CC BY

http://dx.doi.org/10.35596/1729-7648-2025-23-6-80-86

УДК 004.75; 621.311

ИНТЕГРАЦИЯ БЛОКЧЕЙНА И ФАЙЛОВОЙ СИСТЕМЫ ДЛЯ КОНФИДЕНЦИАЛЬНОСТИ ХРАНЕНИЯ ДАННЫХ

В. А. ВИШНЯКОВ, ИВЭЙ СЯ

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. В статье рассмотрена интеграция технологий блокчейн, распределенной файловой системы и виртуализации (включая Virtual SAN, VSAN) для повышения конфиденциальности и эффективности хранения данных. Приведены ограничения традиционных централизованных моделей хранения, такие как уязвимость к фальсификации, малая гибкость в управлении доступом, сложность аудита и низкая эффективность использования ресурсов. Предложена концепция интегрированной системы хранения данных, основанная на умных контрактах в блокчейне, которая включает шифрование данных, реализацию стратегии управления доступом на основе атрибутов блокчейна, использование виртуализации с оптимизацией через VSAN, распределенное управление ключами и технологии усиления конфиденциальности (доказательство с нулевым разглашением, доверенная вычислительная среда). Предложенная архитектура обеспечивает гибкое управление доступом, эффективную обработку данных и высокий уровень безопасности в публичной или частной блокчейн-среде.

Ключевые слова: хранение данных, блокчейн, распределенная файловая система, конфиденциальность, управление доступом, умные контракты, технологии виртуализации, VSAN.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Вишняков, В. А. Интеграция блокчейна и файловой системы для конфиденциальности хранения данных / В. А. Вишняков, Ивэй Ся // Доклады БГУИР. 2025. Т. 23, № 6. С. 80–86. http://dx.doi.org/10.35596/1729-7648-2025-23-6-80-86.

INTEGRATING BLOCKCHAIN AND FILE SYSTEM FOR DATA PRIVACY

ULADZIMIR A. VISHNIAKOU, YIWEI XIA

Belarusian State University of informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. This article examines the integration of blockchain, distributed file system, and virtualization technologies (including Virtual SAN, VSAN) to improve data storage privacy and efficiency. The limitations of traditional centralized storage models are presented, such as vulnerability to tampering, limited flexibility in access control, difficulty in auditing, and low resource efficiency. A concept for an integrated data storage system based on blockchain smart contracts is proposed. This system incorporates data encryption, implementation of an access control strategy based on blockchain attributes, the use of virtualization optimized through VSAN, distributed key management, and privacy-enhancing technologies (zero-knowledge proof, trusted computing environment). The proposed architecture provides flexible access control, efficient data processing, and a high level of security in a public or private blockchain environment.

Keywords: data storage, blockchain, distributed file system, confidentiality, access control, smart contracts, virtualization technologies, VSAN.

Conflict of interests. The authors declare that there is no conflict of interests.

For quoting. Vishniakou U. A., Yiwei Xia (2025) Integrating Blockchain and File System for Data Privacy. *Doklady BGUIR*. 23 (6), 80–86. http://dx.doi.org/10.35596/1729-7648-2025-23-6-80-86 (in Russian).

Введение

Безопасность данных и защита конфиденциальности становятся ключевыми задачами на локальном и глобальном уровнях. Традиционные централизованные системы хранения сталкиваются с технологическими и доверительными вызовами при решении задач предотвращения утечек данных, защиты от внутренних угроз и соблюдения требований аудита. Технология блокчейн [1] обеспечивает неизменяемость аудиторских записей и прозрачность, распределенные файловые системы [2] предлагают избыточность данных и масштабируемость, а технологии виртуализации (включая виртуальные машины, контейнеры и виртуальные сети хранения данных (VSAN)) [3] повышают эффективность использования базовых ресурсов, упрощают управление и обеспечивают динамическое масштабирование, что позволяет оптимизировать общую производительность и эффективность системы данных.

Интеграция блокчейна и распределенных файловых систем с использованием технологий VSAN для построения виртуализированной инфраструктуры хранения данных позволяет одновременно обеспечивать конфиденциальность данных, управление доступом и гибкость в адаптации к изменениям нагрузки и распределению ресурсов. Технология VSAN объединяет традиционные устройства хранения в единый виртуализированный пул общей памяти, повышая производительность ввода-вывода, упрощая управление хранилищем. При наложении распределенных файловых систем на эту инфраструктуру под управлением политики доступа, реализованной в блокчейне, возможно создание высокопроизводительной и безопасной экосистемы хранения данных.

С развитием гипервизоров и их широким применением абстракция и виртуализация ресурсов хранения стали более практичными, что привело к появлению концепции программно-определяемого хранения (Software-Defined Storage, SDS). В этом контексте технологии VSAN предложили стандартизированные и коммерчески доступные решения для виртуализации хранения, позволяя унифицировать устройства различных типов и производителей в высокопроизводительный и гибко управляемый пул ресурсов.

Одновременно с этим распределенные файловые системы также эволюционировали. От простых сетевых файловых систем с использованием протоколов NFS, CIFS до масштабируемых структур распределенного хранения данных, таких как Hadoop Distributed File System (HDFS), а в последние годы – до децентрализованных систем контент-адресации – IPFS и Filecoin. Современные распределенные файловые системы используют контент-адресацию, избыточность данных, шифрование и механизмы стимулирования, чтобы обеспечить высокую доступность и целостность данных.

Появление платформ для умных контрактов (Ethereum) и корпоративных блокчейн-решений (Hyperledger Fabric) позволило расширить сферу применения блокчейна, включая отслеживание поставок, управление доступом к данным и подтверждение прав на данные. Блокчейн способен сохранять метаданные файлов и правила доступа в неизменяемом виде, что особенно важно для аудита и восстановления доверия.

Рассмотрим разработанную архитектуру интегрированной системы, объединяющей блокчейн и распределенную файловую систему, с использованием VSAN для построения виртуализированной и конфиденциальной инфраструктуры хранения данных. Решены задачи по детализации клиентского компонента, умных контрактов, распределенного управления ключами, распределенной файловой системы IPFS, виртуального хранилища VSAN, модуля усиления конфиденциальности и разработки алгоритма умного контракта.

Техническая концепция интеграции

Для предотвращения фальсификации данные перед загрузкой в распределенные файловые системы (IPFS, Filecoin) должны быть зашифрованы на локальном уровне. Для этого часто используются симметричные алгоритмы шифрования (AES), которые позволяют быстро зашифровать большие файлы, создавая зашифрованный текст C, и управлять сравнительно коротким симметричным ключом K. Преимущество симметричного шифрования заключается в высокой скорости операций шифрования и дешифрования. Однако безопасность хранения и передачи ключа K и управление доступом к нему становятся ключевыми задачами.

Для решения этой проблемы предлагается разработать умные контракты в блокчейне, чтобы записывать контентный идентификатор зашифрованного файла (CID), политики доступа и зашифрованный симметричный ключ Enc(K). Enc(K) может быть защищен с использованием асимметричного и атрибутивного шифрования (ABE), что позволяет получить и дешифровать ключ только тем пользователям, которые соответствуют заданной политике доступа.

Размещение политик доступа в блокчейне является ключевым этапом для реализации распределенного управления доступом. Умные контракты в блокчейне представляют собой программируемые правила, которые невозможно изменить после публикации. При запросе доступа к определенным данным пользователь должен предоставить умному контракту доказательство с нулевым разглашением (Zero-Knowledge Proof, ZKP) [4] или другие данные, соответствующие условиям политики, например, обладание определенными ролями, атрибутами или правами.

Умные контракты обрабатывают запросы, используя данные, хранящиеся в блокчейне, включая параметры политик доступа, зашифрованные ключи и метаданные. Они фиксируют процесс и результаты запросов, формируя аудит, доступный для проверки. Технология VSAN обеспечивает высокую производительность хранения, необходимую для работы узлов блокчейна, включая хранение состояния контрактов и журналов. Это позволяет умным контрактам читать и записывать данные даже при высоком уровне одновременных запросов, поддерживая стабильность и плавность работы системы. Внедрение технологии VSAN дает возможность виртуализировать устройства хранения HDD, SSD и NVMe, объединяя их в единый виртуальный пул памяти, на основе которого работают узлы распределенных файловых систем, например, IPFS [5] и Filecoin.

В сценариях управления доступом пользователи часто не хотят раскрывать излишнюю информацию о своих атрибутах или конфиденциальных данных. Технология доказательства ZKP позволяет пользователям подтверждать соответствие определенным политикам доступа, не раскрывая содержание своих атрибутов. Доверенные вычислительные среды (Trusted Execution Environment, TEE) обеспечивают выполнение чувствительных вычислений, таких как восстановление ключей и авторизация расшифровки, в изолированной аппаратной среде, предотвращая утечку открытых ключей. Использование гомоморфного шифрования (HE) [6] позволяет выполнять вычисления непосредственно с зашифрованными данными, что открывает возможности для анализа и обработки данных без их расшифровки. Для обеспечения баланса между безопасностью, производительностью и стоимостью могут быть применены следующие стратегии.

1. Оптимизация избыточности. В сценариях с низким уровнем требований к безопасности или невысокой частотой доступа можно уменьшить количество избыточных копий или использовать кодирование с исправлением ошибок [7] вместо простого дублирования. Это снижает объем занимаемого пространства, но требует дополнительных вычислительных ресурсов для обработки кодирования и декодирования.

2. Многоуровневое хранение [8]. Данные классифицируются на основе частоты доступа и требований к задержке. Горячие данные размещаются на высокопроизводительных носителях (например, SSD или NVMe), в то время как холодные данные хранятся на более дешевых устройствах или в архивных уровнях.

3. Очистка и управление жизненным циклом данных. Удаление устаревших, избыточных или неиспользуемых данных освобождает место для хранения.

4. Внеконтурное хранение (Off-Chain Storage). Основной контент хранится в распределенных файловых системах, а в блокчейне фиксируются только хеши данных.

Архитектура системы интеграции и ее работа

Предлагаемая архитектура состоит из шести компонент: клиентского блока, умных контрактов, распределенного управления ключами, распределенной файловой системы IPFS, виртуализации и VSAN, модуля усиления конфиденциальности (рис. 1). Эти компоненты обеспечивают безопасное хранение данных, выполнение политик доступа и аудит.

1. Клиентский блок предоставляет конечным пользователям интерфейс для шифрования файлов и их загрузки. Пользователь локально в своей среде (на персональном компьютере или мобильном устройстве) шифрует файл с использованием симметричного алгоритма шифрования (например, AES), создавая зашифрованный текст C и симметричный ключ K. Этот подход позволяет пользователям загружать на сервер только зашифрованные данные, что снижает риск утечки информации при их передаче или хранении.

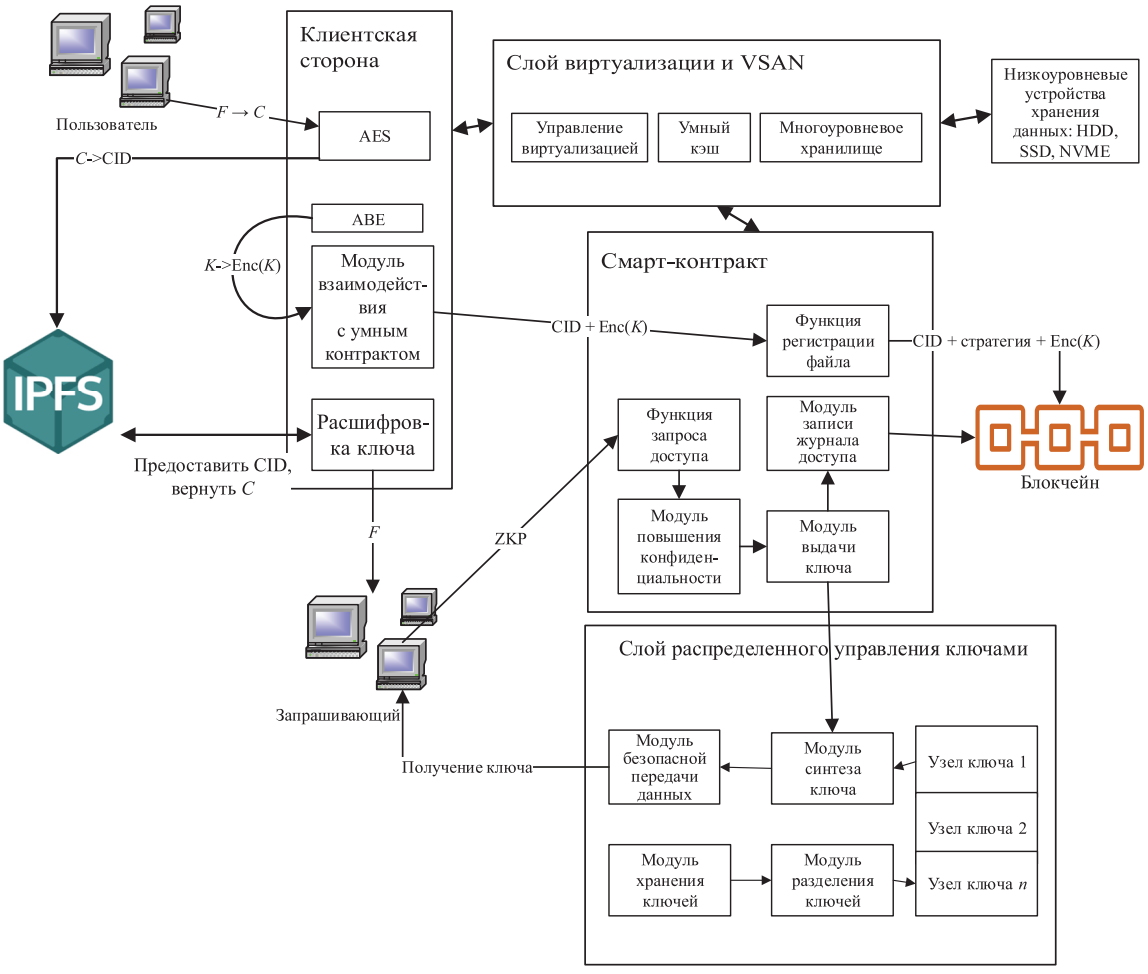

Рис. 1. Архитектура системы с распределенным управлением данными и усилением конфиденциальности
Fig. 1. System architecture with distributed data management and privacy enhancement

Клиентский интерфейс (веб-интерфейс) работает в облачной среде с поддержкой виртуализации и VSAN, что обеспечивает его масштабируемость и высокую гибкость при больших нагрузках. При загрузке файла пользователь локально шифрует исходный файл F, получая зашифрованный файл C и ключ K. Затем через клиентский интерфейс файл C отправляется в сеть IPFS, где генерируется его идентификатор CID. После этого ключ K шифруется с использованием технологии асимметричного шифрования, создавая Enc(K). Пользователь вызывает функцию RegisterFile умного контракта, чтобы записать CID, Enc(K) и политику доступа (на основе атрибутов, ролей или временных окон) в блокчейн. Это создает правила доступа и управления ключами на уровне блокчейна.

2. Умные контракты, программируемые на платформе блокчейна, предоставляют неизменяемую среду для определения политик доступа к данным, для управления ключами и аудита. Умные контракты хранят CID, Enc(K), политики доступа, выполняют проверку доступа и ведут аудит запросов. На этапе регистрации файлов пользователь вызывает функцию RegisterFile для записи CID, Enc(K) и политик доступа в блокчейн. На этапе запроса доступа пользователь отправляет запрос RequestAccess с ZKP, чтобы подтвердить соответствие политикам доступа. Умный контракт проверяет доказательство и в случае успеха уведомляет слой управления ключами для выпуска ключа K.

3. Слой распределенного управления ключами использует методы пороговой криптографии, такие как схема разделения секрета Шамира (Shamir Secret Sharing), для разделения симметричного ключа K на n фрагментов, которые хранятся на независимых узлах управления ключами. Для восстановления ключа K требуются одновременное участие не менее t фрагментов и авторизация умного контракта. После проверки доступа умным контрактом узлы управления ключами извлекают свои фрагменты ключей. Затем в TEE выполняется безопасное восстановление клю-

ча *K*, который остается защищенным от несанкционированного доступа. Полученный ключ *K* передается авторизованному пользователю через безопасный канал.

4. Слой распределенной файловой системы IPFS отвечает за фрагментацию зашифрованного файла *C* и его хранение с использованием контентного адреса. IPFS разделяет *C* на блоки данных, которые распределяются между различными узлами для повышения отказоустойчивости и доступности данных. На этапе загрузки файл *C* передается в сеть IPFS, где вычисляется хеш-функция, генерирующая CID, а блоки данных распределяются между узлами. На этапе доступа пользователь, имея ключ *K*, с помощью CID запрашивает и восстанавливает зашифрованный файл *C*, затем локально дешифрует его, получая исходный файл *F*.

5. Слой виртуализации и VSAN виртуализируют различные устройства хранения данных (HDD, SSD, NVMe), объединяя их в единый пул ресурсов. Это позволяет обеспечить высокую производительность ввода-вывода (IO) и гибкость для узлов блокчейна, IPFS и управления ключами. VSAN автоматически перераспределяет ресурсы в зависимости от нагрузки и типа данных (горячие или холодные), применяет стратегии избыточности и многоуровневого хранения. Быстрое извлечение данных из высокопроизводительных кэшей и перенос холодных данных на более дешевые устройства минимизируют задержки и оптимизируют использование ресурсов.

6. Модуль усиления конфиденциальности включает технологии доказательства с ZKP, TEE и HE. Эти технологии обеспечивают проверку доступа и управление ключами без раскрытия конфиденциальной информации. ZKP позволяет пользователю доказать соответствие политике доступа без раскрытия атрибутов. TEE обеспечивает выполнение операций восстановления ключей и других чувствительных вычислений в защищенной среде, не позволяя выполнять вычисления непосредственно над зашифрованными данными, сохраняя их конфиденциальность.

Алгоритмы смарт-контракта

Разработаны алгоритм умного контракта и его функции в управлении доступом к данным. Алгоритм работы смарт-конкракта показан на рис. 2, схема его работы включает следующие этапы.

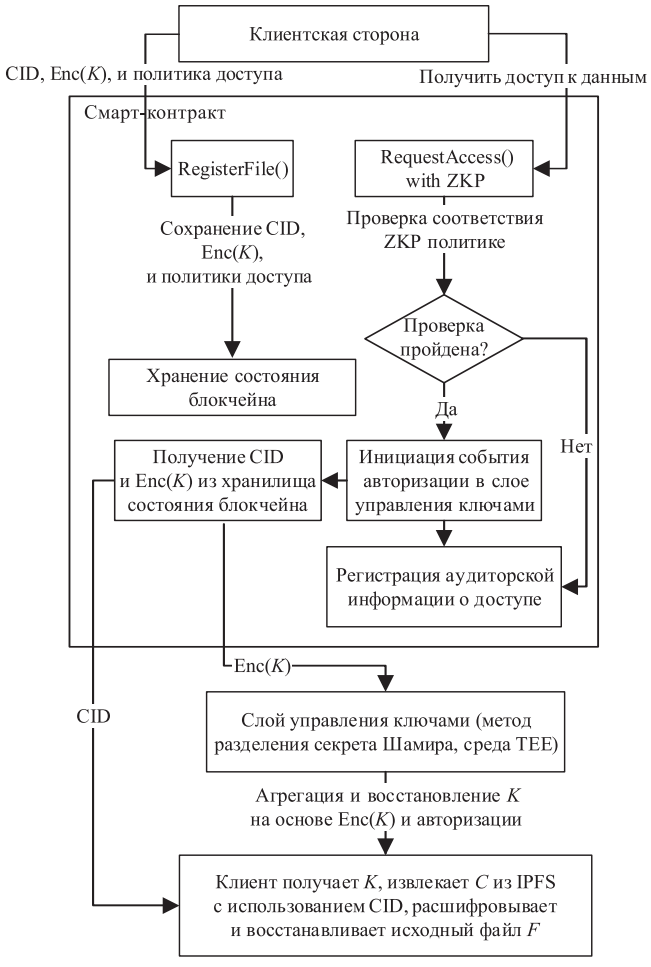

Рис. 2. Алгоритм смарт-контракта для управления доступом к данным
Fig. 2. Smart contract algorithm for data access management

A. Регистрация файлов и запись в блокчейн:

• пользователь локально шифрует файл *F* с использованием AES, получая *C* и *K*;

• ключ *K* шифруется с использованием ABE или асимметричного шифрования, создавая Enc(*K*);

• файл *C* загружается в IPFS, где вычисляется CID;

• пользователь вызывает функцию RegisterFile, чтобы записать CID, Enc(*K*) и политику доступа в блокчейн.

B. Запрос доступа и проверка:

• пользователь отправляет запрос RequestAccess с ZKP;

• смарт-контракт проверяет ZKP с использованием данных из блокчейна;

• в случае успеха смарт-контракт уведомляет о разрешении в слое управления ключами.

C. Выпуск ключа и дешифрование данных:

• узлы управления ключами извлекают фрагменты из VSAN;

• в TEE происходит восстановление ключа *K*;

• пользователь использует *K* для дешифрования *C*, восстанавливая файл *F*.

D. Аудит и управление:

• все взаимодействия записываются в блокчейне для аудита;

• системы VSAN и блокчейн совместно управляют очисткой данных и архивацией.

Заключение

1. Представлена архитектура хранения данных, основанная на интеграции технологий блокчейн, распределенных файловых систем и виртуализации/VSAN, направленная на повышение конфиденциальности данных, гибкости управления доступом и производительности системы. Определение политик доступа в умном контракте и шифрование данных с их хранением в распределенных файловых системах, дополненное технологиями усиления конфиденциальности (ZKP, TEE, HE) и поддержкой виртуализированного пула хранения VSAN, позволяют создать высокозащищенную, масштабируемую систему хранения и доступа к данным.

2. Разработан алгоритм умного контракта, включающий шифрование файла *F* и запись CID, Enc(*K*), политики доступа в блокчейн. При запросе доступа от пользователя умный контракт проверяет ZKP с использованием данных из блокчейна, при успехе уведомляет о разрешении слой управления ключами, последний извлекает фрагменты из хранилища VSAN (ключ *K* для восстанавливая исходного файл *F*). Все взаимодействия записываются в блокчейне для аудита.

3. Архитектура интегрированной системы состоит из шести компонент: клиентского блока, умных контрактов, распределенного управления ключами, распределенной файловой системы IPFS, визуализации и VSAN, модуля усиления конфиденциальности. Она выполняет регистрацию файлов и запись в блокчейне, запрос доступа и проверку, выпуск ключа и дешифрование данных, аудит и управление. Преимущества этой системы перед аналогами заключаются в обеспечении конфиденциальности данных и баланса между безопасностью, производительностью и стоимостью за счет оптимизации избыточности, многоуровнего хранения и управления жизненным циклом данных, в их защите благодаря криптографии блокчейна.

Список литературы

1. Вишняков, В. А. Использование блокчейна Ethereum в сети интернета вещей для IT-диагностики / В. А. Вишняков, Ивэй Ся, Чуюэ Юй // Цифровая трансформация. 2024. Т. 30, № 3. С. 61–68. http://dx.doi.org/10.35596/1729-7648-2024-30-3-61-68.
2. Pan, X. Navigating the Landscape of Distributed File Systems: Architectures, Implementations, and Considerations / X. Pan, Z. Luo, L. Zhou // arXiv preprint arXiv:2403.15701. 2024.
3. Современные технологии хранения данных в условиях Industry 4.0 / В. А. Касумов [и др.] // Доклады БГУИР. 2024. Т. 22, № 5. С. 95–103. http://dx.doi.org/10.35596/1729-7648-2024-22-5-95-103.
4. Kalbantner, J. ZKP Enabled Identity and Reputation Verification in P2P Marketplaces / J. Kalbantner // 2024 IEEE International Conference on Blockchain (Blockchain). 2024. P. 591–598.
5. A Closer Look into IPFS: Accessibility, Content, and Performance / R. Shi [et al.] // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2024. Vol. 8, No 2. P. 1–31.
6. Sok: Fully Homomorphic Encryption Accelerators / J. Zhang [et al.] // ACM Computing Surveys. 2024. Vol. 56, No 12. P. 1–32.

7. Data Repair Accelerating Scheme for Erasure-Coded Storage System Based on FPGA and Hierarchical Parallel Decoding Structure / J. Chen [et al.] // Cluster Computing. 2024. Vol. 2. P. 1–21.
8. Cloud Storage Cost: A Taxonomy and Survey / A. Q. Khan [et al.] // World Wide Web. 2024. Vol. 27, No 4.

Поступила 29.09.2025 Принята в печать 14.11.2025

References

1. Vishniakou U. A., Ywey Xia, Chuey Yu (2024) Using the Ethereum Blockchain in the Internet of Things Network for IT Diagnostics. *Digital Transformation*. 30 (3), 61–68. http://dx.doi.org/10.35596/1729-7648-2024-30-3-61-68 (in Russian).
2. Pan X., Luo Z., Zhou L. (2024) Navigating the Landscape of Distributed File Systems: Architectures, Implementations, and Considerations. *ArXiv preprint arXiv:2403.15701*.
3. Gasimov V. A., Aliyeva Sh. Kh., Garashli T. J., Asadova M. Y. (2024) Modern Data Storage Technologies in the Context of Industry 4.0. *Doclady BGUIR*. 22 (5), 95–103. http://dx.doi.org/10.35596/1729-7648-2024-22-5-95-103 (in Russian).
4. Kalbantner J. (2024) ZKP Enabled Identity and Reputation Verification in P2P Marketplaces. *IEEE International Conference on Blockchain (Blockchain).* 591–598.
5. Shi R. A., Cheng R., Han B., Cheng Y., Chen S. (2024) Closer Look into IPFS: Accessibility, Content, and Performance. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*. 8 (2), 1–31.
6. Zhang J., Cheng X., Yang L., Hu J., Liu X., Chen K. (2024) Sok: Fully Homomorphic Encryption Accelerators. *ACM Computing Surveys*. 56 (12), 1–32.
7. Chen J., Yang S., Wang Y., Ye M., Lei F. (2024) Data Repair Accelerating Scheme for Erasure-Coded Storage System Based on FPGA and Hierarchical Parallel Decoding Structure. *Cluster Computing.* 2, 1–21.
8. Khan A. Q., Matskin M., Prodan R., Bussler C., Roman D., Soylu A. (2024) Cloud Storage Cost: A Taxonomy and Survey. *World Wide Web.* 27 (4).

Received: 29 September 2025 Accepted: 14 November 2025

Вклад авторов

Вишняков В. А. выполнил постановку задачи, предложил концепцию интеграции, предоставил информацию о выбранной экспериментально платформе интернета вещей.

Ивэй Ся разработал алгоритм смарт-контракта, провел детализацию архитектуры.

Author's contribution

Vishniakou U. A. completed the task statement, proposed the concept of integration, and provided information about the experimentally selected Internet of things platform.

Yiwei Xia developed the algorithm for a smart contract, carried out a detailed architecture.

Сведения об авторах

Вишняков В. А., д-р техн. наук, проф. каф. инфокоммуникационных технологий, Белорусский государственный университет информатики и радиоэлектроники

Ивэй Ся, асп. каф. инфокоммуникационных технологий, Белорусский государственный университет информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 44 486-71-82
E-mail: vish@bsuir.by
Вишняков Владимир Анатольевич

Information about the authors

Vishniakou U. A., Dr. Sci. (Tech.), Professor at the Department of Infocommunication Technologies, Belarusian State University of Informatics and Radioelectronics

Yiwei Xia, Postgraduate at the Department of Infocommunication Technologies, Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 44 486-71-82
E-mail: vish@bsuir.by
Vishniakou Uladzimir Anatolievich