В. А. Вишняков[1], Д. А. Качан[2]
[1]vish2002@mail.ru
Белорусский государственный университет информатики и радиоэлектроники,
Минск, Беларусь
[2]kachanofficialmail@gmail.com
НИИ Гипросвязь, Минск, Беларусь

МОДЕЛЬ И РЕАЛИЗАЦИЯ СМАРТ-КОНТРАКТА В ОБРАЗОВАНИИ

В докладе представлена модель смарт-контракта, ее проверка и реализация на базе технологии блокчейн для контроля достоверности документов об образовании. Предложено использование объектного идентификатора для решения проблемы обезличенной доверенной третьей стороны.

Ключевые слова: смарт-контракт, модель, блокчейн, проверка, реализация.

Uladzimir A. Vishniakou[1], Dmitry A. Kachan[2]
[1]vish2002@mail.ru
Belarusian State University of Informatics and Radioelectronics,
Minsk, Belarus
[2]kachanofficialmail@gmail.com
RII Giprosviaz, Minsk, Belarus

MODEL SND REALIZATION OF SMART-CONTRACT IN EDUCATION

The report presents a smart contract model, its verification and implementation based on blockchain technology to control the authenticity of educational documents. The use of an object identifier to solve the problem of an impersonal trusted third party is proposed.

Keywords: smart contract, model, blockchain, verification, implementation.

Введение

В соответствии с докладом «Global Corruption Report: Education», подготовленным организацией Transparency International в 2018 году, в образовании сложилась устойчивая тенденция роста учреждений образования, выдающих поддельные документы, лицензии и др. Одним из методов противостояния является использование технологии блокчейн. В работе [1] построена модель процесса выдачи и верификации цифровых дипломов, а также рассмотрен ряд проблем, связанных с практической реализацией данной задачи. В работе [2] рассмотрено применение технологии блокчейн для подтверждения достоверности документов об образовании. Установлена роль доверенной третьей стороны в процессе проверки. Приводится модель подтверждения на основе технологии распределённых реестров, которая позво-

ляет устранить ограничения и недостатки существующих подходов. Эмиссия документа осуществляется на основании автоматического выполнения смарт-контракта по результатам обработки запроса пользователя в приложении, указывающего свои персональные данные и/или номер полученного документа об образовании и год его выдачи.

Модель смарт-контракта

Формальное представление смарт-контракта может быть отражено в виде математической модели конечного автомата, представляющего 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; $\delta : Q * \Sigma \to Q$ – 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 [3]:

$$\gamma \xrightarrow{T_x} \gamma`$$

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

Проверка смарт-контракта

Процедура проверки осуществляется по следующему алгоритму – проверяющей стороной вычисляется хэш-значение электронной версии документа и сравнивается полученное значение со значением, указанным в транзакции, изменившей состояние смарт-контракта. 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 «номера счета» предъявителя. Механизм для автоматизированного подтверждения достоверности документа на основе использования TPP охватывает лишь две участвующих стороны (предъявитель и проверяющий), что может быть недостаточно в ряде случаев – эмитент или осуществляющий его роль участник должен присутствовать в модели в качестве доверенной третьей стороны (ДТС).

Реализация модели смарт-контракта

Для реализации модели смарт-контракта предлагается использование двухуровневой архитектуры: приватной сети блокчейн для создания и ведения регистра записей и публичной сети, предназначенной для обеспечения доступа третьей стороны при запросе на публикацию документа и подтверждение его достоверности.

Первый уровень модели – приватная сеть блокчейн – обеспечивает хранение полных копий распределенного реестра транзакций, обеспечивая их сохранность, достоверность хранимых данных. Уровень имеет ограниченное регламентированное число участников: учреждения образования, органы госуправления и подчиненные им государственные учреждения, отвечающие за сбор, хранение и обработку данных, хранимых в реестрах.

Второй уровень – это одна или несколько публичных сетей блокчейн, отвечающих требованиям решаемых задач (поддержка смарт-контрактов).

Внедрение объектного идентификатора направлено на решение проблемы наличия обезличенной доверенной третьей стороны (ДТС). Использование стандартизированного объектного идентификатора позволяет решить проблему подтверждения достоверности и существования эмиссионного центра, издавшего рассматриваемый документ об образовании. 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 2 (метка JOINT-ISO-ITU-T).

Выполнение смарт-контракта в сети блокчейн

Для реализации алгоритма публикации документа в сети блокчейн и целей последующей проверки используем возможности смарт-контрактов [4]. Для разработки и тестирования смарт-контакта используем тестовую блокчейн сеть на локальной вычислительной машине, создаваемую на основе приложения Ganache [5]. Ganache предоставляет возможность создания виртуальной сети блокчейн, состоящий максимально из 10 участников (в работе используется 3 участника) – адресов Ethereum. При активации создаются адреса с закрытыми ключами, а также каждому адресу присваивается сумма криптовалюты в размере 100 единиц Ethereum для осуществления транзакций и отладки взаимодействий.

Другим инструментом, используемым для разработки смарт-контактов, является Remix – среда разработки, применяемая не только для создания смарт-контактов, но и для их отладки, публикации в сеть блокчейн (в том числе, созданную для проведения тестов на локальной машине), проверки работоспособности и т.д., используя язык разработки solidity.

Общее взаимодействие осуществляется посредством алгоритмов на языке Python. Смарт-контакт для публикации данных в блокчейн-сеть Ethereum представлен в виде следующего кода:

```
pragma solidity >=0.4.21;
contract Storage {
string public number;
function Store() public {
number = 'Enter';
   }
function setNumber(string _number) public {
number = _number;
   }
function retrieve() view public returns (string) {
return number;
   }
}
```

Алгоритм представлен в виде 3-х функций, позволяющих выполнить задачи:

– сохранение значения в сети блокчейн (в контексте работы – значения хэш-функции файла электронного документа об образовании);

– задание значения, сохраняемого в сети блокчейн;

– возврат значения по запросу.

После публикации контракта в среде Remix контракт становится доступным для его использования с заданными параметрами. Для смарт-контракта используем алгоритм:

1. Вычисляется значение хэш-функции нормализованного документа pdf-формата с использованием криптографического алгоритма (SHA1) и формируется сообщение, состоящее из значения хэш-функции документа, цифровой подписи и номера транзакции в сети блокчейн, необходимое для подтверждения достоверности размещения.

2. Сообщение шифруется ассиметричным шифрованием с использованием полученного от пользователя в запросе открытым ключом и передаётся в приложение пользователя, где расшифровывается закрытым ключом и может быть преобразовано из pdf-формата в вид документа, пригодный к формальному графическому представлению, пригодному для человеческого восприятия..

По итогам выполнения получает следующие результаты:

– сформированный файл электронного документа об образовании установленного образца, содержащий необходимые данные – 1014598.pdf;

– значение хэш-функции SHA1 электронного документа 1014598.pdf – 6d80deff635c5e3b4c6d1cbd491cd8c558027688;

– номер транзакции публикации хэш-суммы в сети блокчейн – 0x22a3057d8a4aba41720c54b246f50bc32af5d89c81eb63a7bc0e371eaab5c4a5;

– адрес отправителя – 0x3994Dacf68A445Af612F8fDd2ff34c9a5c4a8D23;

– значение хэш-функции в виде tx data, опубликованное в сети блокчейн – 0x9f2ad4c0000000000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000028366438306465666636335633565336234633664316362643439316364386335353830323736383800000000000000000000000000000000000000000000000.

Проверка достоверности осуществляется следующим образом: пользователь, получивший ранее обозначенные данные и осуществляющий проверку, вычисляет хэш-значение электронного документа, используя либо отдельное программное обеспечение либо интернет-сервисы (например, https://emn178.github.io/online-tools/sha1_checksum.html).

Полученное значение хэш-функции совпадает с предоставленным, осуществляется проверка значения, в сети блокчейн. Для этого необходимо найти транзакцию 0x22a3057d8a4aba41720 c54b246f50bc32af5d89c81eb63a7 bc0e371eaab5c4a5 в сети Ethereum по адресу https://etherscan.io и по номеру транзакции получить данные tx data (inputdata).

Далее необходимо осуществить конвертацию данных из шестнадцатеричной системы счисления в ASCII текст, используя программные продукты для преобразования или онлайн-сервисы (например, https://www.rapidtables.com/convert/number/hex-to-ascii.html).

Сравнивая представленные значения, делаем вывод о достоверности загруженного документа. Необходимо отметить, что при использовании публичной сети Ethereum конвертация Hex-ASCII не требуется, так как это функционал реализован на самой платформе https://etherscan.io.

Заключение

В докладе рассмотрена проблематика подтверждения достоверности документов об образовании, детально рассмотрена модель смарт контракта и ее реализация в сети блокчейн.

Список литературы

1. Шамсутдинова Т. М. Применение технологии блокчейн для выдачи цифровых дипломов: проблемы и перспективы // Открытое образование. 2018. № 22. С. 51–58.

2. 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. / под. общ. ред. М. В. Носкова. Красноярск, Сиб. федер. ун-т, 2020. Ч. 2. С. 61–66.

3. Качан Д. А., В. А. Вишняков. Поддержка информационного управления в образовании с использованием блокчейн // Кодирование и цифровая обработка сигналов в инфокоммуникациях: материалы междунар. науч.-практ. конф. (Республика Беларусь, Минск, 19 апреля 2021 года) / редкол.: В. К. Конопелько, В. Ю. Цветков, Л. А. Шичко. Минск : БГУИР, 2021. С. 19–22.

4. Yu, L. Smart Communications in Heterogeneous Spacecraft Networks: A Blockchain Based Secure Auction Approach [Electronic resource]. 2019. Access mode: https://www.researchgate.net/publication/337503125_Smart_Communications_in_Heterogeneous_Spacecraft_Networks_A_Blockchain_Based_Secure_Approach. Date of access: 10.08.2022.

5. Solaiman, E. Implementation and evaluation of smart contracts using a hybrid on- and off-blockchain architecture / E. Solaiman, T. Wike, I. Sfyrakis // Wiley special issue paper [Electronic resource]. 2020. Access mode: https://onlinelibrary. wiley.com/ doi/epdf/10.1002/cpe.5811. Date of access: 10.09.2020.