DOI 10.37882/2223-2966.2025.02.03

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМЫ ВЕРИФИКАЦИИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЁННОГО РЕЕСТРА

COMPARATIVE ANALYSIS OF THE DATA VERIFICATION SYSTEM USING DISTRIBUTED REGISTRY TECHNOLOGY

M. Altynnikov
D. Sachkov
Yu. Shishkin

Summary. The article discusses the possibilities of using distributed network technology to improve the security, transparency, and efficiency of educational data verification. The analysis of the educational result verification system is carried out with a focus on identifying the key aspects that need to be improved to ensure the reliability and transparency of verification processes. The integration of a system using IPFS and distributed networks for decentralized data storage and verification based on cryptographic methods is proposed. Special attention is paid to the system architecture, component interaction mechanism and algorithms to automate the verification process and strengthen the trust in educational outcomes within the learner's digital footprint.

Keywords: system analysis, distributed networks, verification, higher education institutions, digital footprint, decentralization, IPFS, data management, automation, cryptographic methods.

Алтынников Максим Сергеевич
Аспирант, Иркутский Государственный Университет Путей Сообщения
altynnikovms@yandex.ru
Сачков Дмитрий Иванович
кандидат экономических наук, доцент, проректор по цифровым технологиям, Иркутский Государственный Университет Путей Сообщения
sachkov_di@irgups.ru
Шишкин Юрий Николаевич
кандидат технических наук, начальник управления информатизации, доцент, Иркутский Государственный Университет Путей Сообщения
shishkin_yn@irgups.ru

Аннотация. В статье рассматриваются возможности применения технологии распределённых сетей для повышения безопасности, прозрачности и эффективности проверки образовательных данных. Проведён анализ системы верификации образовательного результата с акцентом на выявление ключевых аспектов, требующих улучшения для обеспечения надёжности и прозрачности процессов проверки. Предложена интеграция системы, использующей IPFS и распределённые сети, для децентрализованного хранения и верификации данных на основе криптографических методов. Особое внимание уделено архитектуре системы, механизму взаимодействия компонентов и алгоритмам, что позволяет автоматизировать процесс проверки и укрепить доверие к образовательным результатам в рамках цифрового следа обучающегося.

Ключевые слова: системный анализ, распределённые сети, верификация, высшие учебные заведения, цифровой след, децентрализация, IPFS, управление данными, автоматизация, криптографические методы.

Цифровой след (в образовании) — данные об обучающемся и его активностях, включающие в том числе видео и аудиозаписи, данные о хронологии взаимодействия с различными средствами обучения и воспитания, о хронологии взаимодействия с другими участниками отношений в сфере образования и информацию о таком взаимодействии, в том числе о полученных квалификациях, о последующем трудоустройстве и профессиональной деятельности, рецензиях и оценках, а также о результатах обучения с использованием учебно-методических данных, представленные в электронном цифровом формате. Все эти наборы данных можно объединить в одну группу — образовательный результат.

Так на примере перечня источников, технических средств, элементов, и показателей для целей сбора цифрового следа в стандарте «Информационно-коммуникационные технологии в образовании. Цифровой след. Общие положения» версия 1.0.3 Университета НТИ «20.35» [4] представлено более 100 источников из которых могут формироваться набор данных о обучающемся. В итоге мы получаем что по одному человеку может быть сформирован значительный набор данных в количественном измерении. Это позволяет в процессе непрерывного образования, использовать для структурирования описания и идентификации, эффективного поиска и применения электронных образовательных ресурсов в электронных информационно-образовательных средах.

Цифровой след может быть, как положительным, так и отрицательным. С одной стороны, он может помочь

в персонализации образовательного процесса и улучшении качества обучения. С другой стороны, важно учитывать вопросы конфиденциальности и безопасности данных, а также необходимость обеспечения верификации и достоверности данных.

Защита цифрового следа в образовании — важная задача, которая требует внимания как со стороны образовательных учреждений, так и самих обучающихся.

В данной статье предлагается рассмотреть вопрос организации решение проблем, связанных с мошенничеством при проверке образовательного результата в контексте цифрового следа обучающегося. Традиционные методы проверки подлинности таких данных часто оказываются дорогостоящими, требуют значительных временных затрат и подвержены риску подделки.

Под системой понимается совокупность элементов, находящихся в отношениях и связях друг с другом для прохождения процесса верификации образовательного результата. В предложенной системе используются преимущества технологии распределенного реестра, включая защиту от несанкционированного доступа и прозрачность записей, для создания надежного и эффективного способа верификации цифровых результатов образовательного процесса.

Система обеспечивает подлинность данных, предотвращает их фальсификацию и другие формы мошенничества, а также способствует прозрачности и подотчетности. Разработка данной системы ориентирована на повышение эффективности, точности и безопасности верификации данных, связанных с результатами обучения. Это, в свою очередь, усиливает доверие к подтвержденным результатам, предоставляемым образовательными учреждениями и различными организациями.

Обзор литературы

Исследование Тианы Лоуренс (2017) показывает, что распределенный реестр представляет собой структурированную информацию, используемую как цифровая книга, содержащая данные, которыми можно делиться с участниками независимой сети.

Ченг, Ли, Чи и Чен (2018) в своей работе «Смарт-контракт для цифровых сертификатов» предложили использовать блокчейн для предотвращения подделок сертификатов, позволяя проверять подлинность цифровых сертификатов и минимизировать подделки, а также применять QR-коды и коды запросов, прикрепляемые к бумажным сертификатам.

В исследовании JS Callan и его коллег (2019) рассматривались методы применения распределенного реестра для обеспечения цифровыми сертификатами устройств Интернета вещей (IoT) без использования центрального удостоверяющего центра. Дева Аю Дита Витами и И Ваян Суартана (2019) выяснили, что восприятие полезности, простоты использования и риска положительно влияет на интерес студентов к блокчейн-системам. Чем выше удобство использования, тем сильнее интерес к данной технологии.

Пол Дж. Тейлор Туска, Даргахи Али и их соавторы в обзоре литературы по кибербезопасности распределенного реестра рассматривают его использование для повышения безопасности в IoT, таких как визуализация сети, криптография с открытым ключом, схемы сертификации и безопасное хранение данных.

В исследовании И. Бандары, Ф. Иораса и МП Аррайзы (2018) анализируются базы данных, реплицируемые и синхронизируемые для валидации в интернете. Архитектура, предложенная авторами, использует децентрализованную систему совместной проверки.

Несмотря на то, что в этих исследованиях рассматривается использование технологии распределенного реестра для аутентификации в различных сферах, необходимо продолжить изучение масштабируемости и совместимости распределенных систем. С увеличением распространения технологии распределенного реестра становится важным обеспечить способность этих систем эффективно обрабатывать большие объемы данных и транзакций, а также интегрироваться с другими системами. Следовательно, будущие исследования могут сосредоточиться на оценке производительности и масштабируемости распределенных решений, особенно в таких областях, как образование, где объем данных значительно велик. Помимо этого, важно будет исследовать методы интеграции распределенного реестра с другими технологиями, чтобы обеспечить совместимость и беспрепятственный обмен данными, что сыграет ключевую роль в успешном внедрении и функционировании таких систем на практике.

Настоящая статья посвящена анализу преимуществ и вызовов при переходе системы верификации данных в высших учебных заведениях на распределенный реестр с использованием IPFS, а также обсуждению ключевых аспектов его внедрения для повышения эффективности и безопасности процессов управления данными.

Анализ существующей системы

В настоящее время в образовательной сфере России широко применяется система верификации данных с использованием электронной подписи. Это стало возможным благодаря активному внедрению цифровых технологий и нормативной базе, поддерживающей их использование.

Система верификации данных на основе электронной подписи (ЭП) использует криптографию для подтверждения подлинности данных и идентификации подписанта. Этот процесс позволяет удостоверить, что данные были подписаны определённым лицом и не были изменёны после подписания. Система работает на основе использования криптографических ключей, а именно пары открытого и закрытого ключей.

Принцип работы системы электронной подписи

Электронная подпись использует пару криптографических ключей: закрытый, который применяется для создания подписи и хранится в секрете, и открытый, доступный для проверки подписи. При подписании данных сначала вычисляется их хэш с помощью хэш-функции (например, SHA-256) [8], затем этот хэш шифруется закрытым ключом, образуя подпись. Для проверки используется открытый ключ: расшифрованный хэш сравнивается с хэшем исходных данных, что подтверждает подлинность подписи и неизменность данных.

Система электронной подписи опирается на инфраструктуру открытых ключей (ИОК), включающую удостоверяющие центры, которые выдают цифровые сертификаты, связывающие открытый ключ с конкретным лицом или организацией. Однако для эффективного использования системы необходимо учитывать особенности: обеспечение защиты закрытого ключа, сложность внедрения, срок действия ключей и возможные проблемы совместимости между разными платформами.

Анализ предлагаемой системы

Предлагаемая система позволит организации безопасно передавать защищаемые данные для удалённой верификации и, как следствие, повысит качество предоставляемых услуг и общую производительность. Разрабатываемая система будет использовать архитектуру распределенной сети, что обеспечит высокий уровень безопасности данных и гарантирует, что доступ к ним будет предоставлен только тем участникам, которые действительно имеют интерес к этой информации.

Так же для хранения хэш функций будет использоваться технология IPFS.

Система верификации набора данных на основе IPFS (InterPlanetary File System) использует децентрализованную технологию хранения и распространения данных, чтобы обеспечить целостность, доступность и подлинность.[8] В отличие от традиционных методов, таких как электронные подписи, IPFS фокусируется на хранении данных и их метаданных в распределенной сети, что обеспечивает высокую степень децентрализации.

Предложенная архитектура IPFS системы с поддержкой распределённой сети включает 3 ключевых компонента: 1. Узлы IPFS, 2. Контракт для верификации по хэшам, 3. Распределенная сеть На рисунке 1 представлено, как эти три компонента взаимодействуют в рамках единой системы, обеспечивая её целостность и устойчивость.

1. Узлы IPFS: Эти узлы образуют децентрализованную сеть, которая служит распределенным хранилищем для реальных наборов данных. Файлы загружаются на узлы, которые совместно хранят и реплицируют данные в виде отдельных объектов. Использование IPFS позволяет сократить затраты на хранение и ускоряет доступ к данным за счёт распределенного хранения, избегая избыточного дублирования, даже при значительных объемах данных.

Каждый объект данных в IPFS может содержать до 256 КБ. Если объем данных превышает этот размер, они разбиваются на несколько связанных объектов IPFS, которые объединяются для обеспечения целостности данных [10]. Для доступа к данным в сети используются идентификаторы содержимого (CID) (Рисунок 2), которые позволяют находить и извлекать оригинальные наборы данных из IPFS.[9]

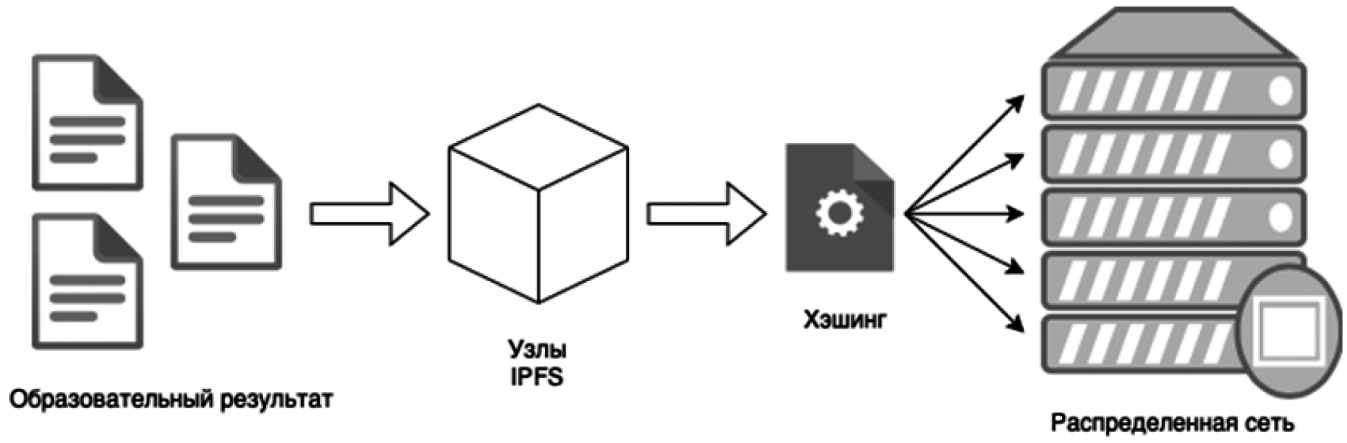

Рис. 1. Механизм взаимодействия компонентов системы

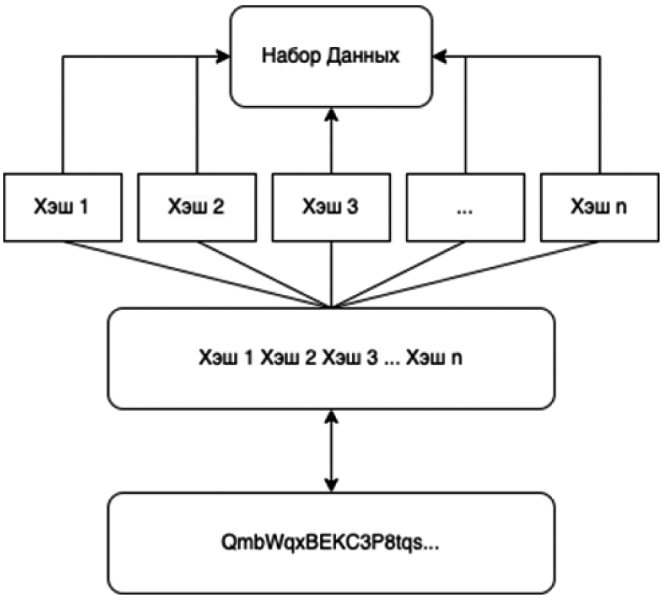

Рис. 2. Моделирование CID IPFS

2. Процесс верификации включает несколько этапов (Рисунок 3):

Добавление данных: Пользователь загружает файл в IPFS — децентрализованное хранилище, которое присваивает данным уникальный хэш (похожий на цифровой отпечаток). Этот хэш указывает на конкретный данные и позволяет его быстро найти в сети IPFS. Затем пользователь добавляет этот IPFS-хэш в распределенную сеть через контракт. Распределенная сеть, в свою очередь, хранит информацию о данных, включая IPFS-хэш и данные об пользователе.

Проверка данных: Любой пользователь может запросить у системы информацию о данных, используя его хэш. Система проверяет, есть ли они в базе, и если да, то сообщает: когда данные были добавлены, кто его добавил и где его можно найти в IPFS.

Удаление данных: Авторизованный пользователь может удалить хранящиеся хэши из распределенного реестра, при условии, что они были загружены им же.

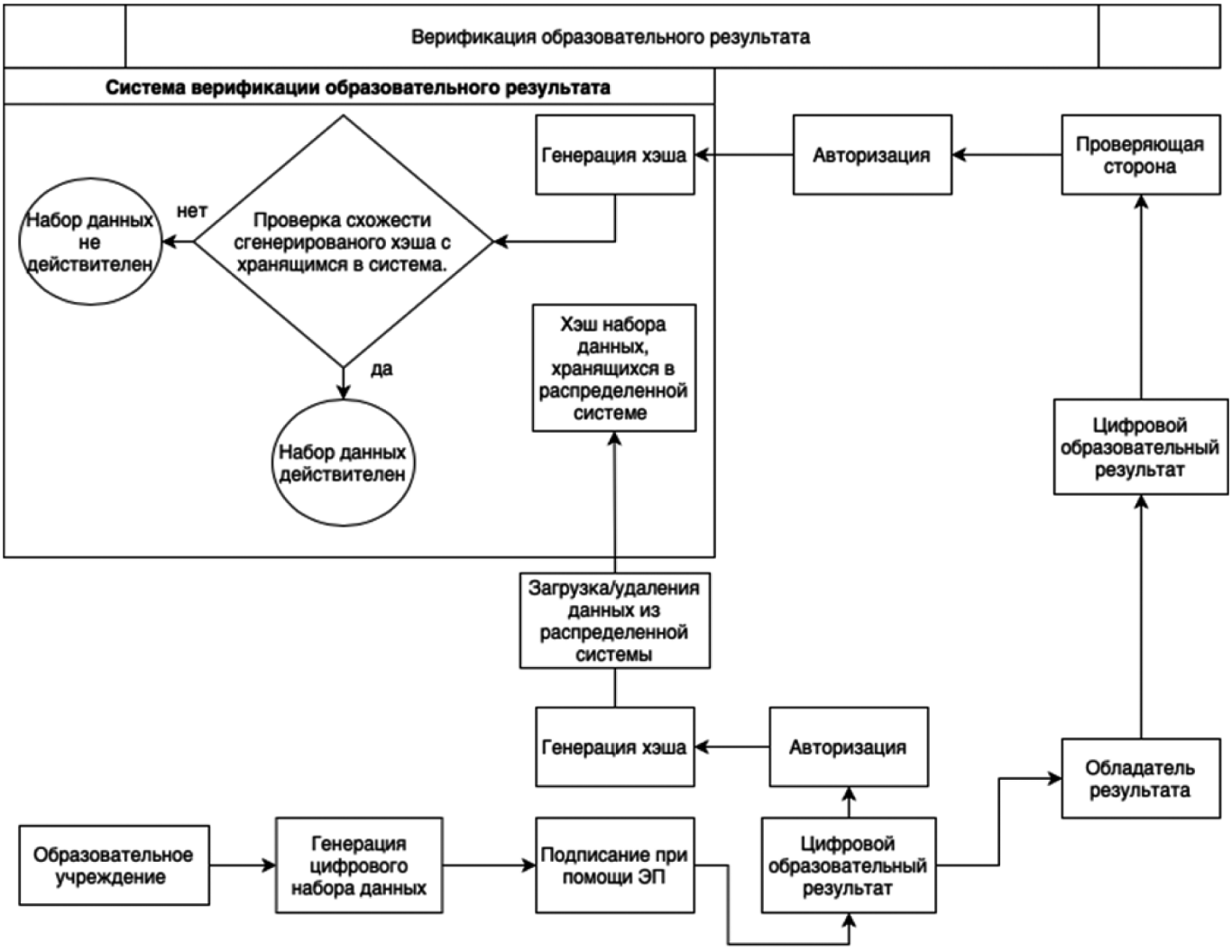

Рис. 3. Модель системы верификации

Для работы системы предлагается использовать смарт-контракт на языке Solidity для управления экспортными данными в децентрализованной системе. В дополнение к этому, для визуализации и описания бизнес-логики процессов может быть применён Язык моделирования бизнес-процессов (IDFE0).

Важные моменты:

- Владелец контракта имеет полные права на добавление и удаление пользователя, а также может изменять информацию об пользователях.
- Пользователи могут добавлять документы в систему, но только если они были зарегистрированы в контракте, и только если их информация совпадает с информацией, указанной в записи данных.
- Контракт использует хэши данных для их уникальной идентификации и для взаимодействия с системой хранения файлов IPFS.

В данной работе разработана уникальная модель верификации образовательных результатов, основанная на технологии распределенных сетей, которая значительно улучшает процесс проверки подлинности данных. Эта система повышает безопасность, достоверность и конфиденциальность образовательных документов, минимизируя риски подделки. Предложенная модель выгодна как для образовательных учреждений, выдающих подтверждения об образовательных достижениях, так и для студентов и работодателей, использующих эти данные. Ее ключевым преимуществом является хранение всей необходимой для проверки информации в распределенной сети, что исключает возможность несанкционированного изменения данных. Кроме того, данная модель прекрасно вписывается в концепцию цифрового следа, предоставляя возможность пользователям отслеживать и подтверждать историю своих образовательных достижений с высоким уровнем доверия к данным.

ЛИТЕРАТУРА

1. Алтынников М.С. Использование блокчейн технологии в организации систем в образовательных учреждениях / М.С. Алтынников // World of science: сборник статей VI Международной научно-практической конференции, Пенза, 30 ноября 2023 года. — Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. — С. 83–86. — EDN CVVKSB.
2. Сачков Д.И. Создание единого технологического решения автоматизации деятельности образовательных организаций / Д.И. Сачков, Ю.Н. Шишкин, А.А. Шедиков // Baikal Research Journal. — 2024. — Т. 15, № 1. — С. 205–213. — DOI 10.17150/2411–6262.2024.15(1).205-213. — EDN TBGQWM.
3. Архитектура IBM Hyperledger Fabric. [Электронный ресурс]: URL https://www.ibmskillsacademy.com/.
4. «Информационно-коммуникационные технологии в образовании. Цифровой след. Общие положения» версия 1.0.3 Университета НТИ «20.35»
5. Consensus Algorithm (Proof-of-Work). [Электронный ресурс] URL: https://cointelegraph.com/explained/proof-of-work-explained (дата обращения: 15.9.2024).
6. Дегтярев Ю.Н. Системный анализ и исследование операций // учебник. М.: Высш. шк., 1996. — С. 335.
7. Cynthia Dwork, Moni Naor Pricing via Processing or Combatting Junk Mail // The Weizmann Institute of Science [Электронный ресурс] URL: wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf (дата обращения: 4.9.2024)
8. Способ контроля целостности данных на основе применения хэш-функции по принципу сочетаний хэш-значений / А.О. Лачинов, А.В. Решотка, А.В. Лавриненко [и др.] // Информатика: проблемы, методы, технологии : Материалы XXI Международной научно-методической конференции, Воронеж, 11–12 февраля 2021 года. — Воронеж: Общество с ограниченной ответственностью «Вэлборн», 2021. — С. 991–996. — EDN ZUKSFO.
9. Dwivedi S.K. Smart contract and IPFS-based trustworthy secure data storage and device authentication scheme in fog computing environment / S.K. Dwivedi, R. Amin, S. Vollala // Peer-to-Peer Networking and Applications. — 2023. — Vol. 16, No. 1. — P. 1–21. — DOI 10.1007/s12083-022-01376-7. — EDN YWLIYG.

© Алтынников Максим Сергеевич (altynnikovms@yandex.ru); Сачков Дмитрий Иванович (sachkov_di@irgups.ru);
Шишкин Юрий Николаевич (shishkin_yn@irgups.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»