



МРНТИ 81.93.29

<https://doi.org/10.56132/2791-3368-2026-3-67-168-181>



Е.Е. Бегимбаева^{1,2}, О.А.Усатова^{1,2}, Ш.К. Кадиркулов³

¹ Institute of Information and Computational Technologies CS MSHE RK,
Алматы, Казахстан

² Energo University, Алматы, Казахстан

³ National Defense University of the Republic of Kazakhstan,
Астана, Казахстан

E-mail: ye.begimbayeva@aes.kz

ИНТЕГРИРОВАННАЯ СИСТЕМА АУТЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ЦИФРОВЫХ АКАДЕМИЧЕСКИХ ДОКУМЕНТОВ НА БАЗЕ БЛОКЧЕЙНА

Аннотация. Несмотря на то, что перевод академических документов в цифровой формат облегчил их хранение и обмен, вопросы аутентификации документа, выявления несанкционированных изменений и обеспечения безопасного использования между различными информационными системами остаются актуальными. В статье предлагается архитектура системы DNEP для регистрации и верификации академических документов. Данная система основана на гибридной модели данных OnChain/OffChain. Проанализированы серверные, блокчейн и интеграционные компоненты системы. Взаимодействие компонентов было проверено в локальной тестовой сети блокчейн. Для хранения операционной информации в разработанной архитектуре используется база данных OffChain на основе PostgreSQL, для академических записей и регистрации выполненных операций используется блокчейн. С помощью ролевой модели осуществляется ограничение доступа на уровнях API и смарт-контрактов. Интеграция с платформой SmartBridge позволяет проверять согласие субъекта при запросе персональных данных. В ходе эксперимента была проведена транзакция для регистрации академического транскрипта, результаты которой были проанализированы с помощью BlockScout. Был зарегистрирован статус success транзакции, израсходовано 233 389 единиц газа. Первоначальное время подтверждения было менее 15 секунд. Transaction Hash, событие TranscriptSaved и изменения состояния блокчейна позволили впоследствии проверить выполненную операцию. Данные результаты показали, что полная технологическая цепочка работает от регистрации академической записи в прототипе DNEP до подтверждения в блокчейне. В связи с тем что, эксперимент ограничен локальной тестовой средой, оценка производительности, а также масштабируемости системы требует дальнейшего изучения в условиях многопроцессорной нагрузки.



Ключевые слова: информационная безопасность, верификация, академические документы, блокчейн, смарт-контракт, архитектура OnChain/OffChain, управление ролевым доступом.

Введение.

Хранение в электронном виде дипломов и транскриптов и обмен между информационными системами стали нормальной частью современной образовательной инфраструктуры. При этом наличие электронной версии документа само по себе не подтверждает его подлинность. Важно во время верификации определить неизменность данных в документе, какая организация сформировала запись, какие операции с данными были выполнены.

В «Концепции цифровой трансформации, развития сферы информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы» определено развитие цифровых сервисов и обеспечение информационной безопасности в Казахстане как направления государственной цифровой политики [1]. В случае обмена данными с государственными информационными ресурсами системы образования задача безопасности не ограничивается только передачей информации. Также необходимо контролировать, кто получает доступ к персональным данным, и проверять, не изменилась ли электронная запись.

Проверка достоверности академического документа требует обращения в базу данных, хранящую документы в централизованной системе, или в организацию, выпустившую документ. Хотя этот метод удобен для повседневного использования, у этого метода есть ограничения. Они ограничивают возможность независимой проверки соответствия записей в различных системах и формирования неизменной истории выполненных операций. Одной из возможных технологических основ решения этих задач являются свойства блокчейна для распределенного реестра и регистрации транзакций в неизменном виде [2-4].

Данный метод используется в сфере образования в Blockcerts и других решениях для подтверждения академических credentials через блокчейн [5-7]. Однако сохранение записи в блокчейне само по себе не обеспечивает ее достоверности. Необходимо учитывать данные о том, кто внес документ, кто имеет полномочия, и кто имеет доступ к персональным данным. Поэтому в системе верификации академических документов недостаточно ограничиться компонентом блокчейна. Необходимо определить, какие данные хранятся в блокчейне, управлять оставшейся информацией в OffChain среде, распределять полномочия пользователей и организовывать безопасное взаимодействие с существующими информационными сервисами. Указанные задачи рассматриваются в статье в рамках единой архитектуры системы DNER.

Разработка гибридной архитектуры блокчейна OnChain/OffChain, решающие задачи регистрации, хранения и верификации академических



документов, и оценить ее работоспособность в тестовой среде являются целью исследования.

В предлагаемой архитектуре академические данные распределяются между уровнями OnChain и OffChain в зависимости от их деятельности. Управление доступом осуществляется через ролевую модель на уровнях API и смарт-контрактов, а обмен данными с внешними информационными сервисами организуется через SmartBridge. Для проверки работоспособности архитектуры академическая запись была зарегистрирована в тестовой сети блокчейна, а результаты выполнения транзакции были проанализированы с помощью BlockScout.

В предлагаемом решении не все академические данные хранятся в блокчейне: записи, необходимые для верификации, регистрируются на уровне OnChain, а операционные данные обрабатываются в среде OffChain. В архитектуре DNEP регистрация академических записей в блокчейне дополняется ролевым доступом на уровнях API и смарт-контрактов, проверкой согласия субъекта данных через SmartBridge и неизменным аудиторским следом транзакций. Объединение этих механизмов в одной системе составляет основное отличие предлагаемого решения.

В предлагаемой архитектуре работоспособность оценивалась экспериментально на основе выполнения транзакций смарт-контрактов в тестовой среде блокчейна и анализа их результатов через браузер блокчейнов BlockScout.

Обзор литературы и проблема исследования.

Возможность определения изменения записанной записи, отслеживание истории выполненных с ней операций при верификации цифровых документов является одним из основных преимуществ использования блокчейна. Использование криптографических методов и распределенный реестр позволяют документу или связанному с ним числовому аргументу фиксировать метку времени и формировать неизменный аудиторский след [2-4].

Метод proof – of-existence или hash-anchoring является одним из наиболее распространенных вариантов подтверждения цифровых документов в блокчейне. При таком подходе в блокчейн записывается не сам документ, а его криптографическое хеш-значение. При проверке пересчитанный хеш из документа сравнивается со значением в реестре. В результате исходный документ может храниться в среде OffChain и использоваться в качестве числового аргумента для проверки целостности блокчейна [3, 4]. В сфере образования такой подход используется для выдачи и проверки академических свидетельств, сертификатов, дипломов. Например, открытый стандарт Blockcerts позволяет третьей стороне проверять академический или профессиональный сертификат, не обращая напрямую к организации, которая его выпустила [5]. В исследованиях верификации академических документов с помощью блокчейна снижение зависимости от



централизованных сервисов и независимая проверка происхождения документа указываются как важные преимущества [6].

Неизменяемый реестр не является подтверждением подлинности внесенных сведений, если не была проведена предварительная проверка прав субъекта на совершение данной операции. Технологическая неизменность данных в распределенном реестре не обеспечивает автоматическую валидность академических документов. Следовательно, верификационный процесс требует комплексного подхода: помимо идентификации субъекта, выдавшего документ, необходимо осуществлять аудит его прав на осуществление соответствующих академических транзакций [6, 7].

Verifiable Credentials Data Model от W3C определяет структуру представления и проверки цифровых сертификатов. Стандарт предусматривает разделение ролей issuer, holder и verifier и предоставление сертификата в формате, который может быть обработан машиной и проверен криптографическими методами [8]. DNER не реализует этот стандарт напрямую, поэтому в исследовании он использовался для сравнения архитектурных решений. Взаимодействие с внешними информационными системами также важно для DNER, поскольку компонент блокчейна не работает отдельно от существующей инфраструктуры. Подобные решения, связывающие блокчейн с традиционными информационными системами, встречаются и в других прикладных областях [9].

При проектировании блокчейн системы, часть данных, которые регистрируются на уровне OnChain, часть которые хранятся в среде OffChain заранее определены. Поскольку размещение всех данных в блокчейне приводит к увеличению объема хранилища и транзакционных издержек, при использовании смарт-контрактов необходимо учитывать вопросы безопасности и масштабируемости [3, 4, 10]. Поэтому записи, которые регистрируются неизменным образом, вставляются в блокчейн, а объемные и ежедневно обрабатываемые данные хранятся в среде OffChain.

В рассмотренных работах представлены различные способы регистрации и проверки академических документов. Однако при их применении в конкретной информационной системе сохраняются вопросы проверки полномочий эмитента, организации взаимодействия данных OnChain и OffChain и ограничения доступа к персональным данным. К этому добавляется также необходимость обмена данными с государственными и образовательными информационными системами и последующей проверки выполненных операций.

В литературе перечисленные механизмы часто описываются в виде отдельных решений. В архитектуре DNER они объединяются в единую систему: академические данные распределяются между уровнями OnChain и OffChain, доступ управляется через роли в API и смарт-контрактах, а взаимодействие с внешними информационными сервисами осуществляется через интеграционный компонент. Транзакции, зарегистрированные в



блокчейне, используются для последующей проверки выполненных операций.

Материалы и методы.

Исследование включало программные, интеграционные, блокчейн-компоненты, которые разрабатывают процессы регистрации, хранения и верификации академических документов в экосистеме DNER. Проанализирована архитектура системы, модель данных OnChain/OffChain, управление ролевым доступом и интеграция с сервисами SmartBridge. Работоспособность предлагаемого решения была проверена путем выполнения транзакции регистрации академической записи в тестовой среде блокчейна.

Архитектура системы DNER.

Архитектура DNER объединяет клиентское веб-приложение, серверные API, базу данных OffChain на основе PostgreSQL и сеть блокчейнов. Запросы пользователей, поступающие из Веб-приложения, передаются и обрабатываются в DNER API. Операционные данные хранятся в среде OffChain. Академические записи, регистрируемые в блокчейне, отправляются в API сети блокчейн. Чтение данных OnChain также выполняется через этот интерфейс. DNER API управляет обменом данными между веб-приложением, базой данных OffChain и блокчейном.

В серверной части DNER используется подход Clean Architecture, в структуру которого входят Application, Domain, Infrastructure и Web. Включены уровни Api. Это распределение позволяет развивать бизнес-логику без прямой зависимости от баз данных и внешних интеграционных сервисов.

Схема взаимодействия компонентов DNER представлена на рисунке 1.

Организация данных OnChain и OffChain.

Архитектура DNER базируется на гибридном подходе к хранению данных, разделяя их на OnChain и OffChain сегменты в соответствии с интенсивностью использования. В то время как PostgreSQL-база берет на себя функции репозитория для операционных и справочных сведений, блокчейн-уровень задействуется исключительно для фиксации академических данных и транзакций, критически важных для обеспечения верификации. Таким образом, распределенный реестр в данной системе выполняет роль инструмента подтверждения подлинности, а не хранилища всей совокупности информации.

В Смарт-контракте структура Transcript используется для обработки академических транскриптов на уровне блокчейна. Часть идентификационных и академических атрибутов транскрипта обрабатывается на уровне OnChain. Идентификаторы образовательной организации и обучающегося объединяются при индексации записей. Ключ типа bytes32 генерируется алгоритмом Кескак-256. В системе DNER хэш не

заменяет полное содержание академического документа, он используется для поиска и идентификации записи OnChain.

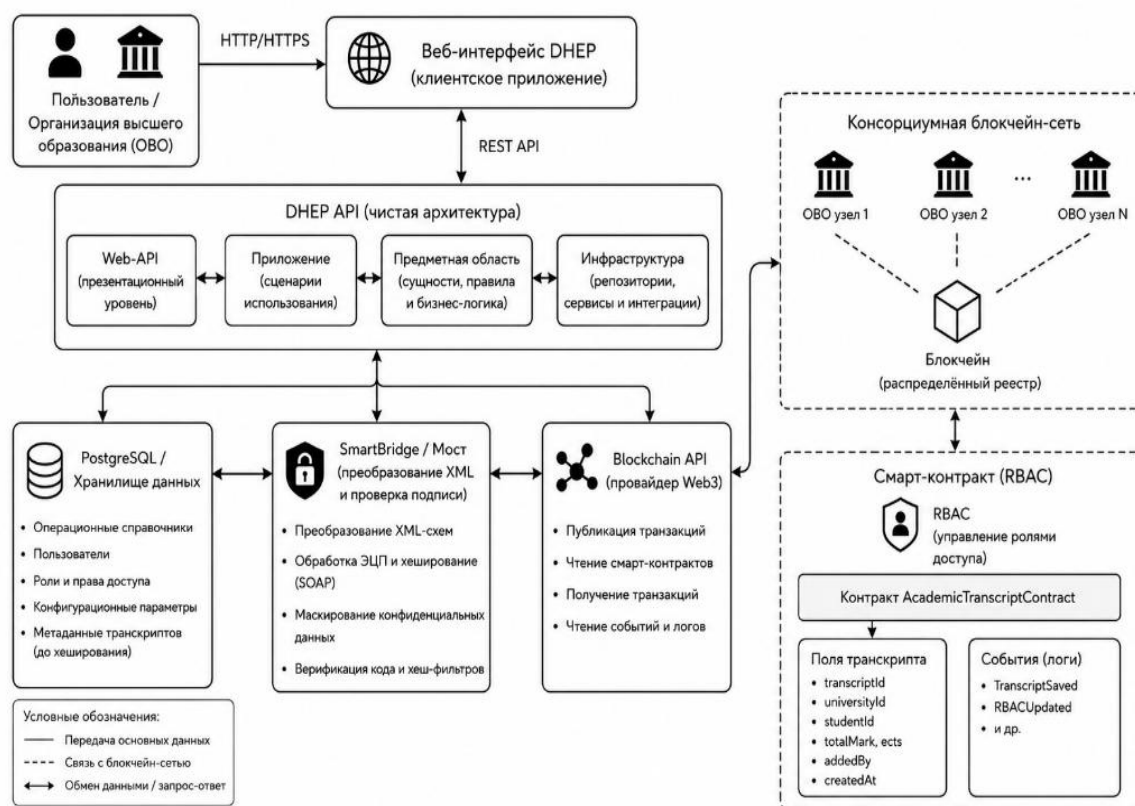


Рисунок 1 - Архитектура системы DHER для верификации академических документов

Таким образом, предлагаемая архитектура не ограничивается тем, как классический документ записывает только хеш-значение в блокчейн. Хеширование используется как инструмент для индексации академических записей. А фиксированная часть академических данных обрабатывается в состоянии смарт-контракта.

Механизм управления доступом.

Доступность контролируется на двух уровнях в dher. Серверные API используют разрешения permission для конкретных операций, а также роли USER, ADMIN, SUPER_ADMIN и API_USER. Данный механизм позволяет отдельно управлять общей ролью пользователя в системе и его правом на выполнение отдельных функций.

На уровне блокчейна авторизация выполняется через смарт-контракт RBAC. Вызов функции saveTranscript, которая регистрирует академический транскрипт, ограничен ролью "issuer", а для административных операций требуется роль "admin". Таким образом, право на ввод академической записи проверяется до выполнения операции, изменяющей статус блокчейна.



Такой подход позволяет отдельно управлять функциональными разрешениями на уровне API и полномочиями на выполнение операций, изменяющих состояние блокчейна.

Регистрация академической записи в блокчейне.

Запрос на регистрацию академического транскрипта передается компоненту блокчейна через API DHER. функция saveTranscript регистрирует запись транскрипта на основе принятых параметров. msg, который выполнил операцию в поле addedBy.адрес sender сохраняется. Когда Транзакция выполняется, событие TranscriptSaved регистрируется в журнале блокчейна. Полученный идентификатор транзакции связывается с академической записью в OffChain, а затем используется для проверки статуса его выполнения.

Интеграция с платформой SmartBridge.

Платформа SmartBridge выступает связующим шлюзом для интеграции DHER с государственными информационными сервисами. Чтобы получить персональные данные, система отправляет в веб-сервис контроля доступа к персональным данным (КДПД) подписанный ЭЦП XML-запрос. Ответ от сервиса приходит в формате SOAP, где указывается статус доступности информации. Этот шаг необходим для подтверждения академических документов

Обмен информацией между узлами DHER осуществляется посредством защищенных SSL-протоколов и авторизованных API-интерфейсов. Предварительный аудит показал наличие механизмов системы разграничения прав доступа и наличие инструментов логирования операций. При этом установлено, что дополнительное шифрование к хранящимся образовательным данным не применяется. Тем не менее, отсутствие сквозного шифрования данных в состоянии покоя (at rest) не позволяет классифицировать текущую архитектуру как полностью конфиденциальную. Обеспечение защиты хранимой информации определено как приоритетная задача для последующих этапов модернизации системы.

Среда разработки Смарт-контрактов.

Разработка и функциональная проверка Смарт-контрактов проводились в среде Hardhat; для компиляции использовались инструменты Solidity 0.8.20, а для тестирования-инструменты Chai/Mocha.

Экспериментальная среда блокчейна.

Работоспособность предлагаемой архитектуры была проверена в локальной тестовой среде, имитирующей сеть блокчейнов консорциума. Экспериментальная сеть была создана на основе Private Ethereum и в качестве блокчейн-клиента использовалась Go-Ethereum (Geth) v1.13.15. Три узла валидатора были запущены в контейнерах Docker и связаны через bridge network с подсетью 172.21.0.0/16.

В тестовой сети использовался консенсусный механизм Proof of Authority (PoA) и алгоритм Clique. Значение сетевого Chain ID составляет 1234, интервал формирования блока – 15 секунд, лимит блокировки Gas – 8



000 000. Эксперимент проводился в локальной среде, состоящей из трех валидаторов. Следовательно, полученные показатели характеризуют работоспособность архитектуры DNEP в пределах этой конфигурации и не используются для оценки производительности географически распределенной производственной линии.

Основные параметры экспериментальной среды приведены в таблице 1.

Таблица 1- Конфигурация экспериментальной среды блокчейна

Параметры	Значение
Блокчейн платформа	Private Ethereum
Blockchain client	Go-Ethereum (Geth) v1.13.15
Консенсус	Proof of Authority (Clique)
Количество валидаторов	3
Chain ID	1234
Block Time	15 с
Block Gas Limit	8 000 000
Размещение	Docker контейнеры
Сетевая топология	Bridge network, 172.21.0.0/16
Smart-contract framework	Hardhat
Solidity	0.8.20
Тестирование	Chai/Mocha

Результаты и обсуждение.

В ходе эксперимента академический транскрипт была зарегистрирована в локальной сети Private Ethereum с помощью прототипа DNEP. Данные транзакции были зарегистрированы в BlockScout, а статус ее выполнения и время подтверждения были проверены. Также были проанализированы объем отработанного газа, комиссия, события смарт-контракта и изменения состояния блокчейна после транзакции.

Результаты выполнения транзакции.

Транзакция регистрации академического транскрипта была проведена 29 января 2026 года и зарегистрирована в BlockScout со статусом Success. Операция получила уникальный Transaction Hash, а время первоначального подтверждения, указанное в интерфейсе, составляло менее 15 секунд.

В таблице 2 приведены основные количественные показатели экспериментальной операции.

Таблица 2- Результаты транзакции регистрации академического транскрипта

Показатели	Полученные значения
Статус транзакции	Success
Transaction Hash	0xea774a...a78ece
Время подтверждения	< 15 с
Gas Used	233 389



Transaction Gas Limit	236 409
Доля использования Gas	98,72 %
Transaction Value	0 ETH
Transaction Fee	0,00023338906768281 ETH
Экспериментальная среда	Local Private Ethereum testbed

На выполнение сделки было израсходовано 233 389 единиц газа, что соответствует 98,72% значения Gas Limit = 236 409, установленного для транзакции. Value = 0 ETH, потому что операция не связана с криптоактивным переводом и была выполнена для регистрации академической записи в смарт-контракте.

Анализ событий Смарт-контракта.

Данные Events/Logs в BlockScout выявили событие TranscriptSaved, созданное при регистрации академической записи. В журнале хранится идентификатор события topics[0], ABI-кодированные данные и адрес блокчейна, по которому была отправлена транзакция. Операция, выполненная с помощью этих данных, может быть сопоставлена с фактической транзакцией и адресом, по которому она была отправлена.

Анализ данных Raw Input.

В поле Raw Input отображались ABI-кодированные значения параметров, заданных функции смарт-контракта, в формате hexadecimal. Эти данные использовались для анализа входных параметров выполненного вызова функции. Поскольку ABI-кодирование не шифрует данные, результаты Raw Input не оценивались как показатель, подтверждающий конфиденциальность информации.

Анализ управления доступом.

В DNER API доступ управляется ролями и разрешениями permission, а на уровне смарт-контракта используется механизм RBAC. Поскольку не существует полного протокола отдельных транзакций negative-test для каждой роли, эффективность механизма авторизации не оценивалась количественными показателями в этой работе. Проведенный эксперимент подтвердил, что этапы регистрации академической записи в блокчейне и проверки ее транзакции с помощью BlockScout выполняются в тестовой среде.

Заключение.

В исследовании рассматривалась архитектура DNER, адаптированная к задачам регистрации и верификации академических документов. В системе академические данные распределяются между уровнями OnChain и OffChain, доступ управляется через роли в API и смарт-контрактах. Обмен данными с внешними информационными сервисами осуществляется через платформу SmartBridge, а транзакции, зарегистрированные в блокчейне, используются для последующей проверки операций, выполняемых с помощью академической записи.



Прототип DNEP был протестирован в тестовой сети Private Ethereum, состоящей из трех валидаторов. Транзакция регистрации академического транскрипта завершилась статусом Success. На его выполнение было потрачено 233 389 единиц газа, для транзакции был установлен Gas Limit = 236 409, а время первоначального подтверждения, указанное в BlockScout, составляло менее 15 секунд. Анализ данных Events / Logs, Raw Input и State Changes подтвердил, что можно отслеживать выполнение транзакции и связанные с ней записи блокчейна.

Эксперимент был ограничен локальной тестовой средой и функциональным сценарием регистрации одной академической записи. Следовательно, полученные показатели нельзя рассматривать как оценку производительности или масштабируемости системы DNEP. На следующем этапе необходимо протестировать систему на многопроцессорной нагрузке, выполнить сценарии negative-test для различных ролей и проверить безопасность смарт-контрактов с помощью методов формальной верификации и статического анализа [11, 12]. Усиление конфиденциальности академических данных, хранящихся на уровне OnChain, также требует отдельного исследования.

Финансирование. Исследование выполнено в рамках программно-целевого финансирования Комитета науки Министерства науки и высшего образования Республики Казахстан 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»).

СПИСОК ЛИТЕРАТУРЫ

1. Правительство Республики Казахстан. Об утверждении Концепции развития цифровой трансформации, информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы: постановление Правительства Республики Казахстан от 28 марта 2023 года № 269.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008.
3. Zheng Z., Xie S., Dai H.-N., Chen X., Wang H. Blockchain challenges and opportunities: A survey // International Journal of Web and Grid Services. — 2018. — Vol. 14, No. 4. — P. 352–375.
4. Casino F., Dasaklis T. K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues // Telematics and Informatics. — 2019. — Vol. 36. — P. 55–81.
5. Blockcerts. The Open Standard for Blockchain Credentials: Introduction and Technical Documentation [Electronic resource]. URL: официальный сайт Blockcerts
6. Bapat C. Blockchain for Academic Credentials. — 2020. — arXiv:2006.12665.



7. Pathak S., Gupta V., Malsa N., Ghosh A., Shaw R. N. Smart contract for academic certificate verification using Ethereum // *Advanced Computing and Intelligent Technologies. Lecture Notes in Electrical Engineering*. — Vol. 914. — Springer, 2022. DOI: 10.1007/978-981-19-2980-9_29.
8. World Wide Web Consortium (W3C). Verifiable Credentials Data Model v1.1. — 2022.
9. Putra P. O. H., Muda I., Bakry M. R., Yusuf C., Santosa I. A framework for integrated e-notary services based on blockchain for civil law notaries: The case of Indonesia // *International Journal on Informatics Visualization*. — 2025. — Vol. 9, No. 1. — P. 153–162. DOI: 10.62527/joiv.9.1.3170.
10. Taherdoost H. Smart contracts in blockchain technology: A critical review // *Information*. — 2023. — Vol. 14, No. 2. — Art. 117. DOI: 10.3390/info14020117.
11. Yang Z., Dai M., Guo J. Formal modeling and verification of smart contracts with Spin // *Electronics*. — 2022. — Vol. 11, No. 19. — Art. 3091. DOI: 10.3390/electronics11193091.
12. Kezadri Hamiaz M., Driss M. Ethereum smart contracts under scrutiny: A survey of security verification tools, techniques, and challenges // *Computers*. — 2025. — Vol. 14, No. 6. — Art. 226. DOI: 10.3390/computers14060226.

REFERENCES

1. Pravitel'stvo Respubliki Kazahstan. Ob utverzhdenii Konceptii razvitiya cifrovoj transformacii, informacionno-kommunikacionnyh tehnologij i kiberbezopasnosti na 2023-2029 gody: postanovlenie Pravitel'stva Respubliki Kazahstan ot 28 marta 2023 goda № 269.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008.
3. Zheng Z., Xie S., Dai H.-N., Chen X., Wang H. Blockchain challenges and opportunities: A survey // *International Journal of Web and Grid Services*. — 2018. — Vol. 14, No. 4. — P. 352–375.
4. Casino F., Dasaklis T. K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues // *Telematics and Informatics*. — 2019. — Vol. 36. — P. 55–81.
5. Blockcerts. The Open Standard for Blockchain Credentials: Introduction and Technical Documentation [Electronic resource]. URL: oficial'nyj sajt Blockcerts
6. Bapat C. Blockchain for Academic Credentials. — 2020. — arXiv:2006.12665.
7. Pathak S., Gupta V., Malsa N., Ghosh A., Shaw R. N. Smart contract for academic certificate verification using Ethereum // *Advanced Computing and Intelligent Technologies. Lecture Notes in Electrical Engineering*. — Vol. 914. — Springer, 2022. DOI: 10.1007/978-981-19-2980-9_29.
8. World Wide Web Consortium (W3C). Verifiable Credentials Data Model v1.1. — 2022.



9. Putra P. O. H., Muda I., Bakry M. R., Yusuf C., Santosa I. A framework for integrated e-notary services based on blockchain for civil law notaries: The case of Indonesia // International Journal on Informatics Visualization. — 2025. — Vol. 9, No. 1. — P. 153–162. DOI: 10.62527/joiv.9.1.3170.

10. Taherdoost H. Smart contracts in blockchain technology: A critical review // Information. — 2023. — Vol. 14, No. 2. — Art. 117. DOI: 10.3390/info14020117.

11. Yang Z., Dai M., Guo J. Formal modeling and verification of smart contracts with Spin // Electronics. — 2022. — Vol. 11, No. 19. — Art. 3091. DOI: 10.3390/electronics11193091.

12. Kezadri Hamiaz M., Driss M. Ethereum smart contracts under scrutiny: A survey of security verification tools, techniques, and challenges // Computers. — 2025. — Vol. 14, No. 6. — Art. 226. DOI: 10.3390/computers14060226.

Енлик Бегимбаева, PhD, профессор, Institute of Information and Computational Technologies CS MSHE RK, Energo University, Алматы, Қазақстан, ye.begimbayeva@aues.kz

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

Шингис Кадиркулов, ә.ғ.к., PhD, қауымдастырылған профессор, National Defense University of the Republic of Kazakhstan, Астана, Қазақстан, ksh777@mail.ru

БЛОКЧЕЙН НЕГІЗІНДЕ ЦИФРЛЫҚ АКАДЕМИЯЛЫҚ ҚҰЖАТТАРДЫ АУТЕНТИФИКАЦИЯЛАУ МЕН ВЕРИФИКАЦИЯЛАУДЫҢ ИНТЕГРАЦИЯЛАНҒАН ЖҮЙЕСІ

Аңдатпа. Академиялық құжаттарды цифрлық форматқа көшіру оларды сақтау мен бөлісуді жеңілдетсе де, құжаттың аутентификациясы, рұқсат етілмеген өзгерістерді анықтау және әртүрлі Ақпараттық жүйелер арасында қауіпсіз пайдалануды қамтамасыз ету мәселелері өзекті болып қала береді. Мақалада академиялық құжаттарды тіркеу және тексеру үшін dher жүйесінің архитектурасы ұсынылады. Бұл жүйе OnChain / OffChain гибриді деректер моделіне негізделген. Жүйенің серверлік, блокчейн және интеграциялық компоненттері талданады. Компоненттердің өзара әрекеттесуі жергілікті blockchain сынақ желісінде тексерілді. Өзірленген архитектурада операциялық ақпаратты сақтау үшін PostgreSQL негізіндегі offchain дерекқоры пайдаланылады, академиялық жазбалар мен орындалған операцияларды тіркеу үшін блокчейн қолданылады. Рөлдік модельдің көмегімен API және ақылды келісімшарттар деңгейлерінде қол жетімділікті шектеу жүзеге асырылады. SmartBridge платформасымен Интеграция дербес деректерді сұрау кезінде субъектінің келісімін тексеруге мүмкіндік береді.



Эксперимент академиялық транскрипті тіркеу үшін транзакция жүргізді, оның нәтижелері BlockScout көмегімен талданды. Success транзакция мәртебесі тіркелді, 233 389 бірлік газ жұмсалды. Бастапқы растау уақыты 15 секундтан аз болды. Transaction Hash, transcriptsaved оқиғасы және блокчейн күйінің өзгеруі кейіннен орындалған операцияны тексеруге мүмкіндік берді. Бұл нәтижелер толық технологиялық тізбек dher прототипіндегі академиялық жазбаны тіркеуден бастап блокчейнде растауға дейін жұмыс істейтінін көрсетті. Осыған байланысты эксперимент жергілікті сынақ ортасымен шектеледі, өнімділікті бағалау, сондай-ақ жүйенің ауқымдылығы көп процессорлы жүктеме жағдайында одан әрі зерттеуді қажет етеді.

Түйінді сөздер: ақпараттық қауіпсіздік, тексеру, академиялық құжаттар, блокчейн, ақылды келісімшарт, OnChain/offchain архитектурасы, рөлге қол жеткізуді басқару.

Yenlik Begimbayeva, PhD, professor, Institute of Information and Computational Technologies CS MSHE RK, Energo University, Astana, Kazakhstan, ye.begimbayeva@au.es.kz

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

Shyngys Kadirkulov, candidate of military sciences, PhD, associate professor, National Defense University of the Republic of Kazakhstan, Astana, Kazakhstan, ksh777@mail.ru

INTEGRATED SYSTEM OF AUTHENTICATION AND VERIFICATION OF DIGITAL ACADEMIC DOCUMENTS BASED ON BLOCKCHAIN

Abstract. Despite the fact that the digitization of academic documents has facilitated their storage and exchange, the issues of document authentication, detection of unauthorized changes and ensuring safe use between different information systems remain relevant. The article proposes the architecture of the DHER system for registration and verification of academic documents. This system is based on a hybrid OnChain/OffChain data model. The server, blockchain, and integration components of the system are analyzed. The interaction of the components was tested on the local blockchain test network. The developed architecture uses an OffChain database based on PostgreSQL to store operational information, and a blockchain is used for academic records and registration of completed operations. The role model restricts access at the API and smart contract levels. Integration with the SmartBridge platform allows you to verify the consent of the subject when requesting personal data. During the experiment, a transaction was carried out to register an academic transcript, the results of which were analyzed using BlockScout. The success transaction status was registered, and



233,389 units of gas were consumed. The initial confirmation time was less than 15 seconds. The Transaction Hash, the TranscriptSaved event, and changes in the state of the blockchain made it possible to subsequently verify the completed operation. These results showed that the full technological chain works from the registration of an academic record in the DHEP prototype to the confirmation in the blockchain. Due to the fact that the experiment is limited to a local test environment, evaluating the performance and scalability of the system requires further study under multiprocessor load conditions.

Keywords: information security, verification, academic documents, blockchain, smart contract, OnChain/OffChain architecture, role-based access management.

Поступила: 09 июля 2026 года

Рецензирована: 01 сентября 2026 года

Принята: 08 сентября 2026 года