http://dx.doi.org/10.35596/1729-7648-2020-18-7-14-22

УДК 334.029.3

Оригинальная статья
Original paper

ПОДХОД И МОДЕЛИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ ДЛЯ ПОДТВЕРЖДЕНИЯ ДОСТОВЕРНОСТИ ДОКУМЕНТОВ В ОБРАЗОВАНИИ

КАЧАН Д.А., ВИШНЯКОВ В.А.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

Поступила в редакцию 20 февраля 2020

Аннотация. Целью данной статьи является анализ методов, подходов, средств технологии распределенных реестров для работы с документами в образовании. Задачами статьи являются анализ проблем с подтверждением достоверности документов об образовании, разработки новых структурных решений с использованием технологии блокчейн, рассмотрение двух моделей, а также оценка возможности их использования для документов об образовании.

Подтверждение документов об образовании осуществляется с использованием государственных реестров, что является сложным и ресурсоемким процессом. В мире наблюдается рост количества поддельных документов, что ставит под сомнение эффективность применяемых современных механизмов. Технология распределенных реестров (блокчейн) является устойчивым технологическим трендом, влияющим на развитие и качество цифровой экономики. Наличие механизма проверки достоверности документов об образовании, устойчивого к злонамеренному манипулированию, является актуальной задачей, выходящей за рамки сферы образования, возможные способы решения которой предложены в данной работе.

В статье приведена краткая характеристика технологии распределенных реестров. Рассмотрен подход применения технологии для подтверждения достоверности документов об образовании, состоящий из двух основных этапов: эмиссия цифрового документа об образовании и проверка. Рассмотрена роль доверенной третьей стороны в процессе эмиссии и проверки. Приводятся модели эмиссии и подтверждения цифрового документа на основе технологии распределенных реестров, которая позволяет устранить ограничения и недостатки существующих подходов, выявлена эффективность подхода на базе предложенных моделей. Сформулированные подходы могут быть применимы в различных социально-экономических сферах и сфере государственного управления для работы с аналогичными документами.

Ключевые слова: технология распределенных реестров, блокчейн, смарт-контракт, информационные технологии в образовании, подтверждение подлинности.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Качан Д.А., Вишняков В.А. Подход и модели применения технологии распределенных реестров для подтверждения достоверности документов в образовании. Доклады БГУИР. 2020; 18(7): 14-22.

APPROACH AND MODELS FOR USING DISTRIBUTED LEDGER TECHNOLOGY TO AUTHENTICATE EDUCATIONAL DOCUMENTS

DMITRY A. KACHAN, ULADZIMIR A. VISHNIAKOU

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Submitted 20 February 2020

Abstract. The purpose of this article is to analyze methods, approaches, and tools of distributed ledger technology (DLT) for working with documents in education. The objectives of the article are to analyze problems with the authentication of educational documents, develop new structural solutions using block chain technology, consider two models, and evaluate their use for educational documents.

Authentication of educational documents is carried out using state registers, which is a complex and resource-intensive process. There is an increase in the number of forged documents in the world, which calls into question the effectiveness of modern mechanisms. Distributed ledger technology (block chain) is a sustainable technological trend that affects the development and quality of the digital economy. The existence of a mechanism for verifying the authenticity of educational documents that is resistant to malicious manipulation is an urgent task that goes beyond the sphere of education, possible solutions to which are proposed to be considered in this paper.

The article provides a brief description of DLT and considers the approach of using the technology to authenticate educational documents. It consists of two main stages: the issue of a digital educational document and its verification. The role of a trusted third party in the issue and validation process is considered. The paper presents the models for issuing and validating digital documents based on distributed ledger technology, which allows one to eliminate the limitations and shortcomings of existing approaches. The effectiveness of the approach based on the proposed models is revealed. The formulated approaches can be applied in various socio-economic areas and public administration to work with similar documents.

Keywords: distributed ledger technology, blockchain, smart contract, information technologies in education, authentication.

Conflict of interests. The authors declare no conflict of interests.

For citation. Kachan D.A., Vishniakou U.A. Approach and models for using distributed ledger technology to authenticate educational documents. Doklady BGUIR. 2020; 18(7): 14-22.

Введение

Проблема подтверждения достоверности документов об образовании за последние двадцать лет обострилась. В соответствии с докладом «Global Corruption Report: Education», подготовленным организацией Transparency International в 2018 году, в образовании сложилась устойчивая тенденция лавинообразного роста так называемых «degree mill» – учреждений образования, выдающих поддельные документы об образовании, лицензии и др. [1]. В работе [2] приводятся следующие данные:

– в мире насчитывается более 3300 непризнанных университетов, которые осуществляют выдачу поддельных документов об образовании;

– на счету международного преступного синдиката, территориально расположенного в Европе и на Ближнем Востоке, по всему миру получили распространение более 450 000 поддельных дипломов;

– количество ежегодно полученных степеней PhD в США составляет от 40 000 до 45 000 каждый год, количество поддельных – свыше 50 000.

Другой причиной, определяющей необходимость внедрения универсального механизма подтверждения документов об образовании, является миграция населения. Вынужденная

миграция, обусловленная политическими и экономическими факторами, может сопровождаться полной потерей бумажных носителей, подтверждающих полученные квалификации. Сюда также можно добавить стихийные бедствия, реструктуризацию учреждений, что в ряде случаев делает сложным или невозможным подтверждение полученных квалификаций.

Особенности технологии распределенных реестров

Технология распределенных реестров (ТРР) − блокчейн является одним из прорывных решений в рамках белорусской программы «Цифровая экономика». Благодаря заложенному при создании потенциалу и научному заделу, ТРР имеет широкие границы применения и постоянно совершенствуется, открывая все новые способы использования не только как средства осуществления финансовых транзакций [3], но и как средства оптимизации методик управления, в том числе наиболее сложной его разновидности – информационного управления [4]. В работе [5] выделены основные этапы распространения технологии распределенных реестров:

– ТРР версии 1.0 связана с применением криптовалют для финансовых транзакций;

– ТРР версии 2.0 расширяет применимость до заключения цифровых контрактов, дополняя или заменяя традиционные формы договоренностей;

– ТРР версии 3.0 обозначает расширение применения технологии в нефинансовых институтах – сфера государственного управления, здравоохранения, образования и др.

Консенсус в сети ТРР означает согласие участников с определенным состоянием системы как с истинным состоянием и приводит к тому, что все вычислительные узлы совместно используют одни и те же данные, а изменение общего знания происходит по заданному общепринятому алгоритму [6]. Реализация механизма консенсуса осуществляется различными способами, наиболее популярным из которых является механизм POW (Proof-of-Work), предложенный создателем блокчейн-сети Bitcoin [7]. Критика по предложенному алгоритму достижения консенсуса, ввиду неэффективного использования вычислительных мощностей, привела к развитию усовершенствованных алгоритмов, лишенных большинства недостатков POW. В их числе: POS (Proof-of-Stake), POET (Proof-of-Elapsed Time), SBFT (Simplified Byzantine Fault Tolerance), POA (Proof-of-Authority), IBFT (Istanbul Byzantine Fault Tolerance), DAG (Directed Acyclic Graphs) и др. [6].

Дополнительным понятием, используемым при описании особенностей процессов информационного обмена участников сети ТРР, является криптографический токен – вид внутрисетевой «валюты» [8]. С точки зрения информационных технологий токен – это подтверждение прав на выполнение какой-либо транзакции или управление правами доступа. Криптографический токен, используемый в ТРР, совмещает два принципа: метафорическое понимание традиционного платежного средства, его область влияния и права доступа в сети блокчейн. На начальном пути использования ТРР вошло понятие «майнинга» – процесса добывания криптографических токенов [9] – это вознаграждение участникам за предоставление своих вычислительных мощностей для поддержки работы всей сети, поддерживающей ТРР.

Подходы к подтверждению документов на основе блокчейн

Технологически подтверждение достоверности документов является одной из ключевых характеристик технологии распределенных реестров. Технология ТРР позволяет осуществлять подтверждение достоверности (существования) записи в виде хэш-суммы контролируемого документа. Это позволяет построить сервис, который сравнивает представленный документ с хранимым в сети блокчейн, не нарушая конфиденциальность данных – сами документы в сеть не попадают, сравнение осуществляется только на основе их хэш-значений.

Доказательство существования (Proof of Existence). Для получения возможности использования этого механизма используется функция OP_RETURN, отвечающая

за «уничтожение» криптовалютных токенов (используется в механизме консенсуса Proof-of-Burn – подтверждение уничтожения), которой присваивается хэш-значение документа.

Функция OP_RETURN с 2015 года имеет ограничение на длину данных в 40 байт, что является оптимальным значением ввиду используемого алгоритма вычисления хэш-функции SHA-2 (256 бит) – полученное значение хэш-функции имеет длину в 32 байта [10]. Процедура проверки осуществляется по следующему алгоритму – проверяющей стороной вычисляется хэш-значение электронной версии документа и сравнивается полученное значение со значением, указанным в первой транзакции, когда данные были отправлены в блокчейн. На основании сравнения принимается решение о достоверности документа.

Текущее состояние. Учреждения образования осуществляют выдачу дипломов в бумажном виде. Полученные дипломы на бумажных носителях подвержены уничтожению в случае стихийных бедствий и фальсификации. Необходимо установление отдельных связанных подпроцессов для учреждения образования, определяющих выпуск цифровых документов об образовании с использованием TPP для хранения цифровых «аналогов» документов, а также определение эффективного механизма проверки достоверности документа без участия третьей стороны. Преимущества: надежность хранения, отсутствие посредников в процессе проверки, достоверность полученных данных.

Ограничения. На текущий момент имеется три ограничения. Отсутствует единый формат цифрового документа, что может решаться в рамках Болонского процесса. Отсутствуют производительные информационные системы, способные обеспечить выполнение алгоритмов выдачи/проверки в автоматическом режиме. Отсутствуют законодательные основы цифрового подтверждения достоверности без участия уполномоченного лица – подтверждение документов об образовании осуществляется путем проставления апостиля на копию либо оригинал документа в соответствии с постановлением Гаагской конвенции 1961 года.

Проблема проверки достоверности. Транзакции, связанные с механизмами подтверждения авторства или достоверности с помощью цифрового аналога документа, применяются для предъявления доказательства одной стороны другой. Проверяющая сторона сверяет хэш-значение, временную метку транзакции и принадлежность записи предъявителя. Механизм для автоматизированного подтверждения достоверности документа на основе использования TPP охватывает лишь две стороны (предъявитель и проверяющий), что недостаточно в случае официальных документов, эмитент которых обязательно должен присутствовать в модели в качестве доверенной третьей стороны (ДТС). Модель подтверждения должна устанавливать не только принадлежность документа эмитенту, но и подтверждать полномочия эмитента на осуществление данного вида деятельности и дополнительные сведения (например, для сферы образования – перечни специальностей подготовки в определенный период времени в соответствии с лицензией). В результате возникает задача получения достоверных данных о ДТС, что говорит о необходимости наднационального органа (в рамках ЕС), хранящего информацию о ДТС. Возможные сценарии подтверждения достоверности: проверка на основании электронно-цифровой подписи; проверка на основании транзакции в сети блокчейн.

Для обоих сценариев проверяющей стороне необходима информация о достоверности предоставленных публичных ключей (их принадлежность к эмитенту) или о принадлежности эмитенту аккаунтов, с которых были совершены транзакции в сеть блокчейн. В обоих случаях требуется доказать полномочия эмитента, в том числе в заданном временном промежутке.

Для целей проверки достоверности документов об образовании в системе Blockcerts (США, Массачусетский институт технологий) используются собственная модель распределенных цифровых идентификаторов, разработанная на основании уникального универсального идентификатора UUID [11], адаптированная модель связанных данных JSON-LD (Linked Data), собственный метод нормализации документа. В качестве одного из основных цифровых идентификаторов предлагается использование URL учреждения образования, достоверность документа зависит от доступности сетевого ресурса сервиса.

Модели эмиссии и подтверждения цифрового документа

Структурная модель процесса эмиссии и выдачи цифрового документа, выполненная в системе условных обозначений бизнес-процессов BPMN 2.0 по TPP, приведена на рис. 1. В основе модели лежит специализированное используемое пользователем мобильное приложение, имеющее функционал электронного криптовалютного «кошелька».

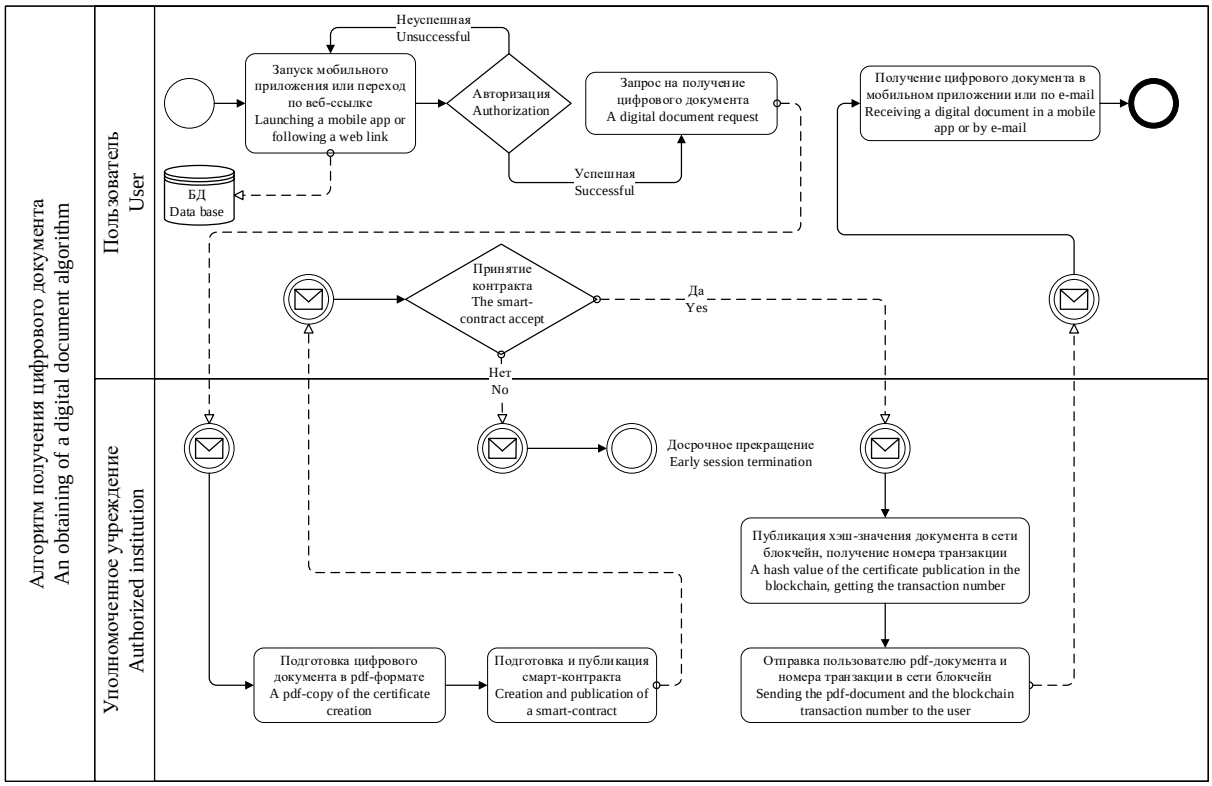

Рис. 1. Модель процесса получения цифрового документа
Fig. 1. Model of the process of obtaining a digital document

Регистрация пользователя (обучающегося) может осуществляться централизованно для лиц, находящихся в процессе обучения, и лиц, данные которых содержатся в базах данных учреждения образования. Для лиц, закончивших обучение и данные которых не содержатся в электронных базах данных, механизм подтверждения может состоять из отправки электронной копии документов об образовании, а также персональных данных для подтверждения регистрации в приложении, установления достоверности документов и последующей подготовки их электронной версии.

После успешной авторизации в приложении пользователь принимает решение об оформлении электронного запроса на получение цифрового документа об образовании. В случае наличия данных пользователя в существующих базах данных дальнейшие шаги осуществляются автоматически на основании заданных в программном обеспечении последовательностей действий: осуществляется проверка более ранних обращений пользователя, при которых процедура подготовки цифрового документа и размещения его хэш-суммы в сети блокчейн уже осуществлялась.

В случае отсутствия записей о ранних обращениях происходит автоматическое формирование цифрового документа в JSON-формате, осуществляется его нормализация (приведение к некому стандартизированному представлению) и происходит публикация смарт-контакта между пользователем и учреждением по выполнению размещения документа в сети блокчейн.

Пользователь получает извещение о предложении заключения смарт-контракта в приложении, и в случае положительного решения происходит следующая последовательность действий: вычисляется значение хэш-функции нормализованного документа JSON-формата с использованием криптографического алгоритма (SHA-2) и формируется сообщение,

состоящее из значения хэш-функции документа, цифровой подписи и номера транзакции в сети блокчейн, необходимое для подтверждения достоверности размещения. Сообщение шифруется асимметричным шифрованием с использованием полученного от пользователя в запросе открытого ключа и передается в приложение пользователя, где расшифровывается закрытым ключом и может быть преобразовано из JSON-формата в вид документа, пригодный к формальному графическому представлению, понятному для человеческого восприятия. В случае если в базе данных содержится информация о предыдущей выдаче запрашиваемого документа об образовании, пакет документов из архива предоставляется пользователю без размещения в сети блокчейн.

Для последующего подтверждения достоверности информация, содержащаяся в реестре ДТС, интегрируется непосредственно в документ, а именно хэш-значение данных о лицензии учреждения, адреса аккаунтов учреждения в сети блокчейн, необходимые номера транзакций, URL для проверки достоверности данных учреждения и др.

Модель подтверждения цифрового документа. Структурная модель процесса подтверждения выданного цифрового документа, без непосредственного участия третьей стороны, выполненная в системе условных обозначений бизнес-процессов BPMN 2.0, приведена на рис. 2. Для подтверждения достоверности проверяющая сторона сверяет данные ДТС с предоставленными данными. Основная решаемая задача на первом этапе проверки – определение достоверности данных об эмитенте. При установлении соответствия происходит второй этап – проверка достоверности документа, а именно его принадлежность эмитенту, достоверность подтверждающей транзакции, хэш-значение и соответствие указанных данных.

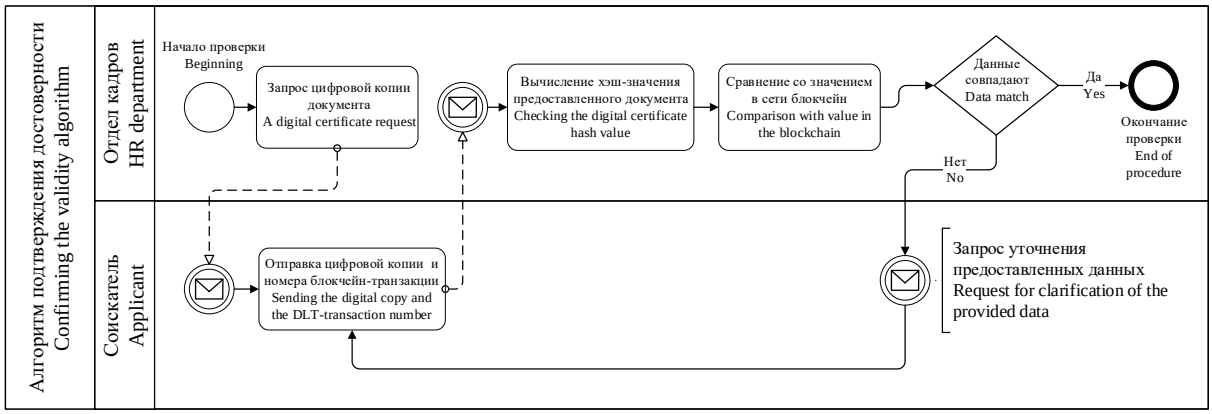

Рис. 2. Модель подтверждения достоверности документа
Fig. 2. Document validation model

Эффективность предложенного метода на основе блокчейн

По сложности итоговой системы подходы на основе цифровой подписи и блокчейн-платформы являются относительно эквивалентными. Оптимальным решением стоит считать сочетание обоих подходов, что даст эффект и повысит надежность системы. Использование блокчейн-платформы в процессах подтверждения достоверности документов предоставляет следующие дополнительные возможности:

– технология распределенных реестров имеет огромный потенциал использования. Наличие ДТС, хранящей данные об электронных аккаунтах учреждений, позволяет построить систему проверки достоверности персональных документов сотрудников и обучающихся, используя схожие механизмы;

– система, построенная на основе блокчейн, практически неуязвима для злонамеренного манипулирования данными;

– использование только электронно-цифровых подписей имеет следующий недостаток: рост вычислительных возможностей делает неустойчивыми ретроспективные данные, а документы об образовании имеют жизненный цикл, значительно превышающий жизненный цикл технологий криптографии;

– криптографическая стойкость сети блокчейн адаптируется в соответствии с вычислительной мощностью вовлеченных участников и находится на постоянно высоком уровне;

– социальные факторы – электронный аккаунт, как подтверждение авторства, адекватно воспринимается пользователями;

– технология распределенных реестров на текущем уровне развития является известным и описанным технологическим трендом и имеет высокий уровень технологической готовности – не ниже TRL9 (технология, прошедшая испытания, имеющая сопроводительную документацию и готовая к промышленному применению) в соответствии с принятой классификацией, предложенной в США (NASA);

– технология прошла пик завышенных ожиданий кривой Гартнера, сохранив достаточный потенциал и доказав свою жизнеспособность [4].

Оценка применимости ТРР. Исходя из особенностей архитектуры, ТРР применима для систем, имеющих следующие признаки:

– необходима общедоступная база данных (база, используемая при подтверждении достоверности документов, не содержит персональных данных) для значительного количества пользователей;

– в течение жизненного цикла системы происходит взаимодействие большого количества участников;

– существуют единые правила для всех сторон, взаимодействующих с системой;

– все процессы в системе прозрачны;

– все процессы, связанные с работой системы, на момент внедрения оцифрованы.

Условия внедрения технологии. Обязательным условием внедрения данных цифровых решений является завершенный процесс информатизации, который предполагает наличие базового информационного слоя – поддерживаемых в актуальном состоянии информационных систем, позволяющих осуществлять автоматизированную обработку данных. Фактически речь идет о «цифровом двойнике» университета – совокупности информационных систем, регистров, баз и банков данных, описывающих его внутренние процессы.

Множество цифровых двойников цифрового университета включает следующие компоненты:

– цифровой двойник обучающегося – реестр, содержащий персонифицированные данные об обучающемся, а также данные о его учебном прогрессе;

– цифровой двойник сотрудника университета – прообраз расширенной кадровой учетной системы, включающий обновляемые данные о научно-исследовательской деятельности, публикационной активности, отдельных индексах, характеризующих эффективность специалиста (индексы цитирования научных статей и др.);

– цифровой двойник инфраструктуры университета – реестр записей о текущем состоянии инфраструктуры, позволяющий осуществлять планирование ее использования, модернизации и развития;

– электронный документооборот.

Заключение

Проведено исследование применимости ТРР для подтверждения достоверности документов. Дано краткое описание ТРР применительно к сфере образования. Приведены подходы к подтверждению документов на основе блокчейн. Разработаны структурные модели эмиссии и подтверждения цифрового документа. Приведены составляющие эффективности от использования подходов и моделей.

В качестве последующей работы необходима программная реализация этих моделей. Базовой платформой для построения определена блокчейн-платформа Microsoft. Требуются моделирование наднациональной ДТС и построение тестовой модели механизма подтверждения достоверности условного документа.

Список литературы

1. Transparency International. Global Corruption Report. *Education.* New York: Routledge; 2013:418-420.
2. Allen E., Bear J. *The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas.* Updated ed. New York: Prometheus Books; 2019.
3. Качан Д.А. Технологии распределенных реестров и перспективы их использования в системе образования. *Цифровая трансформация*. 2018;4(5):44-55.
4. Вишняков В.А. Использование интеллектуальных и блокчейн технологий в информационном управлении. *Системный анализ и прикладная информатика*. 2018;1:45-50.
5. Свон М. *Блокчейн: схема новой экономики.* Москва: Олимп-Бизнес; 2017.
6. Клечиков А.В., Пряников М.М., Чугунов А.В. Блокчейн-технологии и их использование в государственной сфере. *Международный журнал открытых информационных технологий*. 2017;5(12):123-129.
7. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Coindesk.* 2009;5:9-13.
8. Равал С. *Децентрализованные приложения. Технология Blockchain в действии.* Серия «Бестселлеры O'Reilly». С.-Петербург: Питер; 2017.
9. Rivest R.L., Shamir A. PayWord and MicroMint: Two simple micropayment schemes *Security Protocols, Springer.* 1997;5:69-87.
10. Crespo de Pedro A.S., García L.I.C. Stampery Blockchain Timestamping Architecture (BTA). *Version 6 LTS.* 2017;11:1-21.
11. Leach P., Mealling M., Salz R. *A Universally Unique IDentifier (UUID) URN Namespace.* Proposed standard; 2005.

References

1. Transparency International. Global Corruption Report. *Education.* New York: Routledge; 2013:418-420.
2. Allen E., Bear J. *The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas.* Updated ed. New York: Prometheus Books; 2019.
3. Kachan D.A. [Distributed ledger technologies and prospects of their use in the education system]. *Digital transformation.* 2018;4(5):44-55. (In Russ)
4. Vishnyakou U.A. [Use of intellegent and blockchain technologies in information management]. *System analysis and applied informatics.* 2018;1:45-50. (In Russ)
5. Swan M. [*Blockchain. Scheme new economy*]. Moscow: Olymp-Biznes; 2017. (In Russ)
6. Clechikov A.V., Prianikov M.M., Chugunov A.V. [Blockchain technologies and their use in the public sphere]. *International Journal of Open Information Technologies.* 2017;5(12):123-129. (In Russ)
7. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Coindesk.* 2009;5:9-13.
8. Raval S. [*Decentralized applications. Blockchain technology in action*]. "O'Reilly bestsellers" series. St.-Petersburg: Piter; 2017. (In Russ)
9. Rivest R.L., Shamir A. PayWord and MicroMint: Two simple micropayment schemes *Security Protocols, Springer.* 1997;5:69-87.
10. Crespo de Pedro A.S., García L.I.C. Stampery Blockchain Timestamping Architecture (BTA). *Version 6 LTS.* 2017;11:1-21.
11. Leach P., Mealling M., Salz R. *A Universally Unique IDentifier (UUID) URN Namespace.* Proposed standard; 2005.

Вклад авторов

Качан Д.А. выявил проблемы подтверждения документов в образовании и предложил их решения с использованием блокчейн, разработал модели эмиссии и подтверждения цифрового документа.

Вишняков В.А. детализировал построение технологии распределенных реестров в образовании, определил эффективность метода работы с документами в образовании на основе блокчейн.

Authors' contribution

Kachan D.A. identified the problems of document authentication in education and proposed the blockchain-based solutions, developed models of the issue and authentication of a digital document.

Vishniakou U.A. detailed the construction of distributed ledger technology in education and determined the effectiveness of the blockchain-based method to work with educational documents.

Сведения об авторе

Вишняков В.А., д.т.н., профессор, профессор кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Качан Д.А., соискатель кафедры инфокоммуникационных технологий Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Vishniakou U.A., D.Sci, Professor, Professor of Infocommunication Technologies Department of Belarusian State University of Informatics and Radioelectronics.

Kachan D.A., PhD student of Belarusian State University of Informatics and Radioelectronics, Department of Infocommunication Technologies.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6,
Белорусский государственный университет
информатики и радиоэлектроники
тел. +3750172457569;
e-mail: vish2002@mail.ru
Вишняков Владимир Анатольевич

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki str., 6,
Belarusian State University
of Informatics and Radioelectronics
tel. +3750172457569;
e-mail: vish2002@mail.ru
Vishniakou Uladzimir Anatolievich