**УДК 334.025**
**JEL H110, H190**
**ORCID ID 0000-0002-2495-7670**
**DOI https://doi.org/10.17721/tppe.2021.43.20**

**Diakiv A.,** economist
Taras Shevchenko National University of Kyiv

# BLOCKCHAIN IN PUBLIC SECTOR

*The Internet has radically transformed access to and exchange of information, and it plays a fundamental role in today's society and economy. Yet it was difficult to imagine all the services offered today when the first tools necessary for its democratization were introduced thirty years ago. The blockchain, since the publication of the white paper of bitcoin as the first digital asset, has considerably broadened the range of its fields of application and its potential use cases in ten years; it could play, in different forms, a role comparable to that of the Internet in an area that the latter does not cover: trusted IT and legal transactions. Indeed, while the Internet is the privileged vehicle for the exchange of all digitized forms of information, it is not the guarantor, as a network infrastructure, of its uniqueness or its functioning. Blockchain technology has evolved from a niche subject to the hottest tech disruption buzzword, but there is still a lot of confusion about the subject. Without a clear understanding about what Blockchains are, their potential public sector potential impact is sometimes misunderstood or, more often, ignored. Questions related to their technical complexity, risk, security, and appropriateness often serve as obstacles to government officials' ability to truly engage with this emerging technology. In this article, we consider the key features and types of blockchain technology and describe the potential use of blockchain technology in the public sector. In general, the blockchain can be used in the public sector to address the following tasks: authentication, traceability and uniqueness. We have identified ten potential directions of using blockchain technologies in public sector: self-sovereign identity, contract and vendor management, notarization, aid management, secure data sharing, financial services and banking, voting, verifiable diplomas and certificates, energy utilities, copyrights.*
***Keywords:*** *blockchain, public sector, distributed ledger technology.*

**Problem statement.** Blockchain technologies combine innovations with existing IT solutions on distributed IT systems. They are decisively changing the way organizations, even competitors, confidently issue and transfer data or digital assets, without going through a central control structure.

It may seem paradoxical to reflect on the applications of blockchain in the public sector, when its origin, through the appearance of bitcoin, had a specific objective: to disintermediate state institutions and trusted third parties in the sovereign functions of the government.

If this antinomy is historically legitimate, the objectives of this document are to explain why it is necessary to distinguish the original philosophy of the blockchain from its functional capacity, to show how for several years it has strongly evolved and has been able to demonstrate its compatibility with a regulated environment and its technological maturity.

Moreover, today, wanting to talk about blockchain is a futile exercise. It now comes in different forms with common characteristics (distribution, registry, transparency, traceability, immutability, security) but also significant differences in governance methods, actor authentication, and transaction confidentiality.

**Analysis of publications.** Although the technology is amassing a body of literature, few sources make sense of the technology in accessible ways, and fewer yet focus on its applicability to the public sector, such as ways it can enable collaboration within and across governments and help reduce fraud, errors, and the cost of paper-intensive processes. Problems related to the usage of blockchain in the public sector have been studied in the works of some foreign scientists such as Janssen, Weerakkody, Ismagilova, Sivarajah, & Irani, Ølnes, Ubacht, Zachariadis, Hileman, Scott, Atzori, Meijer, Beck, Müller-Bloch, King, de Filippi, Mannan, Reijers, Werbach, Zachariadis. Also, these problems were reviewed in analytical documents of different international organizations such as OECD, Deloitte, BDO, etc.

**Unresolved parts of the problem.** Further research should give the answers to several fundamental questions:

- How can they contribute to the establishment of an interoperable and common infrastructure, while maintaining the architectures and applications existing in each administration or company involved?
- Are there any particularly interesting perspectives in the face of complex ecosystems where various stakeholders must collaborate around business procedures and logic?
- How to ensure that this collaboration takes place while guaranteeing the quality, source, confidentiality, and transparency of the data exchanged, which has become the only guarantee of trust for the end-user?

**The purpose of the article** is to show that the public sector can benefit from the unique characteristics offered by blockchain technologies, while respecting its values and offering a better experience and enhanced confidence to the user in Ukraine.

**Research methodology.** The information provided in the articles is the result of a comprehensive review of the literature on the blockchain field and of the documentation available. The following methods were used in the research process: comparative analysis (identified features of different types of usage of blockchain technology in public sector) and abstract-logical (generalization and formulation of main conclusions and proposals based on the results of the study).

**Results and discussion.** Blockchain technology, for many, is considered to be as revolutionary as the rise of the Internet, and has been referred to as a new “trust machine” because of its ability to allow people to interact and conduct transactions even though they may not know each other or have a pre-existing trust-based relationship [3].

In order to evaluate the impacts of blockchain technology on the public sector, and anticipate future usage of Blockchains, we need to answer the question what is Blockchain technology?

Blockchain is the most well-known and used distributed ledger technology. A distributed ledger technology (DLT) is a technology that facilitates an expanding, chronologically

ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. Any participant with the right access rights can trace back a transactional event, at any point in its history, belonging to any actor in the network. The technology stores transactions in a decentralized way. Value-exchange transactions are executed directly between connected peers and verified consensually using algorithms over the network [1].

The main difference between blockchain and DLT is that the latter is a technology for the management of a distributed database, whereas the former is a confidence-building technology through the means of consensus mechanisms and sequential registry of information in a chain-type formation [6].

The main benefit of blockchain is reducing middlemen in process of transferring different digital assets. As described by the World Economic Forum, “currently, most people use a trusted such as a bank to make a transaction. But Blockchain networks allow consumers and suppliers to connect directly, removing the need for a third party” [3]. The importance of middlemen exists due to the necessity of reducing digital fraud. For example, somebody would send a digital asset like a digital paper of ownership of a car to someone else, then there is a risk that the sender sends a copy over the internet and still keeps the original paper of ownership. Traditionally, this risk has been mitigated by having trusted third parties or administrators, like banks, to act as a centralized authority keeping track of all transactions. DLT’s shift this responsibility of validating the actual transfer of the asset to the whole network using carefully designed algorithms. This eliminates the need for a centralised database. Every actor in the network has a copy of the record of transactions, and any change of ownership of the digital assets in the system requires validation from its users [1].

Instead of a central authority maintaining a database, in blockchain all nodes have a copy of the ledger and updates to a Blockchain ledger are propagated throughout the network in minutes or seconds. In these networks, a majority of nodes must review and validate a transaction before it can be verified and recorded. This way, nobody can tamper with the ledger, everyone can inspect it, and it can be trusted [3].

Thus, blockchain is the type of a ledger in which value-exchange transactions (in the form of cryptocurrencies, tokens or information) are sequentially grouped into blocks. Each block contains a signature that is based on the exact content (string of data) of that block. The next block contains this signature as well, linking all previous blocks to each other up until the first block. Blocks are immutably recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms [1].

The key characteristic of blockchain is its distributed and shared nature. Distributed: All copies of one document are constantly and automatically synchronised hence identical at all times. Furthermore, “there is no canonical copy; all copies are created equal”. Shared: There is perfect information across all actors in the system. All platform members have access to all members’ information [10].

In addition to the above, all blockchains will have the following characteristics:

1) consensus: on methods and, therefore, registry registrations: an appropriate algorithm ensures that protocol rules are followed and that all transactions take place reliably, which means that all entities have a common real-time and transparent vision.

2) invariance: A transaction or event recorded in a blockchain has a date, historical history, and can no longer be changed or deleted.

3) irrevocability: A transaction that follows business rules and is confirmed according to consensus rules cannot be canceled.

4) origin: Any blockchain-managed asset is tracked transparently and its history is available to eligible entities.

Two main types of blockchain exist. For a participant, they will be differentiated by the access authorization (totally free or administered) and the type of action (writing and / or simple reading) that he can perform.

Blockchains without permission known as «public». They were born with bitcoin. Their development is open source, and all their content (information and transactions) is public. They are accessible to everyone, do not require any access authorization and anyone can carry out transactions. Participants are therefore not identified and use pseudonyms. These networks remunerate the participation of entities responsible for validating network transactions using a token system.

It should be emphasized here that the qualifier of «public» has no connection with the notion of public sector, since on the contrary the very essence of this type of blockchain is based on total decentralization and the absence of any regulatory body. control.

On so-called public networks, the parties do not need to know each other to carry out transactions. Consensus algorithms are the guarantors of trust and the smooth running of transactions. These infrastructures and networks are particularly resilient given their decentralization to thousands of interconnected nodes that register and update the registry.

Permissioned blockchains. These networks emerged in 2016, on the strength of the observation that certain ecosystems made up of regulated and identified players could benefit from dedicated network infrastructures allowing better management of data flows and their sharing. Unlike permissionless blockchains which offer a turnkey network infrastructure, permissioned blockchain technologies appear in the form of open source technological bricks (framework), deployable on demand and whose architecture will depend on the ecosystem and of the underlying issue.

They will be used in cases of use where the anonymity or, more precisely, the pseudonymity of the speakers is not possible or desired. Likewise, they are required in contexts where complete decentralization of governance or the use of a cryptocurrency or token is not required. The participants are perfectly identified. Access and write actions will be subject to authorization, only reading remaining potentially free. The data source is authenticated. They also make it possible to manage at an extremely fine level of granularity, the nature of the data (public, shared or private), to encrypt them and therefore to ensure less transfer of personal data and greater confidentiality of exchanges between stakeholders network.

This type of blockchain most often exists in a regulated or regulated framework, or for a consortium of B2B (business to business) companies. Participants will be able to play different roles depending on the governance adopted and the concept of trust appears.

Unlike a blockchain without (public) permission, the stakeholders are known. Their quality will play a role in the validation of a transaction: this is the fundamental distinction in this typology.

In line with the objective of transparency, all blockchain technologies are by philosophy open source; which brings most of their promoters closer to openness movements such as open government, open data, open science, open education.

In general, the blockchain contributes, without the need for a trusted third party, in simultaneously raising three uncertainties or recurring difficulties in the public sector:

1) authentication: knowing who you are dealing with, that is, with confidence in the legitimacy of the stakeholder, which includes skills or certifications in the case of a service provider in the broad sense. Reputation for a third party becomes a key element which naturally benefits over time from the «network» effect.

2) traceability: have certified knowledge of the evolution of an asset over time via auditability, traceability and certification of the data that represents it in the digital world. This makes it possible to have a reliable and permanent correspondence between a physical asset (a vehicle, a property, etc.) and its digital twin.

3) uniqueness: eliminate the friction between the different stakeholders that currently causes multiple exchanges of emails, files of different formats, discontinuities in the processing of information or even disputes. The digitization of workflows between actors, the reliability of transactions or exchanges carried out and the transparency of the register will drastically reduce the number of these discrepancies and will guarantee, without the need for an external trusted third party, the completeness and quality of the trades.

From the point of view of «business» processes, blockchain represents de facto the beginnings of a profound change in the way organizations in the broad sense, including the public sector, operate in a network, whether among themselves or with external actors.

Other technologies already allow the secure exchange of information, but they rely on processes internal to each organization. The blockchain offers a new possibility: an entity has the capacity to share a sub-part of a process transparently and securely with other stakeholders in its ecosystem while maintaining full control over its own data.

Blockchain technologies should therefore not be considered as a new medium for sending and receiving data, but rather as a register shared by several entities. The information blocks that make up this register contain permanent records which depend on the application domain.

As illustrations in the public sector, a blockchain has the ability to create an immutable and decentralized record:

1) changes of state during the life cycle of a document (visualization by the official of the evolution of the document);

2) the stages that products go through along a supply chain (traceability of customs movements, etc.);

3) financial transactions (monitoring of subsidies, financial flows, etc.).

And since this ledger is duplicated and distributed in real (or near real) time to all of its participants, the blockchain will allow and facilitate the transition from a completely «private» perspective of processes to greater sharing of business data.

In public sector blockchain can be used in three different models:

1) G2G – Government to Government (eg between different national and transnational administrations or public agencies);

2) G2C – Government to Citizen (between an administration and a citizen);

3) C2C – Citizen to Citizen (between citizens including an element relating to the public service).

Government agencies are the essential intermediaries in these transactions and the guarantors of their proper functioning. The documents they issue or certify are the standard means of being able to verify information about people (identity cards, work permits, driving licenses, etc.) and goods (origin of containers, product safety, etc.).

Compared to traditional centralized databases, blockchain guarantees two specificities:

1) by construction, the integrity and real-time traceability of data, for efficient and transparent collaboration between users, without the use of an external trusted third party;

2) the self-execution of smart contracts to automate and secure processes, resulting in efficiency and quality gains.

In the case of public services, this means, for example, that the blockchain can facilitate checks on the integrity and origin of official documents without the need to contact their issuing entity each time. In this case, the sharing of data can be done in a completely secure way between digital wallets.

Since blockchains represent distributed systems with high automation potential, they can be used to efficiently design low-cost platforms, leading to significant savings in data processing, while increasing system robustness.

The solutions implemented in distributed applications (dApp) must be designed like all applications in an ergonomic way.

Based on the analysis of the processed sources, we have identified ten potential directions of using blockchain technologies in public sector:

1) self-sovereign identity. This use case is particularly transverse to all other use cases. It is all the more strategic for States since it is a question of preserving the sovereignty of individuals through their identities and therefore accessibility to secure and quality identity. Self-sovereign identity is a new approach to storing, managing, controlling and sharing data related to individuals, organizations, or objects. There are many possibilities for use in the public sector such a facilitating access to e-government services, the asylum application, the digitization of diplomas, the digitization of identity papers (passport, identity card), drug prescriptions linked to existing social security systems, public licenses and other public documents (driver's license, vehicle registration document), public transport and social transfers (retirement, invalidity, maternity).

2) contract and vendor management. Things such as tracking and paying vendors, managing purchase commitments and transactions, and monitoring schedule performance could all be done in a way the is accessible to all relevant players, as well as the public, as appropriate. In addition to the transparency and accountability angle, Blockchains can

make government contracting more efficient by eliminating a significant amount of overhead and automating processes that lend themselves to the logical “if/then” workflows of smart contracts [3].

3) notarization. This use case actually describes one of the core technologies used within a blockchain solution. This technology which does not date from the blockchain, lies in the use of «hash functions» in cryptography. A computer «hash» allows you to generate a cryptographic fingerprint unique to digital data. This computerized method is more commonly called, notarization. In this sense, the «Notarization» use case aims to demonstrate that in many cases, this single functionality, natively included in the design of a distributed registry infrastructure, would make it possible to solve many problems related to errors relating to the state and probative veracity of a multi-party procedure. A blockchain infrastructure would therefore allow, via this method of notarization, the recording of the digital identity of documents or of the state of the procedure at time T within the distributed register, mechanically creating a link between the data and a historization of it. It would therefore make it possible to reconcile entire procedures on the same infrastructure allowing the following actions: save digital documents, check their authenticity, create a secure and time-stamped history of data, link the digital fingerprints of files and their metadata, exchange digital fingerprints from data with third parties in accordance with the GDPR. This blockchain functionality is used here to create reliable and convincing digital audit trails, allowing the automation of compliance checks and proof of data integrity.

4) benefits, entitlements, and aid. The benefits, entitlements, aid processes of today often involve a significant amount of overhead and checks for compliance. Government programs such as social security and pension payments, medical care benefits, and domestic and international aid could benefit tremendously from Blockchains. For example, smart contracts could be used to automate processes for eligibility verification and disbursement of funds, such as distribution of funds for those affected by a major natural disaster. In addition, Blockchains could help to ensure that benefits reach their intended beneficiaries and are not diverted [3].

5) secure data sharing. In order to provide easy access to information from public/private institutions, can be created a platform that offers the possibility of accessing a single view of current information. This information is accessible by authorization based on the concept of «need to know». This avoids exchanging that data and provides both full traceability and ownership management throughout the data lifecycle.

6) financial services and banking. Blockchain technology can be used by governments to ease the overhead and burden associated with transferring funds among parties (e.g., facilitating inter-bank and international payments). In addition, some countries’ central banks are experimenting with their own digital currencies build upon Blockchain platforms. For example, Canada has experimented with a digital currency called CAD-COIN as a way to better understand the technology first-hand [3].

7) voting. Blockchain technologies have the potential to enable new methods of voting by transforming what often remains a paper-based process in countries, or an electronic process with limited validation and auditability capacities. This can enhance the convenience and confidence for citizens. By ensuring that individual votes are eligible and

counted correctly, use of Blockchains also has the potential to help prevent voting challenges such as ballot rigging, which still persist in many countries. These challenges, if not overcome, can result in a lack of trust in democratic processes and can enable election results that do not reflect the wishes of the public [3].

8) verifiable diplomas and certificates. The use case of digital diplomas aims to the management of «digital credentials»: certificate of successful completion of the diploma, open badges and other credentials, tamper-proof, verifiable, and searchable online. The use of distributed ledger technology and transparent rules aims to create confidence in the authenticity of diplomas (fight against fraud), but also to reduce the time and costs of verification, management, and archiving of these documents.

9) energy utilities. Public energy utilities may benefit from Blockchain technologies for managing of smart energy grids. Blockchains allow for the "recording of autonomous, machine-tomachine transactions regarding electricity use". Blockchains could also be used to managing and tracking contributions from different power plans into a smart grid to ensure each power generator is credited appropriately for their contribution [3].

10) copyrights. Governments often allow for the registration of copyrights or need to adjudicate disputes related to copyrights. As content becomes so multidisciplinary and copyright ownership becomes ambiguous, Blockchains are excellent tools to "timestamp [artists'and content producers'] work, keep a 'vigilant' eye out for anyone violating their copyright, create a permanent record of their work and issue their clients a time-stamped copyright certificate". In this sense, they also serve as proof of ownership and proof of existence [3].

Thus, exist a lot of fields for using blockchain in the public sector.

**Conclusions**. A blockchain should be considered not as a simple application but as an infrastructure aimed at solving many operational issues in an ecosystem, especially in the areas of information sharing and collaboration.

By using a coherent shared data model and a language offering the possibility of modeling automated business logic, it allows the deployment of a network integrating a multi-party workflow that validates and stores transactions in a shared way. It enables the valuation of this shared data, including data sets opened by the administration.

It brings the unique ability to eliminate differences or gaps between data structures and interpretations of these state changes. Thus, blockchain technologies make it possible to reduce or even eventually eliminate the traditional middlemen that have persisted for decades between two entities, in complete transparency and without the need for intermediation.

In a context of digital transformation still too often considered from a purely internal perspective to an organization, a blockchain offers the unique opportunity to build a homogeneous network whose goals are to allow the sharing of data and information with confidence and to offer significant improvements in terms of operational excellence for all stakeholders serving the public service user.

Like any implementation or introduction of new technology, setting up a blockchain is a delicate exercise that requires meeting different imperatives. A comprehensive analysis of

all features of technology and all existing regulatory frameworks is needed for a successful implementation.

**References.**


1. ALLESSIE D, SOBOLEWSKI M, VACCARI L, PIGNATELLI F (2019), Blockchain for digital government, Publications Office of the European Union, Luxembourg. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC115049
2. Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1020–1034.
3. 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.
4. Delloite (2016) Blockchain application in the public sector. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf.
5. BDO (2020) BLOCKCHAIN IN THE PUBLIC SECTOR. Available at: https://www.bdo.sr/getattachment/Insights/BDO-Global-Survey-Blockchain-in-the-public-sector/BDO_Global-survey_Blockchain-in-the-Public-sector_SVK-004-_34595.pdf.aspx?lang=en-GB.
6. Evrim Tan, Stanislav Mahula, Joep Crompvoets (2021) Blockchain governance in the public sector: A conceptual framework for public management. Available at: https://www.sciencedirect.com/science/article/pii/S0740624X21000617
7. K. Werbach (2018) The blockchain and the new architecture of trust The MIT Press, Cambridge, Massachusetts. Canbridge: The MIT Press.
8. M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, Z. Irani (2020) A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors International Journal of Information Management, 50, pp. 302-309. Available at: https://bradscholars.brad.ac.uk/handle/10454/17358
9. Nakamoto, Satoshi, (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, available at: https://bitcoin.org/bitcoin.pdf
10. Rinearson, Tess (2017) Making Money: Bitcoin Explained (with Emoji), Part 1. Available at: https://medium.com/@tessr/makingmoney-530d2bb2b8f7



**Дяків А.О**, економіст
КНУ імені Тараса Шевченка


## БЛОКЧЕЙН В ПУБЛІЧНОМУ СЕКТОРІ

Інтернет радикально змінив доступ до інформації та обмін інформацією, і він відіграє фундаментальну роль у сучасному суспільстві та економіці. З моменту публікації Білої книги біткойна як першого цифрового активу, блокчейн значно розширив діапазон сфер його застосування та потенційних варіантів використання за десять років. Він може в різних формах відігравати різну роль, порівнянну з Інтернетом у сфері, яку останній не охоплює: довірені ІТ та юридичні операції. Хоча Інтернет є засобом для обміну всіма оцифрованими формами інформації, він, як мережева інфраструктура не є гарантом унікальності інформації та її функціональності. Технологія блокчейн перетворилася з нішової на одну із найпопулярніших технологій, що спричиняє технічні розриви, але все ще існує багато не вирішених питань. Без чіткого розуміння того, що таке блокчейн, його потенційний вплив на державний сектор іноді неправильно розуміють або, що частіше, ігнорують. Питання, пов'язані з його технічною складністю, ризиком, безпекою та доцільністю, часто заважають державним службовцям по-справжньому працювати з цією новою технологією. У цій статті ми розглянемо ключові особливості технології блокчейн та опишемо

потенційне використання технології блокчейн у державному секторі. Загалом, блокчейн можна використовувати в державному секторі для вирішення таких завдань: аутентифікація, відстеження та перевірка унікальності. Ми визначили десять потенційних напрямків використання блокчейн-технологій у державному секторі: самостійна ідентифікація, управління контрактами та постачальниками, нотаріальне засвідчення, управління державною допомогою, безпечний обмін даними, фінансові послуги та банківська справа, голосування, підтвердження дипломів та сертифікатів, комунальні послуги, авторські права.

**Ключові слова:** блокчейн, державний сектор, технологія розподіленого журналу.