Method for Ensuring the Reliability and Security of Personal Data in Blockchain Systems of State Registers*

Valeriia Balatska[1,2,†], Vasyl Poberezhnyk[1,†] and Ivan Opirskyy[1,*,†]

[1] Lviv Polytechnic National University, Information Security Department, 79013 Lviv, Ukraine
[2] Lviv State University of Life Safety, Department of Information Security Management, 79007 Lviv, Ukraine

Abstract

Modern state registries play a pivotal role in the storage and processing of data related to citizens, legal entities, and material assets. However, traditional centralized information management systems face numerous challenges, among which the most critical are vulnerability to external attacks, reliance on a single point of failure, scalability issues, and high maintenance costs. Such systems often lack transparency, while data processing is complicated by dependence on human factors, increasing the risks of fraud and manipulation. This study proposes an innovative method for ensuring the integrity and security of personal data in state registries through the integration of blockchain technology with Layer 2 solutions. The foundation of the proposed approach is a decentralized blockchain architecture, which ensures data transparency and immutability. The use of cryptographic hashing guarantees data integrity, while the implementation of smart contracts automates key processes such as data verification, entry, and updates. A key innovation of this approach is the application of Layer 2 solutions, particularly rollups, which reduce the load on the main blockchain by aggregating transactions and recording only their root in the blockchain. This significantly enhances the system's scalability, reduces data storage costs, and ensures fast access to information. Furthermore, integration with the InterPlanetary File System (IPFS) enables efficient storage of large data volumes off-chain, leaving only critical metadata in the blockchain. The study describes the architecture of the proposed method, provides a detailed analysis of its advantages over centralized systems, and explores practical applications in real estate registries, citizen registries, and electoral systems. The practical implementation demonstrates that the combination of blockchain architecture with Layer 2 solutions achieves high efficiency, transparency, and trust in state registries while mitigating the risks of fraud and data loss. The results of the research indicate that the integration of blockchain technology with Layer 2 solutions is a promising pathway for modernizing state information systems. This opens up new opportunities for the development of resilient, reliable, and scalable registries that meet the contemporary demands of the digital society.

Keywords

blockchain, Layer 2, data integrity, public registries, decentralization, information security, smart contracts, rollups, scalability

1. Introduction

Ensuring data integrity, security, and transparency is one of the key challenges for modern information systems, especially in the public administration field. State registries play a pivotal role in storing and processing data about citizens, legal entities, and material assets, serving as the foundation for decision-making, implementation of social programs, and ensuring citizens' rights. However, traditional centralized approaches to organizing state registries face numerous challenges that undermine trust in these systems and reduce their efficiency.

The main problems of centralized registries include:

- Single point of failure. Failures in the central server can lead to data loss or system downtime.

*CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
v.balatska@ldubgd.edu.ua, valeriia.s.balatska@lpnu.ua (V. Balatska); vasyl.poberezhnyk@gmail.com (V. Poberezhnyk); iopirsky@gmail.com (I. Opirskyy)
0000-0002-6262-6792 (V. Balatska); 0000-0002-7523-2557 (V. Poberezhnyk); 0000-0002-8461-8996 (I. Opirskyy)

- Vulnerability to attacks. Centralized databases are often targeted by hackers, increasing the risk of unauthorized access or data manipulation.
- Complex data integrity verification. Centralized systems lack effective mechanisms for transparently tracking changes, complicating audits, and control over information accuracy.
- Limited scalability. The growing volume of data significantly overloads centralized systems, affecting their speed and performance.
- Dependence on human factors. Data verification, entry, and update processes in centralized systems are often performed manually, increasing the risk of errors and misuse.

The development of digital technologies, particularly blockchain, has opened new possibilities for addressing these issues. Blockchain provides a decentralized data storage architecture, where information is stored as transactions in a distributed ledger [1]. Through cryptographic hashing, every record in the blockchain becomes immutable and transparent, ensuring its integrity and accuracy. Furthermore, the introduction of smart contracts allows for the automation of key processes such as data verification, access control, and transaction execution, minimizing dependency on human factors [2].

However, even blockchain has its limitations, particularly in scalability. In this context, Layer 2 solutions, such as rollups, plasma, and sidechains provide an additional level of efficiency by offloading part of the transaction processing to an auxiliary layer. This significantly reduces the load on the main blockchain, ensuring high throughput, scalability, and cost efficiency.

The use of Layer 2 solutions, particularly rollups, in combination with blockchain provides new possibilities for improving the performance of state registries. This approach moves the processing of large volumes of transactions off-chain, leaving only critical data in the main chain. As a result, high-speed performance, economic efficiency, and compliance with the demands of digital transformation are achieved.

This study focuses on the development of a novel method for ensuring the integrity and security of personal data in state registries by utilizing the usage of Layer 2 solutions on top of the blockchain architecture. The proposed approach addresses both the key issues of centralized systems and opens new opportunities for creating transparent, resilient, and scalable information systems.

Problem formulation. State registries are an integral part of the information infrastructure that facilitates the storage and management of critical data about citizens, legal entities, real estate, electoral systems, and more. However, traditional centralized systems for managing such registries have significant shortcomings that jeopardize their functionality, reliability, and security. One of the key challenges of centralized systems is their limited scalability. As transaction volumes increase, database sizes grow, which significantly slows system performance and raises maintenance costs. For state registries, which handle large volumes of information, this represents a critical limitation that requires modern technological solutions.

The primary issues include:

- Dependence on a single point of failure: Centralized systems are vulnerable to technical failures that can lead to data loss, system compromise, or total downtime.
- Susceptibility to cyberattacks: Centralized architecture creates ideal conditions for attackers, allowing them to gain access to vast amounts of information stored at a central node.
- Complexity in ensuring transparency: The absence of mechanisms to track data changes opens opportunities for manipulation and complicates registry audits, undermining citizens' trust in state information systems.
- Limited scalability: As data volumes increase, centralized systems suffer from overloads that severely impact their performance and transaction processing speed.

- Dependence on human factors: In centralized systems, many processes are performed manually, increasing the risks of errors, delays, and internal threats.
- High maintenance costs: Centralized systems require substantial financial resources for infrastructure upkeep, security assurance, and regular updates.

These issues become even more pronounced in the context of digital transformation, where data volumes are continuously growing, and the demands for security, speed, and transparency in registries are becoming increasingly stringent.

At the current stage of technological advancement, blockchain offers a promising approach to addressing these problems. Its decentralized architecture eliminates dependence on a single point of failure, ensures data immutability, and enhances the transparency of all operations. However, even blockchain faces limitations, such as scalability issues and high transaction processing fees in large networks.

A solution to these shortcomings lies in the integration of Layer 2 solutions. Such as rollups, plasma, and sidechains into the blockchain, which enables the offloading of transaction processing to an additional layer, leaving only critical information on the main blockchain. This approach significantly improves system performance, reduces costs, and ensures fast access to data.

Thus, this raises the need to develop a new method for ensuring data integrity and security that combines the advantages of blockchain and Layer 2 solutions, capable of being consistent with the modern challenges and requirements of state registries.

Recent research and publications analysis. Recent research indicates a significant interest in using blockchain technologies to ensure data security, transparency, and availability in various information systems, including public registries [3, 4]. In particular, scientific works demonstrate the advantages of blockchain in ensuring data immutability and the possibility of transparent transaction tracking. Researchers emphasize that the decentralized nature of blockchain allows for minimizing the risks associated with dependence on a single point of failure, which is a typical problem of centralized registries [5]. Blockchain is also distinguished by its ability to store a history of changes that is available to all network participants, thereby ensuring transparency and increasing trust in the system.

One of the key areas of research is the use of cryptographic hashing to ensure data integrity. Hashing allows the creation of unique digital fingerprints of data that change with any intervention, making manipulation attempts obvious. This solution is widely studied in the context of increasing the level of data security in public registries [6]. In addition, the use of hashing in combination with a decentralized architecture provides rapid identification of changes, which is critical for government information systems.

In addition, the implementation of smart contracts is seen as an effective way to automate data access management processes and ensure that operations are performed based on established rules and user consent [7]. Smart contracts eliminate the need for human intervention, reducing the risk of errors and fraud. They can be used to automatically update data in registries, simplify verification procedures, and ensure transparency in query execution.

Of particular interest are works devoted to decentralized file systems, such as IPFS (InterPlanetary File System) [8]. This technology provides increased availability and storage of large amounts of data in a distributed environment, which is an important aspect for government registries that operate with large amounts of information. IPFS is also seen as a tool that allows only critical metadata to be stored in the blockchain, which significantly reduces the cost of its maintenance. Due to its architecture, IPFS can provide high fault tolerance by storing duplicate data on different nodes of the network, which makes the system reliable even in the event of failure of individual components.

At the same time, recent studies emphasize the challenges associated with the scalability of blockchain systems [9]. In this context, Layer 2 solutions such as rollups, plasma, and sidechains might be the way of addressing the challenge. They allow the processing of some transactions outside the main blockchain, reducing the load on it and increasing the speed of the system. This

opens up new opportunities for the use of blockchain in public registries, which require processing a large number of transactions in real-time. Layer 2 solutions also reduce the cost of transactions, which is important for implementing the technology in large-scale projects.

Blockchain in combination with Layer 2 solutions and decentralized data storage systems is a promising direction for solving the problems of public registries. This allows the creation of systems that meet the requirements of digital transformation, providing transparency, fault tolerance, and a high level of trust from citizens. Future research in this area may be aimed at adapting these technologies to the specific conditions of government information systems and ensuring their integration with existing digital platforms.

The purpose of the paper. The purpose of the paper is to develop a concept for an innovative method to ensure the reliability, security, and transparency of data in public registries by integrating blockchain technologies with Layer 2 solutions, which allows for increased efficiency, scalability, and resilience to threats. The main objectives of the paper are:

- Analyze the problems of centralized systems in state registries, in particular their dependence on a single point of failure, vulnerability to attacks, and difficulty in scaling.
- Investigate the properties of blockchain technologies that ensure transparency, immutability, and data security.
- Develop an architecture for integrating blockchain with Layer 2 solutions to reduce the load on the main blockchain and ensure high system speed.
- Assess the possibilities of using smart contracts to automate key processes of data access management in state registries.
- Study the use of decentralized file systems, such as IPFS, for efficient storage of large amounts of data.
- Compare the advantages of the developed approach with traditional centralized systems in terms of transparency, security, and resilience to external threats.

These tasks are aimed at creating an effective and reliable method for ensuring the security, authenticity, and availability of data in state registries that meet modern technological challenges and the requirements of digital transformation.

2. Development and justification of a method for ensuring the reliability and security of personal data in state registers

2.1. Analysis of current challenges and problems in the functioning of state registers

Modern state registries serve as a crucial tool for managing information related to citizens, legal entities, and their assets. They enable the execution of key administrative functions, provision of public services, and support of the legal system. However, the growing volume of data and its processing is accompanied by numerous challenges concerning the reliability, security, and transparency of information.

The centralized architecture of state registries is one of the main drawbacks of traditional systems. This architecture involves storing data in a single repository, which creates risks of unauthorized modification or loss caused by technical failures or cyberattacks. Such vulnerabilities result in situations where changes in registries remain unnoticed or cannot be tracked, jeopardizing the reliability of the data, especially in critically important systems [10].

Another issue is the lack of transparency in data entry and update processes. The absence of effective control mechanisms in centralized systems allows malicious actors or internal staff to introduce incorrect information without proper auditing [11]. This leads to financial losses, legal disputes, and a decline in public trust in state institutions.

The human factor remains one of the key sources of threats to centralized systems. Manual data entry, operator errors, and malicious actions significantly increase the risk of information compromise [12]. Weak validation mechanisms for entered data further expose such systems to unauthorized changes, which is particularly dangerous for state registries [13].

These problems are exacerbated in the context of modern cyber threats. Attacks on state information systems are growing both in frequency and sophistication. Phishing techniques, social engineering, and direct attacks on databases are becoming increasingly advanced, necessitating higher levels of protection for such systems.

In this context, blockchain technologies emerge as a promising solution. Blockchain ensures data immutability through its decentralized structure and the mechanism of chained blocks, where each transaction is recorded chronologically. This addresses the problem of data entry control by enabling auditing and tracking of all changes. Research confirms that the use of blockchain can significantly enhance public trust in state registries due to the transparency of their operations and resistance to unauthorized changes.

Thus, the challenges associated with centralized state registry systems highlight the need to develop innovative solutions to ensure their reliability, security, and transparency. The application of blockchain technologies is one of the promising approaches that allow the modernization of existing systems and improve their resilience to modern threats.

2.2. The potential of blockchain technologies to increase the reliability and security of data in public registers

Blockchain technologies provide an innovative solution to the challenges of ensuring the reliability, security, and transparency of state registries. The primary advantage of blockchain lies in its decentralized architecture, which eliminates dependence on a central data repository. Information in blockchain systems is recorded as sequential blocks linked together by cryptographic hashes, ensuring data immutability and preventing unauthorized modification or deletion [14].

In traditional state registries, data is stored in centralized repositories, exposing them to risks of compromise through cyberattacks or system errors. Blockchain, on the contrary, distributes copies of the registry across network nodes, enhancing reliability and fault tolerance. Every operation is recorded in a block that cannot be altered without the consensus of the entire network, making blockchain systems resistant to forgery and data manipulation [15, 16].

Blockchain systems also provide full transparency, as every transaction is viewable by all network participants. This ensures complete oversight of changes made to the data, enhancing the transparency of state registry operations. Any attempts at unauthorized intervention or erroneous data entries can be easily detected and corrected. This mechanism is crucial for public institutions, as it fosters citizen trust in the information stored in registries [17].

Automation of data validation and entry processes through blockchain-based smart contracts minimizes the risks of human error or intentional manipulation. Smart contracts are self-executing programs that automatically enforce the conditions of agreements between network participants. They allow controlled data updates in the state registry only when predefined rules are met, significantly enhancing security levels [18].

The distributed nature of blockchain systems also increases their resilience to cyberattacks. Unlike centralized systems, where a single point of access can be targeted, attackers would need to simultaneously alter all copies of the registry across all network nodes—a computationally infeasible task.

Blockchain systems also support scalability, enabling state registries to handle large volumes of data with potential for future expansion. Models designed for transaction speed and storage optimization make blockchain adaptable to the needs of government management systems [19].

The main challenges of centralized systems, such as vulnerability to attacks, lack of transparency, and reliance on human intervention, can be effectively addressed through blockchain technologies. Table 1 presents a comparison of the characteristics of centralized and blockchain-based systems, highlighting their capabilities in overcoming these issues.

Table 1
Comparative analysis of blockchain technologies and traditional methods of managing state registers

Criterion	Traditional Centralized Systems	Blockchain Systems
Architecture	Centralized (single point of data storage)	Decentralized (distributed ledger)
Resilience to failures and attacks	Low: risk of attacks on the central server	High: changes require consensus from all network nodes
Transparency	Limited: lack of clear audit trails	High: all changes are recorded and available for verification
Data immutability	Data can be altered or deleted	Immutability is ensured by the chain structure of blocks
Security	Dependent on external protection mechanisms	Built-in security through cryptography and consensus
Process automation	Limited: requires human verification	High: smart contracts automate processes
Control over changes	Low: prone to errors and manipulations	High: all changes are validated by the network
Maintenance costs	High due to centralized infrastructure	Moderate: automation reduces costs

The above comparative analysis shows that blockchain systems significantly outperform traditional centralized solutions in key indicators. Decentralized architecture provides resistance to attacks and failures, and data immutability makes it impossible to modify them without authorization. High transparency and the ability to fully audit all changes increase user trust, which is especially important for state registries.

Thus, the implementation of blockchain technologies creates conditions for ensuring the reliability, transparency, and protection of state registries from modern threats, eliminating the main disadvantages of centralized systems [20].

2.3. Development of a method for ensuring the reliability and security of personal data in state registers based on blockchain technologies

The proposed method for ensuring the reliability and security of personal data in state registers is based on blockchain technology. Its main goal is to create a system that ensures immutability, transparency, and resistance to threats in the process of data processing and storage.

The key idea of the method is a distributed blockchain registry, in which each operation is recorded in blocks that are linked together using cryptographic hashes. *This ensures:*

1. Data immutability: any changes leave a trace in the system.
2. Transparency: all participants have access to records in the registry to verify their reliability.

3. Access control: the system automatically regulates the entry and update of data based on smart contracts.

The architecture of the proposed method consists of four main components:

1. User (Data Submitter)

Initiates requests to enter new data, update
existing records, or view information in the state register.

2. Validation Module

Checks the correctness of the request: data syntax, user access rights, and compliance with the rules for making changes.

3. Smart Contracts

Automatically control the conditions for performing operations. Allow or block changes depending on the specified access rules.

4. Blockchain Registry

A decentralized database that records all confirmed operations. A new block is written to the registry after consensus is reached by network nodes.

Fig. 1 shows the flowchart of the proposed method, which reflects the main stages of interaction between system components.

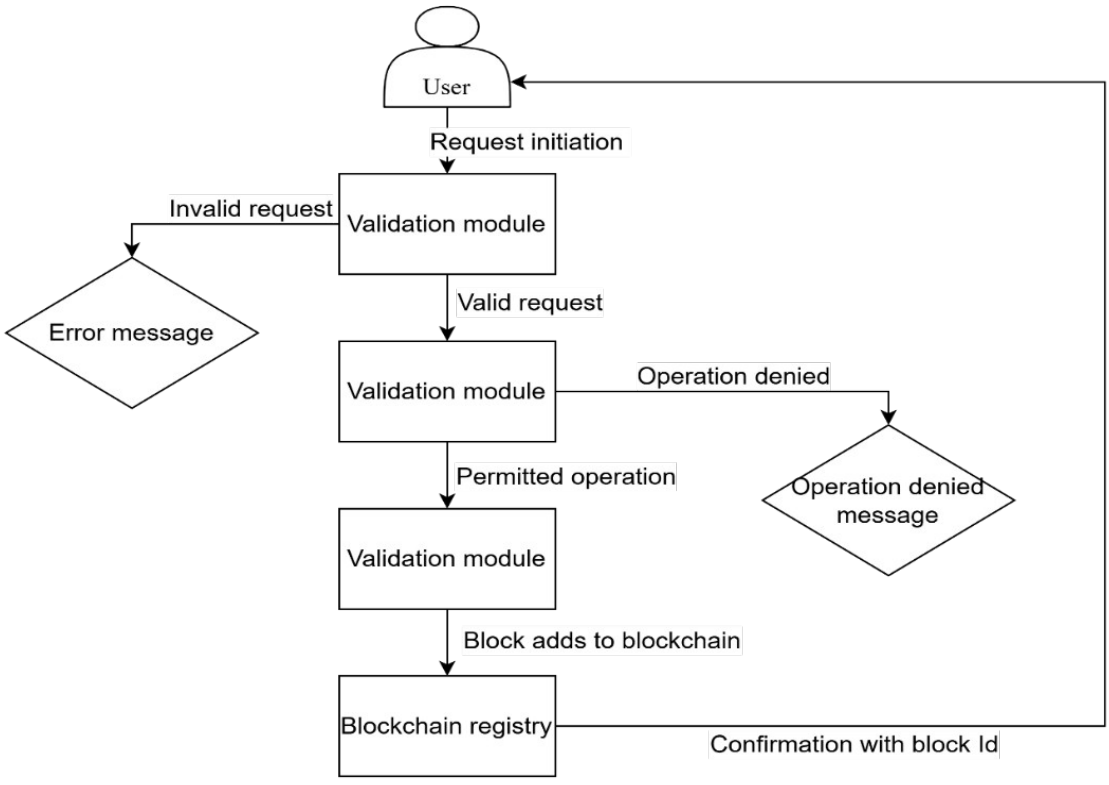

Figure 1: Flowchart of the data assurance method

Step 1. Initiating a request

The user sends a request to enter, update, or view data via the system client interface.

Step 2. Validating the request

The validation module checks:

- The user's identification and access rights.
- The correctness of the structure and content of the request.
- Compliance with the rules for entering data into the registry.

Step 3. Executing the smart contract

After successful validation, the smart contract automatically checks the conditions of the transaction and, if all criteria are met, generates a new block for addition to the blockchain registry.

Step 4. Block generation

The new block contains:

- The hash of the previous block for connection in the chain.
- The timestamp of the transaction.
- User data and the content of the transaction.
- The transaction hash code is a confirmation of data integrity.

Step 5. Recording in the blockchain registry

After reaching consensus, the block is added to the distributed registry, where it becomes available for verification by all network participants.

Step 6. Audit and confirmation of the operation

The user receives confirmation of a successful operation with the identifier of the new block. All records are available for auditing and verification of their authenticity.

Fig. 1 demonstrates the architecture of the method for ensuring the authenticity and security of personal data in blockchain systems of state registries. The basis of the proposed approach is a distributed blockchain registry, in which each operation is recorded in the form of immutable blocks linked by cryptographic hashes. This ensures both the technical impossibility of unauthorized changes and the transparency of the system for all participants. The method integrates automated validation modules and smart contracts that regulate the entry and update of data by the specified access rules [21].

The proposed implementation algorithm is based on a clear interaction between the key components of the system: users, the validation module, smart contracts, and the blockchain registry. The user sends a request to enter or update data, which is automatically checked by the validation module. Smart contracts provide control over the fulfillment of the conditions of the operation, after which a new block is formed. After reaching a consensus among the nodes, the block is added to the blockchain registry, where the data becomes immutable and available for further audit.

A feature of the method is its resistance to external threats due to the decentralized structure, which eliminates the risk of a "single point of failure." Transparency of operations is achieved through the ability to audit any record in the registry, which increases user trust. In addition, the automation of processes provided by smart contracts minimizes the impact of the human factor, and the separation of access rights contributes to effective information management.

Thus, the proposed method provides a reliable mechanism for controlling the entry, updating, and verification of data in state registers, which is confirmed by the scheme in Fig. 1. Its application allows for modernizing traditional registration systems, increasing the level of data reliability, minimizing the risks of manipulation, and ensuring the transparency of the functioning of state information systems.

2.4. Justification of the efficiency of the proposed method based on an analysis of its advantages compared to traditional methods

Modern state registries that rely on centralized data management systems face numerous challenges related to ensuring the reliability, integrity, and security of information. Among the most common issues are vulnerabilities to failures due to single points of failure, low transparency in processes, and dependence on human factors during data processing. Moreover, centralized registries are susceptible to internal threats, as administrators or other authorized personnel can make changes without proper recording in the transaction history [22]. Auditing such systems is a

labor-intensive process that requires additional resources and time, making them less efficient in the dynamic environment of digital transformation.

The proposed method for ensuring the reliability and security of data based on blockchain technologies provides a scientifically justified solution that eliminates the shortcomings of traditional systems through the application of distributed ledgers, automated smart contracts, and cryptographic hashing. Its key feature lies in the immutability of each record within the system, with all changes transparently recorded and accessible for verification. This ensures fundamental data reliability and integrity in registries, which is critical in the context of growing digital threats and information manipulation.

Unlike centralized approaches, the proposed method utilizes a decentralized architecture that eliminates the "single point of failure" problem and significantly increases resilience to both external and internal threats. Data in a blockchain registry is stored across distributed network nodes, with each new block of information cryptographically linked to the previous one. This makes unauthorized changes virtually impossible, as any interference would compromise the integrity of the entire chain. Moreover, blockchain ensures complete process transparency, enabling participants to audit transactions and verify data integrity in real-time. In contrast to centralized systems, where verifying changes requires additional procedures, every operation in a blockchain-based system is automatically recorded and readily available for analysis.

The integration of smart contracts within the proposed method addresses another significant issue of traditional registries—dependence on human factors in request processing. Smart contracts are automated algorithms that control the entry and updating of data according to predefined conditions. This minimizes the risk of errors and accelerates operations, which is especially relevant for state systems that handle large volumes of information daily [23].

The effectiveness of the proposed method is demonstrated in ensuring data immutability, which is critical for property registries, citizen registries, electoral systems, and other information databases where the accuracy and reliability of information determine the legitimacy of administrative decisions. For instance, in property registries, every purchase-sale transaction is recorded as an irreversible transaction, eliminating the possibility of fraud or document forgery. In corporate registries, blockchain technologies enhance transparency and trust by providing access to the history of changes and facilitating effective monitoring of company activities and their beneficiaries.

To verify the authenticity of data obtained from the registry, the proposed model employs the "proof of existence" principle, which ensures that specific data exist in their original state since their creation. This can be achieved through the integration of decentralized principles and blockchain technology.

In such an approach, it is advisable to use technologies other than blockchain for general data storage, as data volume negatively impacts network performance and maintenance costs. Blockchain should be reserved for storing critical data that need to remain immutable and occupy relatively small space, such as data fingerprints. This principle requires the separation of data storage and the preservation of proof of their authenticity.

Data integrity can be ensured using cryptographic hashing, which allows the creation of data fingerprints of a fixed size regardless of the input data volume. Furthermore, cryptographic hashing ensures that the input data cannot be reconstructed from the hash code, making it suitable for processing various types of data, including restricted access, personal data, and classified information.

Additionally, any alteration in the data results in a completely different hash due to the "avalanche effect" [24], effectively making unauthorized changes detectable, as any alteration would result in a modified hash code, immediately indicating data tampering.

The application of IPFS technology is justified by its decentralized nature, which prevents the existence of privileged users in the network while enhancing system resilience by eliminating central points of vulnerability. This ensures system functionality even when some nodes fail. Another advantage of IPFS is the decentralized data storage, allowing data to be stored across

multiple network nodes simultaneously. This approach not only improves data access speed by selecting the closest node to the system user but also ensures data redundancy across various nodes, maintaining access even if the nearest node becomes unavailable.

These technological capabilities make the combination of blockchain and IPFS a promising foundation for systems capable of storing, transmitting, and verifying data for authenticity and integrity. Such a combination can serve as the backbone of next-generation state registries.

Fig. 2 illustrates the structure of the proposed registry.

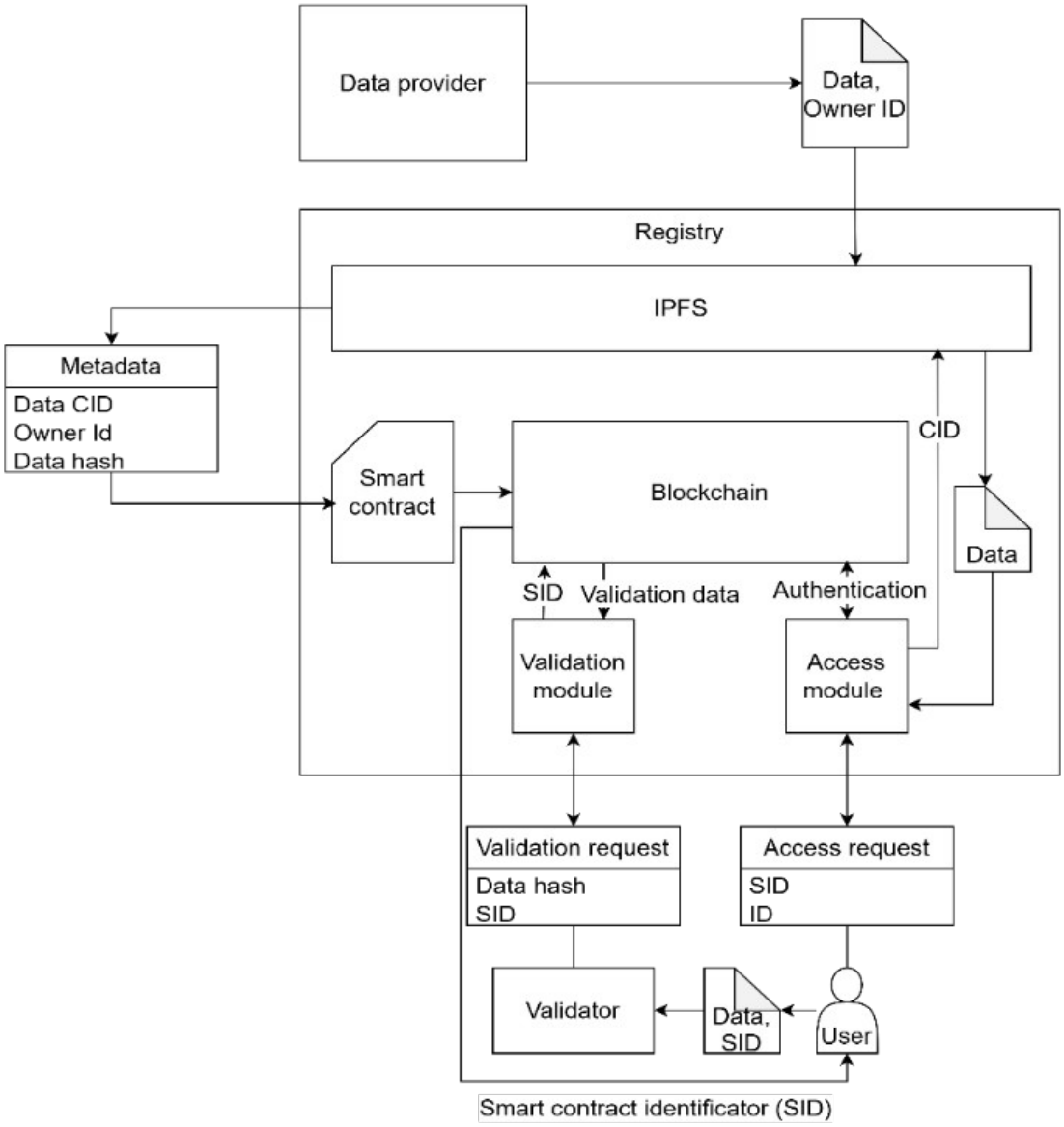

Figure 2: Structure of the proposed registry using blockchain and IPFS

In this concept, each independent unit of data, such as a generated document or a record in a registry, appears in the form of a set of values stored in the blockchain:

$$Entry = \{SID, CID, ID, H\}, \tag{1}$$

where *Entry* is a registry entry; *SID* is a smart contract identifier; *CID* is a data identifier in IPFS; *ID* is an owner identifier; *H* is a data hash.

In addition to the technologies mentioned earlier, this system requires the use of additional technologies, in particular smart contracts, which will allow automation of the operation of the system, which will reduce the amount of human intervention in the system, which will

simultaneously increase trust in the system and minimize the number of users with special rights who could negatively affect the operation of the system or commit unauthorized actions. Moreover, the use of smart contracts will allow automating not only the storage or verification of data but also restricting access if necessary.

When creating a new record in the registry, the data addition algorithm will look like this:

1. The data provider creates new data and transfers it and the data owner identifier (ID) to the IPFS registry.
2. IPFS generates a data identifier (CID) and a cryptographic hash of the data and creates a smart contract based on it.
3. The smart contract specifies the CID, data hash, and owner identifier.
4. The smart contract is stored in the blockchain part of the registry and receives an identifier.
5. The user receives the smart contract identifier and is considered its owner.
6. If necessary, the user receives data from the registry via the access module, providing his identifier and the smart contract identifier.

Obtaining access to data by the user will have the following steps:

1. The user sends a request to the access module, providing the ID and SID.
2. The access module authenticates the request by comparing the received user ID and the user ID stored in the smart contract pointed to by the SID.
3. If the identifiers match, the access module sends a request containing the CID to IPFS, if the identifiers do not match, access is denied.
4. IPFS returns the specified data to the access module, and the access module sends the data to the user.

If necessary, to verify the data received from the user, the validation process will have the following steps:

1. The validator receives the data and the smart contract identifier.
2. The validator calculates a cryptographic hash of the data and sends a validation request containing the calculated hash and the smart contract identifier.
3. The validation module receives data from the blockchain for validation from the smart contract, the identifier of which is the provided SID.
4. If the calculated hash and the hash stored in the smart contract match, the validator receives a response about successful validation, if the hashes do not match, he receives a message about a validation error, if it may indicate a violation of the integrity or reliability of the data.

However, the use of these technologies may also have negative aspects, which are most often associated with the nature of the technologies used. For example, the size of the blockchain will negatively affect the speed of the entire system, since over time it will grow, and the speed of data processing in the network depends on the size of the blockchain. A way to solve this drawback may be to “reset” the blockchain when information from old blocks is deleted, and only the hash of the previous block remains, which allows maintaining the chain in working condition, and the full version of the blockchain is stored in archive nodes. This approach will reduce the level of decentralization in the network since the network will depend on a certain number of archive nodes [25].

Another way to solve the problem of the speed and size of the blockchain can be the use of the Layer 2 approach. The essence of this is to process data outside the blockchain and store only the result of the processing in it. For example, the blockchain roll-up method allows combining several transactions performed outside the blockchain into one transaction, the result of which will be stored in the blockchain. This approach allows for an increase in the scalability and speed of the

blockchain network. At the moment, there are several options for building Layer 2 solutions aimed at increasing the scalability and speed of blockchain networks. Although they are all aimed at solving problems associated with the use of Layer 1, that is, the blockchain itself, they may also have their drawbacks. The advantages and disadvantages of the methods are given in Table 2.

Table 2
Advantages and disadvantages of methods for building layer 2 solutions

Method	Description	Advantages	Disadvantages
State Channel	Creates a separate channel where participants exchange transactions, with the final result recorded on the blockchain.	Low latency. Privacy.	Limited scalability due to the need to maintain the channel between parties.
Sidechain	A provider creates an independent blockchain where transactions occur. A gateway allows data exchange between the main blockchain and the sidechain.	High scalability. Potential for specialized blockchain applications.	Risks associated with independent blockchains.
Plasma	A child blockchain is created, with its security managed by the main blockchain.	Security is governed by the main blockchain.	Implementation complexity and potential challenges with transaction finalization.
Rollups	A block of transactions is created off-chain, compressed, and submitted for verification on the main blockchain.	High scalability. Security is managed by the main blockchain.	Possible delays. Implementation complexity.

Given the characteristics of the described methods, the most suitable for application in registry systems is the rollups-based method. This method aggregates multiple transactions, summarizes them, and records only a single transaction in the blockchain that describes the overall state of the transaction block [8]. For instance, each document or file created can be considered a single transaction, while a set of such transactions of a predetermined size can be grouped as a transaction block. This block can then be represented by a specific value.

In this context, the Merkle tree is particularly well-suited, as it allows the representation of a relatively large volume of data with a comparatively small structure. One of the key advantages of this approach is not only its efficient use of storage but also its capability to verify the integrity of the data it represents. This is achieved because the Merkle tree consists of hashes of data and cumulative hashes.

Fig. 3 illustrates the concept of this approach.

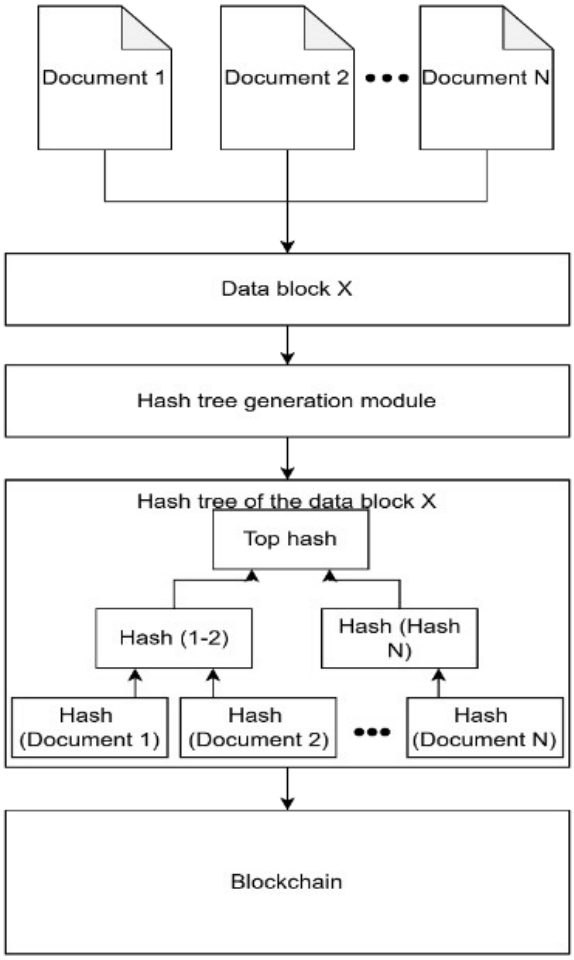

Figure 3: Concept of the method of representing a data block through a hash tree

The criterion for the readiness of a data block can be the number of documents included in one block and their size, it is permissible that the number of documents should not exceed 10 and the block size should not exceed 10 MB, so this method will have the following algorithm:

1. The Layer 2 processor generates a document until their number does not exceed 10 units and the total size is less than 10 MB.
2. When one or both criteria are met, a data block is formed and transferred to the hash tree generation module.
3. The module generates a hash tree and sets the top hash of the tree as the block integrity identifier.
4. The generated hash is stored in the blockchain.

This approach allows to saving of only one hash in the blockchain, which will represent 10 documents, instead of saving 10 separate hashes that represent each document, which will reduce the load on the blockchain network, while maintaining the ability to confirm the integrity of the data that was processed on another layer.

One of the key points of this concept is the identification of data and its belonging to a certain top-level hash, since the presence of a hash of only the data, or only the top-level hash, will not allow to confirm the validity of the data. The solution to this problem is the use of roll-up smart contracts, which will allow to establish a connection between transactions and the top-level hash. Also, the use of smart contracts will allow to determine the owner of the data, by forming pairs between the owner identifier and the data identifier. Fig. 4 presents the concept of such a smart contract.

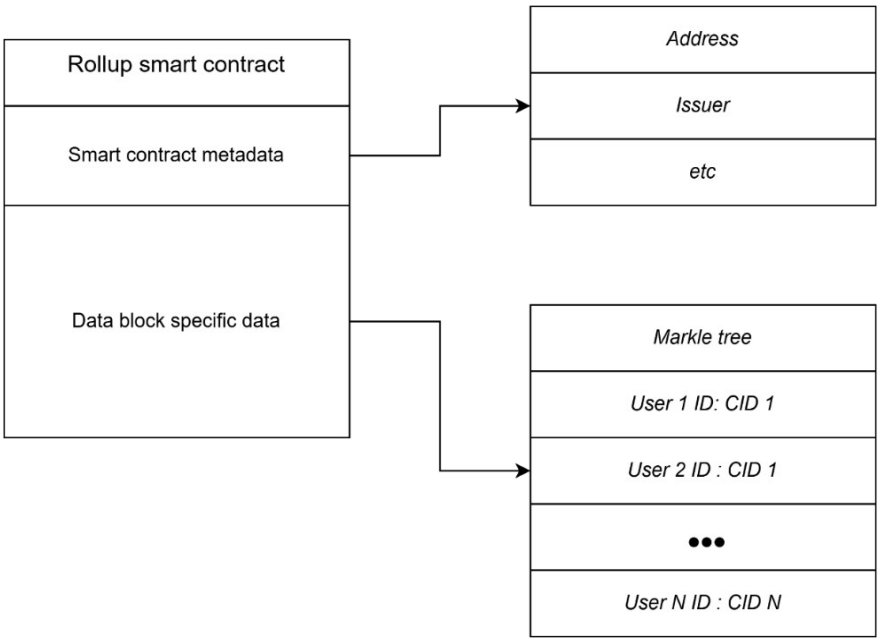

Figure 4: Smart contract structure concept

When using such a model, a smart contract allows to identify of the data and its owner, which allows the ability to differentiate access if necessary [26].

Fig. 5 shows the concept of a registry built based on the proposed method.

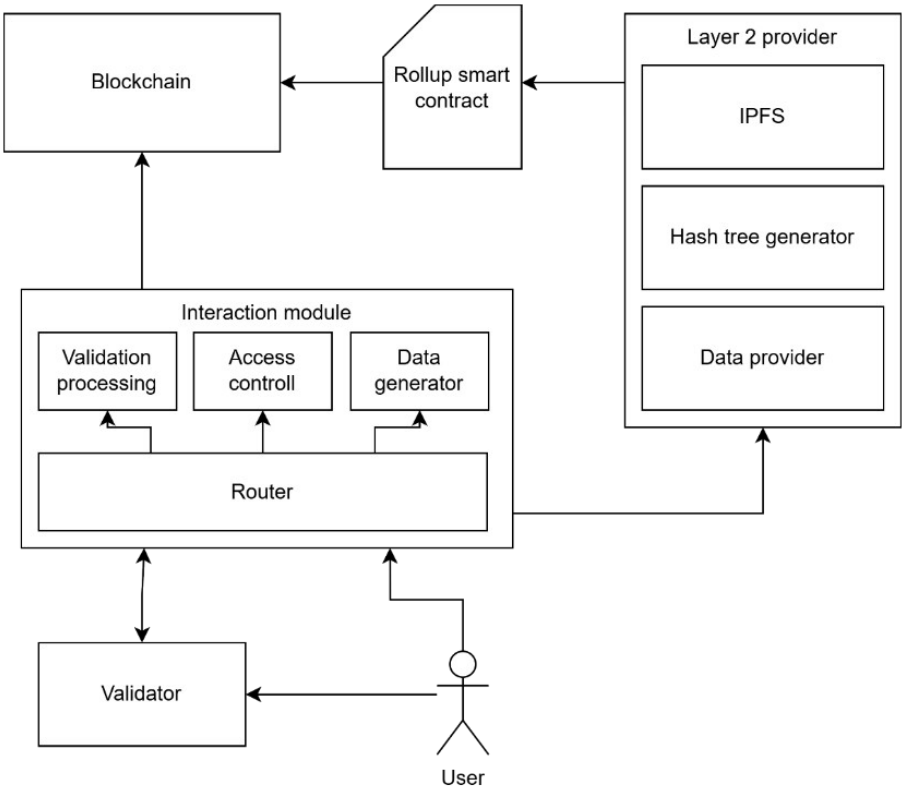

Figure 5: System concept

The proposed system consists of the main blockchain, Layer 2 provider, unifying smart contract, and a module for interacting with the system, which is responsible for data validation, data access, etc.

The Layer 2 provider consists of IPFS, a hash tree generation module, and a data processor, which is responsible for forming data blocks, which will then be represented by a hash tree stored in IPFS.

The blockchain is responsible for storing smart contracts and verifying transactions.

With this approach, three functions can be distinguished that such a system will perform: data creation, data retrieval, and data verification. *Data creation will have the following algorithm:*

1. The user sends the data to be stored in the system through the interaction module.
2. The interaction module transfers them to the Layer 2 data processor.
3. The data provider receives the data and waits for the requirements for forming a data block to be met.
4. After reaching the criteria for creating a new block, it is created and transferred to the hash tree generation module and stored in IPFS.
5. After generating the hash tree, it is written to the smart contract, along with the formed UID: CID pairs, where UID is responsible for user identification, and CID is data identification in IPFS.
6. The smart contract is stored in the blockchain.

Such an algorithm allows you to separate data from the blockchain and transfer their processing outside its boundaries while maintaining the ability to confirm the integrity and authenticity of data by storing their metadata in the blockchain, which reduces the load on the blockchain network, and the presence of pairs of identifiers allows you to establish the owner of the data and delimit access if necessary.

Obtaining data from such a registry must be authorized by the request for receipt, since the data may contain information of various kinds that contradicts the possibility of presenting it in an open form. For this, existing pairs of identifiers are used.

Obtaining data from the proposed system will have the following steps:

1. The user sends the CID to the data access module and the address of the smart contract.
2. The access module receives the smart contract data from the blockchain and verifies the provided pair of identifiers.
3. If the provided pair does not match the one stored in the smart contract, the request is blocked and the user is denied access.
4. If the provided pair of identifiers matches the stored pair, the access module sends a request with the CID to the layer 2 processor.
5. Layer 2 transmits the data to the user via the access module.

The data verification algorithm will have a similar form to the amendment to check the integrity and authenticity of the received data and will have the following steps:

1. The user sends the document and the address of the smart contract to the validator.
2. The validator calculates the hash value of the document.
3. The validator sends the address of the smart contract and the calculated hash value to the validation module.
4. The validation module receives data from the blockchain about the specified smart contract and searches its hash tree for the provided hash.
5. If the provided hash is found in the smart contract, the validator receives a response confirming the data provided to it.
6. If the hash is not found, the validator receives a message about the lack of confirmation of the provided data.

With this approach, data can be confirmed without actually receiving them from the registry, by checking the hash values of the provided data and stored in the blockchain, which allows for

reducing the load on the system, since the volume of data circulating in it with each such request is reduced, namely the calculation of the hash value is performed on the validator side.

It is worth noting that the proposed method has the following drawback: the data generated in this way cannot be updated, since its hash value will change, which will make it impossible to confirm it due to the existing stored value of hash in the blockchain.

However, the proposed system has many ways to improve or modify it depending on the needs. This possibility is due to the use of a combination of the aforementioned technologies, which expand the capabilities and potential of the system.

For example, expanding the functionality of a smart contract can add not only an authorized user for access but also other users or organizations that will have access to the document. Also, through a smart contract, the validity period of a document or its existence in IPFS can be managed, for example, in a smart contract the existence time of a document can be defined and after its expiration, such a document will be deleted from IPFS. Accordingly, even if the user of the system has such a document, its validity will no longer be confirmed because it will not exist in IPFS and its validity period stored in the smart contract will also indicate the termination of the validity of such a document [27]. Another possible improvement is the method of transmitting data to the validator, the role of which can be any interested party that receives documents from the user. In the proposed system, the user provides a document and a smart contract address to verify the document for authenticity, however, when expanding the functionality of the smart contract, which will allow third parties to access the generated documents, the need to transfer the document itself can be avoided. Authorizing the validator to access the document will allow the user to transfer only the CID of the document, which will allow the validator to independently access the document and obtain the document itself from a trusted source.

However, it is worth remembering that when working with systems based on blockchain technology, it is necessary to maintain a balance between the complexity of smart contracts and network maintenance, since the high complexity of contracts leads to an increase in the cost of network maintenance.

The use of blockchain technologies in state registers is not only technically feasible but also a strategically important solution that meets the modern requirements of the global information space and increases the level of trust in state institutions.

Conclusions

With the growth of digital information and increasing demands for personal data security, the importance of reliable, scalable, and transparent systems is becoming crucial. Analysis of modern systems has shown that centralized approaches to data storage have significant limitations, such as dependence on a single point of failure, low transparency, difficulty in scaling, and high risks of attacks. These shortcomings emphasize the need to implement decentralized solutions that can provide a high level of security and trust in government information systems.

The study confirmed that blockchain is an effective tool for ensuring data immutability and transparency of operations. The use of smart contracts allows for the automation of data access management and control over their processing, which minimizes the risks associated with the human factor. Blockchain also provides the ability to instantly verify the legitimacy of operations by providing a transparent data storage structure.

Additionally, the implementation of Layer 2 solutions, such as rollups, allows for a significant reduction in the load on the main blockchain, increasing the speed and scalability of the system. This approach allows for the aggregation of transactions while keeping only key metadata in the main blockchain. This reduces data processing costs and paves the way for blockchain to be used in large-scale government registries.

The use of decentralized file systems, such as IPFS, adds another layer of data protection. This approach provides efficient storage of large amounts of information, leaving only hashes in the

blockchain for verification. This solution not only supports the principles of data confidentiality and availability but also reduces the risks associated with technical failures or centralized attacks.

The results of the study show that the proposed method of integrating blockchain technologies with Layer 2 solutions creates the prerequisites for increasing citizens' trust in government digital platforms. The transparency of the system, data immutability, and process automation increase the efficiency of government agencies and help reduce the risks of fraud. This approach also complies with international data protection standards, such as the General Data Protection Regulation, making it relevant for implementation on a global scale.

The study confirmed that the use of decentralized technologies in public registries is not only technically sound but also strategically important for ensuring their long-term sustainability. Further development of such systems may include optimizing data processing processes, integration with other digital platforms, as well as developing new methods for ensuring information security. This opens up prospects for the creation of a new generation of public registries that will meet the modern challenges of the digital age, ensuring reliability, transparency, and protection of personal data.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] 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.

[2] D. Virovets, et al., Integration of smart contracts and artificial intelligence using cryptographic oracles, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 39–46.

[3] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf

[4] N. Kshetri, J. Voas, Blockchain in developing countries, IT Prof. 20(2) (2018) 11–14. doi:10.1109/MITP.2018.021921645

[5] J. Chen, J. Xu, Q. Lu, Blockchain and layer 2 scaling solutions: A comprehensive survey. doi:10.1109/TETC.2021.3094121

[6] M. Ali, et al., Blockstack: A global naming and storage system secured by blockchains, in: USENIX Annual Technical Conference, 2016, 181–194.

[7] Z. Zheng, et al., An overview of blockchain technology: architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data, 2017, 557–564.

[8] J. Garay, A. Kiayias, S. Leonardos, The Bitcoin Backbone protocol: Analysis and applications, in: Advances in Cryptology, EUROCRYPT, 2020. doi:10.1007/978-3-030-45724-2_1

[9] 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.

[10] V. Poberezhnyk, V. Balatska, I. Opirskyy, Development of the learning management system concept based on blockchain technology, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550, 2023, 143–156.

[11] V. Balatska, et al., Blockchain application concept in SSO technology context, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 38–49.

[12] Y. Kostiuk, et al., A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps, in: 3rd International

Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 249–264.
[13] Y. Kostiuk, et al., Models and algorithms for analyzing information risks during the security audit of personal data information system, in: 3rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.
[14] V. Balatska, N. Slobodian, I. Opirskyy, Blockchain for enhancing transparency and trust in government registries, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3826, 2024, 50–59.
[15] V. Balatska, V. Poberezhnyk, I. Opirskyy. Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR, in: Cyber Security and Data Protection, vol. 3800, 2024, 70–80.
[16] M. Iavich, et al., Classical and post-quantum encryption for GDPR, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 70–78.
[17] X. Xu, I. Weber, M. Staples, Architecture for Blockchain Applications, Springer International Publishing, 2019. doi:10.1007/978-3-030-03035-3
[18] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, 2017.
[19] D. Tapscott, A. Tapscott, Blockchain revolution: How the technology behind Bitcoin is changing money, Business, and the World, Portfolio Penguin, 2016.
[20] V. Buterin, Ethereum: A next-generation smart contract and decentralized application platform. URL: https://ethereum.org/whitepaper
[21] Z. Zheng, et al., An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data, 2017, 557–564.
[22] I. Eyal, E. G. Sirer, Majority is not enough: Bitcoin mining is vulnerable, Commun. ACM 61(7) (2018) 95–102. doi:10.1145/3212998
[23] M. Conoscenti, A. Vetro, J. C. de Martin, Blockchain for the Internet of things: A systematic literature review, in: IEEE/ACS International Conference on Computer Systems and Applications, 2016, 1–6.
[24] K. Delmolino, et al., Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, in: Financial Cryptography and Data Security, 2016, 79–94.
[25] R. Khalil, A. Gervais, Revive: Rebalancing off-blockchain payment networks, in: ACM Conference on Computer and Communications Security, 2017, 439–453.
[26] P. Petriv, I. Opirskyy, N. Mazur, Modern technologies of decentralized databases, authentication, and authorization methods, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 60–71.
[27] A. Narayanan, et al., Bitcoin and cryptocurrency technologies, Princeton University Press, 2016.