



Ж.С. Есенгалиева¹, О.А. Усатова², А.С. Есенгалиева²

¹L.N. Gumilyov Eurasian National University, Астана, Казахстан,

²Institute of Information and Computational Technologies CS MSHE RK,

Алматы, Казахстан

E-mail: olgaussatova@gmail.com

РАЗРАБОТКА ИНТЕГРАЦИОННОГО ПРОГРАММНОГО МОДУЛЯ ДЛЯ ОРГАНИЗАЦИИ БЕЗОПАСНОГО ХРАНЕНИЯ И ОБМЕНА ДАНЫМИ НА ОСНОВЕ БЛОКЧЕЙН

Аннотация. В целях фиксации данных в интеллектуальной антикоррупционной системе защиты информации и валидации учебных достижений, а также официальных документов студентов и выпускников вузов и военных учебных заведений Республики Казахстан разработан программный модуль. В статье рассмотрена технология блокчейн Ethereum на основе обозревателя Blockscout, который фиксирует детали транзакции в тестовой сети. Исследовательской группой представлена практическая реализация системы хранения образовательных документов на базе блокчейна. Запись служит подтверждением успешного выполнения смарт-контракта, предназначенного для передачи академического транскрипта. Использование тестовой сети позволяет верифицировать архитектуру решения, минимизировать издержки на этапе разработки и гарантировать, что каждый транскрипт получает уникальный, криптографически защищенный оттиск в публичном реестре. Также в статье приведен библиографический обзор касательно применения блокчейн Ethereum в сфере образования.

Таким образом, предложен сервис, вызываемый в процессе работы на портале студента или выпускника с применением технологии блокчейн, реализованный с помощью обозревателя Blockscout на языке программирования Solidity.

Ключевые слова: блокчейн, Ethereum, смарт-контракт, Blockscout, транзакции.

Введение.

Блокчейн — информационная технология, способная обеспечить безопасность инфраструктуры передачи и хранения данных [1]. Блокчейн Ethereum разрабатывает эффективные смарт-контракты, которые взаимодействуют с другими смарт-контрактами для принятия решений, хранения данных и отправки эфира другим пользователям [2]. Перспектива



использования блокчейн транзакционных систем, заключается в том, что они по своей природе более надежны, чем предыдущие решения [3].

В эпоху развития различных мошеннических атак в глобальной сети, антикоррупционных рисков, использование технологии блокчейн во многих оцифрованных областях человеческой деятельности позволяет преодолеть всевозможные неверные действия злоумышленников.

К примеру, авторы [4] предлагают решение использования блокчейна, с устранением необходимости централизации, что открывает путь к доверию и безопасности в отношении цифровых учетных данных. Информация о сертификатах надежно хранится в смарт-контрактах на блокчейне Ethereum, что позволяет автоматизировать процессы проверки для повышения эффективности.

Блокчейн Ethereum широко внедряется в образовательную сферу деятельности. К слову, в трудах [5] исследуется возможность использования блокчейна Ethereum для разработки надежной системы на основе невзаимозаменяемых токенов, выпущенные университетом. Токены представляют собой зачетные единицы модулей, выданные его факультетом и принадлежащие студентам после выполнения требований модулей в системе управления зачетными единицами. Децентрализованное приложение NFT-merit размещено в межпланетной файловой системе (IPFS) в виде децентрализованной сети узлов.

Ранее нашей исследовательской группой был проведен обзор платформ блокчейн-технологий, которые применяются с целью повышения безопасности данных посредством передачи цифровых активов без центрального администратора. Данное исследование предлагает уникальную перспективу, предоставляя техническое сравнение блокчейн-платформ с точки зрения теории создания единой цифровой платформы высшего образования для повышения надежности хранимых данных и способов верификации их подлинности. Среди имеющихся блокчейн-технологий для проведения сравнительного анализа выделены следующие платформы – Ethereum, Solana, Algorand. На основе библиографических исследований и сравнительного анализа устойчивости представленных блокчейн-платформ предложены ключевые элементы SWOT-анализа. Результаты сравнительного анализа опубликованы в статье [6].

Проведенный анализ подчеркивает важность адекватной языковой поддержки для ключевых аспектов разработки смарт-контрактов: управления активами, взаимодействия между контрактами и затратами. В частности, специализированные абстракции на уровне типов для создания активов, обмена ими и работы с ними являются фундаментальным элементом предотвращения распространенных ошибок и уязвимостей, таких как потеря активов, двойное расходование средств или несанкционированный перевод. В другой, но связанной учетной записи встроенная поддержка определенных функций базовой платформы (например, пользовательских токенов) имеет решающее значение для обеспечения безопасности и эффективности. С точки

зрения потенциала решения проблем, с которыми сталкивается образовательный сектор Ethereum известен своей функциональностью смарт-контрактов, которая позволяет создавать децентрализованные приложения и автоматизировать сложные рабочие процессы.

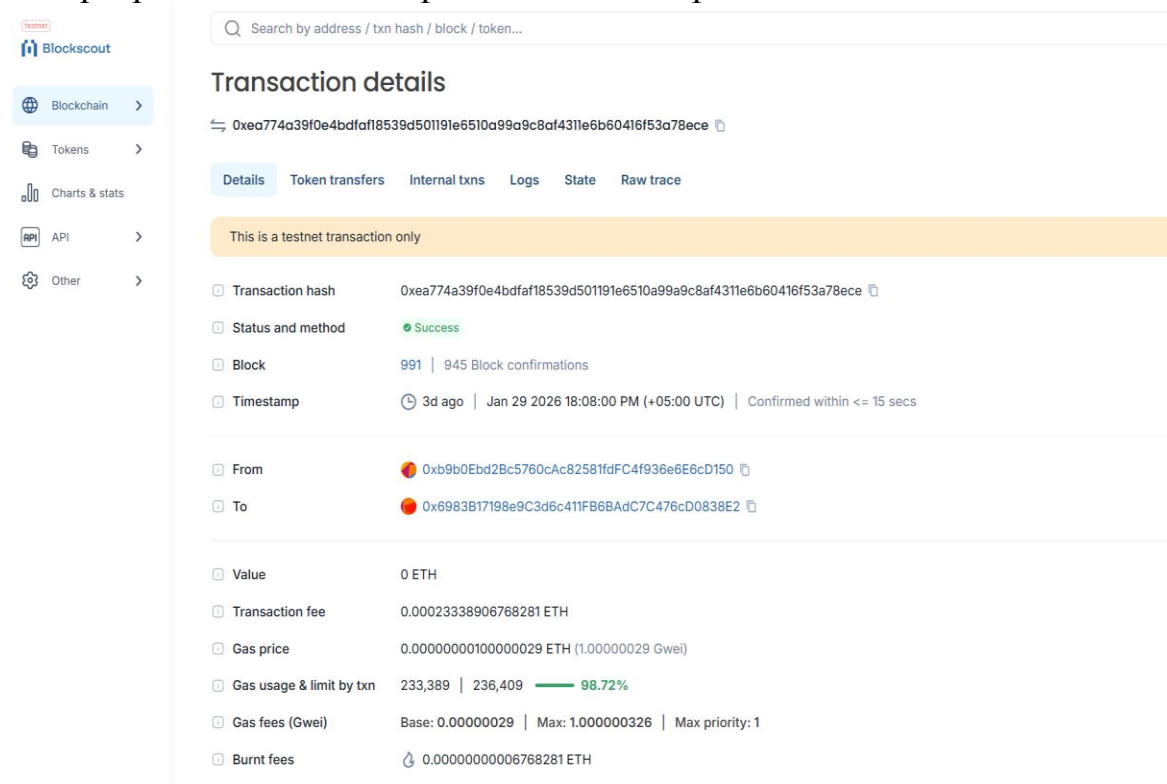
Таким образом, проведен обзор библиографии по применению блокчейн Ethereum, а также по ранее проведенному сравнительному анализу блокчейн-платформ Ethereum, Solana, Algorand выявлены основные параметры в рамках SWOT-анализа блокчейн-платформ [6].

Из обзора имеющихся решений на рынке, исследовательской группой принято решение об использовании блокчейн Ethereum, который позволит обеспечить безопасное хранение сертификатов, аттестатов, дипломов и иметь наличие достоверного, открытого и единого хранилища кандидатов с подтвержденными знаниями.

Материалы и методы.

В качестве материалов в данном исследовании, как описано выше, использована технология блокчейн Ethereum с применением в образовательном секторе Республики Казахстан.

На представленном скриншоте (рисунок 1) отображен интерфейс обозревателя блоков Blockscout, фиксирующий детали транзакции в тестовой сети (testnet). Данная запись служит подтверждением успешного выполнения смарт-контракта, предназначенного для передачи академического транскрипта. Blockscout – программа-оболочка для экосистемы Ethereum. Данная программа-оболочка предоставляет открытый исходник.



The screenshot displays the Blockscout testnet interface. On the left is a sidebar with navigation links: Blockchain, Tokens, Charts & stats, API, and Other. The main area is titled 'Transaction details' and shows a search bar at the top. Below the search bar, the transaction hash is displayed: 0xea774a39f0e4bdfaf18539d501191e6510a99a9c8af4311e6b60416f53a78ece. A yellow banner indicates 'This is a testnet transaction only'. The transaction status is 'Success'. The block number is 991, with 945 block confirmations. The timestamp is 3d ago, dated Jan 29 2026 18:08:00 PM (+05:00 UTC), confirmed within 15 seconds. The 'From' address is 0xb9b0Ebd2Bc5760cAc82581fdFC4f936e6E6cD150 and the 'To' address is 0x6983B17198e9C3d6c411FB6BAdC7C476cD0838E2. The transaction value is 0 ETH. The transaction fee is 0.00023338906768281 ETH. The gas price is 0.000000001000000029 ETH (1.000000029 Gwei). The gas usage is 233,389 out of 236,409, representing 98.72% of the limit. The gas fees (Gwei) are Base: 0.000000029, Max: 1.0000000326, and Max priority: 1. The burnt fees are 0.00000000006768281 ETH.

Рисунок 1 – Данные транзакции



Представленный скриншот демонстрирует практическую реализацию системы хранения образовательных документов на базе блокчейна. Использование тестовой сети позволяет верифицировать архитектуру решения, минимизировать издержки на этапе разработки и гарантировать, что каждый транскрипт получает уникальный, криптографически защищенный оттиск в публичном реестре.

Рассмотрим технические параметры транзакции, представленные в таблице 1:

Таблица 1 - Технические параметры транзакции

Название	Действие	Описание
Идентификатор транзакции	0xea774a39f0e4bdfaf18539d501191e6510a99a9c8af4311e6b60416f53a78ece.	Уникальный хэш обеспечивает неизменность и проверяемость записи в распределенном реестре
Статус исполнения	Success	Операция завершена успешно, что подтверждает корректность логики смарт-контракта
Временная метка	Транзакция зафиксирована 29 января 2026 года в 18:08:00 (UTC +05:00)	Время подтверждения составило менее 15 секунд, что свидетельствует о высокой пропускной способности сети на момент выполнения
Адресаты	From: 0xb9b0Ebd2Bc5760cAc82581fdFC4f936e6E6cD150	Адрес отправителя/инициатора
	To: 0x6983B17198e9C3d6c411FB6BadC7C476cD0838E2	Адрес смарт-контракта транскриптов
Экономические показатели	Value (Переданная стоимость): 0 ETH.	Это характерно для транзакций вызова функций контракта, где основной целью является запись или изменение данных (передача транскрипта), а не финансовый перевод

За технический анализ событий транзакции отвечает раздел Logs, который демонстрирует низкоуровневую фиксацию данных события (Event), инициированного смарт-контрактом по адресу 0x6983B17198e9C3d6c411FB6BadC7C476cD0838E2. Эти логи служат неизменяемым доказательством того, что определенные данные были успешно обработаны логикой контракта (рисунок 2).

Transaction details

0xea774a39f0e4bdfaf18539d501191e6510a99a9c8af4311e6b60416f53a78ece

Details Token transfers Internal txns **Logs** State Raw trace

To see accurate decoded input data, the contract must be verified. [Verify the contract here](#)

Address 0x6983B17198e9C3d6c411EB6BAc7C476cD0838E2 F

36

Topics [0](#) [0xfe18c84aba9622c89f9fb267039b264fcfb2ab599ed213a948ee0551188d41e5](#)

Data

[illegible]

Рисунок 2 – Вкладка Logs

Структура лога состоит из темы и сырых данных, при этом:

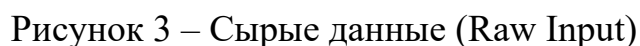
- Topics (Темы): Поле Topics[0] содержит хэш сигнатуры события: 0xfef18c84aba9622c89f9fb267039b264fcfb2ab599ed213a948ee0551188d41e5. В архитектуре EVM (Ethereum Virtual Machine) этот идентификатор позволяет внешним приложениям и исследователям однозначно определить, какая функция события была вызвана, даже если исходный код контракта скрыт.

- Data (Сырые данные): Поле Data содержит основную содержательную часть транскрипта, закодированную в шестнадцатеричном формате.

Использование событий (Events) и раздела Logs является наиболее эффективным способом хранения «доказательств» в блокчейне. Вместо дорогостоящего хранения всего текста транскрипта в состоянии (State) контракта, система генерирует лог. Это обеспечивает проверяемость и экономическую эффективность. То есть запись данных в логи значительно дешевле, чем в хранилище (storage) контракта, что критически важно для масштабируемых академических систем.

Анализ входных данных и параметров вызова (Raw Input). На скриншоте (рисунок 3) представлено поле Raw Input, содержащее шестнадцатеричный код (Hex), который был передан смарт-контракту в теле транзакции. Эти данные определяют, какую операцию выполняет контракт и какие параметры (данные транскрипта) в него записываются.

Использование стандарта EIP-1559 и передача данных в формате Raw Нех подтверждают, что система работает на уровне протокола EVM без посредников. Кодирование транскрипта непосредственно во входные данные транзакции гарантирует, что информация становится частью истории блока. Любое изменение в данных транскрипта приведет к изменению хэша транзакции, что делает подделку документа физически невозможной в рамках вычислительной мощности сети.



В ходе исследования по решению исследовательской группы, как отмечено выше используется технология блокчейн Ethereum. Данная технология реализована на языке Solidity.

Рисунок 4 – Фрагмент кода траскрипта



Solidity — это язык программирования для создания смарт-контрактов на блокчейнах, совместимых с виртуальной машиной Ethereum (EVM).

Представленный код на языке Solidity реализует децентрализованное хранилище транскриптов с интеграцией системы ролевого доступа (RBAC). Логика контракта разделена на три уровня: управление доступом, структурирование данных и неизменяемая фиксация событий.

Архитектурная логика смарт-контракта TranscriptStorage. Контракт не является автономным, а взаимодействует с внешним модулем управления ролями через интерфейс IRBAC. Непосредственно модификатор `onlyRole` используется для ограничения доступа к критическим функциям. Например, функция `saveTranscript` доступна только пользователям с ролью "issuer" (организация-эмитент), а обновление адреса RBAC — только "admin", что в свою очередь гарантирует безопасность и только авторизованные учебные заведения могут вносить записи в реестр.

Для оптимизации хранения и поиска используется комбинированный подход:

1) Объект Transcript группирует 10 ключевых полей, включая идентификаторы (`transcriptId`, `universityId`, `studentId`), академические успехи (`totalMark`, `ects`) и метаданные отправителя (`addedBy`).

2) Хэшированная индексация - функция `getKey`, которая генерирует уникальный ключ типа `bytes32` путем хэширования пары `universityId` и `studentId` с использованием алгоритма Кессак-256.

3) Хранилище `mapping` - все транскрипты студента сохраняются в динамический массив Transcript, доступ к которому осуществляется по сгенерированному ключу. Это позволяет эффективно масштабировать систему для хранения всей истории обучения.

Функция `saveTranscript` выполняет последовательность действий, гарантирующих целостность данных: Валидация, Инициализация, Запись в реестр, Эмиссия события (Вызов события `TranscriptSaved`, который генерирует те самые Logs, видимые в блокчейн-эксплорере).

Связь кода с данными блокчейна (Logs & Input). Когда вызывается `saveTranscript`, параметры (ID, оценки и т.д.) упаковываются в Hex-строку, которую мы видим в деталях транзакции. Событие `TranscriptSaved` дублирует все записанные данные в логи блокчейна. Это создает избыточность: данные хранятся и в состоянии контракта (для работы кода), и в логах (для дешевой и быстрой верификации внешними системами).

Заключение.

Реализованная логика обеспечивает целостность (через неизменяемость блокчейна), авторство (через привязку к `msg.sender`) и прозрачность (через публичные события). Хэширование идентификаторов позволяет структурировать данные без раскрытия связей между ними во внешних поисковых индексах, что повышает уровень приватности системы. В результате данного исследования спроектирован и разработан модуль



программы для интеллектуальной платформы децентрализованного цифрового реестра данных студентов и выпускников организаций высшего и послевузовского образования в существующей цифровой среде Министерства науки и высшего образования Республики Казахстан на основе блокчейна Ethereum.

Финансирование. Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования РК (программно-целевое финансирование на 2024-2026 годы ИРН BR24993014 "Разработка интеллектуальной антикоррупционной системы защиты информации и валидации результатов учебных достижений и официальных документов студентов и выпускников вузов РК").

ЛИТЕРАТУРА

1. Kistaubayev, Y., Mutanov, G., Mansurova, M., Saxenbayeva, Z., & Shakan, Y. (2023). Ethereum-Based Information System for Digital Higher Education Registry and Verification of Student Achievement Documents. *Future Internet*, 15(1), 3. <https://doi.org/10.3390/fi15010003>
2. Vaneetvelde, K. (2018). *Ethereum Projects for Beginners: Build Blockchain-Based Cryptocurrencies, Smart Contracts, and DApps* (1st ed.). Packt Publishing, Limited. <https://doi.org/10.0000/9781789531640>
3. Makarenko, N. (2022). DOCUMENT AUTHENTICATION USING BLOCKCHAIN: DIPLOMA VALIDATION AS A TEST CASE. *Nazarbayev University School of Engineering and Digital Sciences*.
4. S., S. P. F., L., M. S., & Sree, T. R. (2025). Decentralized certificate issuance and verification system using Ethereum blockchain technology. *Journal of Network and Computer Applications*, 242, Article 104190. <https://doi.org/10.1016/j.jnca.2025.104190>
5. Mohan, P. M., Balachandran, V., Quan, O. Z., Xin, J. P. Z., & Divakaran, D. M. (2022). NFT-Merit: An NFT-based Module Credit Management System on Ethereum Blockchain. *Proceedings of IEEE International Conference on Teaching, Assessment, and Learning for Engineering (Online)*, 472–476. <https://doi.org/10.1109/TALE54877.2022.00083>
6. Сравнительный анализ действующих блокчейн платформ. Мутанов Г., Есенгалиева Ж., Кистаубаев Е., Усатова О., Бегимбаева Е. *Труды Университета*, 2025, Т.2, С.401-407.

REFERENCES

1. Kistaubayev, Y., Mutanov, G., Mansurova, M., Saxenbayeva, Z., & Shakan, Y. (2023). Ethereum-Based Information System for Digital Higher Education Registry and Verification of Student Achievement Documents. *Future Internet*, 15(1), 3. <https://doi.org/10.3390/fi15010003>



2. Vaneetvelde, K. (2018). *Ethereum Projects for Beginners: Build Blockchain-Based Cryptocurrencies, Smart Contracts, and DApps* (1st ed.). Packt Publishing, Limited. <https://doi.org/10.0000/9781789531640>
3. Makarenko, N. (2022). DOCUMENT AUTHENTICATION USING BLOCKCHAIN: DIPLOMA VALIDATION AS A TEST CASE. Nazarbayev University School of Engineering and Digital Sciences.
4. S., S. P. F., L., M. S., & Sree, T. R. (2025). Decentralized certificate issuance and verification system using Ethereum blockchain technology. *Journal of Network and Computer Applications*, 242, Article 104190. <https://doi.org/10.1016/j.jnca.2025.104190>
5. Mohan, P. M., Balachandran, V., Quan, O. Z., Xin, J. P. Z., & Divakaran, D. M. (2022). NFT-Merit: An NFT-based Module Credit Management System on Ethereum Blockchain. *Proceedings of IEEE International Conference on Teaching, Assessment, and Learning for Engineering* (Online), 472–476. <https://doi.org/10.1109/TALE54877.2022.00083>
6. Sravnitel'nyj analiz dejstvujushhih blokchejn platform. Mutanov G., Esengalieva Zh., Kistaubaev E., Usatova O., Begimbaeva E. *Trudy Univeriteta*, 2025, T.2, S.401-407.

Жанна Есенгалиева, PhD, доцент, L.N. Gumilyov Eurasian National University, Астана, Қазақстан, jannayess@gmail.com

Ольга Усатова, PhD, доцент, Institute of Information and Computational Technologies CS MSHE RK, Алматы, Қазақстан, olgaussatova@gmail.com

Аида Есенгалиева, сарапшы, Institute of Information and Computational Technologies CS MSHE RK, Алматы, Қазақстан, aidayess11@gmail.com

БЛОКЧЕЙН НЕГІЗІНДЕ ҚАУІПСІЗ САҚТАУ ЖӘНЕ ДЕРЕКТЕР АЛМАСУ ҮШІН ИНТЕГРАЦИЯЛЫҚ ПРОГРАММАЛЫҚ МОДУЛЬДІ ӘЗІРЛЕУ

Аңдатпа. Ақпаратты қорғаудың зияткерлік сыбайлас жемқорлыққа қарсы жүйесінде деректерді тіркеу және оқу жетістіктерін валидациялау, сондай-ақ Қазақстан Республикасының жоғары оқу орындары мен әскери оқу орындары студенттері мен түлектерінің ресми құжаттары мақсатында бағдарламалық модуль әзірленді. Мақалада Ethereum blockchain технологиясы blockscout шолғышына негізделген, ол транзакция туралы мәліметтерді сынақ желісіне түсіреді. Зерттеу тобы блокчейн негізінде білім беру құжаттарын сақтау жүйесін практикалық іске асыруды ұсынды. Жазба академиялық транскрипт беруге арналған ақылды келісімшарттың сәтті орындалғанын растайды. Сынақ желісін пайдалану шешімнің архитектурасын тексеруге, әзірлеу кезеңіндегі шығындарды азайтуға және әрбір транскрипт қоғамдық тізілімде бірегей, криптографиялық қорғалған әсер алуын қамтамасыз етуге мүмкіндік береді. Сондай-ақ, мақалада



Ethereum блокчейнін білім беру саласында қолдануға қатысты библиографиялық шолу берілген.

Осылайша, solidity бағдарламалау тілінде blockscout шолғышының көмегімен жүзеге асырылатын блокчейн технологиясын қолдана отырып, студент немесе түлек порталында жұмыс істеу барысында шақырылатын сервис ұсынылды.

Түйінді сөздер: блокчейн, Ethereum, смарт-контракт, Blockscout, транзакциялар.

Zhanna Yessengaliyeva, PhD, associate professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, jannayess@gmail.com

Olga Ussatova, PhD, associate professor, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, olgaussatova@gmail.com

Aida Yessengaliyeva, expert, Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan, aidayess11@gmail.com

DEVELOPMENT OF AN INTEGRATION SOFTWARE MODULE FOR SECURE STORAGE AND DATA EXCHANGE BASED ON BLOCKCHAIN

Abstract. In order to record data in the intellectual anti-corruption information protection system and validate academic achievements, as well as official documents of students and graduates of universities and military educational institutions of the Republic of Kazakhstan, a software module has been developed. The article discusses the Ethereum blockchain technology based on the Blockscout browser, which records transaction details on the test network. The research group presented a practical implementation of a blockchain-based educational document storage system. The recording serves as confirmation of the successful execution of a smart contract designed to transfer an academic transcript. Using the testnet allows you to verify the architecture of the solution, minimize costs during the development phase, and ensure that each transcript receives a unique, cryptographically secure impression in the public registry. The article also provides a bibliographic overview of the use of the Ethereum blockchain in the field of education. Thus, a service is proposed that is invoked while working on the student or graduate's portal using blockchain technology, implemented using the Blockscout browser in the Solidity programming language.

Keywords: blockchain, Ethereum, smart contract, Blockscout, transactions.

Поступила: 04 июня 2026 года

Рецензирована: 08 июня 2026 года

Принята: 12 июня 2026 года