УДК 004.4

О МОДЕЛИРОВАНИИ ПРОЦЕССА СОХРАНЕНИЯ ДАННЫХ В ТЕХНОЛОГИИ БЛОКЧЕЙН

Загурский В.Н., доц., Павлович А.В., студ.

Витебский государственный технологический университет,

г. Витебск, Республика Беларусь

Реферат. *В работе описан учебный программный комплекс, реализующий модель процесса сохранения данных в технологии блокчейн и позволяющий исследовать его статистические характеристики.*

Ключевые слова: блокчейн, доказательство правильности работы, майнинг, биткойн.

С 28 марта 2018 г. в Беларуси вступил в силу декрет № 8 «О развитии цифровой экономики», в соответствии с которым для резидентов белорусского Парка высоких технологий (ПВТ) легализуются новые виды деятельности, включая разработки с применением блокчейн-технологий и другие технологии работы в криптопространстве (использование криптовалют, майнинг, смарт-контракты и т. д.).

Блокчейн (blockchain, цепочка блоков) − это революционная технология, которая уже стала неизбежным аспектом человеческого развития. Первое глобальное применение технологии блокчейна связано с появлением в начале 2009 года первой криптовалюты − биткоина. В 2015 году появилось первое блокчейн-пространство, реализующее идею смарт-контрактов − Ethereum. В течение 2015 года регулирующие органы и крупные корпорации начали усиленно интересоваться технологией блокчейна и уже свыше 1 миллиарда долларов США было инвестировано в блокчейн-стартапы к концу 2015 года.

Технология блокчейна способна серьезно изменить взаимодействие с цифровым миром и высоко поднять уровень доверия к происходящему в Интернете. Блокчейн, по сути своей, является общедоступной, распределенной и 100 % достоверной учетной книгой записей о событиях в цифровом мире. Эта книга распределена и доступна множеству пользователей. Записи в неё можно вносить только с согласия большинства пользователей. И еще, однажды записанная информация уже никогда не может быть изменена или стерта, т.е. никто не сможет сфальсифицировать информацию о прошлых или текущих цифровых событиях. Эти свойства позволяют доверить технологии блокчейн проведение самых ответственных, дорогих и сложных операций в банковской, страховой, транспортной и других сферах.

В данной работе был разработан учебный программный комплекс, который позволяет моделировать процесс сохранения данных в технологии блокчейн и исследовать его статистические характеристики. Программа реализована на языке программирования Python, имеет графический интерфейс пользователя (библиотека Tkinter) и использует научно-техническую библиотеку Scientific Python (SciPy) для статистического анализа полученных данных. Исследовать построенную модель можно как на обычном персональном компьютере, так и на смартфонах под управлением iOS или Android.

Пусть каждый блок блокчейна моделирует строка символов определенной структуры размером 1Кб хранимая в текстовой файле с именем номера блока. Каждый блок представляет собой структуру данных, состоящую из следующих полей: id-block – номер блока; prev-hash – значение криптографической хеш-функции SHA256 предыдущего блока; timestamp – время генерации данного блока; data – данные, сохраняемые в блоке; nonce – целое неотрицательное число X, используемое для доказательства правильности работы. Для добавления блока в блокчейн используется целевое значение C, называемое сложностью.

Главной особенностью блокчейна как защищенной от изменений структуры данных является то, что для закрытия блока и добавления блока в цепочку, необходимо совершить вычислительную работу, сложность которой зависит от цели C – 64-символьного 16-ричного числа. Для этого необходимо к сформированным данным блока L последовательно присоединять целое неотрицательное число X = 0,1,2,… до тех пор, пока значение криптографической хеш-функции SHA256 от общего блока данных не будет меньше заранее заданного числа C цели. Найденное число X есть nonce и является доказательством

правильности работы. Пусть T − время, затраченное на нахождение nonce.

Таким образом, X является доказательством правильности работы, если выполняется условие SHA256(L+X)<C. Поскольку результат хеш-функции SHA256 ведет себя как случайная величина, распределенная по равномерному закону, и является необратимым, то предугадать его невозможно. Поэтому, если мы хотим иметь значение хеш-функции с 7 нулями вначале, то будет нужно, в среднем, перебрать 16 в степени 7 различных значений, прежде чем найдется подходящее число X. Это сложная задача, требующая большой вычислительной мощности и решаемая только посредством прямого перебора значений X. Это означает, что чем меньше значение цели C, тем сложнее задача майнинга, используемого для добавления блока в блокчейн и тем больше значение времени T. Кроме того, вероятность найти решение на любом промежутке фиксированной длины из всего множества возможных чисел является одинаковой. Поэтому эффективным является использование параллельных вычислений. Но поскольку Python не позволяет одной программе использовать несколько процессоров одновременно (GIL), мы моделируем сохранение в блокчейн только на одном процессоре, без использования потоков.

Исследование реализованной нами модели сохранения данных в блокчейн заключается в изучении взаимосвязи двух основных параметров: значении цели C и времени генерации одного блока T. Одна часть программного комплекса параметризована на количество сохраняемых в блокчейн блоков N и время T добавления одного блока в блокчейн. В результате работы программы, мы получаем выборочную совокупность N значений целей C и ее статистические характеристики. Например, мы можем оценить выборочное среднее и среднее квадратичное отклонение значения C для заданного времени T. Вторая часть программного комплекса параметризована на количество сохраняемых в блокчейн блоков N и значение цели C, характеризующей сложность задачи майнинга при добавлении одного блока в блокчейн. В результате работы программы, мы получаем выборочную совокупность N значений времени T и ее статистические характеристики. В этом случае, мы можем оценить выборочное среднее и среднее квадратичное отклонение времени T для заданной величины цели C. Кроме того, программа позволяет проверять целостность построенного блокчейна и обнаруживать измененные блоки.

Программная модель процесса сохранения данных в технологии блокчейн была исследована на персональных компьютерах: Core i7, Core i5, Core i3, DualCore Intel с частотами ядра от 1.8GHz до 3.3GHz, а также на 2-х ядерном процессоре Apple A9 1,8 MHz. Количество оперативной памяти является малосущественным фактором. Мобильный процессор на равных сохраняет блоки в блокчейн с мощнейшими процессорами персональных компьютеров типа Core i7.

Программный комплекс может быть использован на практических занятиях по построению программных продуктов с применением блокчейн-технологий для студентов IT-специальностей.

Список использованных источников

1. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. – The Cryptography Mailing list / metzdowd.com, 2008.
2. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. – "ТВП": Москва, 2001. – 254 с.
3. Бизли, Д. Python. Подробный справочник / Д. Бизли. 4-е изд., 2010. – 858 с.

УДК 004.3

АНАЛИЗ КОНСТРУКТИВНЫХ РЕШЕНИЙ БЕСКОНТАКТНЫХ АКТИВНЫХ 3D-СКАНЕРОВ

Замотин Н.А., асп., Дягилев А.С., к.т.н, доц.

Витебский государственный технологический университет,

г. Витебск, Республика Беларусь

Реферат. *Проведен анализ конструктивных решений бесконтактных активных 3D-сканеров. Результатом анализа стала классификация и ряд сравнительных характеристик базовых конструкций 3D-сканеров. Выбор базовой конструкции*