УДК 004.056.5

О ДОКАЗАТЕЛЬСТВЕ ПРАВИЛЬНОСТИ РАБОТЫ В ПРОЦЕССЕ МАЙНИНГА БИТКОЙНОВ

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

Витебский государственный технологический университет,

г. Витебск, Республика Беларусь

Реферат. *В статье рассмотрена программная модель на языке Python для исследования процесса майнинга биткойнов с решением задачи доказательства правильности работы. Данная модель позволяет формировать и проверять гипотезы о сложности цели, используемой для нахождения доказательства правильности работы.*

Ключевые слова: биткойн, майнинг, доказательство правильности работы.

В 2009 году Сатоси Накамото запустил в глобальной сети Интернет первую и самую известную платежную систему Биткойн с цифровыми деньгами, защищенными криптографией. Платежная система Биткойн представляет собой биткойн-сеть, т.е. запущенные на множестве компьютеров программы-клиенты с биткойн-кошельками, которые соединены между собой в одноранговую сеть, каждый узел которой равноправен и самодостаточен. Это является главной особенностью системы – отсутствие банка или какого-либо его аналога. Проводимые сделки необратимы, электронный платеж между двумя сторонами происходит без посредников. Средства никто не может заморозить, даже временно, за исключением самого владельца. Каждый пользователь системы хранит на своем узле в общедоступном открытом виде криптографически связанную цепочку записей – лог транзакций (блокчейн) со всеми утвержденными транзакциями, когда-либо происходившими в системе, с указанием биткойн-адресов отправителей/получателей и количества переданных биткойнов, но без информации о реальном владельце этих адресов, причем это информация на всех узлах постоянно обновляется. Поэтому любое несоответствие, которое попытается внести любой из узлов, будет мгновенно выявлено, и такой блок транзакций будет отвергнут другими узлами и не присоединён к цепи.

Биткоин (1 BTC) как единица валюты – это уникальный цифровой код, являющийся решением математической задачи. Процесс выпуска новых биткоинов в систему называется майнинг – единственный способ получения криптовалюты, построенный на решении компьютерами математических задач.

Суть майнинга биткойнов заключается в том, что узел, отбирает из появившихся за последние 10 минут новых неподтвержденных транзакций в системе, какое-то количество транзакций, проверяет их правомочность по своей последней копии блокчейна, но не может сразу сообщить о результате остальным узлам. Для этого он должен сделать, так называемое доказательство правильности работы. Тот узел, который это сделает первым, получает право включить свои отобранные транзакции в глобальный лог подтвержденных транзакций и вознаграждение в определенное количество биткойнов на свой биткойн-адрес. На данный момент, это 12,5 биткоинов по цене $1,786 за один биткойн. Вероятность получения награды майнером в произвольный десятиминутный период приблизительно равна соотношению его вычислительной мощности к вычислительной мощности всей сети. И если это соотношение очень маленькое, то вероятность получения награды даже за длительный промежуток времени также будет низкой.

С 2009 года процесс майнинга претерпел ряд технологических изменений. С 2009 по 2011 г. майнинг осуществлялся на процессорах обычных персональных компьютеров (CPU). В 2011 году была разработана программа для майнинга на GPU (графический процессор видеокарты). Он справляется с этими расчётами гораздо лучше и позволял проводить параллельные вычисления и ускорить их на несколько порядков. Далее возникли компьютеры с несколькими видеокартами, а затем и целые фермы с десятками и сотнями карт, которые занимались исключительно вычислениями для системы Биткойн. Затем появились пулы - сайты для коллективного майнинга, а одиночный майнинг, полезный для децентрализации сети, стал рискованным и непрактичным. Это продолжалось до 2013 г. Следующим шагом стала разработка специализированных чипов ASIC – интегральных схем

специального назначения, отличающихся высокой скорость расчёта хэшей и низким энергопотреблением. С 2013 года появляются датацентры биткойнов с тысячами ASIC-процессоров в США, Гонконге, Исландии, Швеции и других странах.

В данной работе был разработан учебный программный комплекс, реализующий модель для исследования процесса майнинга биткойнов с решением задачи доказательства правильности работы на процессорах обычных персональных компьютеров и современных смартфонов. Для написания программ были использованы научно-технические библиотеки языка программирования Python (Scientific Python) с применением специальных криптографических модулей.

Пусть сформированный блок неподтвержденных транзакций моделирует случайная последовательность символов L размером 1Мб. К такому блоку будем 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, называемого сложностью. Найденное число X является доказательством правильности работы. Результатом хеш-функции SHA256 является 64-символьное 16-ричное число.

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 10 нулями вначале, то будет нужно, в среднем, перебрать 16 в степени 10 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. Кроме того, вероятность найти решение на любом промежутке фиксированной длины из всего множества возможных чисел является одинаковой. Поэтому эффективным является использование параллельных вычислений.

Одна часть программного комплекса параметризована на количество итераций для нахождения гипотезы о математическом ожидании цели C, для которой решение задачи доказательства правильности работы может быть найдено за время меньшее, чем 10 минут на данном процессоре. Вторая часть программного комплекса проверяет сформированную гипотезу о цели и находит значение дисперсии.

Программная модель решения задачи нахождения правильности работы была исследована на персональных компьютерах: 4-ядерные Core i7, Core i5, Core i3, 2-х ядерный DualCore Intel с частотами ядра от 1.8GHz до 3.3GHz, а также на 2-х ядерном процессоре Apple A9 1,8 MHz. Нами сделаны выводы о том, что задача нахождения X может быть решена за 10 минут на одном ядре современного процессора в том случае, если в записи цели C содержится первые 4-5 нулей и не более. Количество оперативной памяти является малосущественным фактором. Мобильный процессор на равных конкурирует с мощнейшими процессорами персональных компьютеров типа Core i7. Поскольку на сегодняшний день цели в системе Биткойн содержат порядка 54-х первых нулей, то вероятность решения задачи доказательства правильности работы даже на нескольких современных процессорах является слишком низкой. Программный комплекс адекватно формирует и проверяет гипотезы о сложности цели.

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.