



Научная статья

УДК 378

DOI: 10.25688/2072-9014.2022.62.4.05

## ИССЛЕДОВАНИЕ СИСТЕМЫ ТОКЕНИЗАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ СТУДЕНТОВ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Светлана Владимировна Маркова

Финансовый университет при Правительстве РФ, Москва, Россия

svmarkova@fa.ru

**Аннотация.** В данной работе рассмотрены основные проблемы использования частных и публичных блокчейнов для токенизации персональных студенческих данных. Цель исследования: найти альтернативные подходы для токенизации персональных данных студентов и организации безопасного доступа к ним. Задачи исследования: 1) предложить архитектуру системы токенизации персональных данных студентов; 2) разработать и выполнить тестирование прототипа студенческой информационной системы, то есть децентрализованного распределенного приложения (DApp).

**Ключевые слова:** токенизация; блокчейн; студенческие информационные системы; персональные данные студентов.

## Original article

UDC 378

DOI: 10.25688/2072-9014.2022.62.4.05

**A STUDY OF THE TOKENIZATION SYSTEM  
OF STUDENTS' PERSONAL DATA BASED  
ON BLOCKCHAIN TECHNOLOGY****Svetlana V. Markova**

Financial University under the Government of the Russian Federation, Moscow, Russia

svmarkova@fa.ru

**Abstract.** This study examines the major challenges of using private and public blockchains to tokenize personal student data. In this regard. The purpose of the study: Find alternative approaches for tokenizing students' personal data and organizing secure access to them. Research objectives: 1) to propose the architecture of the system of tokenization of students' personal data; 2) develop and test a prototype student information system, i. e. a decentralized distributed application (DApp).

**Keywords:** tokenization; blockchain; student information systems; student personal data.

**Для цитирования:** Маркова, С. В. (2022). Исследование системы токенизации персональных данных студентов на основе технологии блокчейн. *Вестник МГПУ. Серия «Информатика и информатизация образования»*, 4(62), 58–74. DOI: 10.25688/2072-9014.2022.62.4.05

**For citation:** Markova, S. V. (2022). A study of the tokenization system of students' personal data based on blockchain technology. *MCU Journal of Informatics and Informatization of Education*, 4(62), 58–74. <https://doi.org/10.25688/2072-9014.2022.62.4.05>

**Введение**

**Б**локчейн открывает новые горизонты для достижения целостности данных с использованием децентрализованных и хорошо обслуживаемых хранилищ данных. Блокчейн может быть реализован в рамках автоматизированных систем управления отдельными вузами или группами учебных заведений.

Образование — это ключевая область, в которой разные заинтересованные стороны должны обмениваться и изменять общую информацию. Изменение записей может происходить на разных уровнях безопасности. Мотивация использования блокчейна в студенческих информационных системах (далее — СИС) исходит из растущей потребности в обеспечении высокой безопасности и доверия к таким критически важным системам. Кроме того, блокчейн-система делает упор на использование децентрализованного, надежного и высоконадежного леджера, в котором хранится жизненно важная информация.

Несмотря на заметное развитие технологий, растет потребность в надежности и целостности данных. Студенты будут иметь полную независимость при работе со своими персональными данными в блокчейне. Это обеспечит студентам полную независимость от учебного заведения, а также полный контроль за их данными при сохранении целостности и неизменности данных. Блокчейн хранит постоянно записываемые и шифрующиеся данные с использованием криптографических технологий, в децентрализованных блоках [1; 2]. Криптографические процедуры, используемые при генерации блоков и соединении блоков, повышают безопасность каждой транзакции блокчейна, а данные, записанные в блокчейне, являются неизменными записями, состояния которых не могут быть изменены после их создания. Безопасность, устойчивость и необратимость — все это связано с неизменностью [3–5].

Перспективы блокчейна в образовании простираются гораздо дальше, позволяя учащимся добавлять анонимность в свои личные данные, независимость от учебного заведения, неизменность записей официальных документов и сертификатов, а также полное доверие точности и непогрешимости благодаря сетевому дизайну [6; 7]. Предлагаемые модели делают акцент на доступности данных, представленной в способности учащегося получить доступ ко всем своим данным в любое время. Технология блокчейн позволяет использовать альтернативный подход к обучению. Многие учреждения, организации и предприятия создают свои собственные блокчейн-проекты для изучения преимуществ и использования в образовании, представленной в способности учащегося получить доступ ко всем своим данным в любое время [8; 9]. Технология блокчейн позволяет использовать альтернативный подход в сфере образования, для обработки персональных данных студентов [10; 11].

Актуальность данной работы обусловлена тем, что в сфере образования информация студентов имеет решающее значение и должна быть конфиденциальна. Существование суперадминистратора, который может извлекать данные общей информационной системы высшего образовательного учреждения, может рассматриваться как большая уязвимость [12; 13]. В традиционной системе образования, основанной на централизованной системе, существуют некоторые проблемы, связанные с ведением учета персональных данных. Цель этой работы состоит в том, чтобы найти альтернативные подходы для токенизации персональных данных студентов и организации безопасного доступа к ним. Новая модель информационной системы токенизации персональных данных студентов, основанная на технологии блокчейн, может обеспечить более защищенный и надежный способ хранения архивных записей персональных студенческих данных [14–17].

В настоящее время наиболее используемой моделью централизованных вычислений является клиент-серверная модель [18]. Эта модель учитывает существование сервера с большими вычислительными возможностями. Этот сервер, в свою очередь, является объектом, ответственным за прием запросов и предоставление услуг для нескольких пользователей.

Другими словами, несколько клиентов совместно используют одни и те же вычислительные ресурсы, предоставляемые централизованным сервером. Таким образом, количество клиентов, ответивших за определенный период, может быть оценено через общее количество доступных вычислительных ресурсов.

Однако другие эксплуатационные характеристики централизованных систем также важны. Примерами могут служить их алгоритмы распределения ресурсов и планирования. Эти алгоритмы определяют, кто и когда отвечает на конкретные запросы.

На рисунке 1 представлен пример централизованной системы, разработанной в соответствии с моделью «клиент – сервер».

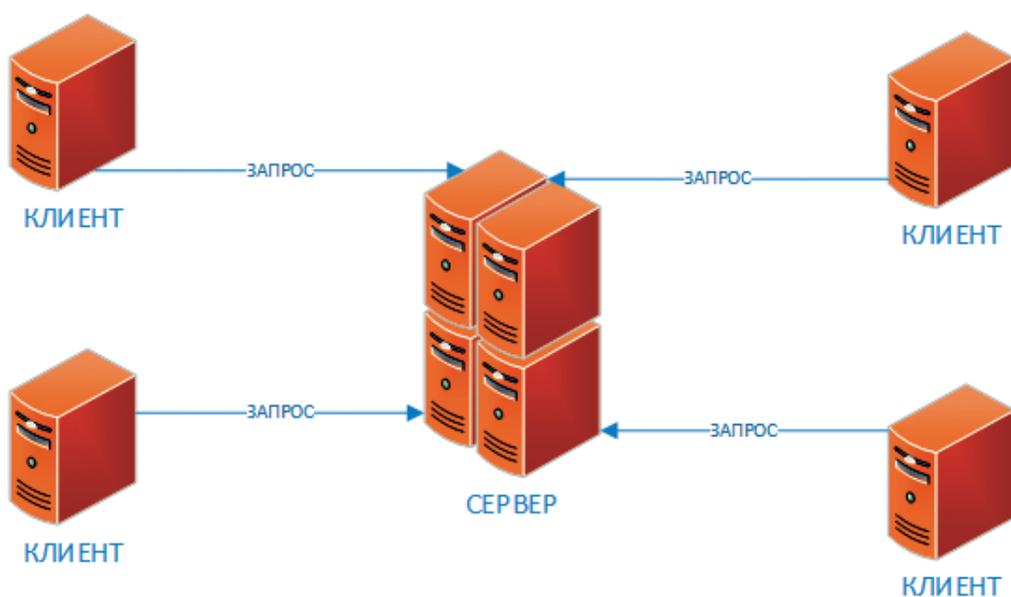


Рис. 1. Централизованная система

Однако необходимо отметить, что централизованные вычисления не ограничиваются моделью «клиент – сервер». Могут, например, использоваться серверы баз данных, которые сохраняют только периодически собираемую информацию и не взаимодействуют с другими системами.

Самое интересное в централизованных системах — это четкое разделение между серверами и клиентами. Эти сущности слабо связаны между собой. Таким образом, можно заменить сервер, не обязательно заменяя клиентов. Кроме того, могут быть разные типы клиентов (мобильные устройства, десктопные компьютеры, ноутбуки и т. д.), получающие доступ к одному и тому же серверу.

Например, компании, размещающие серверы, могут масштабировать вычислительные ресурсы (например, память или вычислительную мощность) и выполнять другие виды обслуживания на сервере без изменений на клиентских компьютерах.

Еще одним интересным свойством централизованной архитектуры является отсоединение клиента от сервера. Поскольку все службы предоставляет уникальный сервер, отключить от них конкретного клиента несложно: для этого достаточно прервать клиентское соединение или заблокировать его, например через брандмауэр.

Однако централизованные системы имеют некоторые недостатки [19].

Первая потенциальная проблема заключается в ограничении процесса масштабирования. В какой-то момент только предоставление большего количества ресурсов серверу просто не повышает его производительность. Существуют и другие ограничения, такие как ОС или сетевые функции, ограничения которых нельзя устранить с помощью использования дополнительных вычислительных ресурсов.

Еще одна проблема заключается в том, что сервер является единственной точкой отказа. Таким образом, если сервер становится недоступным, вся служба завершает работу, даже если все клиенты работают. Таким образом, эксплойты, атаки или любой сбой потенциально могут привести к завершению работы всей системы в целом.

Несмотря на эти недостатки, централизованные системы являются хорошими вариантами для многих приложений. В настоящее время существует несколько готовых серверов, таких как веб-серверы, запускаемых с помощью нескольких команд, что упрощает развертывание новых служб.

Кроме того, существует множество инструментов анализа данных с открытым исходным кодом для централизованных служб. Эти инструменты позволяют владельцам серверов отслеживать, что происходит с предоставляемыми сервисами.

Распределенные вычисления используют несколько компонентов, предоставляющих услугу. Компоненты в распределенной системе, в свою очередь, должны взаимодействовать для обмена информацией и данными. Эта связь обычно осуществляется путем отправки сообщений по Сети [20].

Важно подчеркнуть, что, когда распределенные объекты принимают решения самостоятельно, система децентрализована [21]. Однако, когда сущности каким-то образом координируют свои действия для принятия решений, система является распределенной системой [22].

Существуют различные модели распределенных вычислений, например можно рассматривать саму Всемирную сеть как модель распределенной системы.

Одноранговая модель состоит из набора независимых компьютеров, соединенных между собой при помощи сетевых соединений. Каждый одноранговый узел обладает достаточными возможностями для обработки данных и взаимодействия с другими одноранговыми узлами, сотрудничая с предоставляемой службой.

Как правило, тот, кто хочет получить доступ к сервису, связывается с одним или несколькими одноранговыми узлами, чтобы получить доступ к сервису. В особых случаях сущности, запрашивающие услугу, также становятся равноправными узлами, предоставляющими услугу. Таким образом, услуга

органично растет: чем больше число объектов, запрашивающих услугу, тем больше становится услуга.

Рисунок 2 иллюстрирует представленные характеристики распределенных вычислений в одноранговой модели [23].

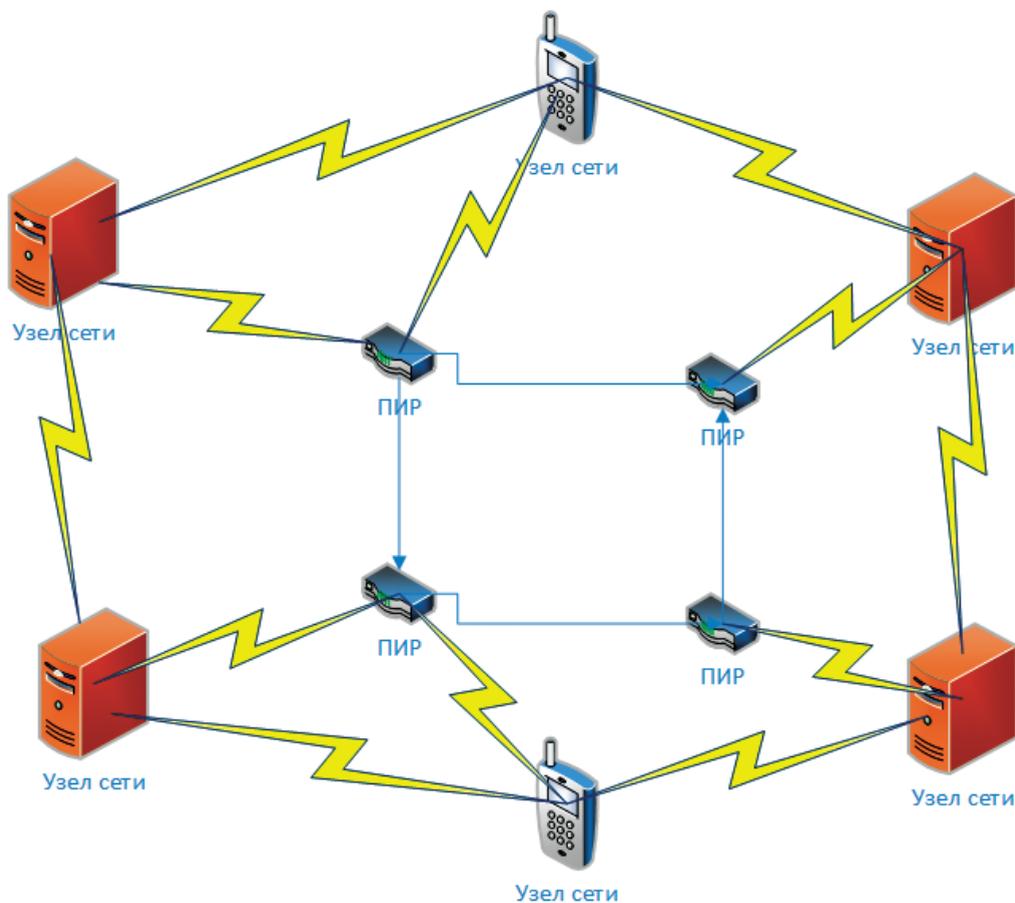


Рис. 2. Одноранговая модель информационной системы

Хотя модель распределенных вычислений и является многообещающей архитектурой во многих аспектах, но она сопряжена с рядом проблем. Примерами таких проблем являются координация и согласование распределенных объектов. Из-за этих проблем распределенные системы становятся особой областью исследований в информатике [24].

Одним из больших преимуществ внедрения распределенной системы является устранение единственной точки отказа централизованных вычислений. В распределенных системах одноранговый узел может выйти из строя, а служба по-прежнему доступна [25].

Это означает, что другие одноранговые узлы могут выполнять задачи однорангового узла, который потерпел неудачу, или, по крайней мере, должны образом информировать запрашивающие объекты о том, что конкретный

одноранговый узел потерпел неудачу. Таким образом, мы можем понимать хорошо спроектированную распределенную систему как надежную систему.

Еще одно преимущество внедрения распределенной системы заключается в расширении процессов. Таким образом, можно добавить дополнительные вычислительные ресурсы к объектам в системе (горизонтальное масштабирование). Однако также можно добавлять новые объекты для предоставления услуг в системе (вертикальное масштабирование).

Возможность добавления новых объектов в систему позволяет поставщикам услуг по-разному удовлетворять конкретные потребности конкретных географических регионов. Например, в населенных пунктах с высокой плотностью пользователей услуг может быть несколько близких организаций, предоставляющих услуги.

Однако у распределенных систем тоже есть множество недостатков.

Существенной трудностью является управление распределенными системами. Поскольку есть автономные организации, работающие вместе, трудно отслеживать и контролировать каждую из них.

Кроме того, необходимо распространять общие обновления среди всех организаций, предоставляющих услуги, что требует сложной стратегии.

Еще одной проблемой являются различные возможности и часы работы объектов в системе. На самом деле, это не совсем проблема, а характеристика. Однако поставщики должны сбалансировать возможности организаций, избегая узких мест и сценариев недостаточного использования.

Ниже, в таблице 1, представлены сравнительный анализ централизованных и децентрализованных систем.

Таблица 1

## Сравнительный анализ

	Централизованная система	Децентрализованная система
Обслуживающий центр	Один	Несколько
Точки отказа	Зависимая (отказ сервера приводит к отказу системы в целом)	Независимая (отказ одного или нескольких узлов не приводит к отказу системы в целом)
Масштабирование	Горизонтальное	Горизонтальное и вертикальное
Мониторинг системы	Одна точка мониторинга — сервер (просто)	Несколько точек мониторинга (сложно)
Примеры использования	Централизованные базы данных, однопользовательские игры и отладочные песочницы	Сети BitTorrent: распределенные одноранговые сети для обмена данными Блокчейн: децентрализованные и распределенные базы данных, в которых данные надежно хранятся несколькими организациями

В данной работе предлагается подход к использованию блокчейна для реализации полнофункциональной студенческой веб-ориентированной информационной системы, ведущей записи данных о студентах, записи о регистрации на курс и оценок студентов. Она дает важные, безопасные и прозрачные методы построения глобальной системы образовательного обучения. Все регулярные транзакции основаны на централизованном консенсусе. Этот подход дает возможность использования множества интересных функций, таких как снижение транзакционных издержек, эффективность и безопасность. Для обеспечения безопасных, быстрых и чистых транзакций вводится понятие связанного списка блокчейнов. Блокчейн-система обрабатывает транзакции, отправленные разными пользователями, в соответствии с их уровнями безопасности, без необходимости вмешательства сторонних служб.

При использовании информационных систем высшими учебными заведениями уходит много усилий и затрат на ведение записей обо всех образовательных транзакциях, происходящих с момента подачи абитуриентами заявлений на поступление, ведения семестрового учета и данных об окончании учебы. В этом контексте возникает множество проблем безопасности и целостности данных [6; 25].

Предлагаемая модель токенизации персональных данных студентов повышает безопасность за счет использования хеширования и доступности данных при децентрализованном хранении данных. Информация о блокчейне, предоставляемом университетом, открыта для всех заинтересованных сторон. Неизменность, чувствительность и удобство хранения записей в блокчейне в целом помогли получить хорошую реализацию студенческой информационной системы. Связанный список блокчейнов может записывать все значения, включая паспортные данные, данные об оценках, полученных сертификатах и т. д.

Наиболее важными требованиями к информационной системе являются целостность данных и использование неизменного леджера в дополнение к возможности безопасного обмена защищенной информацией между заинтересованными сторонами. Функции блокчейна могут удовлетворять этим требованиям, используя три модели. В СИС данные могут быть классифицированы следующим образом:

1. Данные без сохранения состояния СИС: данные, не влияющие на средний балл учащегося и вводимые один раз. Данные СИС без сохранения состояния относительно менее важны для СИС. Типичными данными СИС без сохранения состояния являются список курсов, список преподавателей, список студентов. Для каждого списка данных без сохранения состояния авторизованный сотрудник вводит базовый набор полей, однако заинтересованному пользователю может потребоваться ввести дополнительные данные о себе, например преподаватель или студент, изменяющий свой телефон или адрес.

2. Данные с отслеживанием состояния СИС: данные, вызывающие изменение состояния учащегося, например студент, который записывается/отказывается от курса. Преподаватель вводит оценки за курс/экзамен.

3. Данные без состояния все еще могут рассматриваться как критически важные, но для некоторых систем полезно хранить их в традиционной системе с суперадминистратором, подписывающим контракт о конфиденциальности. Транзакционные данные очень важны во всех аспектах. Транзакция может быть отменена только отправкой другой обратной транзакции.

В СИС узлы в зависимости от ролей могут быть разделены на следующие типы.

1. Административный узел:

- считывает/записывает основные информационные записи студентов и преподавателей без сохранения состояния;
- читает/записывает программу обучения;
- считывает/записывает список назначенных преподавателей курсов;
- считывает/записывает настройки университетских правил, такие как крайние сроки и т. д., которые управляют цепочкой блоков;
- создает блок.

Университет может классифицировать роли администратора по подкатегориям в соответствии с их организацией.

2. Студенческий узел:

- считывает/записывает регистрационные записи курса в соответствии с правилами университета и в установленные сроки;
- считывает/записывает некоторые поля собственных данных студента без состояния, таких как телефон и адрес, в соответствии с правилами университета и в установленные сроки;
- читает только сертификат студента.

3. Преподавательский (профессорский) узел:

- читает/записывает оценки (итоговый экзамен, промежуточный экзамен, курсовая работа);
- считывает/записывает некоторые поля своих собственных данных без гражданства, таких как телефон и адрес, в соответствии с правилами университета и в установленные сроки;
- читает только сертификат студента.
- создает блок.

4. Гостевой узел:

- читает только сертификат студента по одобрению студента;
- читает только обучающую программу после одобрения администратором;
- читает список назначенных курсов только для преподавателей по одобрению преподавателя.

Гостевой узел представляет внешнюю сторону, заинтересованную в наборе информации СИС.

## Методы исследования

В работе предлагается следующая модель. Разрешена консенсусная сеть с транзакциями, принимающими только данные с отслеживанием состояния. В этой модели для построения блокчейна используются самые простые варианты. Это наиболее подходит для небольших организаций. Модель рассматривает разрешенную консенсусную сеть с транзакциями, принимающими только данные с отслеживанием состояния, а все узлы являются полными узлами, где каждый узел хранит полную копию блокчейна. Узел отправителя, добавляющего транзакцию, отвечает за добавление ее в список транзакций, которым обычно может быть база данных SQLite, и за добавление ее в дерево Меркла. Узел отправителя также отвечает за проверку всех полей и проверку того, что аккаунт отправителя имеет разрешение на создание и отправку транзакции в соответствии с правилами СИС, которые встроены в генезис-блок блокчейна во время настройки. В этой модели информация без состояния хранится в обычной системе за пределами блокчейна.

По определению, разрешенный блокчейн — это частная сеть. Никакая учетная запись не может быть создана, если новый пользователь (студент или профессор) не получит закрытый ключ от администрации (администратора) организации и не использует его для настройки нового узла. Новый узел может быть создан только на компьютере внутри сети вуза; следовательно, все узлы хорошо идентифицированы и пользуются высоким доверием. Процесс настройки нового узла не может начаться без действительного закрытого ключа, имеющего открытый ключ контрагента, созданный узлом администратора с использованием предопределенного алгоритма. Закрытый ключ используется для шифрования любых транзакций, созданных и отправленных любым узлом. Он используется в качестве подписи, которая позволяет блокчейну идентифицировать владельца любой транзакции для аудита.

## Результаты исследования

Жизнеспособность и производительность разработанного прототипа СИС (DApp) оцениваются методом выполнения разных тестов с внедрением экспериментальной установки, показанной на рисунке 3.

Для проведения оценки используется тестовая сеть Rinkeby 9. Rinkeby — одна из общедоступных тестовых сетей, предоставляемых Ethereum. Он использует алгоритм консенсуса Proof-of-Authority (PoA). Эфир, токен криптовалюты, используемый в Rinkeby, не имеет денежной ценности. API Infura используется для связи с сетью Rinkeby.

Общее время выполнения состоит из времени связи, времени майнинга блоков и времени выполнения соответствующих смарт-контрактов. Поскольку DApp создан для студенческой информационной системы, ему, возможно,

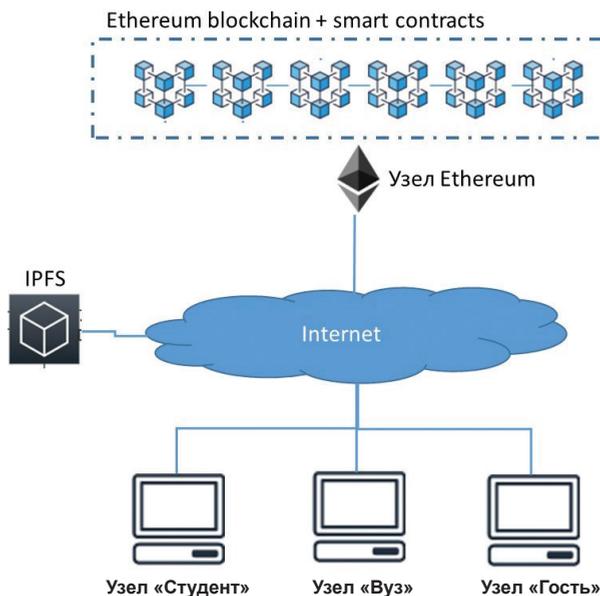


Рис. 3. Экспериментальная тестовая установка

придется обслуживать большее количество запросов, поэтому интересно изучить общее время выполнения пользовательских запросов. Пользователь может отправлять два типа запросов в блокчейн через DApp: одни запросы считывают данные из блокчейна, а другие записывают данные в блокчейн. Чтение данных не требует создания какого-либо блока, поэтому оно занимает незначительное время. Однако, когда пользователь записывает данные в блокчейн, транзакции проверяются и блоки добываются, поэтому это занимает некоторое время. Согласно официальному сайту, среднее время обработки транзакции/запроса в тестовой сети Rinkeby составляет 15 сек. Для оценки производительности разработанного DApp выполняются два разных типа тестов.

В защищенной версии DApp загрузка учетных данных требует от вузов выполнения следующих задач:

- вычисление исходного хеша учетных данных;
- получение открытого ключа студента из блокчейна и шифрования учетных данных с помощью этого ключа;
- загрузка зашифрованных учетных данных на IPFS и получение хеш IPFS;
- скачивание метаданных из блокчейна.

Однако если защита конфиденциальности не включена, то задачи 1 и 2 не выполняются. С точки зрения производительности блокчейна время выполнения загрузки учетных данных не изменится ни с защитой конфиденциальности, ни без защиты конфиденциальности. Причина в том, что задача 1 выполняется локально (т. е. на интерфейсе DApp), в то время как задача 2 — это просто операция чтения в сети блокчейн. Таким образом, независимо от того, какое изменение наблюдается во времени выполнения для загрузки

учетных данных без конфиденциальности и с конфиденциальностью, это связано с изменением времени на проверки сети блокчейн.

Чтобы выяснить среднее время и отличия во время выполнения, было выполнено 100 итераций путем последовательной отправки запросов на загрузку учетных данных. Среднее значение ответа от экспериментальной сети блокчейн составляет 16,00337 сек., в то время как официальный сайт утверждает, что оно составляет 15 сек.; разница между наблюдаемым средним временем и официальным средним временем составляет 1,00337 сек. Эта дополнительная задержка связана с выполнением смарт-контрактов и временем, затрачиваемым Ethereum на проверку, и майнингом новых блоков, а также с задержкой связи (рис. 4).

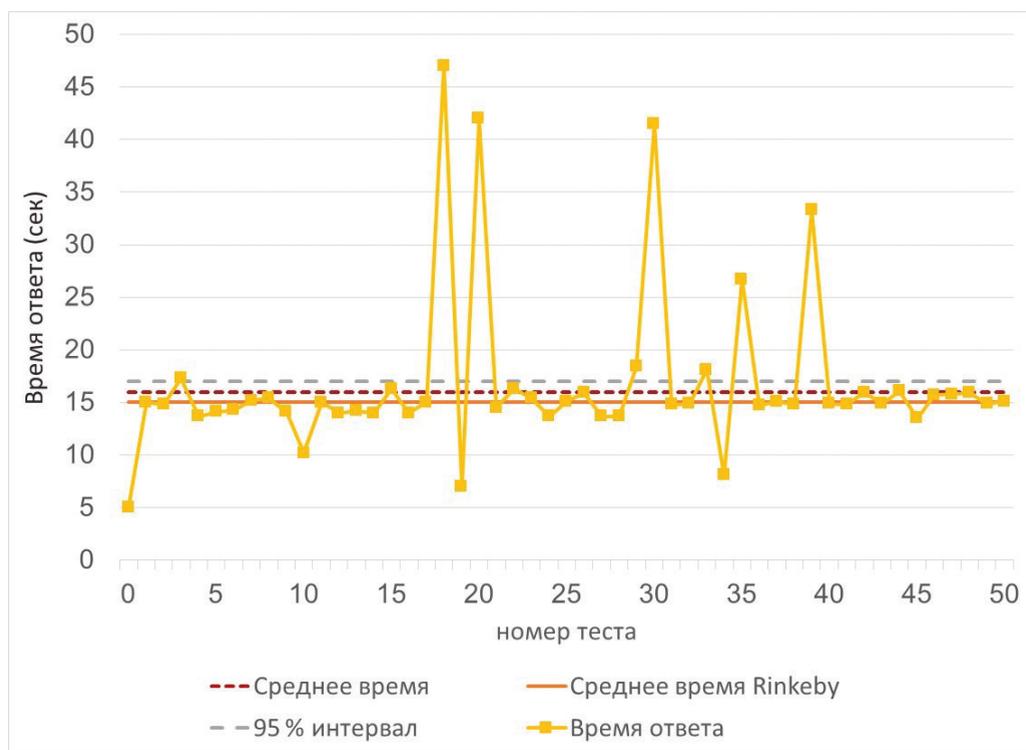


Рис. 4. Время, затраченное на загрузку учетных данных

В защищенном DApp отправка запроса на доступ и предоставление права включает следующие задачи:

1. Гость посылает запрос на доступ к данным студента.
2. Студент просматривает запрос и одобряет его, после чего следует шифрование запрашиваемых учетных данных с помощью открытого ключа гостя.
3. Затем студент загружает зашифрованные учетные данные в IPFS и получает хеш IPFS.
4. Студент временно загружает метаданные в блокчейн.

Однако если защита конфиденциальности не включена, то задачи 2 и 3 не выполняются. Более того, задача 2 выполняется локально на стороне клиента, поэтому она занимает незначительное количество времени.

Кроме того, задача 3 (закрывающаяся в загрузке файла в IPFS) также занимает незначительное количество времени по сравнению с временем, необходимым для одной операции записи. Среднее время загрузки и среднее время загрузки в IPFS для размера файла, равного 1 МБ, составляют менее 0,2 сек. Таким образом, время выполнения для отправки запроса на доступ и предоставление права доступа с конфиденциальностью и без нее будет почти одинаковым. Любое заверенное изменение зависит от времени, необходимого блокчейну для выполнения двух операций записи, соответствующей заданию 1 и заданию 4.

Чтобы выполнить тест, сначала гость посылает запрос на учетную запись студента. Во-вторых, студент просматривает запрос, а затем предоставляет доступ. Оба запроса были обработаны для расчета общего затраченного времени. Здесь предполагается, что студент немедленно одобряет все входящие запросы. Кроме того, чтобы выяснить среднее время и отличия во время выполнения, было проведено 100 итераций таких запросов. Среднее время без конфиденциальности — 31,09165 сек., тогда как с конфиденциальностью оно составляет 34,74195 сек.

Поскольку официальный сайт утверждает, что время обработки каждого запроса составляет 15 сек., поэтому для двух операций записи оно должно составлять 30 сек. Следовательно, разница между наблюдаемым средним временем и официальным средним временем с конфиденциальностью составляет 4,74195 сек., а без конфиденциальности — 1,09165 сек. Хотя наблюдения показывают, что разница выше с защитой конфиденциальности, чем без защиты конфиденциальности. Следует отметить, что для одного запроса доступа со стороны гостя, требующей доступа для нескольких учетных данных, это приведет к общему количеству операций записи, которые должны быть выполнены в блокчейне. Это операция записи для отправки одного запроса на доступ и количество операций записи для загрузки метаданных по количеству запрошенных учетных данных.

## Заключение

В данной работе были рассмотрены ключевые концепции и возможности использования технологии блокчейн в сфере образования.

Как показали проведенные исследования прототипа студенческой информационной системы для токенизации персональных данных студентов, основной проблемой на глобальной общедоступной платформе Ethereum является низкая производительность обработки (15 транзакций в сек.). Однако для частных и консорциумных блокчейнов майнинг с помощью поддельного эфира значительно ускоряет процесс и решает проблемы производительности.

В качестве примера использования предлагаемой технологии рассматривается задача безопасного обмена учетными данными студентов в веб-ориентированной студенческой информационной системе. Предложена архитектура системы токенизации персональных данных студентов, в которой перечислены разные заинтересованные стороны, их роли и основные функциональные возможности. Для проверки концепции предлагаемой архитектуры с защитой конфиденциальности разработан и протестирован прототип студенческой информационной системы.

### Список источников

1. Носиров, З. А., Фомичев, В. М. (2021). Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки. *Системы управления, связи и безопасности*, 2, 37–75.
2. Шафиков, А. А., Воробьев, Е. С. (2022). Исследование блокчейн-технологии: основы архитектуры и ее разработка. *Системы управления, информационные технологии и математическое моделирование*, 288–293.
3. Сошников, Д. В. (2021). Принципы информационной безопасности на основе blockchain-технологий. *Научно-исследовательский центр «Technical Innovations»*, 2, 166–173.
4. Круглова, С. Д. (2021). Совершенствование информационной составляющей экономической безопасности организации на основе технологии блокчейн. *Проблемы и перспективы развития российской экономики*. Сборник статей по материалам X Научно-практической конференции (с. 79–81). Москва: Перо.
5. Нестеренко, В. Р., Маслова, М. А. (2021). Использование технологии Blockchain для обеспечения безопасности в распределенном интернете вещей. *Научный результат. Информационные технологии*, 6(2), 3–8.
6. Чиндяев, А. Е., Яковлева, В. И. (2021). Технология блокчейн и ее возможное внедрение в сферу образования. *Студенческий научный форум*, 47–49.
7. Аскарбек, К. К., Халилова, М. В. (2021). Развитие технологии блокчейн и ее применение в системе образования. *Евразийское Научное Объединение*, 5–3, 164–171.
8. Крупнина, П. Г., Чхеидзе, Е. П. (2021). Информатизация образования в КНР и перспективы внедрения технологии блокчейн. *Управление бизнесом в цифровой экономике*, 363–369.
9. Григорьев, В. В. (2020). Блокчейн в образовании. *Информация и инновации*, 15(2), 18–26.
10. Кузнецова, В. П., Бондаренко, И. А. (2018). Блокчейн как инструмент цифровой экономики в образовании. *Вопросы регулирования экономики*, 9(1), 102–109.
11. Корчагин, С. (2016). О текущих трендах в развитии технологии блокчейн. *Свободная мысль*, 4, 31–38.
12. Наджафова, М. Н. (2021). Тенденции развития информационных технологий, внедряемых в системе образования. *Балтийский гуманитарный журнал*, 10, 1(34), 182–185.
13. Атаян, А. М., Гурьева, Т. Н., Шарабаева, Л. Ю. (2021). Цифровая трансформация высшего образования: проблемы, возможности, перспективы и риски. *Отечественная и зарубежная педагогика*, 1(2), 7–22.
14. Покровская, Н. Н., Гелих О. Я., Гильдингерш, М. Г., Молодькова, Э. Б., Попова О. А. (2022). Блокчейн-платформы для токенизации репутационного капитала

университета. *Проектирование и обеспечение качества информационных процессов и систем*. Сборник докладов Международной конференции, г. Санкт-Петербург, 15–17 марта 2022 г. (с. 157–160). Санкт-Петербург: ЛЭТИ им. В. И. Ульянова (Ленина).

15. Шматко, О., Борова, Т., Евсеев, С., Милов, О. (2021). Токенизация образовательных активов на основе блокчейн-технологий. *Педагогическое образование*, 3(42), 4–10. DOI: 10.15587/2519-4984.2021.232321

16. Gunawan, I. K., Lutfiani, N., Aini, Q., Suryaman, F. M., Sunarya, A. (2021). Smart Contract Innovation and Blockchain-Based Tokenization in Higher Education. *Journal of Education Technology*, 5, 4, 636–644.

17. Sivadanam, Y. L., Ramaguru, R., Sethumadhavan, M. (2022). Distributed Ledger Framework for an Adaptive University Management System. *Proceedings of International Conference on Computational Intelligence and Data Engineering* (pp. 295–306). Springer, Singapore.

18. Стяжкова, Т. Н., Чекалдин, Ю. С. (2021). Информационные системы в сфере электронного документооборота. *Современные технологии документооборота в бизнесе, производстве и управлении*, 74–77.

19. Трофимец, И. А. (2022). Преимущества и недостатки новой информационной системы учёта граждан в Российской Федерации. *Вестник Омского университета. Серия «Право»*, 19(1), 25–37.

20. Кульба, В. В., Сомов, С. К., Шелков, А. Б. (2022). Анализ влияния использования информационной избыточности на показатели надежности распределенных информационных систем. *Надежность*, 22(1), 4–12.

21. Даденова, Г. (2022). Основы проектирования информационных систем. *Central Asian Journal of STEM*, 3(1), 41–44.

22. Ягодкин, Д. А., Уханов, Д. В., Игнатьева, Д. С. (2021). Системы распределенной обработки данных и основные их разновидности. *Цифровизация образования: теоретические и прикладные исследования современной науки*, 56–59.

23. Михайленко, Н. В., Мурадян, С. В., Вихляев, А. А. (2022). Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях. *Аудиторские ведомости*, 1, 140–145.

24. Хряшев, В. В., Ненашев, А. В. (2021). Эффективность внедрения одноранговой распределенной системы хранения и обработки защищаемой информации (THEOOL PROJECT). *Моделирование систем и процессов*, 14(3), 82–89.

## References

1. Nosirov, Z. A., & Fomichev, V. M. (2021). Blockchain technology analysis: fundamentals of architecture, examples of use, development prospects, problems and shortcomings. *Control Systems, Communications and Security*, 2, 37–75. (In Russ.).

2. Shafikov, A. A., & Vorobyov, E. S. (2022). Blockchain technology research: fundamentals of architecture and its development. *Control systems, information technologies and mathematical modeling*, 288–293. (In Russ.).

3. Soshnikov, D. V. (2021). Principles of information security based on blockchain technologies. *Scientific Research Center «Technical Innovations»*, 2, 166–173. (In Russ.).

4. Kruglova, S. D. (2021). Improving the information component of the economic security of an organization based on blockchain technology. *Economic security of society, the state and the individual: problems and directions of provision*. Collection of articles based on the materials of the X Scientific and Practical Conference (pp. 79–81). (In Russ.).

5. Nesterenko, V. R., & Maslova, M. A. (2021). Using Block-chain technology to ensure security in the distributed Internet of things. *Scientific result. Information Technology*, 6(2), 3–8. (In Russ.).
6. Chindyaev, A. E., & Yakovleva, V. I. (2021). Blockchain technology and its possible implementation in the field of education. *Student Scientific Forum*, 47–49. (In Russ.).
7. Askarbek, K. K., & Khalilova, M. V. (2021). Development of blockchain technology and its application in the education system. *Eurasian Scientific Association*, 5–3, 164–171. (In Russ.).
8. Krupnina, P. G., & Chkheidze, E. P. (2021). Informatization of education in the PRC and prospects for the introduction of blockchain technology. *Business management in the digital economy*, 363–369. (In Russ.).
9. Grigoriev, V. V. (2020). Blockchain in education. *Information and innovations*, 15(2), 18–26. (In Russ.).
10. Kuznetsova, V. P., & Bondarenko, I. A. (2018). Blockchain as an instrument of digital economy in education. *Economic regulation issues*, 9(1), 102–109. (In Russ.).
11. Korchagin, S. (2016). On current trends in the development of blockchain technology. *Free Thought*, 4, 31–38. (In Russ.).
12. Nadzhafova, M. N. (2021) Trends in the development of information technologies implemented in the education system. *Baltic Humanitarian Journal*, 10, 1(34), 182–185. (In Russ.).
13. Atayan, A. M., Guryeva, T. N., & Sharabaeva, L. Yu. (2021). Digital transformation of higher education: problems, opportunities, prospects and risks. *Domestic and foreign pedagogy*, 1(2), 7–22. (In Russ.).
14. Pokrovskaya, N. N., Gelikh, O. Ya., Gildingersh, M. G., Molodkova, E. B., & Popazova, O. A. (2022). Blockchain platforms for tokenization of university reputational capital. *Design and quality assurance of information processes and systems*. Collection of reports of the International Conference, St. Petersburg, 2022, March 15–17 (pp. 157–160). St. Petersburg: V. I. Ulyanov (Lenin) LETI. (In Russ.).
15. Shmatko, O., Borova, T., Yevseiev, S., & Milov, O. (2021). Tokenization of educational assets based on blockchain technologies. *Pedagogical Education*, 3(42), 4–10. <https://doi.org/10.15587/2519-4984.2021.232321>
16. Gunawan, I. K., Lutfiani, N., Aini, Q., Suryaman, F. M., & Sunarya, A. (2021). Smart Contract Innovation and Blockchain-Based Tokenization in Higher Education. *Journal of Education Technology*, 5, 4, 636–644.
17. Sivadanam, Y. L., Ramaguru, R., & Sethumadhavan, M. (2022). Distributed Ledger Framework for an Adaptive University Management System. *Proceedings of International Conference on Computational Intelligence and Data Engineering* (pp. 295–306). Springer, Singapore. (In English).
18. Styazhkova, T. N., & Chekaldin, Yu. S. (2021). Information systems in the field of electronic document management. *Modern technologies of document management in business, production and management*, 74–77. (In Russ.).
19. Trofimets, I. A. (2022). Advantages and disadvantages of a new information system for registering citizens in the Russian Federation. *Bulletin of the Omsk University. Series «Right»*, 19(1), 25–37. (In Russ.).
20. Kulba, V. V., Somov, S. K., & Shelkov, A. B. (2022). Analysis of the influence of the use of information redundancy on the reliability indicators of distributed information systems. *Reliability*, 22(1), 4–12. (In Russ.).

21. Dadenova, G. (2022). Fundamentals of information systems design. *Central Asian Journal of STEM*, 3(1), 41–44. (In Russ.).
22. Yagodkin, D. A., Ukhanov, D. V., & Ignatieva, D. S. (2021). Distributed data processing systems and their main varieties. *Digitalization of education: theoretical and applied research of modern science*, 56–59. (In Russ.).
23. Mikhailenko, N. V., Muradyan, S. V., & Vikhlyaev, A. A. (2022). Actual issues of monitoring and counteracting cyber threats in peer-to-peer networks. *Auditorskie Vedomosti*, 1, 140–145. (In Russ.).
24. Khryashchev, V. V., & Nenashev, A. V. (2021). Efficiency of implementing a peer-to-peer distributed system for storing and processing protected information (THEOOL PROJECT). *Modeling systems and processes*, 14(3), 82–89. (In Russ.).

Статья поступила в редакцию: 15.06.2022;  
одобрена после рецензирования: 04.08.2022;  
принята к публикации: 02.09.2022.

The article was submitted: 15.06.2022;  
approved after reviewing: 04.08.2022;  
accepted for publication: 02.09.2022.

***Информация об авторе:***

**Светлана Владимировна Маркова** — кандидат технических наук, доцент, доцент департамента математики, Финансовый университет при Правительстве РФ, Москва, Россия,  
svmarkova@fa.ru

***Information about the author:***

**Svetlana V. Markova** — Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Mathematics, Financial University under the Government of the Russian Federation, Moscow, Russia,  
svmarkova@fa.ru