УДК 004.056.57:032.27

ПОДДЕРЖКА ИНФОРМАЦИОННОГО УПРАВЛЕНИЯ В ОБРАЗОВАНИИ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН

Д.А. КАЧАН, В.А. ВИШНЯКОВ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 4 марта 2021

Аннотация. Предложена концепция и модель информационной поддержки управления в образовании с использованием блокчейн. Представлена модель смарт-контракта. Рассмотрен подход и модель для представления объектного идентификатора.

Ключевые слова: информационное управление в образовании, блокчейн, смарт-контракт, идентификатор

Введение

Сложности построения процессов управления и принятия управленческих решений в образовании обусловлены рядом особенностей, присущих этой области:

многоаспектность происходящих процессов (экономических, социальных и т.п.) и их взаимосвязанность. Это зачастую не позволяет вычленить и детально исследовать отдельные явления – все происходящие процессы должны рассматриваться в совокупности:

– отсутствие достаточной количественной информации о динамике процессов, что вынуждает переходить к качественному анализу процессов;

– изменчивость характера процессов во времени и т.д. Для рассматриваемой слабоструктурированной системы число факторов в различных ситуациях может измеряться десятками;

– особенностями системы управления отраслью.

Существуют различные модели и средства представления данных для лиц, принимающих решение в процессе управления [1]. В качестве одной из перспективных технологий для поддержки управления в образовании предлагается использование технологии распределенных реестров [2].

Концепция и модель информационного управления в образовании с использованием блокчейн

В настоящее время актуальным является использование технологии блокчейн для подтверждения авторства и прав на объекты интеллектуальной собственности [2]. В рамках статьи понятие объекта интеллектуальной собственности расширяется на документы, выдаваемые учреждениями образования. Внедрение подобного подхода определяет необходимость разработки информационной поддержки в образовании с использованием блокчейн (ИПвОБ). Под концепцией ИПвОБ будем понимать реализацию, при котором иметься способность автоматического формирования электронного документа и независимая его верификация в местах предъявления. система должна иметь возможность принять и обработать заявку на формирование электронного нормализованного документа установленного образца и формата, вычислить хэш-значение полученного документа включая уникальный идентификатор учреждения образования, добавить информацию контрольной величие хэш-функции в блок цепей транзакций блокчейн для последующей проверки. В рамках этой концепции сформулируем две задачи [3].

Постановка первой задачи: необходимо разработать технологию для обеспечения подтверждения достоверности документов об образовании на основе технологии распределенных реестров с использованием смарт-контрактов. Для второй задачи в ИПвО надо

разработать модель, чтобы сбалансировать потребности промышленности и выпускников и поддержать это технологией блокчейн.

Тогда обобщенную модель M_{mse} для ИПвОБ представим в виде:

$$M_{mse} = (M_{edd}, M_{sdd}, M_{ebe}),$$

где M_{edd} – модель генерации цифрового документа в образовании, M_{sdd} – модель подтверждения цифрового документа в образовании; M_{ebe} – модель сбалансирования потребностей экономики и выпуска специалистов в образовании.

Подтверждение достоверности является одной из ключевых характеристик технологии распределенных реестров. Технология TPP позволяет осуществлять подтверждение достоверности (существования) записи в виде хэш-суммы интересуемого документа. Это позволяет построить сервис для сравнения предоставленного документа с хранимым в сети блокчейн, не нарушая конфиденциальность данных – сами документы в сеть не попадают, сравнение осуществляется только на основе хэш-значений.

Принцип работы публикации документа следующий – производится вычисление значения хэш-суммы документа, проводится транзакция в сети блокчейн, содержащая вместо адреса получателя данной транзакции полученное хэш-значение с используется функций OP_RETURN для блокчейн-сети Bitcoin. Функция OP_RETURN имеет ограничение на длину данных в 40 байт, что является оптимальным значением ввиду используемого алгоритма вычисления хэш-функции SHA – полученное значение хэш-функции имеет длину в 32 байта [4]. Для блокчейн-сетей Ethereum транзакция имеет дополнительный атрибут, что позволяет использовать сеть для хранения данных без ограничений по длине [2].

Модель сматр-контракта

Для публикации документа в сети блокчейн предполагается использовать возможности смарт-контрактов. Формальное представление смарт-контракта может быть отражено в виде математической модели конечного автомата, представляющего в теории алгоритмов математическую абстракцию или модель дискретного устройства, имеющего один вход, один выход и в каждый момент времени находящегося в одном состоянии из множества возможных:

$$M = (Q, \Sigma, \delta, s_0, F),$$

где Q – конечное множество всех возможных состояний смарт-контракта; Σ – набор всех входных событий смарт-контракта; δ – множество переходных функций смарт-контракта; $\delta : Q \cdot \Sigma \to Q$ – конечное состояние смарт-контракта, F – конечное состояние смарт-контракта $F \in Q$; s_0 – начальное состояние смарт-контракта $s_0 \in Q$.

Обозначив начальное состояние блокчейн-сети γ получаем переход сети в новое состояние при условии совершения успешной транзакции:

$$\gamma \xrightarrow{T_x} \gamma'.$$

Новое состояние сети блокчейн влияет в разной степени на многие учетные записи в сети, а также на другие смарт-контракты, которые в свою очередь оказывают влияние на данные в цепочке блоков.

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.

Транзакции, связанные с механизмами подтверждения авторства или достоверности с помощью цифрового отпечатка, применяются для предъявления доказательства одной стороны другой, когда проверяющая сторона сверяет хэш-значение, временную метку транзакции и, что наиболее важно, подлинность (принадлежность) криптовалютного "кошелька" предъявителя.

Механизм для автоматизированного подтверждения достоверности документа на основе использования TPP охватывают 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).

Модель объектного идентификатора

Для реализации модели идентификаторов предлагается использование приватной сети блокчейн в части создания и ведения регистра записей, а также публичной сети, для обеспечения доступа третьей стороны при необходимости подтверждения достоверности документа. Приватная сеть блокчейн обеспечивает хранение полных копий распределенного реестра транзакций, обеспечивая их сохранность и достоверность хранимых данных. Реестр содержит записи о документах об образовании и программные модули (смарт-контракты), которые позволяют участникам распределенной сети осуществлять взаимодействие с реестром и друг с другом.

Взаимодействие ответственных за ведение реестра, обучающихся, представителей третьих сторон, заинтересованных в проверке достоверности данных, осуществляется на основании смарт-контрактов на выполнение конкретных действий, которые позволяют участникам вызывать различные события для управления записями в сети.

Использование стандартизированного международного объектного идентификатора позволяет решить проблему подтверждения достоверности и существования эмиссионного центра, издавшего рассматриваемый документ об образовании, в том числе позволит проверить данные о существовавших ранее эмиссионных центрах, а также о внесенных изменениях, связанных с их функционированием (наименование, уровни подготовки, местонахождение).

Предложенное решение данной проблемы основано на использовании реестра 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 (метка JOINT-ISO-ITU-T) [5]. Международный объектный идентификатор (OID) представляет собой запись, состоящую из комбинации последовательных идентификаторов, сформированных в соответствии с принятыми правилами.

Для рассматриваемого случая идентификатор Республики Беларусь, состоящий из цепочки идентификаторов "первичный международный идентификатор – идентификатор группировки государств – идентификатор государства Республика Беларусь", может быть выражен тремя различными способами:

1. В нотации ASN.1: {joint-iso-itu-t(2) country(16) by(112)}.
2. В нотации dot: .16.112.
3. В нотации OID-IRI: /Country/BY.

При анализе предложенных нотаций очевидно, что нотации 1 и 3 содержат страновой идентификатор "BY". При обозначении стран используются идентификаторы Alfa-2 code (состоит из двух романских символов), Alfa-3code (состоит из трех романских символов), числовой код (numeric code, для Республики Беларусь принят равным 112).

В связи с этим предлагается использование dot-нотации, представляющей собой последовательности числовых идентификаторов, разделенных точками.

Каждое число, отделяемое от последующего (и предыдущего для не первого) точкой, условно обозначим уровнем идентификатора. Таким образом, получаем следующее базовое дерево идентификаторов, в которых уровни 1–3 уже определены:

1. Уровень1 – совместный идентификатор ITU-T и ISO, значение – 2.
2. Уровень2 – страновой идентификатор (country), значение – 16.
3. Уровень3 – Республика Беларусь, значение –112.
4. Уровень4 – территориальные единицы Республики Беларусь.

Формирование данного уровня дерева OID-идентификаторов осуществим на основе международных обозначений территориального деления Республики Беларусь, принятых в [6, 7]. Численные обозначения регионов целесообразно принять в соответствии с Общегосударственным классификатором Республики Беларусь "Система обозначений объектов административно-территориального деления и населенных пунктов" (классификатор СОАТО, уровень 1). Для уровня 4 предлагается введение территориального деления Республики Беларусь. Уровень 5 – предлагается включить рассматриваемую отрасль (образование). Присвоим идентификатору отрасли образования значение 1.

Подобная логика построения OID-идентификатора позволит охватить все отрасли народного хозяйства при использовании результатов работы за рамками системы образования. OID Белорусского государственного университета информатики и радиоэлектроники, выраженный в формате dot-нотации, будет представлять собой последовательность 2.16.112.5.1.1, при обозначении направления подготовки с присвоением квалификации "бакалавр" в рамках данного учреждения образования – 2.16.112.5.1.1.1, а степени "магистр" – 2.16.112.5.1.1.2.

Заключение

Предложена концепция информационной поддержки в образовании с использованием технологии блокчейн. Представлена интегрированная модель для концепции, включающая модель для подтверждения достоверности документов об образовании (эмиссия цифрового документа об образовании, его проверка) и модель оптимизации выпуска специалистов под потребности отраслей промышленности. Формальное представление смарт-контракта отражено в виде математической модели конечного автомата. Расширен идентификатор для цифровых документов в образовании до шести уровней.

THE SUPPORT OF INFORMATION CONTROL IN EDUCATION USING BLOCKCHAIN

D.A. KACHAN, U.A. VISHNYAKOU

Abstract. The concept and model of information support of management in education using blockchain is proposed. A smart contract model is presented. An approach and a model for representing an object identifier are considered**.**

Keywords: information management in education, blockchain, smart contract, identifier.

Список литературы

1. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. М.: Институт проблем управления им. В.А. Трапезникова, ФИЗМАТЛИТ, 2010.
2. Свон М. Блокчейн: схема новой экономики. М.: Олимп-Бизнес, 2017.
3. Качан Д.А., Вишняков В.А. // Докл. БГУИР. 2020. № 7.С. 14–23.
4. Crespo A.S. Blockchain Timestamping Architecture (BTA) [Электронный ресурс]. URL: http ://arxiv.org/abs/1711.04709%0A.
5. 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, 2011.
6. ISO3166-1:2013. Codes for the representation of names of countries and their subdivisions. Part 1: Country codes, 2013.
7. ISO3166-2:2013. Codes for the representation of names of countries and their subdivisions. Part 2: Country subdivision code, 2013.