УДК 528.8.04, 528.88

В. А. Вишняков[1], Д. А. Качан[2]
[1]vish2002@mail.ru; [2]dkachan@protonmail.com
Белорусский государственный университет информатики и радиоэлектроники,
Минск, Республика Беларусь

АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПОДТВЕРЖДЕНИЯ ДОСТОВЕРНОСТИ ДОКУМЕНТОВ ОБ ОБРАЗОВАНИИ НА ОСНОВЕ БЛОКЧЕЙН

В докладе рассмотрено применение технологии блокчейн для подтверждения достоверности документов об образовании. На основании разработанных моделей представлены алгоритмы: выдачи цифрового документа об образовании, верификация запроса, создание цифровой копии документа, заключение смарт-контракта и публикация документа, подтверждение его подлинности. Алгоритмы реализованы программно, внедрены в информационную систему БГУИР.

Ключевые слова: блокчейн, документы об образовании, алгоритмы, смарт-контракт.

Uladzimir A. Vishniakou[1], Dmitry A. Kachan[2]
[1]vish2002@mail.ru; [2]dkachan@protonmail.com
Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

ALGORITHMIC SUPPORT FOR CONFIRMATION OF ACCURACY OF EDUCATION DOCUMENTS ON BLOCKCHAIN BASED

The report discusses the application of blockchain technology to confirm the reliability of education documents. Based on the developed models, algorithms are presented: issuing a digital document on education, verification of the request, creating a digital copy of the document, the conclusion of a smart contract and the publication of the document, confirming its authenticity. Algorithms are implemented programmatically and can be applicable in information management in other fields of activity.

Keywords: blockchain, education documents, algorithms, smart contract.

Введение. Проблема подтверждения достоверности документов об образовании значительно обострилась и стала носить эпидемический характер общемирового масштаба [1]. В работах [2, 3] авторами предложена концепция и модели представления и обработки цифровых документов с использованием технологии блокчейн. В данном докладе представлены алгоритмы для развития моделей [4].

Алгоритм получения цифрового документа. Алгоритм выдачи цифрового документа об образовании (рис. 1) включает:

- запрос на выдачу цифрового документа;
- верификация эмитентом предоставленных данных;
- создание цифровой копии выданного документа об образовании в установленном формате представления;
- смарт-контракт для публикации цифрового документа;
- загрузка значения хеш-суммы документа в публичную сеть блокчейн;
- отправка цифрового документа получателю.

Формирование запроса на получение цифрового документа заключается в заполнении веб-формы на интернет-портале эмитента документа либо организации, уполномоченной осуществлять данные действия. Форма запроса содержит контактный e-mail отправившего запрос для обратной связи.

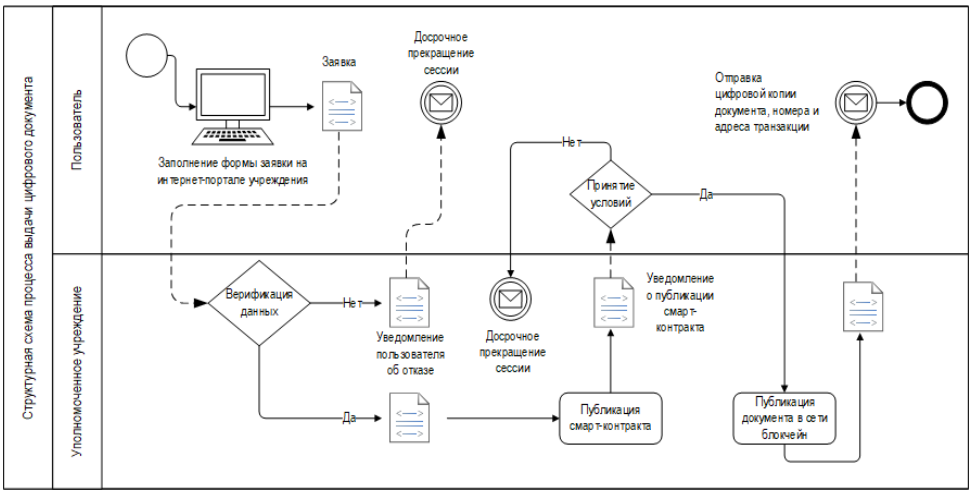

Рис. 1. Алгоритм процесса выдачи цифрового документа

Для поиска данных в электронных базах пользователь может использовать следующие идентификаторы: номер диплома; ФИО, на которые был выдан документ; год поступления; год окончания; персональный номер. Автоматическую работу алгоритма целесообразно строить на основе запроса номера документа об образовании, автоматизированные механизмы использовать лишь в случае отсутствия номера документа на основании уточнения данных оператором. После отправки формы данные заносятся в специально созданную промежуточную БД для формирования очереди запросов для последующей обработки и публикации в сети блокчейн. Структурная схема запроса на получение цифрового документа представлена на рис. 2.

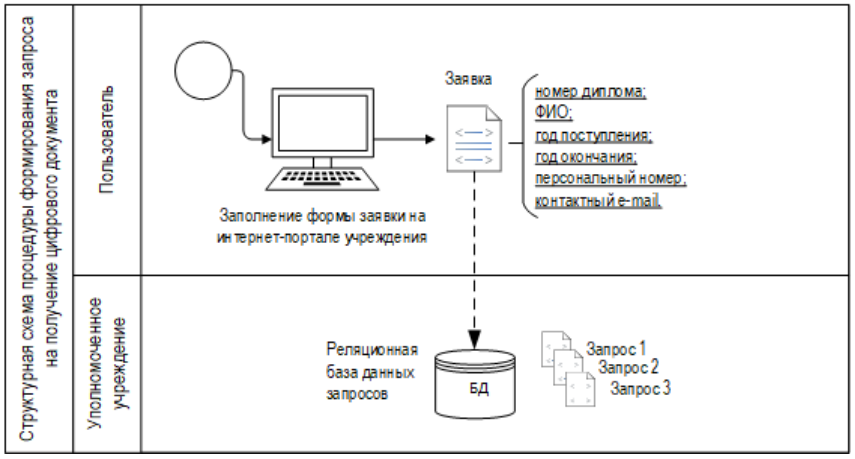

Рис. 2. Формирования запроса на получение цифрового документа

На шаге 2 происходит проверка введенных пользователем данных с учетом ряда особенностей – для верификации предлагается реализация двух способов:

- набор данных: персональный номер, ФИО, год поступления и окончания;
- набор данных: номер документа, ФИО.

После проверки записей в реляционных базах данных учреждения, содержащих указанные в форме запроса данные, выполняется серия запросов в локальные реляционные БД для получения данных с целью последующего формирования цифрового документа. Полученные результаты запросов записываются в отдельную не реляционную БД подготовленных к формированию смарт-контракта документов.

Дополнительно осуществляется запрос в НБД архивных документов, где хранятся данные документов об образовании, опубликованных в сети блокчейн. В данном случае на указанный при регистрации адрес электронной почты отправляется pdf-файл цифровой копии документа об образовании и адрес транзакции в сети блокчейн для подтверждения достоверности.

В случае отсутствия записей на основании обработки данных формы запроса на указанный контактный адрес электронной почты отправляется уведомление, а также устанавливается запрет на регистрацию на период 1 024 секунды для подтвержденных данных в полях персональный номер, номер документа об образовании и контактный e-mail. Структурная схема верификации запроса представлена на рис. 3.

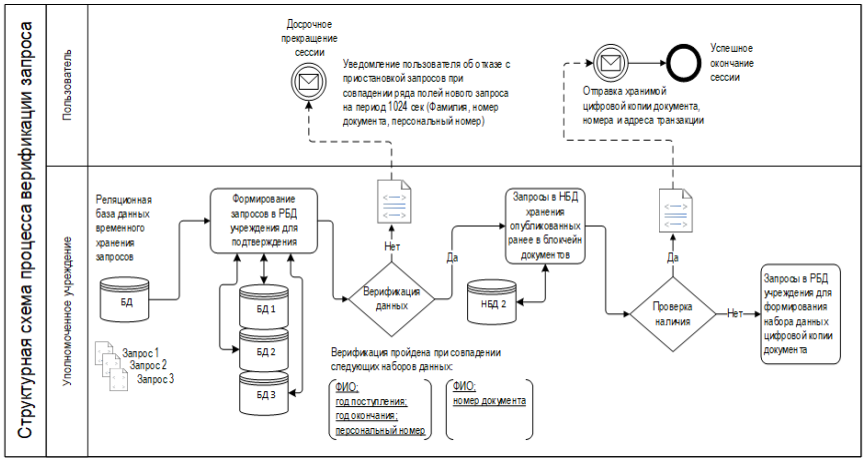

Рис. 3. Структурная схема процесса верификации запроса

Создание цифровой копии документа об образовании осуществляется на основании данных, сформированных в НБД. Цифровой документ содержит данные документа об образовании утвержденной формы, а также включает персональный номер и фотографию. Документ формируется в pdf-формате. Структурная схема процесса формирования цифровой копии документа представлена на рис. 4.

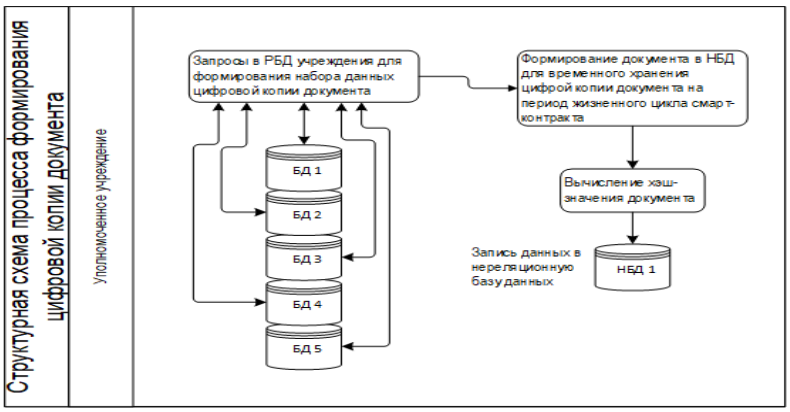

Рис. 4. Процесс формирования цифровой копии документа

Заключение смарт-контракта и публикация документа. На основании подтвержденного наличия данных об образовании пользователя в базах и подготовки цифровой копии документа пользователю предлагается заключение смарт-контракта с уведомлением в виде ссылки на смарт-контракт в публичной сети блокчейн. Для возможности взаимодействия пользователь проходит авторизацию в специализированном приложении, обеспечивающем взаимодействие с собственной учетной записью в сети блокчейн (криптовалютный кошелек).

При принятии условий цифрового договора на публикацию данных в сети блокчейн пользователь выполняет транзакцию некоторой суммы криптовалюты для компенсации затрат учреждения-эмитента.

В случае отказа от принятия контакта по истечении заданного периода времени либо после выполнения смарт-контракта происходит его автоматическое удаление.

Для повышения уровня контроля операций в смарт-контракт может вводиться третья сторона в качестве независимого арбитра для обеспечения гарантий выполнения договоров сторонами. Публикация документа в публичной сети блокчейн осуществляется на основании выполнения условий смарт-контракта.

Структура транзакции имеет следующий вид:

- Nonce (порядковый номер транзакции, осуществленной из данного аккаунта);
- Gas price, Start gas («сервисные» значениями, которые определяются особенностями построения сети блокчейн Ethereum и обеспечение ее работы. Фактически представляют собой стоимость транзакции, в которую входят расходы на поддержание сети);
- Destination (адрес отправки заданного в Value значения криптовалюты);
- Value (отправленная сумма криптовалюты);
- Data (поле, способное содержать как произвольные данные, так и целую структуру, определяющую программный алгоритм для виртуальной машины);
- Signature (подпись автора транзакции и публичный ключ, которым будет проверяться эта подпись).

Алгоритм подтверждения достоверности документа об образовании предполагает возможность использования проверки без обращения к третьей стороне, а также ее информационным ресурсам. Алгоритм проверки заключается в вычислении хеш-значения предложенной цифровой копии документа об образовании в формате pdf и сравнении его со значением, опубликованным в сети блокчейн. Дополнительно сравниваются адреса в регистре JOINT-ISO-ITU-T и адрес отправителя транзакции в блокчейн.

Заключение. В докладе рассмотрена проблематика подтверждения достоверности документов об образовании, определены соответствующие алгоритмы подтверждения достоверности с применением технологии распределенных реестров, дана краткая характеристика этапов для алгоритмов. Разработка внедрена в БГУИРе.

Список литературы

1. Transparency International. Global Corruption Report: Education [Electronic resource]. New York: Routledge, 2013. P. 418. URL: http://files.transparency.org/content/download/675/2899/file/2013_GCR_Education_EN.pdf (accessed: 10.04.2021).

2. Качан Д. А. Технологии распределенных реестров и перспективы их использования в системе образования // Цифровая трансформация. 2018. Т. 4. № 5. С. 44–55.

3. Качан Д. А., Вишняков В.А. Подход и модели применения технологии распределённых реестров для подтверждения достоверности документов в образовании // Доклады БГУИР. 2020. № 7. С. 14–23.

4. Вишняков В. А., Качан Д. А. Модели и средства подтверждения документов об образовании с использованием технологии распределенных реестров // Информатизация образования и методика электронного обучения: цифровые

технологии в образовании : материалы IV Междунар. науч. конф., Красноярск, 6–9 октября 2020 г. : в 2 ч. Ч. 2 / Под общ. ред. Н.В. Носкова. Красноярск, Сиб. федер. ун-т, 2020. С. 61–66.