Е. А. Воробьев

РАСПРЕДЕЛЕННЫЙ СЕРВИС СЕРТИФИКАЦИИ НА БЛОКЧЕЙН ПЛАТФОРМЕ ETHEREUM

В работе рассматриваются вопросы, необходимые для создания и управления распределенной сетью для хранения сертификатов, а также возможные алгоритмы решения этой задачи.

Введение

Ethereum — это распределенная сеть открытых блоков, которая фокусируется на запуске программного кода любого децентрализованного приложения. Проще говоря, это всемирная платформа для обмена информацией, которой нельзя манипулировать и которую нельзя изменять. Реализована как единая децентрализованная виртуальная машина. Был предложен основателем журнала Bitcoin Magazine Виталием Бутериным в конце 2013 года, сеть была запущена 30 июля 2015 года. Технология Ethereum даёт возможность регистрации любых сделок с любыми активами на основе распределённой базы контрактов типа блокчейн, не прибегая к традиционным юридическим процедурам. Эта возможность является конкурентной по отношению к существующей системе регистрации сделок

I. Цели создания системы

Одно из не самых очевидных применений блокчейн-технологий — сертификация товаров и услуг. Особенности технологии распределенного реестра отлично подходят для защиты продукции от фальсификации. Это выгодно и для производителей, и для продавцов, и для конечных потребителей. Разберем применение распределенного реестра и его технологий для сертификации алкогольной продукции — одной из наиболее часто фальсифицируемых категорий товаров. Как сегодня производители ведут борьбу с подделками? Наклеивают специальные этикетки с водяными знаками и голограммами, что не дает практически никакого положительного эффекта. Многие изготовители контрафакта с легкостью подделывают любые знаки. Проблема усугубляется тем, что далеко не все конечные потребители хорошо разбираются в алкоголе. Они не могут отличить настоящую продукцию от поддельной не то, что во время выбора и покупки, но и даже по итогам дегустации напитка. В результате производитель теряет существенную долю прибыли, государство недополучает налоги (фальсификаторы их, естественно, не оплачивают), а торговцы вынуждены терпеть нападки покупателей.

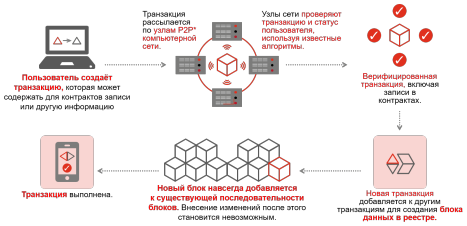

Рис. 1 – Программная модель

Одно из решений проблемы — это оснащение бутылок с алкогольной продукцией так называемыми «умными» этикетками. Каждая такая этикетка содержит уникальный электронный код соответствия оригинальному качеству с указанием времени и места производства продукта. В отличие от бумажных этикеток, штрихкодов и различных голограмм подделать электронный код не представляется возможным независимо от используемых средств. Вернемся к примеру с бутылкой алкоголя, сертифицированной с применением блокчейна и укомплектованной электронным кодом. Каждую единицу товара уникальный код сопровождает на каждом этапе следования от производителя до конечного потребителя. Для проверки подлинности продукта достаточно вбить код в общую базу, и просмотреть подробные сведения по конкретной бутылке или другой единице товара. Все, что для этого нужно — компьютер или любое мобильное устройство с подключением к Интернету. Проверить оригинальность может не только покупатель, но и продавец после получения партии товара от поставщика. Этим он убережет себя от реализации некачественных товаров.

II. Описание системы

На рисунке 2 представлена блок-схема алгоритма системы.

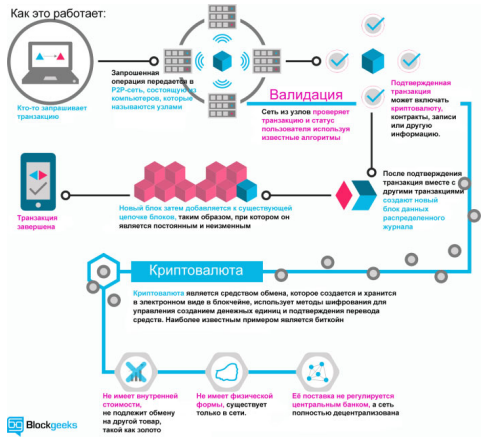

Рис. 2 – Блок-схема алгоритма системы

Блокчейн (цепочка блоков) — это распределенная база данных, у которой устройства хранения данных не подключены к общему серверу. Эта база данных хранит постоянно растущий список упорядоченных записей, называемых блоками. Каждый блок содержит метку времени и ссылку на предыдущий блок. Если объяснять на пальцах, то блокчейн часто сравнивают со стандартным дневником или картотекой, куда последовательно в хронологическом порядке вносятся записи о том, что сделано – поспал, поел, постирал, погулял, взял в долг, заплатил 100 долларов за ужин и т.д. Чтобы никто посторонний не мог внести по своему усмотрению изменения в дневник, вся информация особым образом шифруется, причем шифр продуман качественно. Если дневник в одном экземпляре, с ним всякое может случиться – сгорел дом и он вместе с ним, украли, при огромнейшем желании расшифровали и внесли коррективы. А потому для надежности дневник имеет множество копий, которые хранятся в разных местах. Причем, когда в дневник вносится новая информация, она после проверки обновляется на всех экземплярах. Применение шифрования гарантирует, что пользователи могут изменять только те части цепочки блоков, которыми они «владеют» в том смысле, что у них есть закрытые ключи, без которых запись в файл невозможна. Кроме того, шифрование гарантирует синхронизацию копий распределенной цепочки блоков у всех пользователей. В технологию блокчейн изначально заложена безопасность на уровне базы данных. Концепцию цепочек блоков предложил в 2008 г. Сатоши Накамото (Satoshi Nakamoto). Впервые реализована она была в 2009 г. как компонент цифровой валюты — биткоина, где блокчейн играет роль главного общего реестра для всех операций с биткоинами. Благодаря технологии блокчейна биткоин стал первой цифровой валютой, которая решает проблему двойных расходов (в отличие от физических монет или жетонов, электронные файлы могут дублироваться и тратиться дважды) без использования какого-либо авторитетного органа или центрального сервера.

III. Выводы

В мире существует потребность в системе, которая способна сохранять и отслеживать все данные относящиеся к сертификации, которая сможет облегчить процесс сертификации, сделать его прозрачнее и надежнее.

1. Карпов О. Э., Клименко Г. С., Лебедев Г. С. Создание смарт-контрактов Solidity для блокчейна Ethereum. Практическое руководство. 2016. № 2. – С. 7–23.
2. Alex Popp B. Г. Mastering Ethereum is a book for developers, 2016.–№ 6–7. – С. 32–33.
3. Лебедев Г. С., Мухин Ю. Ю. Блокчейн изнутри // часть 2, 2015, с. 98–105.

Воробьев Егор Александрович, магистрант кафедры информационных технологий автоматизированных систем БГУИР, e.vorob8@gmail.com.

Научный руководитель: Свито Игорь Леонтьевич, доцент кафедры ТОЭ БГУИР, кандидат технических наук, доцент, kaftoe@bsuir.by.