УДК 528.8.04, 528.88

**В. А. Вишняков[1], Д. А. Качан[2]**

[1]e-mail: vish2002@mail.ru; [2]e-mail: dkachan@protonmail.com
Белорусский государственный университет информатики и радиоэлектроники,
Минск, Беларусь

# МОДЕЛИ И СРЕДСТВА ПОДТВЕРЖДЕНИЯ ДОКУМЕНТОВ ОБ ОБРАЗОВАНИИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Подтверждение документов об образовании осуществляется с использованием государственных реестров, что является сложным и ресурсоёмким процессом. В мире наблюдается рост количества поддельных документов, что ставит под сомнение эффективность современных механизмов. Технология распределённых реестров является устойчивым технологическим трендом, влияющим на качество цифровой экономики. В работе рассмотрено применение технологии для подтверждения достоверности документов об образовании. Установлена роль доверенной третьей стороны в процессе проверки. Приводится модель подтверждения на основе технологии распределённых реестров, которая позволяет устранить ограничения и недостатки существующих подходов, сформулированные подходы могут быть применимы в информационном управлении во всех сферах деятельности.

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

Vladimir A. Vishniakou[1], Dmitry A. Kachan[2]

[1]e-mail: vish2002@mail.ru; [2]e-mail: dkachan@protonmail.com
Belarusian State University of Informatics and Radioelectronics,
Minsk, Belarus

# MODELS AND MEANS OF VALIDITY CONFIRMATION OF EDUCATIONAL CERTIFICATES USING DISTRIBUTEDLEDGER TECHNOLOGY

Confirmation of documents on education is carried out using state registers, which is a complex and resource-intensive process. The world has seen an increase in the number of fraud documents, which call doubt on the effectiveness of modern mechanisms. Distributed ledger technology is a sustainable technological trend that affects the quality of the digital economy. The paper discusses the use of technology to confirm the education documents. The role of a trusted third party in the verification process is established. A confirmation model based on the technology of distributed ledgers is presented, which allows to eliminate the lim-

itations and shortcomings of existing approaches, the formulated approaches can be applied in information management in all areas of activity.

*Keywords: distributed ledger technology, blockchain, smart contract, information technologies in education, education degree documents, confirmation of the authenticity.*

Проблема подтверждения достоверности документов об образовании значительно обострилась и стала носить эпидемический характер общемирового масштаба. В соответствии с докладом «Global Corruption Report: Education», подготовленным организацией Transparency International в 2013 г., в образовании сложилась устойчивая тенденция лавинообразного роста количества так называемых «degree mill» – учреждений образования, выдающих поддельные документы об образовании, сертификаты и лицензии [1]. О степени распространения можно судить по наличию и содержанию информационного ресурса в сети Интернет, содержащего данные о домашних животных, получивших образовательные дипломы и сертификаты посредством подобных «degree mill» (для ознакомления доступно по ссылке https://en.wikipedia.org/wiki/List_of_ animals_with_fraudulent_diplomas).

В источнике [2] приводятся следующие данные, основанные на расследованиях, проводимых Федеральным бюро расследований в США:

- в мире насчитывается более 3300 непризнанных университетов, которые осуществляют выдачу поддельных документов об образовании;
- на счету международного преступного синдиката, территориально расположенного в Европе на Ближнем Востоке и в Великобритании, распространение более 450 000 поддельных дипломов по всему миру;
- количество ежегодно присуждаемых степеней PhD в США составляет от 40 000 до 45 000 каждый год, количество поддельных – свыше 50 000 в год.

Другой причиной, определяющей необходимость внедрения универсального механизма подтверждения документов об образовании, является миграция населения, оцениваемая на уровне 87 млн человек в год [3]. Для добровольной миграции характерен ряд сложностей, связанных с подтверждением полученных квалификаций, зачастую носящих транснациональный характер. 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 делает сложным или невозможным подтверждение полученных квалификаций в ряде случаев.

Наличие механизма проверки достоверности документов об образовании, устойчивого к злонамеренному манипулированию, является достаточно актуальной задачей, выходящей за рамки сферы образования, над возможными способами решения которой в Белорусском государственном университете информатики и радиоэлектроники в текущее время ведутся

работы. В основе предлагаемого механизма лежит использование технологии распределенных реестров.

**Технологии распределённых реестров.** Технология ведения распределенных реестров впервые была предложена криптографами Райвестом и Шамиром в работе «PayWord and MicroMint: two simple micropayment schemes» [4], определившей основы обеспечения безопасности инновационной системы микротранзакций и содержащей принципы функционирования двух различных по принципу работы систем осуществления финансовых транзакций. Можно утверждать, что одна из двух платежных систем (MicroMint) является прародителем технологии блокчейн в том виде, в котором она стала популярна. Попытки внедрения данной инновации столкнулись с проблемой доступности вычислительных мощностей и низким уровнем развития ИКТ в тот период в целом.

Рост популярности технологии распределенных реестров принято связывать с публикацией работы «Bitcoin: A Peer-to-Peer Electronic Cash System» [5]. Основная задача, решаемая предложенной технологией, – создание механизма формирования реестра записей о транзакциях в условиях отсутствия доверительных отношений между участниками, т. е. создание журнала транзакций, из которого ни один участник не может удалить запись или подделать ее. Основным принципом доверенной среды является децентрализация хранения журнала и механизм гарантии его идентичности.

Технология распределенных реестров (блокчейн) – это решение, базирующееся на ряде существовавших ранее технологий [6], среди которых можно выделить технологию построения структуры данных путем вычисления хэш-функций (дерево Меркла) на основе патента США № 4309569, опубликованного 05.01.1982. Несомненным достижением авторов блокчейн можно считать изобретение механизма обеспечения работоспособности этой технологии. В основу блокчейн положена гонка вычислительных мощностей участников с целью получения вознаграждения за успешно проведенные вычисления, обеспечивающие добавление новых записей в цепи транзакций. Записи транзакций остаются неизменными и могут быть проверены в любой момент за весь жизненный цикл работы системы.

Технология распределённых реестров имеет широкие границы применения и постоянно совершенствуется и на текущий момент вышла далеко за пределы осуществления финансовых микротранзакций. В настоящий момент рассматривается возможность практического использования блокчейн для совершенствования методов информационного управления [7, 8].

Еще одним понятием, нашедшим применение благодаря распространению блокчейн-технологий, стал смарт-контракт [9]. Смарт-контракты представляют собой программные модули, интегрированные в реестры блокчейн и вызываемые пользователями при заключении договоренностей. Выполнение или невыполнение договорных обязательств контролируются

программными алгоритмами, но допускается и использование людей-арбитров (становится актуально в случае взаимодействия с материальными объектами для контроля выполнения обязательств и их качества). В целом смарт-контракт представляет собой достаточно тривиальный программный алгоритм с IF-THEN-логикой.

Таким образом, технология распределённых реестров представляет собой совокупность технологических решений, позволяющих формировать неизменяемые распределённые реестры данных в одноранговой (пиринговой) сети участников. Блокчейн использует нецентрализованные приложения – класс программных приложений, обеспечивающих сетевые взаимодействия, и не требует наличия клиент-серверной архитектуры для обмена данными.

**Мировой опыт применения блокчейн для подтверждения достоверности.** Подтверждение достоверности транзакций является одной из ключевых характеристик технологии распределённых реестров. Впервые о практической идеей альтернативного использования сети блокчейн было заявлено в 2013 г. – был описан вариант подтверждения существования и достоверности нотариальных бумаг и разработан сервис подтверждения достоверности (https://www.proofofexistence.com). Заявленный принцип работы: посредством запуска приложения проводится транзакция в сети блокчейн, содержащая полученное хэш-значение в текстовом поле. Осуществляется процедура проверки, сравнивается полученное значение со значением, указанным в первой транзакции, когда данные были отправлены в блокчейн. На основании сравнения принимается решение о достоверности документа.

Для целей проверки достоверности документов об образовании в Массачусетском институте технологий был разработан схожий сервис – Blockcerts (https://www.blockcerts.org). Особенностью сервиса является привлечение учреждений образования для использования услуг сервиса, при котором Blockcerts является доверенной третьей стороной и арбитром.

**Модели и средства подтверждения достоверности.** Подтверждение достоверности документов об образовании предлагается рассматривать как процесс, состоящий из двух подпроцессов: подтверждение достоверности и подтверждение авторства транзакции, осуществившей публикацию в реестр данных. Для реализации механизма подтверждения достоверности прежде всего необходимо решение проблемы ведения общедоступного реестра адресов в сети блокчейн, которые подтверждают авторство транзакций. Указанные выше сервисы предлагают собственные услуги для ведения реестра адресов, определяющих принадлежность к тому или иному учреждению образования, выступая как доверенная третья сторона. На наш взгляд, подобный подход лишает процесс подтверждения достоверности документов об образовании объективности. Во избежание этого

разрабатываемая модель подтверждения предполагает использование наднациональных реестров международного регистрационного органа, в качестве которого выступает совместный орган Международного союза электросвязи ITU-T и Международной организации по стандартизации ISO, ответственного за назначение идентификаторов объектов верхнего уровня с первичным целочисленным значением 2 (метка JOINT-ISO-ITU-T) [10, 11]. Это позволяет решить проблему подтверждения достоверности и существования эмиссионного центра, издавшего рассматриваемый документ об образовании, в том числе позволит получать ретроспективные данные о существовавших ранее эмиссионных центрах, а также о внесённых изменениях, связанных с их функционированием (наименование, уровни подготовки, местонахождение и т. п.). В этом случае возникает понятие международного объектного идентификатора (OID), представляющего собой адрес записи в реестре JOINT-ISO-ITU-T, состоящий из комбинации последовательных идентификаторов, сформированных в соответствии с принятыми правилами (нотациями). В примере ниже приведен идентификатор Республики Беларусь, опубликованный на текущий момент в реестре (http://www.oid-info.com) и состоящий из цепочки идентификаторов «первичный международный идентификатор», «идентификатор группировки государств», «идентификатор государства Республика Беларусь»:

а) в нотации ASN.1: {joint-iso-itu-t(2) country(16) by(112)};

б) в нотации dot: 2.16.112;

в) в нотации OID-IRI: /Country/BY.

Предполагается регистрация учреждений-эмитентов и в полях данных размещение блокчейн-адресов учреждений, необходимых для подтверждения авторства транзакции как в ручном режиме по месту предъявления и проверки документов, так и за счет обращения разрабатываемых автоматизированных приложений.

Подтверждение достоверности документов об образовании состоит из процедур выдачи цифрового документа (эмиссии), опубликования его хэш-значения в виде транзакции в сети блокчейн, передачи документа и данных о транзакции пользователю для последующего предъявления, проверка документа путем самостоятельного вычисления хэш-значения документа и сравнения полученных значений в транзакцией и сравнение адресов эмиттента на основании OID.

Эмиссия документа осуществляется на основании автоматического выполения смарт-контракта по результатам обработки запроса пользователя в приложении, указывающего свои персональные данные и/или номер полученного документа об образовании и год его выдачи. После обработки запроса система оповещает пользователя о готовности к обслуживанию (либо об отказе обслуживания при неверно указанных данных запроса) и предлагает заключить смарт-контракт в публичной сети блокчейн на эмиссию докумен-

та. После принятия условий контракта пользователем происходит формирование электронного документа путем обращения к ведомственным электронным базам. Далее происходит вычисление хэш-значения полученного JSON-документа и его публикция в сети блокчейн. Система осуществляет проверку опубликования в блокчейн-записи и пользователю отправляется электронный документ, номер транзакции в сети блокчейн, а также OID-идентификатор эмиттента для возможности проверки. Проверка возможна как в ручном режиме – путем сравнения адресов и хэш-значений человеком, так и с использованием автоматизированных приложений, осуществляющих получение и сравнение данных без участия человека.

В работе рассмотрена проблематика подтверждения достоверности документов об образовании, определены модели и средства подтверждения достоверности с применением технологии распределенных реестров, дана краткая характеристика технологии. Рассмотренная модель подтверждения достоверности предлагает усовершенствованное решение без явного участия доверенной третьей стороны, что повышает объективность системы оценки.

**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: 10.10.2019).

2. Allen E., Bear J. The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas. Updated ed. New York: Prometheus Books, 2019. 466 p.

3. UNESCO. Global Education Monitoring Report: Migration, displacement and education [Electronic resource]. UNESCO Publishing, 2018. P. 362. URL: http://unesdoc.unesco.org/images/0026/002658/265866E.pdf (accessed: 10.10.2019).

4. Rivest R. L., Shamir A. PayWord and MicroMint: Two simple micropayment schemes // Security Protocols / ed. Lomas M. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997. P. 69–87.

5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. 2009. P. 9. URL: https://bitcoin.org/bitcoin.pdf (accessed: 10.10.2019).

6. Качан Д.А. Технологии распределенных реестров и перспективы их использования в системе образования [Electronic resource] // Цифровая трансформация. 2018. Vol. 4. № 5. P. 44–55. URL: https://dt.giac.by/jour/article/view/116/81 (accessed: 10.10.2019).

7. Вишняков В.А., Качан Д.А. Управление интернет-маркетингом в системе образования с использованием блокчейн-технологий // Доклады БГУИР. 2020. Vol. 18, № 2. С. 30–36.

8. Вишняков В. А. Использование интеллектуальных и блокчейн технологий в и нформационном управлении // Системный анализ и прикладная информатика. 2018. № 1. С. 45–50.

9. Szabo N. J. Smart Contracts [Electronic resource]. 1994. URL: http://tutorweb.net/comp/crypto251.0/lec47100/sl47110 (accessed: 10.10.2019).

10. ITU-T. ITU-T X.660 Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree // Int. Telegr. Teleph. Consult. Com. Recomm. X.660. 2011.

11. ITU-T. Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs beneath the top-level arc jointly administered by ISO and ITU-T // ITU-T X-SERIES Recomm. 2008.