3. LW-криптография: шифры для RFID-систем. [Электронный ресурс]. – Режим доступа: www.habr.com. – Дата доступа: 03.04.2019.

4. Урбанович, П. П. Компьютерные сети: учебное пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 399 с.

УДК 004.056+003.26

Студ. А.А. Чопик
Науч. рук. проф. П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

РЕАЛИЗАЦИЯ СЕРВЕРА ДЛЯ ПРЕДОСТАВЛЕНИЯ УДОБНОГО ИНТЕРФЕЙСА К ДАННЫМ БЛОКЧЕЙНА ECHO И ВОЗМОЖНОСТИ ПОДПИСАТЬСЯ НА ИХ ОБНОВЛЕНИЕ

В современном мире широкое распространение получили криптовалюты и технология блокчейн (Blockchain), которая лежит в основе большинства из них. По своей сути блокчейн – это реестр, представляющий собой неразрывную цепочку из блоков, содержащих транзакции с информацией и расположенную на множестве узлов независимо друг от друга [1]. Под транзакциями понимаются любые действия, совершаемые участниками сети (отправка денежных средств, покупка какого-либо контента, установление прав собственности и др.). Кроме новой информации в блоке хранится зашифрованная информация о предшествующих блоках. Реестр автоматически обновляется на всех устройствах системы, после чего начинается генерация следующего блока. Шифрование основывается на определенных криптоалгоритмах [2, 3].

Основными причинами популярности технологии блокчейн в настоящее время являются проблемы обеспечения безопасности цифровой инфраструктуры и в частности распределенных реестров, а также проблемы доверия к проведению денежных транзакций.

Распространены блокчейны трех видов: блокчейн без необходимости в разрешениях, открытый блокчейн с разным уровнем разрешений, закрытый блокчейн с разным уровнем разрешений [4].

Под блокчейном без необходимости в разрешениях понимаются блокчейны без управляющего органа, подтверждающего транзакции. При отправке транзакции происходит публичное анонсирование и об этом узнает вся сеть. После этого начинается процесс подтверждения транзакции, причем не известно, кто именно подтвердит транзакцию. Это пример по-настоящему демократичной системы, в которой поль-

зователи обладают некоторой степенью анонимности. Данный вид блокчейна хорошо подходит для защиты особо важной информации.

В открытом блокчейне с разным уровнем разрешений транзакции подтверждают определенные люди. Просматривать информацию может любой пользователь.

Закрытый блокчейн с разным уровнем разрешений похож на открытый, с единственным отличием – данные в нем не открыты для всех. Данный вид хорошо подходит в ситуациях, когда узлам нужно хранить в блокчейне приватную информацию.

Для исследования был использован блокчейн Echo, который в качестве основы использует Graphene и встроенную виртуальную машину Ethereum. Echo – это блокчейн-платформа, которая может использоваться в качестве концептуальной основы и среды для широкого спектра приложений и сервисов на основе смарт контрактов. Особенностями являются: новая модель организации и функционирования сети, инновационная виртуальная машина, поддержка интеграции с другими блокчейнами посредством технологии SideChain, усовершенствованная система управления аккаунтом, поддержка смарт контрактов с использованием не только языка solidity, но и C, и C++.

В данный момент в разработке находится сервер для предоставления удобного интерфейса к данным блокчейна Echo (рабочее название «EchoDB»). При разработке сервера используются программная платформа Node.js, язык программирования TypeScript и документоориентированная СУБД MongoDB. Сервер состоит из двух модулей - парсер блокчейна Echo, который заносит информацию из блокчейна в базу данных, и публичного API (GraphQL + WS) для получения этой информации сторонними приложениями.

Парсинг происходит следующим образом – в момент первого запуска парсера из блокчейна получается и создается в базе данных документ, содержащий информацию о так называемом core ассете. Ассет – форма валюты в сети Echo, которая может быть создана и выпущена пользователями. После этого начинается парсинг блоков – по порядку, начиная с первого, из блокчейна запрашивается блок, при помощи библиотеки echojs-lib, затем из него получают транзакции, которые в свою очередь содержат различные операции. На данный момент существует около 50 операций с блокчейном, например, создание нового аккаунта, создание нового ассета, перевод ассетов на другой аккаунт и другие. В зависимости от типа операции и полученной транзакции в базу данных сохраняются различные документы, а также срабатывают различные события, на которые пользователь может подписываться, чтобы получить новую информацию. После того

как все операции в блоке будут обработаны парсером начинается парсинг следующего блока.

Одновременно с парсером работает модуль публичного API. Он использует технологию GraphQL– язык запросов, основанный на графах. При помощи которого можно гибко составлять запросы к базе данных и указывать какую конкретно информацию сервер должен вернуть в ответе. Кроме того, на сервере используется библиотека apollo-server-express, поэтому существует возможность подписаться на какие-либо события и если в процессе парсинга будет вызвано данное событие, то сервер вернет информацию о событии. Также эта библиотека предоставляет стандартный пользовательский интерфейс, позволяющий ознакомиться с существующими методами и опробовать API. На рисунке 1 приведен вид стандартного пользовательского интерфейса.

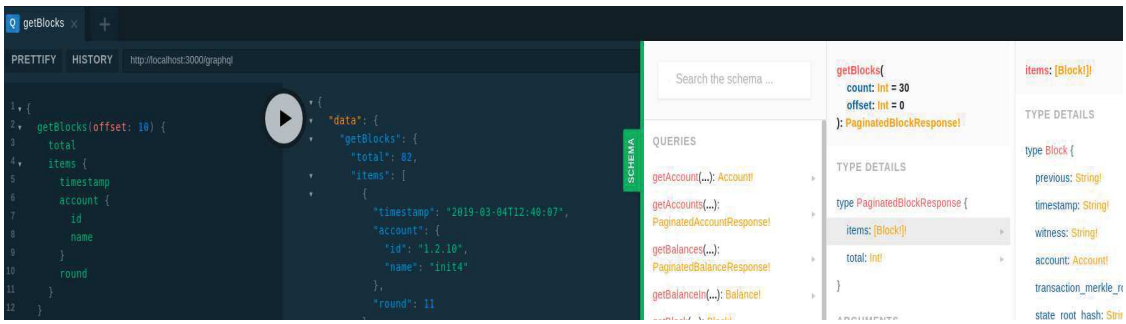

Рисунок 1 – Стандартный пользовательский интерфейс

ЛИТЕРАТУРА

1. Ethclassic – Все о BTC: Новости, события, анализ. Чем различаются блокчейн и распределенный реестр. [Электронный ресурс]. – Режим доступа: https://ethclassic.ru/2018/04/11/chem-otlichayutsya-blokchejn-i-raspredelenny-reestr/. – Дата доступа: 12.04.2019.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ Урбанович П.П. – Минск: БГТУ, 2016. – 220 с.

3. Урбанович, П. П. Информационная безопасность и надежность систем: учебно-методическое пособие по одноименному курсу для студентов специальности 1-40 01 02-03 "Информационные системы и технологии" / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Минск: БГТУ, 2007. – 87 с.

4. BitNovosti – Все о мире Bitcoin: новости, события, факты, курс, анализ. Три распространенных вида блокчейна. [Электронный ресурс]. – Режим доступа: https://bitnovosti.com/2018/04/25/3-popular-types-of-blockchains/. – Дата доступа: 12.04.2019.