Blockchain for enhancing transparency and trust in government registries

Valeriia Balatska[1,†], Ivan Opirskyy[1,*,†] and Nataliia Slobodian[2,†]

[1] Lviv Polytechnic National University, 12 Stepan Bandera str., 79013 Lviv, Ukraine
[2] Vinnytsia National Technical University, 95 Khmelnytska rd., 21021 Vinnytsia, Ukraine

Abstract

In contemporary society, the efficiency and transparency of government registries play a crucial role in ensuring public trust in the government. Using blockchain technology to enhance data protection and transparency offers new opportunities to reduce corruption, protect personal data, and improve the quality of public services. This paper examines blockchain as a tool for creating more reliable and secure government registries. The paper proposes a concept for using blockchain technology to ensure the immutability of records in government registries, transparency of transactions, and enhanced protection of personal data. Key elements of blockchain implementation are discussed, such as ensuring confidentiality, managing data access through smart contracts, and enabling automatic auditing of user actions. Blockchain technology allows for data storage in a distributed system, which prevents unauthorized changes or deletions of information and provides traceability. Smart contracts automate access management processes, allowing for the establishment of clear rules for data interaction in the registry. Additionally, blockchain ensures data integrity through cryptographic mechanisms and audits, increasing trust in government structures. The paper also presents a mathematical model for quantitatively assessing the level of trust and transparency achieved through blockchain technology. Indicators of confidentiality, data reliability, and transparency are defined to evaluate the effectiveness of implementing this technology. The goal of this work is to explore the potential of blockchain technology for enhancing transparency, security, and trust in government registries. The main tasks include analyzing the advantages and disadvantages of blockchain in the context of public administration and developing a mathematical model that quantitatively assesses the effectiveness of this approach in terms of ensuring confidentiality, reliability, and data auditability. The paper also aims to determine the prospects of implementing this technology in government systems and assess its compliance with current personal data protection requirements.

Keywords

data protection, blockchain, government registries, transparency, data security, confidentiality, smart contracts, audit, personal data, mathematical model, trust

1. Introduction

In the contemporary information society, the state plays a central role in storing and processing citizens' data, which is crucial for ensuring legal, economic, and social interactions. Government registries, which contain information about property rights, civil status records, legal entities, and individual entrepreneurs, are essential elements of e-government infrastructure. However, traditional centralized approaches to maintaining registries face numerous challenges, including data security, confidentiality, and protection against falsification. Risks of data loss, information manipulation, and corruption are persistent threats to such systems, undermining public trust in government institutions and processes [1].

Given this, there is an increasing need to develop new approaches to ensure the transparency and reliability of government registries. Innovative solutions that guarantee the immutability, reliability, and security of data are becoming especially relevant. According to modern international standards, such as the General Data Protection Regulation (GDPR), the protection of personal information has gained new importance, requiring technological solutions that ensure data confidentiality and transparent oversight.

One such innovative technology that could address these challenges is blockchain. Blockchain technology, as a form of distributed ledger, ensures data immutability and decentralization, significantly enhancing protection against unauthorized changes [2]. Blockchain operates through a distributed network of participants, where each block of information is linked to the previous one and protected by cryptographic mechanisms. Thus, the technology blocks unauthorized interference with the system and allows for the creation of immutable records that cannot be deleted or altered without the consent of network participants.

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

[*] Corresponding author.
[†] These authors contributed equally.

valeriia.s.balatska@lpnu.ua (V. Balatska);
iopirsky@gmail.com (I. Opirskyy);
nslobodian61@gmail.com (N. Slobodian)

0000-0002-6262-6792 (V. Balatska);
0000-0002-8461-8996 (I. Opirskyy);
0000-0002-2111-1434 (N. Slobodian)

The application of blockchain technology in government registries opens new horizons for increasing transparency, providing integrated control over information flows, and protecting personal data. Additionally, the technology can significantly enhance the effectiveness of anti-corruption efforts, as it provides access to registries for all interested parties without the possibility of interference in processes not aligned with network rules.

At the same time, the use of blockchain is not without challenges, particularly related to scalability, energy intensity, and the complexity of integrating it into existing government structures. It is also important to consider the need to align blockchain technologies with national and international data protection standards, such as GDPR, which sets legislative requirements for personal information protection.

The aim of this work is a comprehensive analysis of the possibilities for using blockchain technology to enhance the transparency and security of government registries, as well as the development of a mathematical model to assess the effectiveness of blockchain in ensuring confidentiality, immutability, and data auditability. The paper examines the advantages and disadvantages of blockchain solutions in the context of public administration, as well as the prospects for their implementation considering modern information security requirements.

Problem formulation. Information systems for government registries are crucial tools for storing and processing data about citizens, their rights and obligations, legal entities, property, and other important aspects of legal and economic activities [3–5]. However, traditional approaches to their organization face numerous issues that negatively impact the effectiveness and reliability of such systems. The main problems include:

- Most government registries are centralized systems, where data is stored and processed by a single entity or institution. Such centralization creates significant risks for data security, as malicious access to the central server can lead to the compromise of the entire system, data loss, or information falsification.
- Many government registries lack mechanisms that ensure sufficient transparency of operations and data management. This can facilitate abuse, corruption, and falsification, especially regarding property rights or other economic interactions. The absence of open auditing of records and changes in systems significantly reduces public trust in government institutions.
- Traditional centralized registries often face issues with ensuring data integrity. For example, due to technical malfunctions or human errors, data can be modified or deleted without proper registration of these changes. This undermines confidence in the accuracy and reliability of the information stored in the registries.
- According to GDPR requirements and other international standards, government registries must provide reliable protection of citizens' data, avoid information leaks, and prevent unauthorized access to confidential data. However, in practice, this is often a problem due to the vulnerabilities of centralized systems and limited access control capabilities.
- Centralized registry systems have inadequately developed tools for continuous monitoring of operations and changes in the registry. The inability to verify each operation and its origin complicates the detection of errors, abuses, or attacks on the system.

Given these problems, contemporary scientific thought increasingly turns to innovative technologies to enhance the efficiency and reliability of government registries. One of the most promising approaches is the implementation of blockchain technology, which, due to its properties of distributed ledger and data immutability, can address many of the aforementioned issues.

The problem is that despite the significant potential of blockchain for improving transparency, trust, and security in government registries, there are no clear methodologies and models that allow for the quantitative assessment of such implementation. There is a need for the development of mathematical models that measure the level of transparency, security, and reliability of data in registries using blockchain, and to determine the criteria for evaluating the feasibility of its implementation in public administration.

Thus, the task is to conduct a comprehensive analysis of the potential of blockchain technology to solve these problems and develop models that will assess its effectiveness in the context of government registries.

Recent research and publications analysis. In recent years, blockchain technologies have gained widespread adoption across various sectors, including financial systems, logistics, healthcare, and e-government. Given their unique ability to provide data immutability, transaction transparency, and decentralized control over information, blockchain is also being actively considered as a tool for reforming government registries. Many researchers highlight the potential of blockchain to enhance transparency in government processes, increase public trust in government institutions, and provide better protection for personal data.

Among the early research in this field are the works of Nakamoto (2008), which introduced the fundamental principles of blockchain as a distributed ledger. These studies initiated a wave of new publications exploring the potential applications of blockchain in various fields, including public administration. However, most of this research focuses on the technical aspects of the technology, while practical applications in the context of government registries are only beginning to receive detailed examination [6].

The study by Tapscott and Tapscott (2016) noted that blockchain could become a key technology for governments, particularly for ensuring transparency and combating corruption. The authors state that the decentralized nature of blockchain not only allows for recording all data operations but also makes them accessible to the public, significantly increasing trust in government processes. Other researchers, such as Atzori (2017) and

Mattila (2016), emphasize that blockchain can be used to ensure the security of government registries by creating immutable records that are accessible only under clearly defined conditions [7, 8].

Research by Crosby et al. (2016) focuses on the technical aspects of blockchain security. They examined encryption mechanisms and data protection in distributed systems and concluded that blockchain could significantly enhance the resilience of government registries against breaches and falsifications compared to traditional centralized systems. Additionally, the authors point to the possibility of creating automated audit mechanisms using smart contracts, which allows for real-time monitoring of processes in registries.

Among the works directly related to the application of blockchain in government registries is the study by Griggs (2017), which analyzes the impact of blockchain technologies on the reform of property and ownership registration systems. He highlights that the use of blockchain can significantly reduce instances of fraud and legal disputes by ensuring record immutability and providing open access to data.

The study by Hileman and Rauchs (2017) focuses on the potential of blockchain technologies to ensure compliance with international data protection standards, such as the General Data Protection Regulation (GDPR). The authors note that decentralized data storage with blockchain, combined with access management mechanisms via smart contracts, allows for maintaining high levels of privacy and personal data protection.

Regarding government initiatives, several countries have already started pilot projects implementing blockchain solutions in their registration systems. For example, Estonia has implemented the KSI Blockchain system, which ensures data security and integrity in government registries. The work by Kotliar and Priisalu (2016) describes Estonia's experience, demonstrating the significant benefits of using blockchain to reduce attacks on government registries and enhance process transparency.

However, despite numerous studies and projects related to the use of blockchain in public administration, the real effectiveness and cost of implementing such technologies remain insufficiently researched. One of the main challenges is the lack of mathematical models that allow for the quantitative assessment of the benefits and drawbacks of using blockchain technologies in the context of ensuring transparency and security in government registries [9].

Thus, the analysis of existing publications indicates significant scientific interest in using blockchain in government registries. However, there is a need for further research that covers not only technical but also methodological aspects of implementing these technologies, as well as a quantitative assessment of their effectiveness.

The purpose of the paper. The purpose of the paper is to study the possibilities of using blockchain technologies to increase the transparency, reliability, and security of state registers. The work proposes the development of a mathematical model that will allow a quantitative assessment of the effectiveness of the implementation of blockchain technologies in registration systems. The main objectives of the paper are:

- Analysis of the current state of state registers and identification of the main problems related to centralization, lack of transparency, unreliability of data, and insufficient level of protection of personal information.
- Review of scientific research and publications on the application of blockchain technologies in government systems, in particular, to ensure security, transparency, and protection of personal data.
- Analysis of the advantages and disadvantages of blockchain technologies in the context of public registries, including their impact on process transparency, reducing corruption risks and ensuring compliance with international standards such as GDPR.
- Development of a mathematical model for quantitative assessment of the effectiveness of the implementation of blockchain solutions in state registration systems, taking into account such indicators as reliability, security, transparency, and speed of data processing.
- Assessment of the prospects for the implementation of blockchain in state registers and determination of the key areas of development of this technology in the context of public administration.
- Formulation of recommendations on the application of blockchain technologies to improve the efficiency of state register management and personal data protection.

These tasks are aimed at achieving a deep understanding of the potential of blockchain technologies in reforming state registration systems, as well as at solving current problems related to ensuring transparency, reliability, and security of personal data. They include a comprehensive analysis of the existing problems of centralized registration systems, an assessment of the opportunities and challenges that arise when implementing blockchain solutions, as well as the development of a methodology for quantitatively measuring the effectiveness of such technologies. Ultimately, these tasks will contribute to the development of practical recommendations for the use of blockchain in public registries to increase the trust of citizens and ensure compliance with modern data protection requirements.

2. Assessment of the current state and challenges of state registers

2.1. Analysis of the current state of state registers

State registries play a critical role in the functioning of state institutions, ensuring the registration of property, property rights, acts of civil status, voting rights, and other important information. They are a database that ensures the provision of administrative services, legal protection of citizens, and transparency of state administration. However, modern registration systems face several challenges that can reduce their effectiveness and citizens' trust in them [10].

Most state registries operate based on centralized data storage systems, where all information is accumulated and processed in centralized repositories under the control of one or more state institutions.

This approach carries risks associated with:

- A single point of failure where centralized systems are vulnerable to infrastructure failures or cyber-attacks that can lead to the loss or corruption of large amounts of information.
- Corruption risks, in particular, centralized control over data increases opportunities for unauthorized data changes by attackers or even government officials.
- Monopolization of access to data, where limited access to centralized registers makes it difficult to verify the veracity of information by independent participants.

Many public registries do not allow citizens to freely and transparently track changes in records. This can cause distrust in the operation of such systems and increase the risks of data manipulation. The lack of open verification mechanisms also complicates the process of monitoring changes in registries, which can be used for fraud or hidden changes in registration records [11].

Given the complexity of the administration of centralized systems, errors or violations in the process of data entry and processing are possible.

This can lead to:

- Incorrect data may enter the registers due to incorrect information entry, human factors, or technical failures.
- Loss or damage of data due to malfunctions of storage systems or infrastructure.
- Uncertainties in the relevance of data, namely centralized systems can delay information updates, which affects their relevance.

Increasing attention to the issue of privacy and protection of personal data in the era of digital technologies raises concerns about the security of public registries. The main problem that centralized registries face is their vulnerability to cyber-attacks, which makes them an attractive target for hackers who can gain access to large amounts of sensitive data. This poses a serious threat to information security, as attackers can not only steal personal data but also make changes to it. In addition, users of centralized systems are deprived of the opportunity to control who and how their data is used. This situation contradicts the basic principles of the General Data Protection Regulation (GDPR) and other international standards, which provide for the right of citizens to manage their information and the transparency of its processing.

Many countries face the problem of slow introduction of innovative technologies into state structures due to regulatory barriers, bureaucratic procedures, or insufficient funding of such projects. This delays the modernization of state registers and leaves them vulnerable to the challenges of today's digital world.

Therefore, the existing problems of state registers, in particular, centralization, lack of transparency, unreliability of data, and insufficient level of protection of personal data, create the need to find new approaches to their reform. Blockchain technologies can become one of the key technologies capable of solving these challenges and increasing the efficiency of public registries.

Below is Table 1, which compares the advantages and disadvantages of blockchain technologies with traditional centralized systems for public registries:

Table 1

Comparative analysis of advantages and disadvantages of blockchain technologies and centralized systems in state registers

Criterion	Blockchain technologies	Centralized systems
Transparency of processes	High transparency through decentralized transaction recording. Each participant has access to the complete history of changes.	Limited transparency; access to data is usually controlled by a central authority.
Corruption risks	Reduced due to data immutability and decentralized control. Transactions are visible to all participants.	High risk of corruption due to centralized control and the possibility of hidden changes.
Data security	High level of security through cryptographic methods and decentralized nature. No single point of failure.	Less reliable protection, there is a single point of failure. Vulnerability to cyber attacks.
User control	Increased control with cryptography and the ability to protect access control through smart contracts.	Limited control; users cannot independently manage access to their data.
GDPR compliance	Can be adapted to GDPR through encryption and access control mechanisms, but difficult to implement the right to be forgotten.	It is easier to implement GDPR compliance, including the right to be forgotten, but data control may be limited.
Speed of transactions	Can be free through a process of confirmation and consensus.	Faster transaction processing due to centralized control.
Scalability	Limited scalability due to high network load and the need to process each transaction.	Easier to scale with a centralized architecture.
Cost of implementation	High cost due to the need for new technologies, provided and training personnel.	Lower implementation costs, but support costs can be high in the event of failures or attacks.
Legal and regulatory challenges	There may be difficulties in complying with existing legal regulations, especially in terms of data immutability.	Easier to comply with legal regulations, including GDPR, but transparency and access issues are possible.
Ensuring data integrity	High integrity due to the immutability of data blocks; any changes are recorded and available for review.	Integrity issues may occur due to human error technical failures; or lack of transparency of changes.

The analysis of the table comparing blockchain technologies and traditional centralized systems in the context of public registries shows that blockchain offers several significant advantages, such as increased transparency, reduced corruption risks, and ensuring a high level of data security. Due to the decentralized nature of blockchain technology, each transaction is recorded in an open and immutable ledger, making data more verifiable and less prone to manipulation.

However, despite these advantages, blockchain also has significant disadvantages, such as limited scalability and high implementation costs. Blockchain transaction processing speed may be slower due to complex consensus algorithms, and its scalability is limited by the large number of nodes in the network. The cost of implementing new technologies and training staff is also a significant barrier.

Traditional centralized systems, on the other hand, provide faster data processing and easier scalability, but have serious drawbacks in the form of less transparency and a higher risk of corruption. They may also have problems ensuring full control over data and compliance with international standards such as GDPR [12].

Overall, blockchain technologies have the potential to significantly improve the management of public registries, especially in terms of transparency and security. However, their implementation should take into account existing technical and financial challenges [13]. A comprehensive approach to the integration of blockchain technologies into government systems, including an assessment of all advantages and disadvantages, will help to find the optimal solution for increasing the efficiency of data management.

3. Models and prospects for the implementation of blockchain technologies in state registers

3.1. Development of a mathematical model for quantitative assessment of the effectiveness of the implementation of blockchain solutions in state registration systems

In the conditions of rapid development of digital technologies and growing requirements for data protection, state registration systems are faced with the need to improve their information processing and storage mechanisms. Traditional centralized systems, which are widely used at present, show limitations in terms of transparency, security, and efficiency [14]. The need for new solutions to increase reliability and data protection leads to the active study of blockchain technologies as a possible tool for the transformation of these systems.

Blockchain, due to its unique properties such as decentralization, immutability, and transparency, promises significant advantages in the management of public registries. However, to objectively assess the feasibility of implementing blockchain solutions, it is necessary to develop a mathematical model that would allow quantitative assessment of their effectiveness based on critical indicators. This model should take into account not only the positive aspects but also the possible shortcomings that may affect the overall efficiency of the system.

The scientific novelty of this work lies in the creation of a complex mathematical model for evaluating the effectiveness of the implementation of blockchain technologies in state registration systems. The model takes into account key indicators such as reliability, security, transparency, and speed of data processing, which allows for a comprehensive analysis of the impact of blockchain solutions on these systems.

This work proposes a new approach to the integration of blockchain technologies into state registries, which includes taking into account the specific characteristics of blockchain architecture and their impact on the main functional aspects of registration systems. The model also takes into account possible scenarios of implementation and operation of the systems, which allows to evaluate the efficiency at different stages of the life cycle of the system.

Description of model details

The mathematical model developed to evaluate the effectiveness of the implementation of blockchain solutions includes the following stages and components:

- **Reliability (R):** System reliability is observed as the probability of failure-free operation. It is calculated as the ratio of the time without failures to the system's total operating time. High reliability is blocked due to the decentralized nature of blockchain technologies, which reduces the probability of simultaneous failure of all nodes. It is calculated as follows (1):

$$R = \frac{T_{operational} - F}{T_{operational}}, \tag{1}$$

where $T_{operational}$ is the total uptime of the system and **F** is the number of failures or errors.

- **Security (S):** The security assessment is based on the analysis of vulnerabilities and the probability of their implementation. Blockchain provides a high level of security due to its cryptographic protection and distributed nature, which makes attacks on the entire network unlikely (2):

$$S = \frac{1}{1+NV}, \tag{2}$$

where ***NV*** is the number of known vulnerabilities in the system.

- **Transparency (T):** Transparency is defined as the number of transactions or ledger entries available for inspection. Blockchain provides high transparency because all transactions are visible to all participants and it is impossible to change information without the knowledge of the entire network (3):

$$T = \frac{V}{N}, \tag{3}$$

where ***V*** is the number of visible or verified transactions or records and ***N*** is the total number of transactions or records in the system.

- **Data processing speed (P):** Data processing speed is measured as the time required to complete transactions. While blockchain can have slower processing due to the need for consensus, technological innovations such as sharding and decision level 2 can significantly increase speed (4):

$$P = \frac{1}{T_{processing}}, \tag{4}$$

where $\boldsymbol{T_{processing}}$ is the average processing time of a transaction or request.

Formulation of a complex model

To integrate all indicators into a single performance metric, we use a weighted average. Each indicator is evaluated according to its weight, which reflects the importance of this aspect to the overall performance of the system. The mathematical formula for calculating the overall efficiency E has the form:

$$E = w_R \cdot R + w_S \cdot S + w_T \cdot T + w_P \cdot P$$

where *E* is the overall efficiency of the system,

$\boldsymbol{w_R, w_S, w_T, w_P}$ are weighting factors for each of the indicators (reliability, security, transparency, processing speed),

R, S, T, and P are the values of the corresponding indicators.

***Determination* of weighting factors**

Weighting factors w_R, w_S, w_T, *and* w_P can be determined based on the priorities of a specific system. For example, in systems where safety is critical, the w_S weighting factor may be higher. The weights must sum to 1 to ensure proper normalization:

$$w_R + w_S + w_T + w_P = 1 \tag{5}$$

An example of calculations

Let us assume that for a specific system the weighting coefficients and values of the indicators are as follows:

- Reliability ***R*** = 0.95
- Security ***S*** = 0.85
- Transparency ***T*** = 0.90
- Processing speed ***P*** = 0.80

Weighting factors:

- W_R = 0.25
- W_S = 0.30
- W_T = 0.20
- W_T = 0.25

Then the total efficiency ***E*** is calculated as (6):

$$\boldsymbol{E = 0.25 \cdot 0.95 + 0.30 \cdot 0.85 + 0.20 \cdot 0.90 + 0.25 \cdot 0.80} \tag{6}$$

The use of weights in the model allows you to adjust the emphasis according to the specific needs and priorities of the system. This makes it possible to effectively assess the advantages and disadvantages of blockchain solutions in the context of specific tasks, such as registration management, and to provide reasonable support for decisions about their implementation.

The model is supported by modern scientific research, which demonstrates that blockchain technologies can significantly improve the reliability and security of systems compared to traditional centralized solutions. Research also points to the possibility of reducing corruption risks and increasing the transparency of processes due to decentralization and the possibility of open monitoring of transactions. Thus, the developed model is a useful tool for evaluating and comparing the effectiveness of technologies in the context of specific application examples.

After analyzing and developing a mathematical model for quantifying the effectiveness of implementing blockchain solutions into state registration systems, it is important to move on to the practical aspect of implementing these solutions. A mathematical model allows you to estimate potential benefits and determine key indicators for the successful implementation of technologies, but for real applications, a clear system architecture must be developed.

It is worth focusing on the basics of developing the architecture of the blockchain system for state registers.

3.2. Development of the architecture of the blockchain system in state registers

The implementation of blockchain technologies in state registration systems is based on several key aspects. Technological prerequisites include the selection of an appropriate blockchain platform, which should provide the necessary scalability and speed of transaction processing, as well as the ability to integrate with existing registration systems [15]. It is also important to take into account the requirements for data storage and their security, as well as ensuring effective interaction between various system components.

The organizational prerequisites are focused on the need for the new system to meet the requirements of state administration and ensure integration with existing state processes. This involves adapting internal procedures and changing approaches to data processing. System development also requires the participation of stakeholders, such as government agencies, technology providers, and citizens, which will ensure proper implementation and effective operation of the system [16].

Security aspects are critical to the successful implementation of blockchain solutions. This includes ensuring protection against possible cyber-attacks, protecting personal data, and ensuring compliance with international security standards such as GDPR. All these factors form the basis for the development of a detailed and effective system architecture Fig. 1, which ensures a high degree of transparency, security, and reliability in the management of state registers.

The main components of the architecture:

1. Users and interfaces:

- Citizens: submission of applications, verification of data.
- State authorities: management of registrations, verification, and approval of data.

2. Client applications:

- Web applications: Interfaces for citizens and civil servants.
- Mobile applications: Access to services from mobile devices.

3. Server part:

- API Layer: interfaces for interaction between client applications and the blockchain system.
- Authentication services: user management, authentication, and authorization.

4. Blockchain layer:

- Consensus mechanism: processing transactions and maintaining data consistency (for example, Proof of Stake, Proof of Work).
- Smart contracts: automation of processes (for example, registration, data verification).

5. Data and records:

- Transactions: records of registrations and changes.
- Metadata: information about transactions and their status.

6. Storage system:

- Decentralized storage: Use IPFS or other decentralized systems to store large amounts of data.

7. Analysis and reporting:

- Analytical tools: for system monitoring and analysis, and generation of reports.
- Auditing tools: Check data and transactions for compliance.

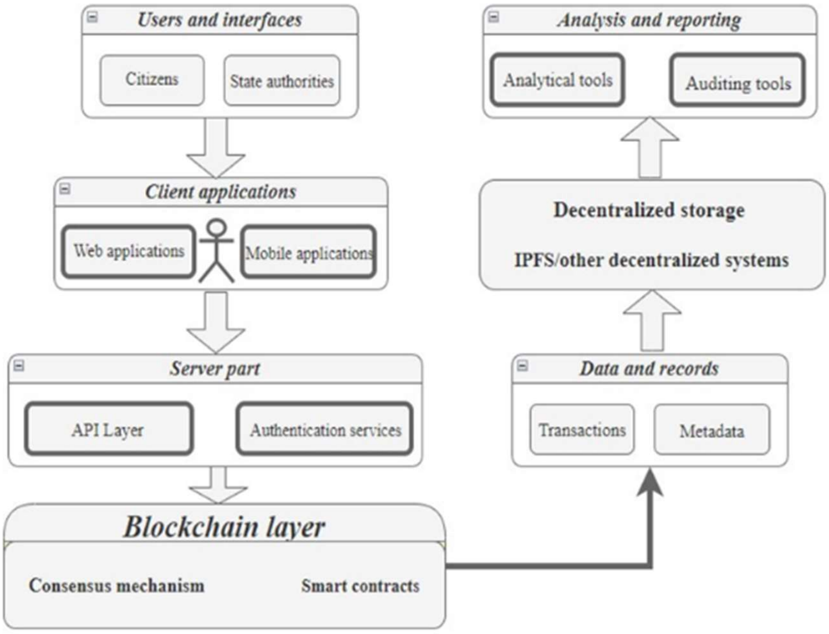

Figure1: Architecture diagram

In this approach, the architecture of the blockchain system for public registries shows its significant advantage over traditional centralized systems, particularly in terms of security, transparency, and trust. The use of blockchain in public registries allows for solving several fundamental problems, such as vulnerability to cyber-attacks, lack of control of users over their data, and reduction of corruption risks, thanks to the immutability of records and decentralized processing of transactions.

A key feature of this architecture is the integration of several technological components, including smart contracts, an authentication system, and decentralized file storage via IPFS. Smart contracts ensure the automatic fulfillment of conditions related to access to data, which allows for an increase in the efficiency of managing access to personal data and compliance with GDPR requirements. Decentralized storage in the IPFS system provides increased resistance to data loss and ensures the availability of information, even in the event of a central server failure [17]. From a scientific point of view, the proposed architecture makes an important contribution to researching the possibilities of integrating blockchain technologies into the field of public administration. The solution covers not only the technological aspects but also provides a foundation for the development of new approaches to ensuring the privacy and security of information. It is innovative to use the technological stack to achieve a higher level of trust of citizens in public institutions and ensure their right to control their data.

Thus, the architecture is a significant step towards the modernization of state registration systems, which will reduce the level of corruption, improve transparency, protect data, and ensure compliance with international standards.

3.3. Assessment of the prospects for the implementation of blockchain in state registers and the identification of key directions for the development of this technology in the context of public administration

An assessment of the prospects for the implementation of blockchain technologies in state registers indicates their significant potential for the transformation of public administration systems, especially in the context of digitization and increasing citizens' trust in state institutions. Blockchain has several key advantages that make it a promising solution for implementation in state registration systems [18].

First, increasing transparency and immutability of data is one of the main factors contributing to the use of blockchain in the public sector. Entries in the blockchain cannot be changed or deleted without leaving a trace, which reduces the possibility of data manipulation and corruption. This is particularly important for systems that are critical to public administration, such as land registries, voter registries, or business registries.

Secondly, the decentralization of data storage provides an additional level of protection against cyber-attacks. Since the data is not stored centrally on a single server, it is more difficult to hack or delete it. This significantly increases the level of system security and reduces the risk of losing important data [19].

Another promising direction is the implementation of smart contracts, which allow automating the execution of procedures and decisions that require compliance with clear rules and conditions. For public registries, this could mean simplifying and automating processes such as registering property rights, paying benefits, or entering into contracts with government agencies [20].

The key areas of development of blockchain technologies in public administration include the following:

- For the successful implementation of blockchain solutions in state registries, it is necessary to develop a legal framework regulating the use of this technology, in particular, to comply with international standards for the protection of personal data (GDPR).
- Blockchain integration with existing information systems. A promising direction is the creation of interfaces that will allow the integration of blockchain solutions with existing registry management systems, ensuring a seamless transition to the new technology.
- Investments in scientific research and pilot projects will allow the testing of various blockchain models adapted to the needs of public institutions and the development of the most effective solutions for specific use cases.
- For the successful implementation of blockchain, public servants must receive proper training in working with new technologies, in particular, in matters of data security and smart contract management.

Thus, the prospects for the implementation of blockchain technologies in state registers are quite optimistic. This solution can increase the transparency, security, and efficiency of public administration while ensuring compliance with international standards and requirements for the protection of personal data. However, successful implementation requires comprehensive measures for legal regulation, integration with existing systems, and training.

To assess the prospects for the implementation of blockchain technologies in state registration systems, it is important to consider how these technologies can affect various aspects of data management, comparing them with traditional centralized systems. Table 2 offers a comparative analysis of the key characteristics and potential benefits as well as disadvantages of each approach. This allows for a better understanding of the benefits of blockchain, as well as identifying areas where traditional systems can be more efficient.

Table 2
A comparison of the prospects for introducing blockchain into state registration systems

Direction of development	Status of current systems	Prospects of blockchain solutions
Protection of personal data	Risk of leakages due to centralization and limited control	More reliable protection thanks to decentralization and cryptography
Transparency of registration processes	Minimal transparency, difficult to verify changes or manipulations	High transparency, each record is stored forever and available for review
Compliance with GDPR requirements	Limited management of user consent and auditing	Users can control access to their data, automated consent management
Corruption risks	High risks, possible manipulation of data without proper control	Significant risk reduction due to data immutability and auditability
Cost of use	High costs for updating and maintaining centralized systems	Potentially high initial investment, but lower maintenance costs in the long run
Flexibility and scalability	Limited scalability, requires large upgrade costs	High flexibility, easy to integrate new functions and systems
Speed of decision-making	Depends on administrative centralization and bureaucracy	Automation of processes through smart contracts accelerates processes
Resistance to failures and attacks	Vulnerability to failure of servers or centralized nodes	High stability due to decentralized structure and distributed storage

After looking at the table, several key conclusions can be drawn. The transition to blockchain technologies in public registries promises significant advantages in terms of transparency, security, and data control. The high transparency of the blockchain makes it possible to reduce opportunities for manipulation and corruption, which is a significant step forward in ensuring trust in state institutions.

Blockchain also increases the level of protection of personal data due to its decentralized structure and use of cryptography, which makes it less vulnerable to cyber-attacks compared to traditional centralized systems [21]. However, the implementation of this technology is accompanied by high initial costs and the requirement for significant investments in the development of legal and technical infrastructure.

At the same time, existing centralized systems have certain advantages, such as already-established processes and familiarity with the technology [22]. However, their limitations in terms of flexibility and transparency point to the need for modernization.

Thus, although the implementation of blockchain technologies in state registries is promising, it requires careful planning and consideration of possible costs and challenges [23]. This technology can provide significant improvements in data protection and management efficiency, but its success depends on a comprehensive approach to integration and support. Going forward, it is important to focus on developing a clear implementation strategy that takes into account both technical and legal aspects to maximize the potential of blockchain in public administration.

4. Conclusions

In this work, a comprehensive analysis of the introduction of blockchain technologies into state registration systems was conducted. Both the advantages and disadvantages of blockchain solutions compared to traditional centralized systems are considered, and a mathematical model is developed for several evaluations of the effectiveness of such implementations.

Analysis of the current state of state registers has shown that traditional centralized systems arise with significant problems. Also, these systems are vulnerable to cyber-attacks that can lead to the compromise of large amounts of sensitive data. The lack of transparency in centralized systems makes it difficult to control data changes and creates a favorable environment for corruption. Also, an important aspect is the limited control users have over their data, which meets the requirements of modern privacy and information protection standards such as GDPR.

The advantages of blockchain technologies include a high level of transparency through decentralized architectures, which allows effective monitoring of transactions and data changes. Reduces opportunities for manipulation and unauthorized access to information. In addition, the use of cryptography in the blockchain provides a high level of security, which is a place to protect data from cyber-attacks. However, the implementation of blockchain solutions is associated with high initial costs and requirements for the adaptation of existing legal and technical structures.

The mathematical model developed to evaluate the effectiveness of blockchain technologies in state registration systems includes such key indicators as reliability (N), security (S), transparency (T), and performance (P). The model demonstrates that blockchain can significantly improve transparency and security, but also highlights the need for significant investment to integrate the technology. The results of the mathematical model confirm that the blockchain solution can significantly increase the efficiency of data management in state registers, however, to achieve the maximum output, a comprehensive approach to integration and obtaining results is necessary.

An assessment of the prospects for the implementation of blockchain technologies shows that these technologies have significant potential for the modernization of state registration systems. They can improve transparency and security, as well as compliance with modern international standards. The protest must use technical, legal, and economic aspects for successful implementation. It is important to develop a clear integration strategy that includes adaptation of existing systems and provision of appropriate support and risks.

Thus, blockchain technologies are of significant scientific and practical interest for the modernization of state registration systems, providing the potential to increase their efficiency and public trust. However, to achieve the desired results, it is necessary to complete all aspects of implementation and develop a binding plan that allows realizing the potential of this technology in public administration.

References

[1] M. Dong, et al., Blockchain for Secure and Trustworthy IoT: A Survey, IEEE Access, 9 (2021) 4955–4971. doi: 10.1109/JIOT.2019.2920987.

[2] V. Zhebka, et al., Methodology for Choosing a Consensus Algorithm for Blockchain Technology, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 106–113.

[3] D. Virovets, et al., Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 182–190.

[4] S. Obushnyi, et al., Ensuring Data Security in the Peer-to-Peer Economic System of the DAO, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3187 (2021) 284–292.

[5] S. Obushnyi, et al., Autonomy of Economic Agents in Peer-to-Peer Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 125–133.

[6] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

[7] W. Mougayar, The Business Blockchain: Promise, Practice, and the Application of the Next Internet Internet, Wiley (2016).

[8] D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Penguin (2016).

[9] V. Buterin, Ethereum: The Ultimate Smart Contract and Decentralized Application Platform (2013). URL: https://ethereum.org/en/whitepaper/

[10] M. Szmigiera, Global Blockchain Technology Market Size & Share Report, 2021–2028, Grand View Research (2021). URL: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

[11] X. Li, et al., A Survey on Blockchain Technology and Its Applications, IEEE Access, 5 (2017) 12293–12305. doi: 10.1109/ACCESS.2017.2717926.

[12] S. Al-Sarawi, A. Alzahrani, A. Al-Ali, Blockchain-based Framework for Secure Data Storage and Management, IEEE Access, 6 (2018) 56495–56506. doi: 10.1109/ACCESS.2018.2876714.

[13] H. Wu, S. Wang, Blockchain Technology for Information Security and Privacy Protection: A Review, IEEE Transactions on Industrial Informatics, 16(5) (2020) 3320–3328. doi: 10.1109/TII.2019.2952072.

[14] Z. Zheng, et al., Blockchain Challenges and Opportunities: A Survey, Int. J. Web Grid Serv. 14(4) (2018) 352–375. doi: 10.1504/IJWGS.2018.095275.

[15] V. Balatska, V. Poberezhnyk, I. Opirskyy, Development of the Learning Management System Concept based on Blockchain Technology, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 143–156.

[16] V. Balatska, et al., Blockchain Application Concept in SSO Technology Context, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 38–49.

[17] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2009).

[18] Z. Zheng, et al., Blockchain Technology: Principles and Applications, IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (2017). doi: 10.1109/ICBC.2017.7958760.

[19] R. Trishch, et al., Assessment of Safety Risks using Qualimetric Methods, MM Sci. J. 2023(10) (2023) 6668–6674. doi: 10.17973/MMSJ.2023_10_2023021.

[20] S. Yevseiev, et al., Models of Socio-Cyber-Physical Systems Security: Monograph, PC Technology Center (2023).

[21] V. Poberezhnyk, I. Opirskyy, Developing of Blockchain Method in Message Interchange Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 148–157.

[22] W. Mougayar, The Business Blockchain: Promise, Practice, and the Application of the Next Internet Internet, Wiley (2021).

[23] O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 398–409.