscientist.com/article/2369304-cryptocurrency-ethereum-has-slashed-its-energy-use-by-99-99-per-cent/
- Special Investigation Service of the Republic of Lithuania. (2019). "Strengthening Analytical Skills in Order to Protect EU Financial Interests". Available at: https://www.stt.lt/en/news/7481/_2019/strengthening-of-analytical-skills-in-order-to-ensure-the-protection-of-eu-financial-interests:2639
- Sruthi E R (2024). "Understand Random Forest Algorithms With Examples". *Analytics Vidhya*. Available at: https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/
- Stamping.io. "APIConnector to decentralized services of #web3". Available at: https://stamping.io/
- Stanford Online (n.d.) "Popular Blockchain Use Cases across Industries". Available at: https://online.stanford.edu/popular-blockchain-use-cases-across-industries
- Stöffelbauer, A. (2023). "How Large Language Models Work. From Zero to ChatGPT". *Medium.com*. Available at: https://medium.com/data-science-at-microsoft/how-large-language-models-work-91c362f5b78f

- Stokel-Walker (2023). "AI Chatbots Could Hit a Ceiling after 2026 as Training Data Runs Dry". *New Scientist*. Available at: https://www.newscientist.com/article/2353751-ai-chatbots-could-hit-a-ceiling-after-2026-as-training-data-runs-dry/
- Tam, A. (2023). "What are Large Language Models? Machine Learning Mastery". Available at: https://machinelearningmastery.com/what-are-large-language-models/
- Tartu Observatory. (2019). "Information System SATIKAS Helps to Detect Moving by Using Satellite Data. University of Tartu. Available at: https://kosmos.ut.ee/en/content/information-system-satikas-helps-detect-mowing-using-satellite-data
- Titl, V., Mazrekaj, D. and Schiltz, F. (2024). "Identifying Politically Connected Firms: A Machine Learning Approach". *Oxford Bulletin of Economics and Statistics,* 86: 137-155. https://doi.org/10.1111/obes.12586
- Tribunal de Contas Da União (2022). "TCU e BNDES lançam Rede Blockchain Brasil". Available at: https://cryptopotato.com/brazil-launches-a-blockchain-network-to-better-trace-public-expenditures/
- UK Parliament (2023). "House of Lords Communication and Digital Select Committee Inquiry: Large Language Models". Available at: https://committees.parliament.uk/writtenevidence/122665/pdf/
- Unviersidad Carlos III de Madrid (2018). „Acreditaciones de Competencias Utilizando la Tecnología Blockchain en Cursos Spocs". Available at: https://www.uc3m.es/sdic/articulos/2018/acreditaciones-utilizando-blockchain
- US Citizenship and Immigration Services. (2018). "Meet Emma, Our Virtual Assistant". Uscis.Gov. https://www.uscis.gov/tools/meet-emma-our-virtual-assistant
- US Government Accountability Office (2024). "Artificial Intelligence: GAO's Work to Leverage Technology and Ensure Responsible Use". Available at: https://www.gao.gov/products/gao-24-107237
- US Government Accountability Office (n.d.). "About". Available at: https://www.gao.gov/about
- Van Hoek, Remko & Lacity, Mary (2020). "How the Pandemic Is Pushing Blockchain Forward". *Harvard Business Review*. Available at: https://hbr.org/2020/04/how-the-pandemic-is-pushing-blockchain-forward
- Van Noordt and Misuraca. (2020). "Exploratory Insights on Artificial Intelligence for Government in Europe". Available at: https://journals.sagepub.com/doi/abs/10.1177/0894439320980449
- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). "Attention Is All You Need. Advances in Neural Information Processing Systems". Available at: https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf
- Vistra (2023). "ECJ Ruling on Access to Beneficial Ownership Information: Balancing Transparency and Privacy". Available at: https://www.vistra.com/insights/ecj-ruling-access-beneficial-ownership-information-balancing-transparency-and-privacy
- VSoft Consulting (n.d.) "12 Global Government Agencies That Use Chatbots". Available at: https://blog.vsoftconsulting.com/blog/15-governments-agencies-that-use-chatbots

- Wegner, D., da Silveira, A.B., Marconatto, D. et al. (2023), "A Systematic Review of Collaborative Digital Platforms: Structuring the Domain and Research Agenda". Available at: https://link.springer.com/article/10.1007/s11846-023-00695-0
- Wieler, Anne-Christine. "Überblick zum Wettbewerbsregister". Lutz Label. 7 April 2023. Available at: https://www.lutzabel.com/artikel/20210407-ueberblick-zum-wettbewerbsregister
- Williams-Elegbe, S. (2019). "Public Procurement, Corruption and Blockchain Technology in South Africa: A Preliminary Legal Inquiry". *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3458877
- Wolfewicz, A. (2023). "Deep Learning vs. Machine Learning – What's The Difference?". *Levity*. Available at: https://levity.ai/blog/difference-machine-learning-deep-learning
- World Bank Group (2017). "Benchmarking Public Procurement". Available at: https://documents1.worldbank.org/curated/en/121001523554026106/Benchmarking-Public-Procurement-2017-Assessing-Public-Procurement-Regulatory-Systems-in-180-Economies.pdf
- World Economic Forum (2019). "Here's How Blockchain Could Stop Corrupt Officials from Stealing School Lunches". Available at: https://www.weforum.org/agenda/2019/05/heres-how-blockchain-stopped-corrupt-officials-stealing-school-dinners/
- Zaazaa, Oualid, El Bakkali, Hanan El (2023). "Unveiling the Landscape of Smart Contract Vulnerabilities: A Detailed Examination and Codification of Vulnerabilities in Prominent Blockchains". *Cornell University*. Available at: https://arxiv.org/abs/2312.00499

APPENDIX C: INTERVIEWS

EU level interviews

Name	Commission's DGs and other EU bodies	Role
Frank Sébert	European Commission, REGIO.DAC	Director
Lothar Kuhl	European Commission, REGIO.DAC.7	Head of Unit
Cristina Asturias	European Commission, REGIO.DAC.1	Head of Unit
James Sweeney	OLAF.C	Director of OLAF Knowledge Centre (Directorate C)
Georg Roebling	OLAF.C.2	Head of Unit
Laurentiu Dumitrica	EPPO	Senior Case Analyst (Team IBOAs)
Roberto Bianchin	EPPO	Senior Case Analyst Acting Head of the Sector "Operational Support Services"
Daniela Ciobanu	European Commission, DG AGRI.H.1	Head of Unit
Juan Luis Roldan	European Commission, DG AGRI.H.2	Deputy Head of Unit
Ernestas Petraitis	European Commission, DG AGRI.R.4	Deputy Head of Unit
Magdalana Lazar	European Commission, DG AGRI	Senior Policy Officer
Bernadette Frederick	European Commission, DG ECFIN	Director, DG ECFIN.R
Stanislav Ranguelov	European Commission, DG EMPL	Head of Unit EMPL.G4
Mikolaj Solik (Written comments)	European Commission, DG BUDG	DG BUDGET, Coordination of Inter-institutional Relations
(Written comments)	European Commission, DG DIGIT	
Alexis Peroulakis	European Commission, DG ECFIN	Internal Control Officer
Agnes Thibault	European Commission, DG ECFIN	Deputy Head of Unit R4 Control and Evaluation
Farid Rahmi	European Commission, DG ECFIN	Head of IT development

National level interviews

Belgium	Flemish Audit Authority (VAA)	Tony Mortier
Czechia	Ministry of the Environment, Department of EU Funds	Jaroslav Michna
Czechia	Ministry for Regional Development of the Czech Republic Department of European Territorial Cooperation Czech Republic	Martina Kvasilová
Germany	Bundeskartellamt (an independent higher federal authority assigned to the Federal Ministry for Economic Affairs and Climate Action)	Christian Heuser, Abteilung Wettbewerbsregister Referat W3
Germany	Bundeskartellamt	Till Wiesner
Germany	Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF)	Peter Grönwoldt
Germany	Federal Ministry for Family Affairs, Senior Citizens, Women and Youth (Federal Ministry for the Environment, Nature Conservation and Nuclear Safety, BMFSFJ)	Annette Gehrz, Referat Z15 Europäischer Sozialfonds, Referatsleitung
Germany	Ministry of Finance of Saxony-Anhalt (Ministerium der Finanzen des Landes Sachsen-Anhalt, EU-Verwaltungsbehörde EFRE/ESF/JTF)	Josephine Szigeti, Referentin EU-Verwaltungsbehörde EFRE/ESF/JTF
Germany	Ministry of Economic Affairs, Industry, Climate Action, and Energy of the State of North Rhine-Westphalia (Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen)	Bastian Hoffmann, Referent – IT-System BISAM und Haushalt, Referat 521 – EFRE-Verwaltungsbehörde – Programmsteuerung
Germany	Ministry of Economy, Infrastructure, Tourism and Labor of Mecklenburg-Vorpommern (Ministerium für Wirtschaft, Infrastruktur, Tourismus und Arbeit)	Tobias Stender, Leiter Referat EFRE-Fondsverwaltung/-steuerung/-bescheinigung
Germany	Saxon State Ministry for Economic Affairs, Labour and Transport (Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr, EU-Verwaltungsbehörde EFRE/JTF)	Detlev Noack, Referent, Referat 28 | Verwaltungsbehörde EFRE/JTF
Germany	Saxon State Ministry for Economic Affairs, Labour and Transport	Betty Zschoche, Referentin, Bescheinigungsbehörde
Germany	Saxon State Ministry for Economic Affairs, Labour and Transport	Sven Lederer, Referent, Verwaltungsbehörde EFRE/JTF
Germany	Saxon State Ministry for Economic Affairs, Labour and Transport	Andreas Janthur, Referent, Verwaltungsbehörde EFRE/JTF
Italy	Bocconi University	Francesco Decarolis, Professor of Economics
Italy	Sardinia Region- audit authority	Vincenzo Pavone
Italy	Sardinia Region- audit authority	Antonio Cadeddu

Netherlands	Flemish Audit Authority (FAA) (Vlaamse Auditautoriteit van de Europese Structuurdondsen)	Tony Mortier, Finance Inspector
Portugal	Think Tank. Risco de Fraude recursos financeiros da uniao europeia	Elsa Cardoso, Department of Information Science and Technology (ISTA)
Portugal	Portuguese Court of Auditors, Center for Innovation, Technology and Methodologies (Tribunal de Contas, Centro de Inovação, Tecnologia e Metodologias, CITM)	Pedro Batista, Data Scientist
Portugal	Portuguese Court of Auditors	Maria João Morgado, Jurist/Auditor
Portugal	Portuguese Court of Auditors	Sandra Sousa, Chefe de Divisão da DGFP-DAAG
Portugal	Transparência Internacional Portugal (TI Portugal)	Mr José Fontão, vice-chair
Slovakia	Ministry of Interior of the Slovak republic	Jozef Kubinec, Head of Works and ICT Procurement Department
Slovakia	Proebiz	Zuzana Kawulokova, production manager
Slovakia	Proebiz	Marian Gałuszka, project manager
Slovakia	Cequence	Rasto Koval, CEO
Slovakia	Cequence	Martin Ragan, CRO and Co-founder
Sweden	Swedish National Audit Office	Philippe Jolly, Team Lead, Innovation Strategist, Technology Innovation and Data (TIDA)
Sweden	Swedish National Audit Office	Mattias Ahrens, Innovation Strategist, Technology Innovation and Data (TIDA)
Sweden	Swedish National Audit Office	Anders Tormond
United States	Massachusetts Office of the State Auditor	Thomas Meier, Chief Information Officer
United States	Office of the New York State Comptroller	Tina Kim, Deputy Comptroller Tina Kim for State Government Accountability
United States	Office of the New York State Comptroller	Stephen C Lynch, Assistant Comptroller
United States	Office of the New York State Comptroller	Andrea Inman, Audit Director
United States	Office of the New York State Comptroller	Mary Mueller, Press Secretary
United States	United States Government Accountability Office	Taka Ariga, Chief Data Scientist, Director, Innovation Lab
United Kingdom	University College London	Aliai Eusebi, Cybersecurity expert
United Kingdom	Opsmorth	Giuseppe Maio, Senior Data Scientist

APPENDIX D: GLOSSARY

This section will outline the new technologies that are used, or have the potential to be used, to protect public funds.

Algorithms are computational processes computers are programmed to follow to accomplish a task, usually to make a decision or help human decision making. The computational process can be simple steps, or they can be derived from statistics, machine learning, or other data processing or AI techniques.[298]

Artificial Intelligence (AI), broadly defined by Stanford computer scientist John McCarthy in a much-cited 2004 guide, refers to "the science and engineering of making intelligent machines, especially intelligent computer programmes".[299] Artificial intelligence is often contrasted with human intelligence. For instance, in a 2020 European Parliament article AI is defined as "the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity".[300] However, scholars have noted that the computing power of some AI methods go far beyond human capabilities.[301] In other words, artificial intelligence does not merely match human intelligence but can exceed it. Hence, the European Commission's High-Level Expert Group on AI has offered a more specific definition of AI: "Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions."[302] Artificial intelligence contains many subfields, including machine learning, neural networks, deep learning, and natural language processing (all defined below).

Blockchains are distributed ledgers used to track assets and transmit data safely and transparently. The technology is primarily used to record financial transactions but can also be used to track any other assets, both tangible assets such as cash, property, or land, or intangible assets such as patents, copyright, branding, or intellectual property. Each transaction is recorded once, as it happens, in a 'block'. That block can record various types of information, for instance, who is sending money, how much they are sending, to whom, and under what condition. As an asset moves from place to another, or as it is sold from one person to another, new blocks are created to record the exact time and sequence of transactions. Each block is connected to the block before it, and the block after it, forming an irreversible chain, or a ledger of transactions that cannot be altered. [303]

Chatbots, or virtual assistants are computer programmes that use natural language processing to understand user questions and automate responses. They can respond to questions through text or audio input, in browser windows, social media applications like WhatsApp or Facebook Messenger, or in workplace applications like Slack. The latest generation of chatbots, sometimes referred to as 'intelligent virtual assistants' or 'virtual agents' (e.g. watsonx Assistant) use large language models (LLMs) and can even automate tasks, for instance, preventing fraud by asking customers whether they just made a purchase for a specific amount.[304]

---

[298] Lum, K., & Chowdhury, R. (2021, February 26). What is an "algorithm"? It depends whom you ask. MIT Technology Review.
[299] McCarthy, J. (2007). What is Artificial Intelligence?
[300] European Parliament. (2020, September 4). What is artificial intelligence and how is it used? European Parliament News.
[301] McCarthy, J. (2007). What is Artificial Intelligence?
[302] European Commission. (2022, June 7). High-level expert group on artificial intelligence. European Commission.
[303] IBM. (n.d.). What is Blockchain Technology? Ibm.com.
[304] Interacly AI. (2023, July 28). LLMs and Chatbots: A Match Made in Tech Heaven. Interacly AI.

Data mining is the process of searching large datasets for patterns, trends, and other pieces of valuable information. There are two main techniques to mine data; one aims to describe the data; the other aims to analyse it. Descriptive techniques are often used in combination with data visualisation tools to represent the data in the form of charts, diagrams, or pictures. Analytical techniques are often used in combination with machine learning algorithms for instance to organise the data and to find patterns or relationships.[305]

Deep learning is a subset of machine learning (see below) that uses neural networks (see below) to model and solve complex tasks. Deep learning models that can generate high-quality content such as text, images, software codes, molecules etc. based on the data they were trained on are also known as generative AI.

Large language models (LLMs), also known as foundation models, are large deep learning neural networks that can perform a variety of tasks, including natural language processing tasks, such as translating text from one language to another, or answering questions. LLMs are a form of generative AI, taking input (text prompts, audio, or images) and generating output. They are based on complex artificial neural networks including generative adversarial networks (GANs) and transformers. LLMs are often trained on vast amounts of text data. They recognise patterns and relationships in the training data and use that knowledge to predict the next word in a string of words based on the previous word and its context. Then, they use probability distribution techniques to select the word that has the highest probability of coming next. For instance, a model might learn, based on its training data, that the likeliest next word in the string 'The capital of Belgium' is 'is', and the likeliest word after that is 'Brussels').[306] Examples of AI chatbots or search engines that use large language models are OpenAI's GPT, Google's Bard, or Microsoft's Bing AI.[307]

Machine learning (ML, also referred to as 'predictive analytics', or 'predictive modelling') is a sub-field (and a key technology) of artificial intelligence. It was first defined by computer scientist Arthur Samuel in 1959 as 'a computer's ability to learn without being explicitly programmed.'[308] Whilst the number of machine learning applications has skyrocketed since then, the broad understanding of the term remains the same: Machine learning is the science of developing algorithms (or step-by-step instructions) that receive data, analyse it, and make predictions based on it. Four broad types of machine learning are supervised, unsupervised, semi-supervised and reinforcement learning.[309]

Natural Language Processing (NLP) is a branch of AI that teaches computers to process language, 'understand', and generate human language. NLP uses different statistical, machine learning, and deep learning models. It can be divided into Natural Language Understanding (NLU), with the aim of understanding the intended meaning of text and Natural Language Generation (NLG), with the aim of creating new text. Statistical NLP models extract, classify, and label elements of text or voice data and then determine the likelihood that each element has a certain meaning. NLP is the driving force behind applications such as information retrieval, scanning large volumes of data to find the documents that are most relevant to a query, search engines like google, sentiment analysis, used to analyse emotions, for instance, in social media channels, spam detection in e-mail programmes, autocomplete functions,

305 IBM. (2024). What is Data Mining? Ibm.com.
306 AWS. (2024). What are Foundation Models? - Foundation Models in Generative AI Explained - AWS. aws.amazon.com.
307 Liu, Y., Han, T., Ma, S., Zhang, J., Yang, Y., Tian, J., He, H., Li, A., He, M., Liu, Z., Wu, Z., Zhao, L., Zhu, D., Li, X., Qiang, N., Shen, D., Liu, T., & Ge, B. (2023). Summary of ChatGPT-Related research and perspective towards the future of large language models. Meta-Radiology, 1(2), 100017.
308 Wakefield, K. (2024). A guide to the types of machine learning algorithms. SAS UK.
309 IBM Data and AI Team. (2023, July 6). AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference? https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/

hate speech filters on social media, chatbots used in customer services, machine translation like DeepL or google translate, virtual agents such as Apple's Siri and Amazon's Alexa.[310]

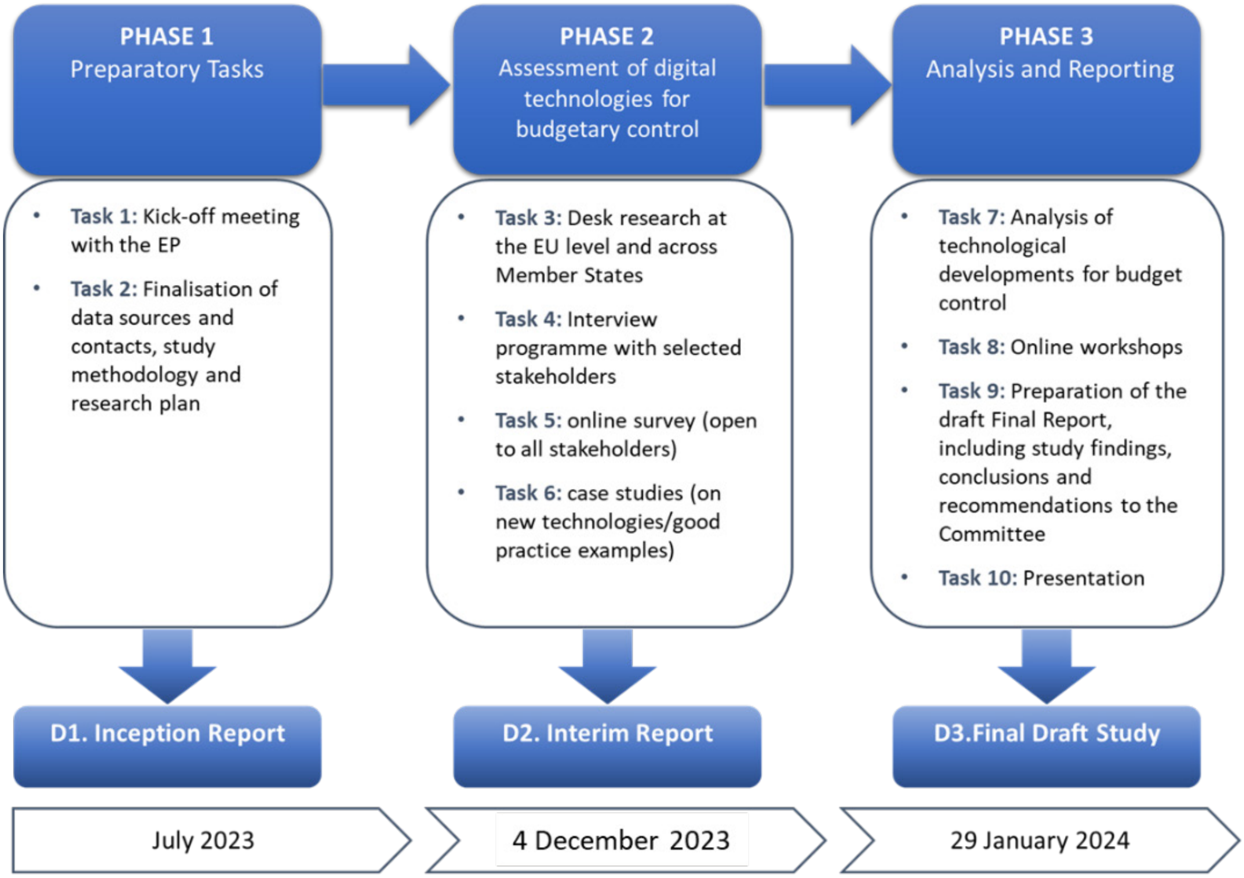
Robotic Process Automation (RPA) or software robotics automates repetitive time-consuming office tasks such as extracting data, filling in forms, moving files etc.[311]

[310] IBM. (2024). What is Natural Language Processing? Ibm.com.
[311] IBM, "What Is Generative AI?"

APPENDIX E: METHODOLOGY

The following chart outlines the research plan for the study, the main milestones and deadlines.

Figure 6.1: Research Plan



Source: Elaborated by the study team

The list of key questions that are being investigated was set out in the technical offer for this study and is reproduced below.

Key Research Questions – The future of digitalisation in budgetary control

Part A: Status quo and scale of the problem

1. What are the IT tools available at the EU level to combat fraud and corruption and recent technological developments in the management and control of EU funds?
2. To what extent are these IT tools used by the Member States? What factors might help explain the differences in the uptake of these tools and what are the main concerns (including in relation to data privacy, collection, accessibility and compliance)?
3. How serious is the problem of a limited digitalisation of budgetary control practices for the EU?

Part B: New technological developments for budgetary control, potential benefits and challenges

4. What are the new technological developments currently available in the field of budgetary control?
5. What are the advantages and potential limitations in the implementation of the identified technologies for budgetary control? Would any combination of these technologies be desirable?
6. Is it possible to identify good practices and lessons learnt in the use of such technologies across the EU and/or from international comparators?
7. Are there any new or upcoming technologies that could be used in the field of budgetary control?

Part C: Potential applications of technologies to protect the Union's budget

8. What are the possible benefits (e.g. prevent and tackle of fraud and corruption, the sound financial management of EU funds, protection of the Union financial interest) and costs (e.g. the costs of digital infrastructure, training, new equipment, timetable of implementation and other) associated with the deployment and implementation of these technologies on the EU budget?
9. To what extent would these technologies (or a combination of these) be achievable across the EU? How effective would these technologies be for the control of expenditure under different funds, and to protect the Union's budget as a whole?

Phase 1 included scoping research and interviews and the finalisation of the research plan and the research tools. The results were presented in an Inception Report that was submitted on 28 July 2023. Phase 2 tasks included: the desk research (Task 3), the interview programme with selected stakeholders (Task 4) and the online survey (Task 5) and case study research (Task 6). Below, we provide a summary of the activities performed in each task. The preliminary results of Phase 2 research were provided in an Interim Report which was submitted on 4 December 2023.

Task 3 – Desk Research

The first step involved a review of important reports and documents published by the European Parliament, the Commission, the European Court of Auditors (ECA), the European Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO) and other publicly accessible documents.

This part of the research aimed at gathering insights on current IT tools and systems introduced by the European Commission to track the use of EU funds and address fraud and corruption (such as Arachne, EDES and the IMS), as well as more recent developments at the EU level. The list of documents we reviewed included past studies carried out by CSES for the European Parliament on the patterns of fraud in shared management funds,[312]and on the impact of organised crime on EU finances[313], recent publications from the European Commission and Parliament and other sources available by the EU bodies.

[312] European Parliament (2022), Identifying Patterns of Fraud with EU Funds under Shared Management - Similarities and Differences between Member States. Study for the European Parliament's Committee on Budgetary Control.

[313] European Parliament (2021), The Impact of Organised Crime on the EU's Financial Interests. Study for the European Parliament's Committee on Budgetary Control.

The research team also conducted in-depth desk research in a sample of countries. The aim was to identify emerging IT technologies, systems and tools used or currently being piloted for the management, control and audit of public expenditure and assess their potential implications for the EU budget. The sample indicated in the Inception Report was adjusted after further research to include countries of particular interest given recent experiences in budgetary control. The final sample was: Czechia, Germany, Hungary, Italy, Poland, Portugal, Romania, Sweden. We also considered two international comparators (the UK and the US). We undertook desk research undertaken to compile 'country factsheets' for each country and used those as a basis to draft 'technology-focused case studies' (Task 6). The desk research was supported by our interview programme (Task 4) and survey (Task 5).

Task 4 – Interview Programme

Task 4 consisted of an interview programme with selected stakeholders at the EU level and in the sample of selected countries. In total, we interviewed 18 stakeholders at the EU level and 39 stakeholders at the national level. At the EU level, we spoke with stakeholders in the Commission (AGRI, BUDG, DIGIT, ECFIN, EMPL, REGIO.DAC), at OLAF, and at EPPO. At the national level, we conducted interviews with stakeholders in Belgium, Czechia, Germany, Italy, the Netherlands, Poland, Portugal, Slovakia, Sweden, the US, and the UK. This included bodies competent for the management, control and audit of funds, as well as Supreme Audit Institutions (SAI), anti-fraud coordination services (AFCOS) and representatives from academia, the private sector, and NGOs concerned with these functions.

Task 5 – Online Survey

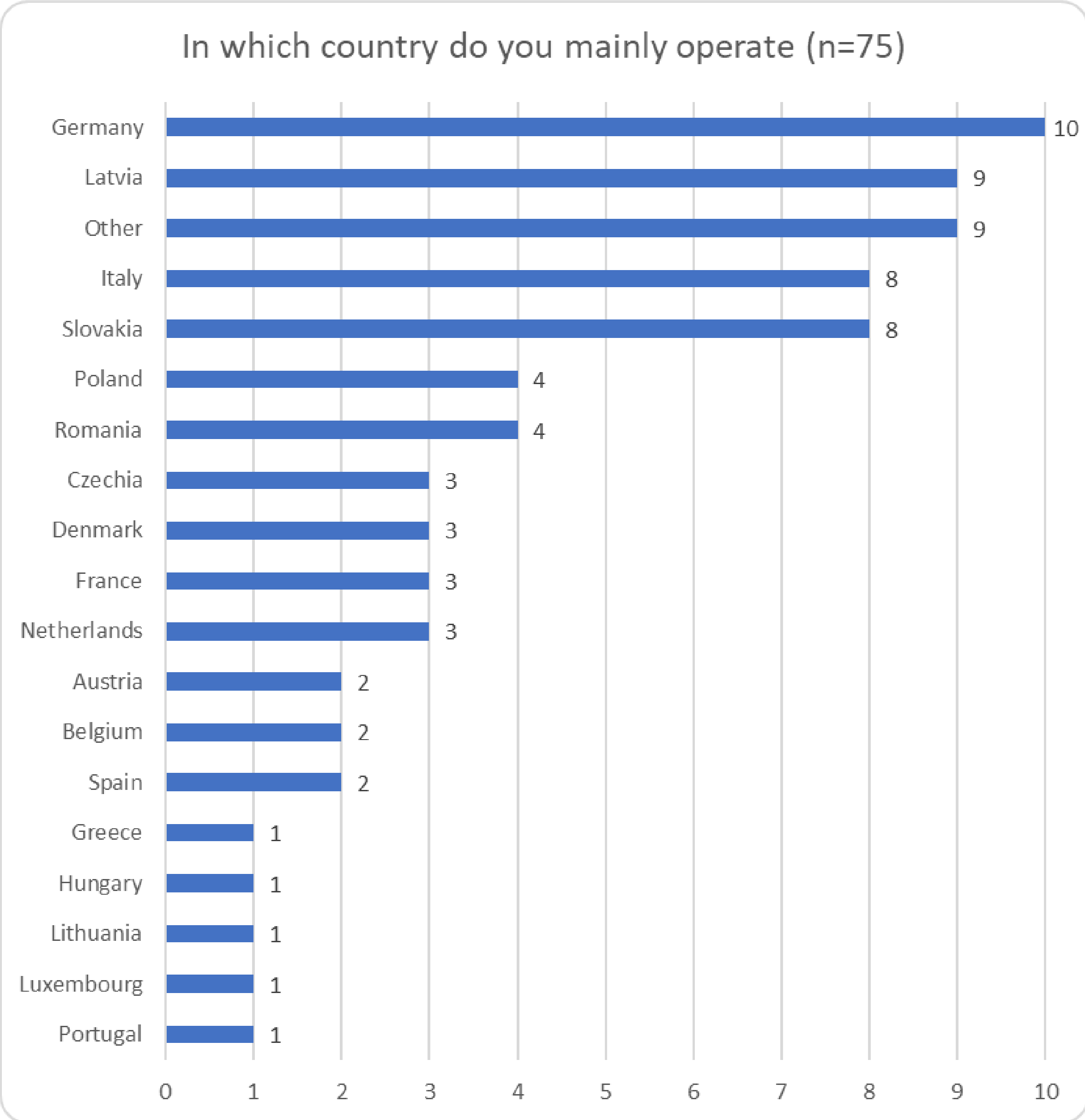
An online survey of public bodies concerning the current and potential future use of new digital technologies in budgetary control, ran between 28 November 2023 and 2 February 2024. The objective was to obtain exploring how public bodies use:

- Existing tools and systems to manage and control EU funds and fight fraud, irregularities and corruption (e.g. Arachne, Early Detection and Exclusion System (EDES), Irregularity Management System (IMS) and others), how well they work, and how they may be improved.
- Other digital tools and systems used to manage and control public funds and fight fraud, irregularities, corruption and misuse of funds in countries. This includes tools that automate repetitive and time-consuming tasks, which use machine-learning algorithms or other types of artificial intelligence (AI).

The survey questionnaire was based on the list of key research issues set out in Box 1-1 above. It was tested with a small number of contacts in order to assess the relevance of the questions and overall survey experience. The survey was implemented via an online system (checkmarket.com).

The survey received 75 full responses (or 110 total responses). The majority of responses came from national public bodies at (46 out of 75 responses), followed by regional public bodies (16). Other respondents included EU institutions, agencies or bodies at (6), local public bodies (5), NGOs, CSOs or academia (1), and others (1). Out of the 75 respondents from national public bodies, 57 indicated that they were responsible for managing/controlling EU funds, 34 national funds, and 14 regional/local public funds. The remainder of responses were from respondents who answered don't know/not applicable (2) or other (2). Most responses came from EU Member States, notably Germany (10), Latvia (9), Italy (8) and Slovakia (8) or from other countries (9).

Figure 6.2: Survey questions: In which country do you mainly operate in? (N=75)



Source: CSES online survey

Task 6 – Case Studies

The research team also produced a series of case studies focused on key IT technologies for budgetary control. The purpose of the case studies was to explore specific technological developments in countries. The case studies present good practices examples, lessons learnt from recent experiences and assess the potential for transferability and replicability of these technologies at the EU level. The case studies draw insights from the interviews, survey and desk research (and country factsheets).

This study, commissioned by the European Parliament's Committee on Budgetary Control, explores new technological developments that are being or could be applied in the field of budgetary control and how these could be used to enhance the prevention of fraud and corruption and ensure sound financial management of EU funds. New technological developments covered by the study include big data analytics, artificial intelligence, digital platforms, robotic process automation, distributed ledger technologies (blockchain) and satellite imagery.

PE 759.623
Print ISBN 978-92-848-1628-6 | doi:10.2861/41262 | QA-02-24-231-EN-C
PDF ISBN 978-92-848-1629-3 | doi:10.2861/521425 | QA-02-24-231-EN-N