В.М.АЛЕФИРЕНКО

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ИНТЕГРАЦИИ ЭЛЕМЕНТОВ НАУЧНЫХ ИССЛЕДОВАНИЙ В УЧЕБНЫЙ ПРОЦЕСС

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, доцент, кандидат технических наук, доцент

Представленные материалы являются логическим продолжением работы [1].

В рамках лабораторно-практических занятий по дисциплине «Методы и технические средства обеспечения безопасности» изучаются вопросы криптографической защиты информации. В качестве элементов научных исследований студентам, имеющим опыт в программировании, была предложена работа по исследованию возможности разработки электронной зачетной книжки учащихся с использованием технологии блокчейн.

Технология блокчейн обеспечивает надежное и безопасное хранение и передачу данных между пользователями. Главным преимуществом технологии в сравнении с распределенными базами хранения данных является невозможность нарушить целостность хранения данных. Система, построенная на технологии блокчейн, обеспечивает два основных свойства информационной безопасности: целостность и доступность данных. Каждый пользователь системы имеет доступ к данным, хранящимся в системе. Каждый узел системы (компьютер пользователя) сохраняет и поддерживает полную копию блоков системы, что обеспечивается специальным механизмом синхронизации. Такая организация системы позволяет исключить возможность ее взлома злоумышленниками, так как при модификации данных на одном узле системы данный факт будет сразу же обнаружен остальными ее участниками на других узлах. Сеть системы исключает централизованное управление, а каждый участник может присоединиться к сети или выйти из нее в любой момент времени. Внутренняя защищенность системы реализуется с помощью криптографических алгоритмов, работающих на основе хэш-функции [2].

Чтобы использовать блокчейн для разработки зачетной книжки учащихся необходимо организовать структуру блоков и непосредственно сам блокчейн, разработать веб-сайт с выполнением принципов UX/UI дизайна, подобрать сервер с подходящими характеристиками.

Блок представляет собой файл с JSON-объектом, который содержит: ФИО студента, номер группы, факультет и все оценки за все семестры. Блоки объединяются в цепочку, причем в каждый новый блок записывается хеш предыдущего, что в совокупности с децентрализацией блокчейна дает безопасное хранение данных. В функции записи блока реализован следующий алгоритм: запрашивается номер файла крайнего блока, вычисляется хэш крайнего блока, формируется новый файл блока, содержащий хэш предыдущего блока, новый файл блока записывается на диск.

Для пользования веб-сайтом учащимся и преподавателям выдается мнемоническая фраза, благодаря которой доступ к профилю есть только у владельца этой фразы. Далее у преподавателя есть возможность выбрать группу и конкретного учащегося, которому нужно выставить оценку. У учащегося в это время будут лишь отображаться его данные, в том числе оценки.

Для разработки программы использовался язык программирования Python. Разработка выполнялась в среде PyCharm IDE, которая является удобным инструментом для написания и отладки кода, имеет встроенный линтер – программу, позволяющую следить за форматированием кода и при необходимости исправлять его. Для самого блокчейна необходимо было организовать способ доступа, удобный как для разработчика, так и для конечного пользователя. Для этой цели был выбран веб-сервер, который запускался на компьютере и позволял получить доступ к блокчейну извне. Для организации программного сервера использовался модуль-библиотека Flask. Данный модуль позволяет создавать небольшие веб-приложения, которые достаточно легко поддерживать. Основная часть кода, написанная с использованием данного модуля, представляет собой набор обработчиков запросов от пользователя. Обработчик выполняет запрашиваемую операцию и отправляет результат операции в виде веб-страницы. Операцию хеширования и другие операции с хэшами упрощает использование модуля Hashlib. Модуль Mnemonic использовался для генерации мнемонической фразы, которая необходима для авторизации в блокчейне. Помимо генерации, модуль позволяет преобразовать мнемоническую фразу в сид-строку и вычислить энтропию фразы. Разработанный самостоятельно алгоритм работы блокчейна включает формирование блоков, внесение их в общую цепочку и операцию проверки целостности цепочки. В алгоритме использовалась операция хэширования и работа с файловой системой сервера. Для удобства дальнейшей поддержки системы алгоритм работы блокчейна записан в отдельном файле, который подключен к основному исполняемому файлу как модуль.

Графический интерфейс реализован при помощи языков разметки HTML и CSS, а также языка программирования JavaScript, который выполняется в браузере на стороне пользователя. Использование языка JavaScript обосновано необходимостью реализации динамически обновляемых элементов графического интерфейса – предоставление информационных блоков в зависимости от выбранного пункта в выпадающем списке. Графический интерфейс сервиса представлен на рисунке 1.

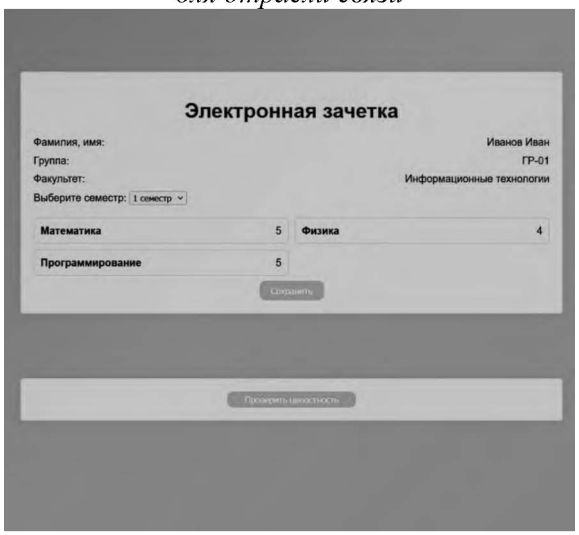


Рисунок 1 – Графический интерфейс сервиса

Внедрение блокчейн-платформы для электронной зачетной книжки учащихся позволит:

– обеспечить целостность и достоверность данных об успеваемости, исключив возможность несанкционированного изменения или подделки записей;

– предоставить учащимся и администрации учебных заведений полный контроль над своими академическими записями;

– упростить и ускорить процессы проверки и обмена информацией об успеваемости между различными подразделениями учебного заведения.

– повысить прозрачность и эффективность системы высшего образования в целом.

Использование технологии блокчейн для электронной зачетной книжки учащихся имеет значительные преимущества по сравнению с традиционными бумажными или централизованными электронными системами. Внедрение этой технологии может стать важным шагом на пути к созданию более надежной, прозрачной и эффективной системы учета академической успеваемости учащихся [3].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алефиренко, В. М. Интеграция научных исследований при проведении лабораторных занятий по дисциплине «Методы и технические средства обеспечения безопасности» / В. М. Алефиренко // Технические средства защиты информации: тезисы докладов XIX Белорусско-российской науч.-техн. конф., Минск, 8 июня 2021 г. / БГУИР. – Минск, 2021. – С. 16–17.

2. Кустов, В. Н. Еще раз о технологии blockchain / В. Л. Кустов, Т. Л. Станкевич // Защита информации. INSIDE. – 2018. – №2. – С. 68–74.

3. Даревский, Д. И. Использование технологии блокчейн для реализации безопасной электронной зачетной книжки учащихся / Д. И. Даревский, П. А. Буйвидович, Н. Д. Оникийчук // Технические средства защиты информации: тезисы докладов XXII Белорусско-российской науч.-техн. конф., Минск, 12 июня 2024 г. / БГУИР. – Минск, 2024. – С. 33.