

# Method of Ensuring Data Integrity and Authenticity based on the Integration of Blockchain Technology<sup>\*</sup>

Ivan Opirskyy<sup>1,\*†</sup>, Vasyl Poberezhnyk<sup>1,†</sup> and Valeriia Balatska<sup>1,2,†</sup>

<sup>1</sup>Lviv Polytechnic National University, 12 Stepan Bandera str., 79013 Lviv, Ukraine

<sup>2</sup>Lviv State University of Life Safety, 35 Kleparivska str., 79007 Lviv, Ukraine

## Abstract

The paper is devoted to the study of a method for ensuring the integrity and authenticity of data in open information and communication environments using blockchain technology. The relevance of the topic is due to the growing requirements for guaranteeing the reliability of digital information in the conditions of decentralization, multilateral interaction and the impossibility of relying on a single center of trust. In many modern systems, such as: e-government, medicine, educational registries and financial platforms — there is a need to create an independent, immutable mechanism for confirming the source of origin and the fact of data integrity, which would not violate confidentiality and would be resistant to unauthorized interference. The research formulated a method that involves the formation of a cryptographic fingerprint of information (hash) and its digital signing by the sender, after which the fingerprint in the form of a hash value and signature is stored in the blockchain network. The data itself is transmitted via a separate channel. The recipient can verify the authenticity and integrity of the message by comparing the locally calculated hash with the reference value in the blockchain. Thus, independent, decentralized verification of information is ensured without the need to place its content in an open distributed environment. Special attention is paid to the analysis of technical and conceptual limitations of blockchain technologies, in particular the impossibility of editing records, the lack of access control, the risk of network overload and the problem of privacy. To eliminate the identified shortcomings, it is proposed to supplement the basic approach with smart contract mechanisms that allow implementing verification logic, time limits on authenticity, as well as automated access rules. An architecture with separate nodes that generate hashes automatically is proposed, which eliminates user intervention in critical stages of fingerprint formation. As a result of the work, a formal model for verifying the authenticity of data was built, a general concept of the system was developed, the mechanisms of interaction between its components were described, and the criteria for making a decision on authenticity were determined. The proposed approach ensures the immutability of evidence, resistance to forgery, the possibility of independent verification, and reduces the load on the network by moving data outside the blockchain. The practical significance of the work lies in creating a universal method that can be adapted to a wide range of information systems, where proof of the source of origin, authenticity, and integrity of digital objects are important.

## Keywords

blockchain, data integrity, authenticity, smart contract, digital signature, hashing, hardhat, nodejs, HMAC

## 1. Introduction

In the context of society digital transformation, the key challenge of information security remains ensuring the integrity and authenticity of data when stored, exchanged and used in open access information and communication environments. Traditional centralized models of data authentication, based on institutional trust in the system administrator or certification center, are increasingly demonstrating their vulnerability to internal violations, data substitution and unauthorized intervention, in particular within critical information infrastructures.

Modern regulatory and technical documents (ISO/IEC 27001, ISO/IEC 27701, NIST SP 800-53) directly indicate the need to verify the source of data, ensure its integrity at each stage of the life cycle, alongside audit the actions of access subjects. In this context, there is growing interest in decentral-

<sup>\*</sup>DECaT'2025: Digital Economy Concepts and Technologies, April 4, 2025, Kyiv, Ukraine

<sup>\*</sup>Corresponding author.

<sup>†</sup>These authors contributed equally.

✉ ivan.r.opirskyy@lpnu.ua (I. Opirskyy), vasyi.poberezhnyk@gmail.com (V. Poberezhnyk); valeriia.s.balatska@lpnu.ua, v.balatska@ldubgd.edu.ua (V. Balatska)

ORCID 0000-0002-8461-8996 (I. Opirskyy), 0000-0002-7523-2557 (V. Poberezhnyk); 0000-0002-6262-6792 (V. Balatska)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

ized technologies, in particular blockchain, which, thanks to the cryptographic consensus mechanism, immutability of records and the absence of a single control center, are potentially able to ensure trust in data without the need for trust in the parties involved in the interaction.

However, the direct usage of blockchain as a data repository is accompanied by a number of technical and conceptual limitations. The publicity of records in the blockchain contradicts the requirements for confidentiality; recording the full volume of primary data creates risks of network overload, increased transaction costs, and also makes it impossible to delete or correct erroneous records. Thus, the classic use of blockchain cannot be directly applied to the tasks of protecting personal data, confidential documentation, or official information.

Considering this, it is relevant to search for methodologies that allow realizing the potential of blockchain not for storing the data itself, but for confirming its integrity and authenticity by preserving cryptographic fingerprints. This approach involves taking data outside the blockchain network, and verification is carried out by comparing the locally calculated hash and electronic signature with the reference record in the block chain. Due to this, the effect of immutability of the proof is achieved without violating the confidentiality of the message content.

In addition to the basic mechanism of storing fingerprints in the blockchain, to eliminate the limitations associated with the lack of access control and time frames of authenticity, it is advisable to integrate smart contracts as tools for automated regulation of access rights, transaction validity periods and digital signature validity conditions. The combined use of hashing, digital signature, blockchain record storage and smart contract logic allows developing a new method of verifying the authenticity of information with a high degree of reliability, which is especially valuable for distributed registration systems, inter-organizational data exchange and protection of critical digital assets.

Thus, the purpose of this work is to formalize and substantiate a method for ensuring the integrity and authenticity of information using blockchain and smart contracts without directly storing data in the public environment. As part of the research, a conceptual model of the system was built, its advantages and limitations were analyzed, and directions for expanding the functionality by usage of contract logic were proposed.

## 2. Literature review

Ensuring the credibility of information in open and distributed information and communication systems remains one of the fundamental problems of information security. Traditional approaches based on a centralized trust model involve the use of cryptographic authentication methods, electronic digital signatures (EDS), as well as means of logging user actions and access control [1, 2]. Although these methods are effective within a homogeneous administrative domain, they are insufficient in scenarios where the parties do not have a common controller or where it is necessary to ensure data verification “post factum” without mediation.

The widespread use of blockchain technology since 2008 [3], led to new approaches to implementing indisputability, immutability, and data transparency that do not require centralized management have emergence. Studies [4, 5] have shown the potential of blockchain in areas such as finance, electronic voting, logistics, and intellectual property protection. The foundation of trust in blockchain is a consensus mechanism that ensures that records cannot be changed or deleted against the consent of the majority of network nodes.

However, studies [6, 7] point to significant limitations in using blockchain as a primary data storage, especially in cases requiring confidentiality or scalability. In particular, storing large or personalized data on a public chain violates the principles of the GDPR [8, 9] and poses risks of privacy compromise. On the technical side, limited network bandwidth, slow transaction processing, and increasing usage costs remain challenges, especially on public networks such as Ethereum or Bitcoin.

To address these issues, researchers propose the concept of off-chain verification, which involves storing only data hashes or metadata on the blockchain, while the data itself circulates off-chain [10, 11]. In such systems, authenticity is verified by comparing the hash value of the received data with

the hash stored on the blockchain. [12] demonstrates how this idea can be implemented in the context of digital certificate management systems, and [13] provides an example of medical record verification.

Moreover, important to emphasize the use of smart contracts—self-executing programs that operate within the blockchain network [14, 15]. Smart contracts allows to automate the logic of interaction between system participants, set rules for accessing resources, and limit the validity period of a transaction or verification [16, 17]. The study [18] describes models that allows to regulate user actions depending on time constraints and the cryptographic state of the system. Thus, smart contracts act as a tool for increasing the flexibility and adaptability of decentralized data verification systems.

Along with scientific works, it is worth noting examples of real-world implementations of data verification concepts using blockchain [19]: the Evernym project in the field of self-identification (Self-Sovereign Identity), the VerifyEd system for verifying academic achievements, as well as projects based on Hyperledger Indy and Fabric, which are already used to build permissioned blockchain systems.

Thus, the literature review indicates that there is a well-established trend to move away from directly storing primary data in the blockchain in favor of external verification mechanisms, with smart contracts acting as a methods of formalizing trust rules. However, the lack of a universal architecture that combines hashing, digital signature, and contract logic in an open environment indicates that there is a niche for improvement and further research.

### **3. Purpose of the research**

The purpose of this paper is to develop the method for ensuring the integrity and authenticity of data in open information environments, based on the combined technologies of blockchain and smart contracts with the transfer of data outside the blockchain network. Such a method should provide the ability to verify the authenticity of information without managing it only by storing it in the blockchain, by registering a cryptographic fingerprint (hash) and a digital signature, as well as allow for expanded access and data exchange rules using contract logic. To achieve the goal set within the scope of this paper, the following tasks are required:

1. Conduct an analysis of modern methods of ensuring data reliability and identify their vulnerabilities in the context of a decentralized environment.
2. Identify the limitations of direct application of blockchain technology for storing primary data in view of the requirements for confidentiality, efficiency, and access control.
3. Justify the feasibility of using hash functions and digital signatures as tools for constructing a verified data fingerprint.
4. Formulate a formal description of a method for verifying data integrity and authenticity using a blockchain network for storing cryptographic evidence.
5. Develop a conceptual model of the system in which the proposed method is implemented, with the identification of key functional components.
6. Explore the possibilities of integrating smart contracts into the system with the aim of eliminating the limitations of the basic method (lack of access control, centralization of fingerprint formation, etc.).
7. Assess the benefits and potential risks of implementing the proposed approach into real information and communication systems.

### **4. Main material**

The use of blockchain technology will ensure the protection of information from loss or forgery. However, due to the limitations inherent in the very nature of the technology, which are both advantages and disadvantages of the system, the main of which are the immutability of information and network transparency, the use of technology for information transmission is impractical: the growth

of the volume of data circulating in the blockchain network negatively affects the speed of the system. Another factor that negatively affects the possibility of using blockchain for the transmission of various data is the transparency of the network: anyone can view the content of the data, therefore there is a threat of unauthorized access to information when transmitted through the blockchain network itself, since the information will not only be available to any network node or external observer, but will also be stored in the system practically as long as the system itself exists.

However, considering other approaches, it is possible to develop an approach to the application of the technology in such a way that the aforementioned limitations will not affect the possibility of using blockchain technology in the scope of the information integrity and authenticity assurance without storing the data itself on the blockchain network. The idea of this method is to use the blockchain network to store not the data itself, but its fingerprint, which will allow to confirm the authenticity, integrity and immutability of the data. Such a fingerprint can be a combination of a data hash and a digital signature of the data author.

Also, the use of such an approach will allow data processing to be moved outside the blockchain network, which will reduce the load on the network, which should positively affect the speed of information processing in the blockchain network and its overall performance.

This distinction allows the use of technologies more suitable for information transmission, instead of blockchain technology, which, despite all its advantages, is an inappropriate technology in the context of transferring relatively large amounts of data.

The idea of the proposed method can be expressed by the following formula:

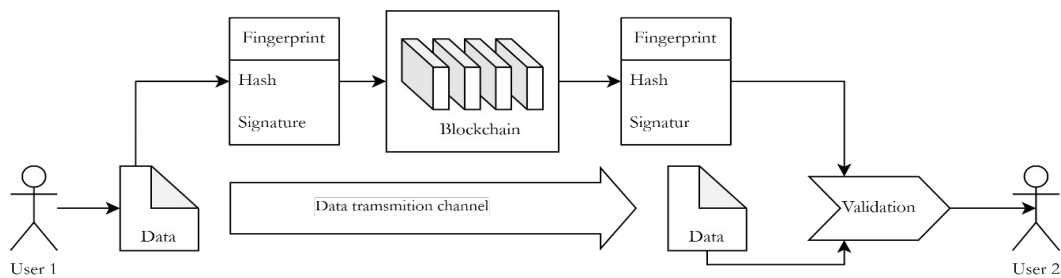
$$Informationcredible \Leftarrow (Hash(D) = H) \wedge (VSig(S, PK, D) = True), \quad (1)$$

where,  $Hash(D)$ —data hash,  $D$ —data,  $H$ —blockchain stored data hash,  $VSig(S, PK, D)$ —function of digital signature validation, which returns truth in case of validity,  $S$ —digital signature,  $PK$ —data owner public key.

It is worth noting that the advantage of such a method is that it allows to check the integrity and authenticity of information without processing to process it within the blockchain network by comparing known information fingerprints stored in the blockchain with values calculated by the recipient of the information himself.

#### 4.1. Developing of the system conception

Based on the formula 1, the concept for a system that would use the proposed method to ensure the integrity and authenticity of information can be developed. Fig.1 shows a conceptual diagram of a possible system.



**Figure 1:** The conceptual diagram of the system the uses proposed method

Considering the peculiarities of blockchain technology and the impossibility of changing the data stored in the network, it is advisable to use fingerprint multiplexing in blockchain blocks. This can be done by storing in blocks a fingerprint of not one unit of information, but several, in order to optimize the usage of blocks. Obviously, this method is limited, since the size of the block itself may be limited, for example, in the Bitcoin network size of block is limited to 1 MB, the Ether network has no limit on

the size of the block, but requires paying a commission that depends on the size of data that is going to be transmitted. Thus, technical limitations exist in the blockchain network and it is necessary to balance between the density of fingerprints in the block and the cost of maintaining the network.

The construction of an adaptive security profile is performed with careful consideration of network architecture, connection dynamics, traffic composition, and specific threat vectors. The peculiarities of an open radio environment demand rigorous oversight of authentication, encryption, access governance, and strict adherence to security policies. Essential profile

The network operation algorithm will look like this:

1. The User 1 wants to send data to the User 2.
2. The User 1 generates the data and its fingerprint.
3. The data fingerprint is stored in the blockchain network.
4. The data is sent via a data transmission channel.
5. The User 2 receives a data fingerprint from the blockchain network and data from the transmission channel.
6. The User 1 validates the data by comparing the received fingerprint from the blockchain and the independently calculated fingerprint from the data received via the transmission channel.
7. The decision on the integrity and authenticity of the data is made based on the fulfillment of two conditions: the first—the received and calculated hashes are identical, the second—the signature of the received data allows identifying the User 1 user as the author.
8. If one of the conditions is not met—the data is identified as having lost its integrity or authenticity.

Considering the algorithm of the method and its conceptual model, it can be concluded that this approach allows integrating the application of the proposed method into existing systems, since it does not require the implementation of a new method of data transmission, but can be used in combination with the existing system, as add-on that will ensure verification of data integrity and authenticity.

However, this method has some drawbacks that can affect both the performance of the method itself and the convenience of its application in different systems that may require different information processing rules. The advantages of the method include the following points:

- Immutability of information.
- Processing only data fingerprints.
- Ability to integrate into existing systems.
- No need to upload the information itself to the blockchain.
- Fingerprint calculations occur on the user side, which reduces the load on the system itself.

The disadvantages of this approach include the following points:

- Network speed depends on the size of the blockchain.
- Lack of control over the process of calculating the fingerprint.
- Possible distrust in the blockchain due to the relative novelty of the technology.
- Lack of access control.

Based on the advantages of the method, it can be concluded that it is potentially suitable for use in various areas that require secure information exchange with an emphasis on the integrity and authenticity of information. However, the aforementioned shortcomings require finding ways to solve them. One of the possible ways to comprehensively solve the shortcomings is the use of smart contracts.

## 4.2. Addressing shortcomings using a smart contract

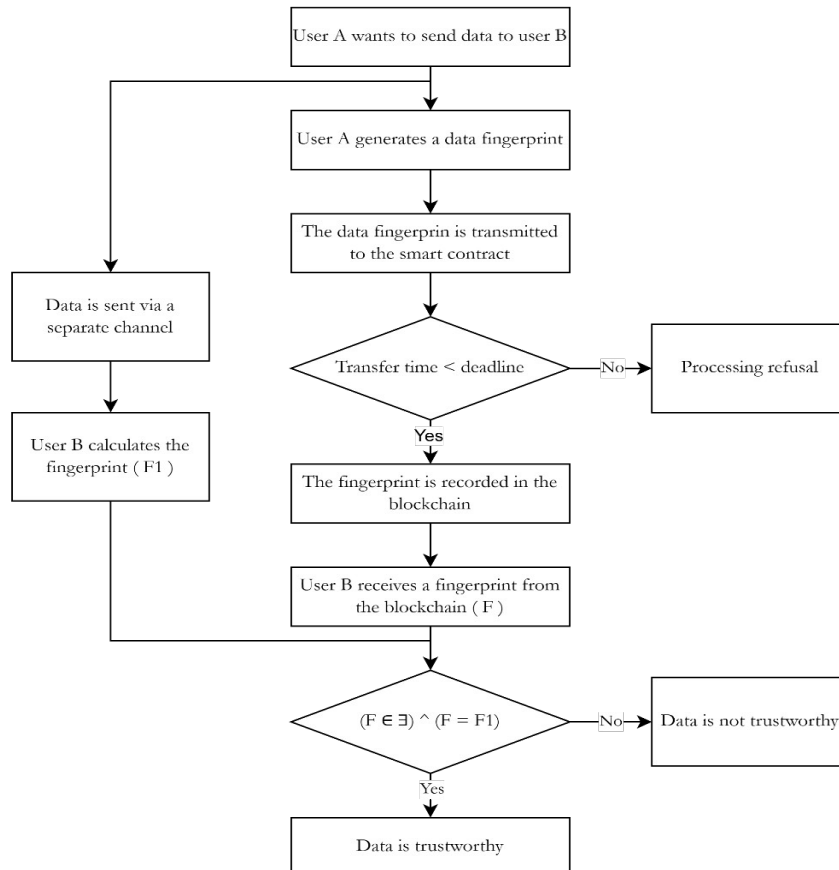
The identified advantages of the proposed method allows to consider its potential, however, the mentioned disadvantages, in particular the lack of access control, create a number of threats, for example, former users who no longer have any relationship with the system can gain access to the ability of fingerprints creation and its further transmission as legitimate due to the limitations of blockchain technology, which does not allow deleting or changing data on the network. This can lead, for example, to the reuse of signatures that are no longer relevant.

Also, the previously mentioned lack of control over the calculation of the fingerprint may raise concerns about the trustworthiness of such a fingerprint, as well as the possibility of forging such a fingerprint. Therefore, such issues must be solved, or their possible negative impact on the system must be minimized. The solution to this drawback may be the use of smart contract technology in combination with blockchain, which will significantly expand the capabilities of the system, while simultaneously solving the mentioned shortcomings.

In this approach, the function of controlling access to the system can be entrusted to smart contracts, which are self-executing code on the blockchain network that is executed when certain criteria are met in the network.

Smart contracts usage makes it is possible, for example, to create various data transmission channels that will allow transmission only between certain categories of system users or for a certain period of time. The use of technology will allow to introduction of instruments into the system that will allow expanding the functionality of the system and making its use more convenient, while leaving the possibility of using the method in combination with existing data transmission systems.

It is worth considering the algorithm of operation of such a smart contract on the example of the time interval criterion, which allows data to be transmitted as long as permission exists, and the data itself will be considered reliable, if it was sent during the existence of such permission. The algorithm of operation of such a contract is shown in Fig. 2.

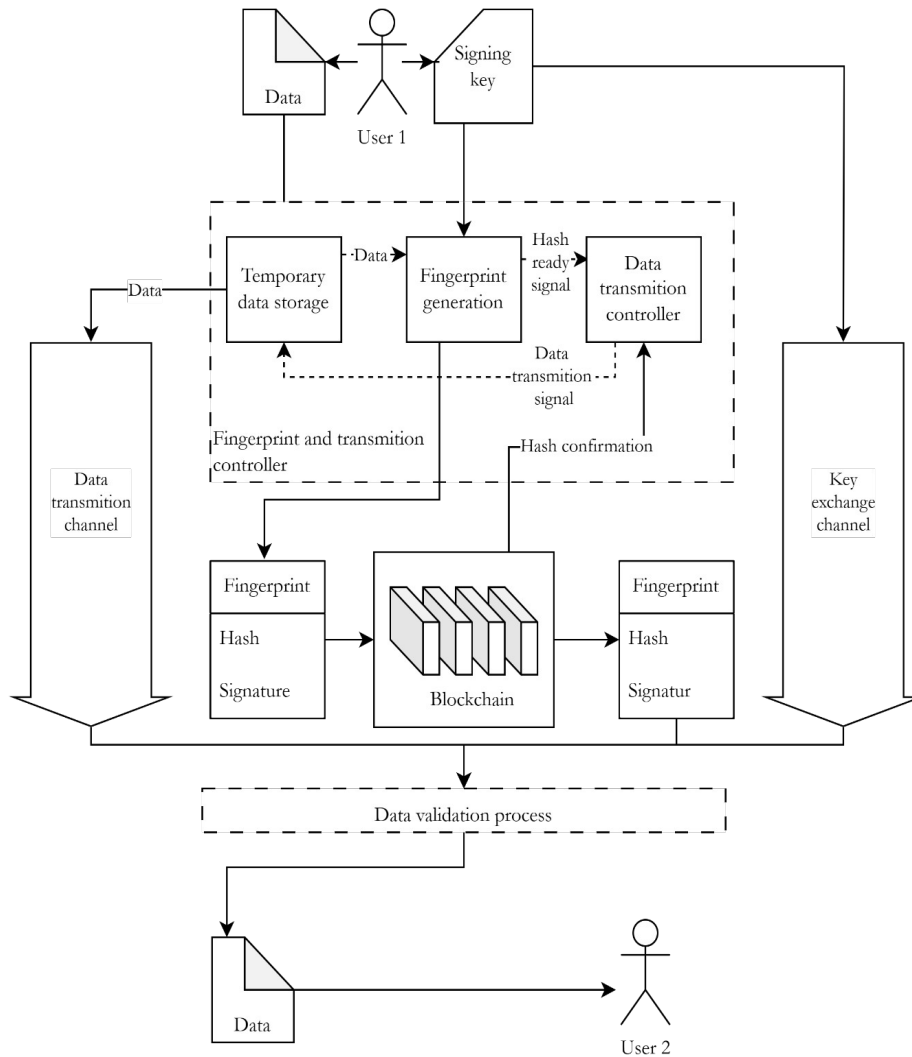


**Figure 2:** Algorithm of time based criterion algorithm

However, when smart contracts are introduced into the algorithm of the method, they allow to control the method logic itself, which not only expands the capabilities of the method, but can also introduce additional vulnerabilities if the logic itself is incorrectly implemented or designed [20].

For example, such an algorithm does not consider the possibility of introducing a fake fingerprint, since it is designed to only check the date of sending information, and considers the fingerprint itself to be authentic, which can lead to new vulnerabilities and opportunities for data forgery.

Thus, the possible solution for this problem is to automate the process of creating a fingerprint. This can be achieved by introducing additional nodes into the system, which will reduce the level of third-party interference in the system. Within this approach, the existing information transmission channels likely undergo a certain level of modifications, since it would be necessary to introduce new nodes into the system that will automatically send data through the channel after the fingerprint is formed. The concept of such system is shown in Fig. 3.



**Figure 3:** Conceptual scheme of automated system

To test the concept in action, a test system was developed that had provide the simplest system that allowed to simultaneously transmit information and confirm its integrity and authenticity using the proposed smart contract-based approach.

For this we used the following tools: Hardhat, Nodejs. Hardhat is a software package that allows to create, debug, deploy smart contracts and run local nodes of the Ethereum network or connect to the test network. Nodejs is an open-source platform that allows to develop network applications and uses the JavaScript as programming language. The entire system was designed to work in CLI mode.

The system operation can be divided into four stages:

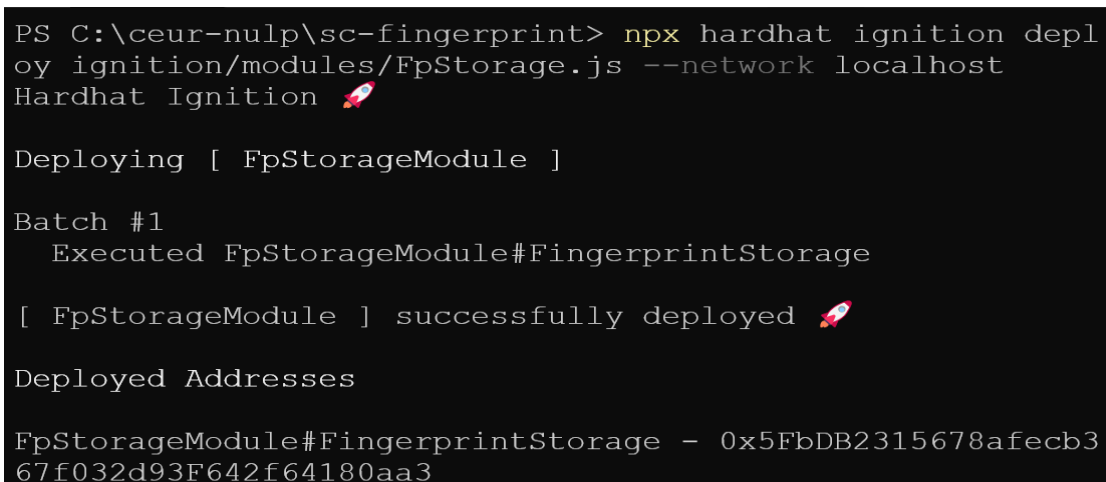
1. The user generates a data fingerprint using the HMAC-SHA256 algorithm and starts the server for data transfer.
2. The user stores a data fingerprint and a link to it in a smart contract and transmits the smart contract address to the recipient.
3. The recipient learns the fingerprint and data location data from the smart contract.
4. The recipient downloads the data and checks the integrity and reliability of the data.

The following is the smart contract code that allows you to store fingerprint data.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract FingerprintStorage {
    string private storedData;
    address private owner;
    constructor() {
        owner = msg.sender; // Set the contract deployer as owner
    }
    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner can modify data");
        _;
    }
    function setData(string memory newData) public onlyOwner {
        storedData = newData;
    }
    function getData() public view returns (string memory) {
        return storedData;
    }
}
```

The fingerprint and location information are stored in the storedData variable, and owner is used to set the owner of the smart contract. This smart contract allows to store data about a single record and only the contract owner, who is determined when the user deploys the contract on the network, can modify such data. The format of recording the data fingerprint and location information is <HMAC-SHA256>::<LOCATION>.

The process of deploying a contract to a local hardhat node is demonstrated in Fig. 4.



```
PS C:\ceur-nulp\sc-fingerprint> npx hardhat ignition deploy ignition/modules/FpStorage.js --network localhost
Hardhat Ignition 🚀

Deploying [ FpStorageModule ]

Batch #1
  Executed FpStorageModule#FingerprintStorage

[ FpStorageModule ] successfully deployed 🚀

Deployed Addresses

FpStorageModule#FingerprintStorage - 0x5FbDB2315678afecb367f032d93F642f64180aa3
```

**Figure 4:** Smart contract deploying resulting



After successful deployment, the terminal will display a message with the address of the smart contract, at which its owner will be able to perform the necessary actions with it, for example, save a data fingerprint.

For interaction with the smart contract, the `interact.js` script is used, which allow to modify the data stored in the `storedData` variable. This script should be used when the data fingerprint is generated and the location of the data itself is known, i.e. after the information is processed by the transfer server.

The next element of the system is the server, which transmits data and forms its fingerprint. JavaScript and Nodejs were used for its development. The principle of operation of the server is relatively simple—in the command line it is indicated the path to the data that needs to be transmitted. After that, it forms a data fingerprint using HMAC-SHA256, and the location from where the data can be obtained. This process is depicted in Fig. 5.

**Figure 5:** Formation of fingerprint and data location

After receiving the necessary data, you can transfer it to a smart contract, where its storage will allow you to verify the integrity and authenticity of the data. To do this, you need to use the previously mentioned script—`interact.js`. Fig. 6 shows an example of the execution of the mentioned script.

```
PS C:\ceur-nulp\sc-fingerprint> npx hardhat run scripts/interact.js --network localhost
Stored Data: 8f23ab83b92cd1fe8b0c09e45f0a36050ef357a6ec0579902b7f4c5625348ea3::localhost:8000
```

**Figure 6:** Execution of `interact.js` script, which allows to store fingerprint in smart contract

After executing the script, you can find a record of the smart contract call in the hardhat node, as shown in Fig. 7.

```
eth_sendTransaction
Contract call:      FingerprintStorage#setData
Transaction:        0x5a269c4a32dd81b245ab07ad75c27195a6d05a2cf4e48c7420896c7670a0abcc
From:               0xf39fd6e51aad88f6f4ce6ab8827279cfff92266
To:                 0x5fbdb2315678afecb367f032d93f642f64180aa3
Value:              0 ETH
Gas used:           35824 of 30000000
Block #3:           0xala8b2024d619b9be64398f5edc19a7f67b775f44b9c37f4d1877e3f2d869221
```

**Figure 7:** Information about smart contract calling

Performing these actions creates the prerequisites for ensuring the possibility of confirming the integrity and authenticity of the sent data. To transfer data, it is enough to transfer the address of the smart contract to the recipient, since the necessary information for receiving and verifying the data is contained in it.

Obtaining the fingerprint data was done by executing the `readData.js` script, which allows to get the data from the specified smart contract. The result of the work is shown in Fig. 8.

```

PS C:\ceur-nulp\sc-fingerprint> node ./scripts/
readData.js 0x5FbDB2315678afecb367f032d93F642f6
4180aa3

Stored Data: 8f23ab83b92cd1fe8b0c09e45f0a36050e
f357a6ec0579902b7f4c5625348ea3::localhost:8000

HMAC: 8f23ab83b92cd1fe8b0c09e45f0a36050ef357a6e
c0579902b7f4c5625348ea3
Location: http://localhost:8000

```

**Figure 8:** Execution of readData.js script by providing smart contract address to it and obtaining of fingerprint data

Once this information is received, the data can be loaded and its authenticity verified. This can be done using the receive.js script. Its arguments are the location of the information, the expected data fingerprint, and the key to verify. It is assumed here that such a key was already known to both parties and its value is *TestPassword*. The result of executing the script is shown in Fig. 9.

```

PS C:\ceur-nulp\transfer-server> node receive "l
ocalhost" 8f23ab83b92cd1fe8b0c09e45f0a36050ef35
7a6ec0579902b7f4c5625348ea3 TestPassword
0.00 MB of data was sent. Total elapsed time is
0.012 s
Finished getting data.
Received data IS authentic and integral

```

**Figure 9:** Execution of receive.js script and successful confirmation of data credibility

To demonstrate a negative scenario, we changed the key, for example to *YouShallNotPass*. Such a scenario is shown in Fig. 10.

```

PS C:\ceur-nulp\transfer-server> node receive "l
ocalhost" 8f23ab83b92cd1fe8b0c09e45f0a36050ef35
7a6ec0579902b7f4c5625348ea3 YouShallNotPass
0.00 MB of data was sent. Total elapsed time is
0.011 s
Finished getting data.
Received data IS NOT authentic and integral

```

**Figure 10:** Execution of receive.js with a deliberately incorrect key

Since the key with which the data was signed and the expected key are not the same, the script decides that the data is neither integral nor authentic.

The implementation of this simple data transmission system with data integrity and authenticity verification demonstrated the possibility of usage of the proposed method, as well as the possibility of using smart contracts to create methods for verifying the authenticity of information. Considering the simplicity of the implemented system, it can be concluded that it allows execution of a fairly simple data transmission and verification scenario, but it allows to confirm the possibility of the proposed method and its practical application. The analysis of the advantages and disadvantages of the proposed approach is presented in the next section.

### 4.3. Method analysis

The advantages of the method allow us to consider it as a promising method for ensuring the integrity and authenticity of information. However, one of the disadvantages inherent in this approach is the lack of data encryption, which would ensure data privacy [21]. This is due to the fact that storing encryption keys in the blockchain is impractical, since such keys will be contained in an open environment, which is a threat to privacy. Accordingly, the method of exchanging encryption keys must be implemented outside the blockchain and smart contract. However, such a disadvantage is not a criterion that would completely block the application of the method, since by providing two characteristics: authenticity and integrity, it can be used to ensure the reliability of information in systems that exchange open information and require proof of the reliability of information.

Another possible disadvantage of the method is the possibility of losing or stealing the private key that identifies the owner of the smart contract [22]. Since in blockchain systems the ability to access is completely dependent on the possession of the private key, the loss of this key can lead to a complete loss of access to the smart contract and the ability to manage the stored data [23]. The theft of this key can lead to the attacker being given full control over the smart contract, and therefore a key point in the data authentication algorithm, since in this case the attacker will be able to decide what information to add, store or delete. Both cases are dangerous from the point of view of cybersecurity, since restoring access to such keys is practically impossible, therefore, the application of the proposed method of data authentication requires a way to restore control over the smart contract.

A possible solution to this is to use a smart contract with multiple control, which requires the consent of several network participants who control it. This approach would allow for control of the smart contract through group decision-making, which could potentially allow for the addition of new contract owners, as well as the prohibition of control to accounts, which lost their private keys. However, despite the advantages of this approach, there is a possibility of collusion between users, which could lead to abuse [24].

Also, a possible drawback is the necessity to modernize existing data transmission systems when introducing automation into the algorithm of work and the method itself. In the implementation proposed in the previous section, the data and fingerprint transmission channels are independent of each other, however, if it is necessary to implement automation of signing and sending data, it will be necessary to modernize the existent data and fingerprint transmission channel. Also, a critical stage is the implementation of a secure channel for transmitting keys for signing, since they are responsible for classifying data as authentic. The solution to this problem may be the use of the Diffie–Hellman protocol, which allows transmitting keys through an unprotected environment.

Another way of solving the problem is to use a public repository with public keys that will allow to confirm the authenticity of the signature. However, when choosing this approach, it is needed to choose a different method of data verification than HMAC, since it does not provide the ability to use public keys to verify data. Such algorithms can be RSA or ECDSA, which will require changes to the data verification algorithm. This method can be appropriate when it is necessary to transfer some information to many recipients.

The advantages of the method includes its relative ease of use for simple tasks and the ability to adapt its algorithms depending on the requirements.

Also, it is worth emphasizing the double protection against data forgery, since in order to transmit malicious data and make the victim believe in its authenticity, the attacker must first steal the private

key of the contract owner, since this is the only way he can upload a false data fingerprint to the system, but also steal the private key used to generate the fingerprint itself; when using smart contracts with multiple ownership, the possibility of such a scenario is even less likely.

After analysis of the advantages and disadvantages of such a method, as well as checking the possibility of implementing the method by simulating the simplest system, we can conclude that this method can become a promising way to ensure the integrity and authenticity of information. However, it must be noted that this method is not a universal method, since more complex scenarios for using such a method may require various kinds of interventions in existing systems for their modernization in order to ensure support for the method. Therefore, the feasibility of using the proposed method and the ways of its implementation should be determined based on the tasks of the system itself, where it will be used.

## Conclusions

The study justifies an approach to ensuring the integrity and authenticity of digital data by implementing the method, which takes into account the technical and conceptual limitations of traditional centralized systems, as well as the limitations of the classic use of blockchain technologies. The proposed method is based on the formation of a cryptographic fingerprint (hash) of data and its digital signing, which provides independent verification of information without the need to store the data itself in the blockchain. This approach minimizes the risks of information disclosure, network overload, and loss of control over the verification process.

In the course of the study, a formal mathematical model of the authentication method was built, which is based on the logical verification of the hash and digital signature, which allows to unambiguously determine the fact of data modification or falsification. The conceptual architecture of the system in which this approach is implemented is studied and described, with the distribution of roles between the participants: the initiator, the network and the verifier. The simulation results prove that the computational load on the network remains low, which makes the proposed method scalable and suitable for implementation in large digital ecosystems.

Considerable attention was paid to the analysis of potential vulnerabilities, in particular, the risk of loss or compromise of the signer's keys, the lack of access control to records, as well as time limits on the validity of records. To eliminate these shortcomings, it was proposed to expand the system through smart contracts, which allow implementing authorization rules, regulation of expiration dates, conditional permissions, and group access control. A prototype of a smart contract in the Solidity language was developed, demonstrating the possibility of storing and controlling data fingerprints, with the ability to restrict access rights to modify recording by others.

The key aspect is the implementation and testing of a local proof-of-concept solution, which confirms the operability of the method in the data exchange mode between the parties via a separate channel. The interaction between the data transfer server, the formation of an HMAC fingerprint, the storage of the result in a smart contract and the subsequent verification of the data on the client side is implemented. The experimental results showed that even in the minimum configuration, the system is able to guarantee the integrity and authenticity of the transmitted data, making it impossible for it to be unauthorized modified without failing the fingerprint validation.

Cryptographic and architectural risks associated with the organization of control over a smart contract are separately analyzed. It is found that the classic single-owner contract management model is vulnerable to the loss of the private key, and also creates a risk of abuse of authority in case of compromise. The use of multi-signature models (multisig) is proposed, which provide collective contract management through a quorum of participants, and also allow the implementation of mechanisms for delegation, revocation and verification of access rights.

The results of the study conclude that the proposed method is appropriate for implementation in systems where independent verification of the source, immutability and compliance of data is required without storing them in an open environment. This approach can be used in educational certificate registries, medical record systems, electronic platforms for judicial document management, or

in supply chains where authenticity control is critical. The method does not require a complete replacement of existing systems, but can be implemented as an additional module or verification service based on an open API.

In further researches, it is advisable to expand the functionality of the proposed model by including cryptographic key exchange protocols, protection against replay attacks, and mechanisms for revocation of records through integration with decentralized identification services (DID). This will allow transforming the proposed method from a partial verification subsystem into a full-fledged digital trust platform that combines the principles of independence, resistance to falsification, and operational efficiency.

## 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] ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. International Organization for Standardization, Geneva, 2022.
- [2] NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, Gaithersburg, MD, 2020.
- [3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. URL: <https://bitcoin.org/bitcoin.pdf>
- [4] Z. Zheng, et al., An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, in: 2017 IEEE Int. Congress on Big Data (Bigdata Congress), IEEE, 2017. doi:10.1109/bigdatacongress.2017.85
- [5] M. Crosby, et al., Blockchain Technology: Beyond Bitcoin, Appl. Innov. Rev. 2 (2016) 6–10.
- [6] X. Xu, I. Weber, M. Staples, Architecture for Blockchain Applications, Springer International Publishing, Cham, 2019. doi:10.1007/978-3-030-03035-3
- [7] N. Atzei, M. Bartoletti, T. Cimoli, A Survey of Attacks on Ethereum Smart Contracts, in: Principles of Security and Trust (POST 2017), LNCS, vol. 10204, 2017, 164–186.
- [8] European Parliament and Council, Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of the European Union L119 (2016) 1–88.
- [9] M. Iavich, et al., Classical and Post-Quantum Encryption for GDPR, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 70–78.
- [10] Y. Chen, S. Ding, Z. Xu, Blockchain-based Medical Records Secure Storage and Medical Service Framework, J. Medical Syst. 43(5) (2019). doi:10.1007/s10916-018-1340-z
- [11] X. Yue, et al., Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, J. Medical Syst. 40, 218 (2016). doi:10.1007/s10916-016-0574-6
- [12] M. Sharples, J. Domingue, The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward, in: Adaptive and Adaptable Learning, Springer International Publishing, Cham, 2016, 490–496. doi:10.1007/978-3-319-45153-4\_48
- [13] A. Azaria, et al., MedRec: Using Blockchain for Medical Data Access and Permission Management, in: 2016 2<sup>nd</sup> Int. Conf. on Open and Big Data (OBD), IEEE, 2016. doi:10.1109/obd.2016.11
- [14] 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.
- [15] M. Adamantis, V. Sokolov, P. Skladannyi, Evaluation of State-of-the-Art Machine Learning Smart Contract Vulnerability Detection Method, in: Advances in Computer Science for Engineering and Education VII, vol. 242 (2025) 53–65. doi:10.1007/978-3-031-84228-3\_5



- [16] V. Buterin, A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum White Paper, 2014. URL: <https://ethereum.org/en/whitepaper/>
- [17] C. Dannen, *Introducing Ethereum and Solidity*, Apress, Berkeley, CA, 2017. doi:10.1007/978-1-4842-2535-6
- [18] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things, *IEEE Access* 4 (2016) 2292–2303. doi:10.1109/access.2016.2566339
- [19] 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.
- [20] V. Balatska, et al., Blockchain Application Concept in SSO Technology Context, in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3654, 2024, 38–49.
- [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] 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.
- [23] V. Zhebka, et al., Methodology for Choosing a Consensus Algorithm for Blockchain Technology, in: *Digital Economy Concepts and Technologies Workshop, DECaT*, vol. 3665 (2024) 106–113.
- [24] V. Balatska, I. Opirskyy, N. Slobodian, Blockchain for Enhancing Transparency and Trust in Government Registries, in: *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024)*, 2024, 50–59.