ОБ ОДНОМ СПОСОБЕ ВАЛИДИРОВАНИЯ академических записей в условиях мобильного обучения

Диана Александровна Богданова,
старший научный сотрудник Института образовательной информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук, кандидат педагогических наук, Москва,

• *технология блокчейн* • *блокчейн биткоина* • *аттестация* • *верификация*

Один из аспектов виртуальной академической мобильности и строительства индивидуальной траектории обучения — вопрос о возможности перезачёта и верификации документов о пройденном обучении. Зачётные ведомости учащихся собираются и контролируются учебными заведениями. После окончания обучения учащийся фактически получает в качестве документа лист бумаги, а если кто-нибудь захочет проверить валидность конкретной записи, он должен будет обратиться в учебное заведение, которое выдало эту бумагу. Многие исследователи видят потенциал технологии блокчейн в качестве надёжного способа подтверждения принадлежности записи к конкретному учащемуся[1].

По мнению специалистов, эта технология может использоваться в качестве децентрализованного неизменяемого хранилища разных видов информации, в том числе и о пройденном обучении. И по этой причине значительная часть исследований о возможностях использовании технологии блокчейн для образования, проводимых в настоящее время, посвящены организации хранения и валидирования академических записей.

Школа программирования Holberton в Сан-Франциско[2], реализующая проектный метод обучения, в качестве альтернативы курсам колледжа уже использовала блокчейн для хранения и доставки выданных сертификатов. Ожидается, что эта мера поможет остановить использование поддельных сертификатов. Сертификат выпускается и фиксируется в базе данных блокчейн. В школе по-прежнему студентам

[1] *Ruff C.* 2016 How Bitcoin Technology Could Make College Credentials More Secure [Электронный ресурс] / C. Ruff. The Chronicle of Higher Education. — 2016, April 19. Режим доступа: http://www.chronicle.com/ article/How-Bitcoin-Technology-Could/236070 (Дата обращения: 15.04.2017).

[2] *Богданова Д.А.* Блокчейн и образование // Дистанционное и виртуальное обучение. — 2017. — № 2. — С. 65—74.

выдают бумажные копии, а в системе генерируется децентрализованный номер (DCN), впоследствии позволяющий потенциальным работодателям провести аутентификацию-верификацию. Массачусетский технологический институт и Университет Никозии поступают аналогичным образом.

Университет Никозии выпустил первые сертификаты о пройденном обучении, подлинность которых может быть проверена с помощью технологии блокчейн биткоина. Эти сертификаты были выданы учащимся, успешно завершившим обучение на массовом открытом онлайновом курсе DFIN-511 «Введение в цифровую валюту», первом университетском курсе, предлагаемом по теме криптовалюты[3].

Рассмотрим, каким образом это было организовано и какие сложности пришлось преодолеть разработчикам.

Параметры проектирования

Начиная работу, проектировщики установили для себя следующие параметры дизайна:
- процесс не будет включать никаких других услуг или продуктов, кроме блокчейн биткоина;
- процесс позволит подтвердить подлинность сертификата Университета Никозии, не обращаясь Университету Никозии;
- процесс позволит кому бы то ни было завершить процедуру, даже если университет Никозии прекратит своё существование (или, что более вероятно, если сайт Университета перестанет существовать в его нынешнем виде, и т.д.).

Чтобы этот процесс работал, необходимо было не только гарантировать, что подлинность сертификатов может быть проверена, но и что не существует способа для кого-либо скопировать весь процесс и создать набор недостоверных сертификатов ещё до первого публичного объявления. Транзакция всегда должна опережать любые потенциально мошеннические представления в блокчейне. В определённом смысле документы, относящиеся к Университету, являются хорошим примером ситуаций подобного рода. Как известно, средний деловой документ может быть действителен на протяжении нескольких месяцев или лет. В ситуации с сертификатом может оказаться, что кто-нибудь захочет проверить подлинность университетского сертификата об обучении через десятилетия или даже столетия после его выпуска. Очевидно, что, скажем, нынешний сайт Университета, уже не будет доступен через 60 лет в его текущем виде.

Дизайнерские решения

Хэши

В качестве основного подхода было использование хеширования документов. Разработчики использовали алгоритм SHA-256 (тот же, что используется в протоколе биткоина[4]). Этот алгоритм принимает в качестве входных любые произвольные данные (в рассматриваемом случае это были документы PDF сертификатов) и создаёт серию уникальных чисел и букв. Невозможно воссоздать документ из хэша, но возможно воссоздать хэш из документа. Если известен конкретный хэш подлинного документа, его невозможно перепроектировать, чтобы узнать, чей это сертификат. Но если имеется копия сертификата, можно применить хэш-алгоритм SHA-256 для воспроизведения этого хэша. Очевидно, что использование хэшей имело решающее значение в реализации общего подхода.

Индекс

Первоначальная идея о вводе хэша каждого сертификата в блокчейн была пересмотрена, и было принято решение создать индексный документ, содержащий

[3] Сайт университета Никозии [Электронный ресурс] / Режим доступа: http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/ (Дата обращения: 15.04.2017).

[4] SHA 256 Pseudocode? [Электронный ресурс] / Stack Overflow сайт сообщества программистов. — 2012, August 13. Режим доступа: stackoverflow.com/questions/11937192/sha-256-pseuedocode (Дата обращения: 15.04.2017).

все хэши всех сертификатов, а затем, впоследствии, обработать индексный документ и ввести его хэш в блокчейн. Это было сделано по двум причинам:

- нецелесообразно отдельно вводить каждый сертификат в блокчейн, так как это добавляет данных больше, чем необходимо для решения стоящей задачи;
- не столь безопасно вводить каждый сертификат по отдельности: можно допустить ошибку при вводе. Вместо этого можно ввести в блокчейн только один хэш. В этом случае можно объявить, что это один-единственный хэш для сертификатов конкретной сессии конкретного года обучения. Альтернативным решением могло бы стать строительство дерева Меркля[5]. Однако, по мнению разработчиков, простота работы с индексом документа предпочтительнее других возможных достоинств.

Запись блокчейн

Хэш документа затем вводится в поле OP_RETURN в безденежной транзакции биткоина, лежащей в основе общего подхода, принятого ранее[6]. Это первый онлайновый сервис, позволяющий пользователю доказать без раскрытия собственных данных, что у него есть некоторая информация с децентрализованной сертификацией, основанной на сети биткоинов. Ключевыми преимуществами являются анонимность, конфиденциальность и получение децентрализованных доказательств, которые не могут быть удалены или изменены кем-либо (третьими сторонами или правительствами).

Сроки и инструкции

Если сертификаты должны быть самоверифицируемыми, сертификат плюс индекс должны содержать все инструкции, необходимые для самоверификации. В этой ситуации возникает проблема яйца и курицы, так как до той поры, пока транзакция не создана, не известно, к какой транзакции будет добавлен хэш. Но если ввести транзакцию в сертификат, это изменит её хэш.

Эта проблема была решена указанием в документах временного диапазона, в течение которого планировалось ввести транзакцию, последующим вводом транзакции и отказом от публичных заявлений до завершения указанного периода. После этого, как считают разработчики, единственный хэш за те сроки, которые могут представлять сертификаты Университета Никозии, — валидный.

Публичный доступ

Индексный документ находится на сайте Университета, но если он появился только там, разработанный процесс не лучше, чем публикация списка хэшей на сайте, и не требует блокчейна. Чтобы этот процесс был децентрализован, нужны люди, чтобы с их участием иметь возможность найти любую копию индекса и иметь возможность самовалидации, а не надеяться на то, что сайт Университета работает. Индекс распространяется по всему миру, в том числе и для студентов Университета, и хэш публично признаваем через Twitter, сайт, страницу Facebook и любой другой механизм. Таким образом, даже если Университет Никозии и его сайт исчезнут, если валидированный хэш всё ещё существует в качестве публичной записи, люди могут определить правильную копию индекса и, исходя из этого, подтвердить подлинность любого сертификата.

Из рассмотренного примера следует, что возможности технологии блокчейн применительно к образованию многообразны, не до конца изучены и испытаны, и специалисты пока что делают первые, но довольно успешные шаги в этом направлении. **НО**

---

[5] Merkle Tree [Электронный ресурс] / Bitcoin — сайт, посвящённый биткоину. Режим доступа: https://bitcoin.org/en/glossary/merkle-tree (Дата обращения: 15.04.2017).

[6] Select a document and have it certified in the Bitcoin blockchain [Электронный ресурс] / Proof of Existence — сайт самоверификации. Режим доступа: www.proofofexistence.com (Дата обращения: 15.04.2017).