http://rosoperator.ru/rameev100/

Всероссийская научно-техническая конференция, посвященная 100-летию со дня рождения одного из основоположников советской вычислительной техники Б.И. Рамеева, на тему: «Информационно-управляющие и телекоммуникационные системы специального назначения». Секция «Биометрическая поддержка криптовалют, блокчейн реестров, облачных сервисов», проводится в конференц-зале Технопарка высоких технологий «Рамеев», доклад 16 мая 2018 года с 14^{15} до 14^{30} (ул. Центральная, д. 1), г. Пенза.

Иванов А.И., Семерич Ю.С.

Майнинг криптовалюты, как способ накапливания избыточных вычислительных ресурсов для обычных пользователей

Аннотация.

Актуальность и цели. Целью работы является анализ возможности накапливания избыточных вычислительных ресурсов обычных пользователей за счет майнинга криптовалюты, выполняемого параллельно решению обычных задач на компьютере пользователя.

Материалы и методы. На руках у множества пользователей находится значительный парк персональных компьютеров, которые в обычных условиях их эксплуатации недогружены. Майнинг биткоинов и иных криптовалют привел к созданию ферм и их объединению в пулы, совместно добывающих значимые единицы «старых» криптовалют. Более того, даже после получения криптовалюты необходима ее поддержка блокчейн реестрами, что требует дополнительных непрерывных затрат электроэнергии и затрат на аппаратную часть поддержки блокчейн реестров.

Результаты. Предложено отказаться от использования обратных криптографических задач для организации «бесполезного майнинга» криптовалюты. Предложено организовывать «полезный майнинг», опираясь на дробление полезных для общества сложных вычислительных задач. Инициатор «полезного майнинга» должен иметь пакет сложных полезных задач, дробить их на фрагменты и раздавать «полезным майнерам». Контроль добросовестности майнеров выполняется дублированием их работы до полного совпадения отчетов о выполнении фрагмента задачи двумя или более майнерами. Политика учетности, затраченных вычислительных ресурсов «полезными майнерами» поддерживается выпуском промежуточной криптовалюты, хождение которой является редкими событиями. Требования к блокчейн реестрам многократно снижаются.

Выводы. У обычных пользователей появляется возможность накапливания ими своих избыточных вычислительных ресурсов, которые позднее каждый пользователь может направить на решение личной задачи высокой вычислительной сложности. Если личная задача пользователя легко распараллеливается, то «организатор» коллективных вычислений может распараллелить ее и раздать другим «полезным майнерам». Когда личная вычислительная задача «полезного майнера» не может быть распараллелена, эмитент промежуточной «полезной криптовалюты» должен иметь страхующий его деятельность собственный вычислительный ресурс, осуществляющий утилизацию, выпущенных ранее единиц криптовалюты.

Ключевые слова: майнинг криптовалюты, эмиссия криптовалюты без майнинга, снижение требований к блокчейн реестрам.

«Пирамида» нерегулируемого майнинга криптовалют, технические издержки на блокчейн поддержку «старых криптовалют»

Одним из способов, задания условия синтеза криптовалюты является подбор значения случайной цифровой последовательности, хэширование, которой дает читаемый (понимаемый) человеком фрагмент. Эта ситуация отображена на рисунке 1.

Рис. 1 «Бесполезный майнинг» криптовалюты непрерывно потребляющий электроэнергию и требующий значительных затрат на аппаратную поддержку

Как только в выходном значении хэш-функции, появится понятное человеку словосочетание на одном из известных языков, обнаруженную комбинацию можно считать «криптомонетой». Стоимость «криптомонеты» может быть определена пропорционально ее редкости. В свою очередь вероятность обнаружения монеты может быть легко вычислена в пространстве расстояний Хэмминга [1, 2, 3].

К сожалению, майнинг этого типа «криптомонет» является высокозатратным для «поздних майнеров». «Первые майнеры» быстро находят «первые криптомонеты», так как их много. Однако по мере майнинга «криптомонет» и занесения их в блокчейн реестры их добыча замедляется. Чем больше обнаружено «криптомонет», тем труднее их добывать и тем труднее их поддерживать блокчейн реестрами. Добыча и поддержка криптомонет требует значительных затрат электроэнергии и значительных аппаратных затрат.

Ситуация меняется, если «криптомонеты» выпускает один или несколько эмитентов в ограниченном количестве под некоторый конкретный технический проект. Эта ситуация отображена на рисунке 2.

Рис. 2 Эмиссия криптовалюты без затрат электроэнергии и без покупки «железа»

Как показано на рисунке 2 эмиссия криптомонет может быть выполнена созданием осмысленного текстового файла, к которому добавлена случайная «соль» и этот текстовый файл должен быть охвачен цифровой подписью эмитентов криптомонеты. В этом случае для выпуска криптомонет нет необходимости тратить значительные вычислительные ресурсы. Стоимость выпуска «криптофлопов» снижается так же как снижается стоимость выпуска бумажных денег по сравнению с золотыми или серебряными монетами.

Структура системы обращения (выпуска и использования) криптофлопов приведена на рисунке 3.

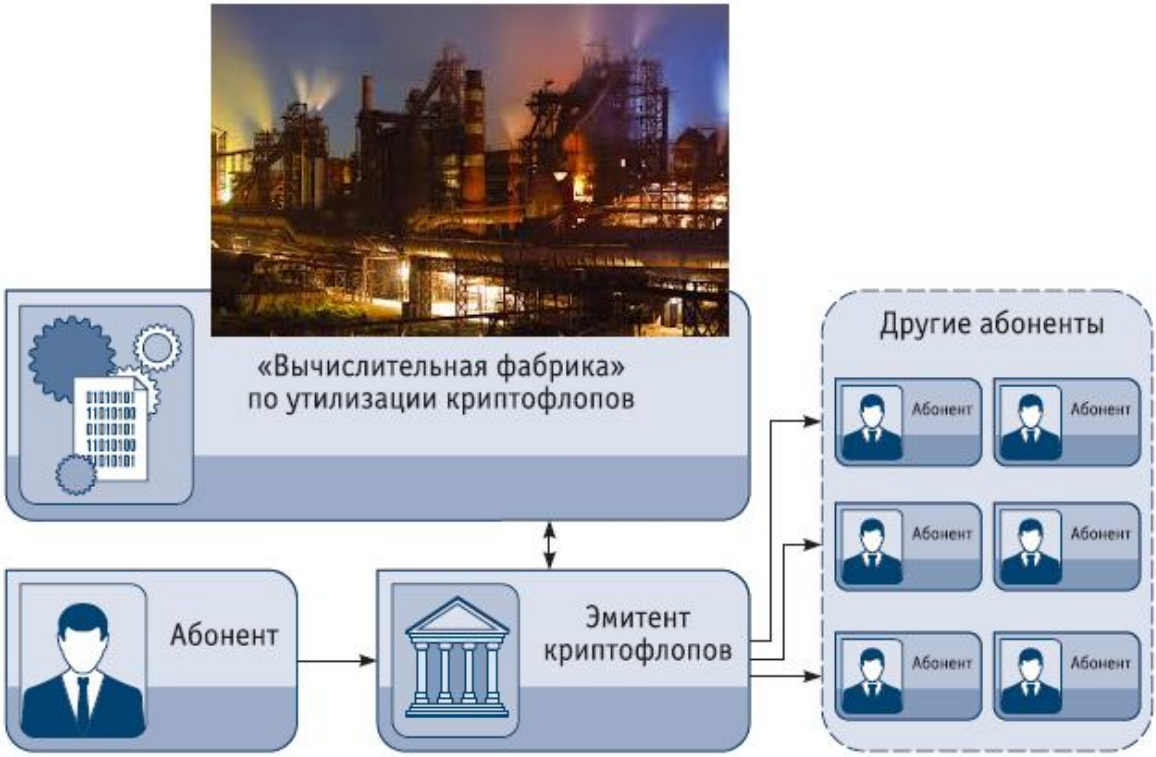

Рис. 3. Абонент, желающий накопить свои вычислительные ресурсы, обращается в банк, эмитирующий криптофлопы, за вычислительной задачей-консервации

Следует подчеркнуть, что «бесполезный затратный майнинг» рисунка 1 характерен тем, что «первые майнеры» вполне могут использовать свои первые криптомонеты для накапливания своих избыточных вычислительных ресурсов. На руках у множества пользователей находится значительный парк персональных компьютеров, которые в обычных условиях их эксплуатации недогружены. То есть «первые майнеры», кто тратит малые вычислительные ресурсы на добычу первых криптомонет могут использовать избыточный ресурс своих компьютеров на добычу «первых криптомонет». Потом, когда криптовалюта «постареет» майнить ее становится не выгодно. Она перестает играть роль накопителя криптофлопов.

Положение меняется, если отказаться от майнинга, построенного на решении бесполезных задач. В этом случае организатор «полезного майнинга» должен иметь важную для всех полезную, но сложную в исполнении вычислительную задачу. Он должен уметь дробить полезную задачу на мелкие фрагменты и раздавать «полезным майнерам». Контроль добросовестности майнеров выполняется дублированием их работы до полного совпадения отчетов о выполнении фрагмента задачи двумя или более майнерами. Политика учетности, затраченных вычислительных ресурсов «полезными

майнерами» поддерживается выпуском промежуточной криптовалюты, движение которой являются редкими событиями. Требования к блокчейн реестрам многократно снижаются.

В этой схеме взаимодействия эмитента и майнеров принципиальным является то, что задача стороннего ЗАКАЗЧИКА должна легко распараллеливаться на небольшие фрагменты для исполнения их «полезными майнерами». В этом случае система начинает работать. При этом эмитент криптофлопов не должен повторять работу за майнерами, проверяя их. Политика учетности, затраченных вычислительных ресурсов «полезными майнерами» поддерживается выпуском промежуточной криптовалюты, хождение которой является редкими событиями. Требования к блокчейн реестрам многократно снижаются из-за общения «полезных майнеров» только с эмитентом криптофлопов.

Еще одним важным условием является возможность получения коротких однозначных отчетов «полезных майнеров» о проделанной ими работе. Рисунок 4 иллюстрирует эту возможность на примере решения вычислительно сложной задачи факторизации длинных чисел.

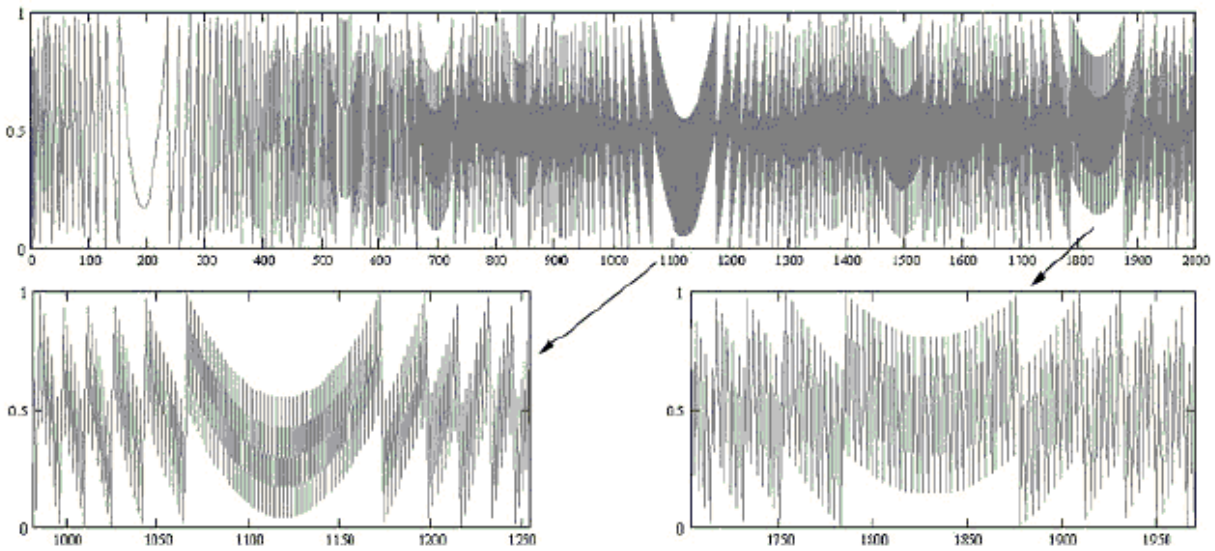

Рис. 4 . Портреты остатков от деления числа N на целые числа, перебираемые при поиске произведения простых сомножителей (pq = N)

«Полезный майнер», получив свой фрагмент просмотра состояний, будет видеть «бабочки» сильно связанных между собой остатков. Он должен формировать список очень близких к решению примеров простых чисел. Эмитент криптофлопов должен сравнивать списки-отчеты двух и более «полезных майнеров». При совпадении списков, проверяемые майнеры признаются добросовесными.

Следует отметить, что «уплотнение» отчетов «полезных майнеров» может быть значительно увеличено, если перейти от линейных портретов чисел (рис. 4) к двухмерным портретам чисел [5], рисунок 5. На этом рисунке видны 16 эллипсов, каждый эллипс описывается двумя параметрами, то есть, представленный портрет есть не что иное, как отображение 32-мерной задачи. Пользуясь этим можно многократно увеличить компактность отчетов о результатах работы «полезных майнеров».

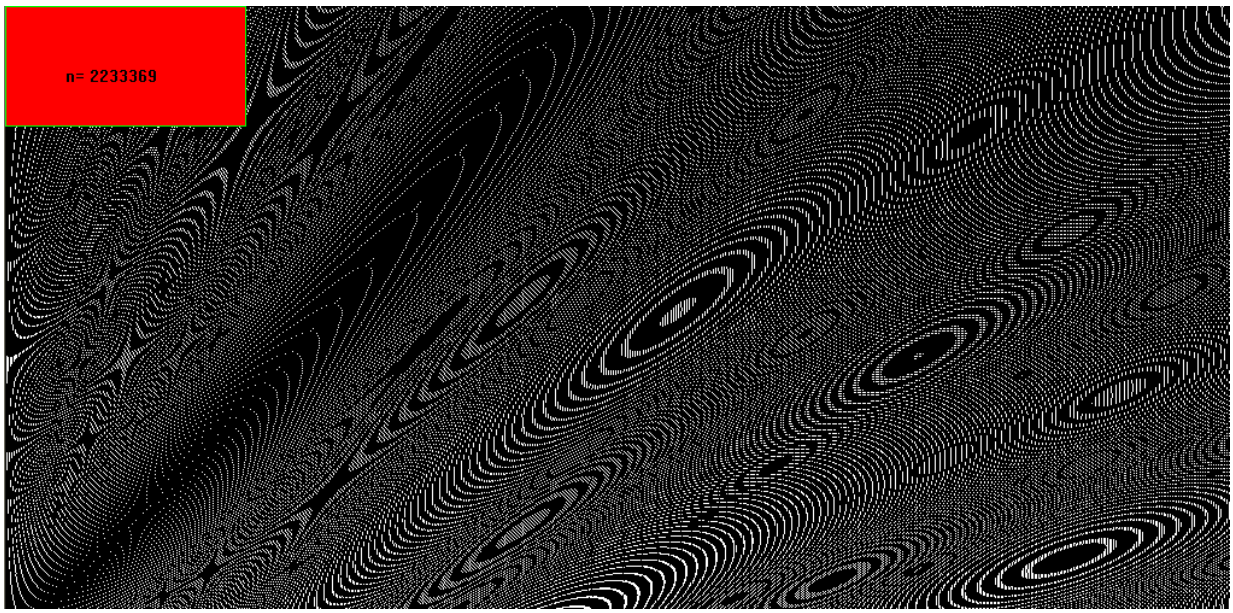

Рис. 5. Двухмерный портрет числа 2233369, полученный из остатков этого числа от деления на проверяемые сомножители, полученные в разных системах счисления

Запасать в прок свои вычислительные ресурсы выгодно в силу того, что «полезный майнер» получает право потратить их на решение его личной сложной задачи. Если личная задача «полезного майнера» легко распараллеливается, то у эмитента криптофлопов проблем не возникает. Он дробит личную задачу одного «полезного майнера» на множество фрагментов и раздает эти фрагменты другим «полезным майнерам». Однако личная задача «полезного майнера» может оказаться сильно связанной, задача ее распараллеливания может оказаться очень сложной сама по себе.

Для того, что бы гарантированно принять (ликвидировать), выпущенные ранее криптофлопы эмитент должен иметь собственные вычислительные ресурсы, способные вернуть «полезным майнерам» их ранее законсервированные ресурсы при решении их личных задач, не поддающихся распараллеливанию.

На данный момент РЫНКА решения сложных личных задач пока нет. Видимо, он будет сформирован в будущем. В приведенной ниже таблице, даны оценки затрат в рублях на затраты электроэнергии при решении ряда сложных в вычислительном отношении задач. «Полезный майнер» нарабатывал криптофлопы на своем компьютере и, соответственно, он не должен тратить свои ресурсы на «железо». При утилизации криптофлопов для их владельца важен срок утилизации. Например, в первой строке таблицы рассматривается задача прогнозирования взаимного совместного поведения 30 пар валют на рынке операций FOREX. Пользователю, заказавшему такой прогноз интересен результат достоверный на время 1 часа, но полученный через 30 минут после запуска ВЫЧИСЛИТЕЛЬНОЙ ФАБРИКИ по утилизации криптофлопов.

Вторя строка таблицы отражает тестирование защищенных нейросетевых контейнеров. Эта задача уже не требует высокой скорости утилизации накопленных ранее криптофлопов. Для пользователя не имеет значения сутки или двое будет решаться его задача. Задачи нового рынка будут разнообразны, так в третьей строке таблицы даются оценки стоимости подбора забытых (утерянных) паролей от архиваторов. Актуальность решения таких задач будет расти по мере развития цифровой экономики. Потенциальная стоимость этого сегмента рынка огромна. Достаточно сказать, что 10% биткоинов утрачены по техническим причинам и в том числе из-за утерянных паролей доступа к криптокошелькам. Видимо, в будущем криптокошельки для хранения криптовалюты будут биометрическими, однако это ослабит проблему, но не снимает ее. Родственники, получившие наследство в форме криптокошелька с биткоинами (возможные реалии

цифровой экономики будущего), должны будут потратить часть наследства на открытие криптокошелька, если ЗАВЕЩАТЕЛЬ специально утаил часть цифр кода доступа [4].

Таблица

№ п/п	Содержание вычислительно сложной задачи	Необходимый ресурс в терафлопах в час и стоимость энергозатрат
1.	Прогноз соотношения пар валют на рынке FOREX, построенный с учетом совместного поведения 30 наиболее значимых валют в течении последнего года (30-ти мерный прогноз)	1000 Тф/ч, 26 тыс. руб.
2.	Полное тестирование собственного нейросетевого преобразователя биометрия-код, защищенного самошифрованием данных [4] Распаковка БиоЗащиты архива с биткоинами	10000 Тф/ч, 260 тыс. руб.
3.	Распаковка архива с утерянным (забытым) паролем:	
	• длинной 8 случайных символов	• 1 Тф/ч, 26 руб.
	• длинной 10 случайных символов	• 1000 Тф/ч, 26 тыс. руб.
	• длинной 12 случайных символов	• 1 000 000 Тф/ч, 26 млн руб.
4.	Превращение малых выборок в большие для обычного статистического прогнозирования 20 опытов в 200 опытов — 26 рублей 30 опытов в 600 опытов — 52 рубля	

Четвертая строка таблицы отражает сегмент перс перспективного рынка пересчета меленьких выборок в большие [6]. Увеличивать реальный объем тестовой выборки не всегда возможно технически или может оказаться слишком дорогим. Так фармакологическая компания, затратив миллиард на новое лекарство, для возврата вложений должная как можно быстрее выйти на рынок. При этом, необходимо проходить длительный этап тестирования нового лекарства. Если удастся сократить время тестирование в несколько раз, то фармакологическая компания быстрее выйдет на рынок и вернет затраченные средства.

ЗАКЛЮЧЕНИЕ

Майнинг и полный блокчен открытый реестр являются весьма и весьма энергозатраными и аппаратнозатраными технологиями. Гораздо менее энергозатраными и аппаратнозатратными являются технологии, построенные на выпуске криптомонет одним эмитентом, подкрепленных его капиталовложением в вычислительные ресурсы, ориентированные на решение полезных задач. Банк полезных, вычислительно емких задач пока не сформирован, однако они существуют и отражены в приведенной выше таблице. При этом выпускаемые эмитентом криптофлопы воспринимаются обычными пользователями как способ консервации их избыточных личных вычислительных ресурсов. Накапливание (консервирование) своих избыточных вычислительных ресурсов

выгодно пользователям и выгодно эмитенту криптофлопов, так как он привлекает для решения «полезных» задач избыточные вычислительные ресурсы обычных пользователей.

Литература:

1. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора. – М., 2011.

2. Ахметов, Б.С. Алгоритмы тестирования биометрико-нейросетевых механизмов защиты информации Казахстан / Б.С. Ахметов, В.И. Волчихин, А.И. Иванов, А.Ю. Малыгин. – Алматы : КазНТУ им. Сатпаева, 2013. – 152 с., ISBN 978-101-228-586-4, http://portal.kazntu.kz/files/publicate/2014-01-04-11940.pdf

3. Малыгин, А.Ю. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации / А.Ю. Малыгин, В.И. Волчихин, А.И. Иванов, В.А. Фунтиков. – Пенза: Издательство Пензенского государственного университета, 2016. – 161 с.

4. Иванов, А.И. Криптографическая валюта, пригодная для накапливания избыточных вычислительных ресурсов частными лицами / А.И. Иванов // Защита информации. INSAID. – 2014. – № 5. – С. 66-71.

5. Иванов, А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции / А.И. Иванов. – Пенза: Издательство АО «ПНИЭИ», 2016. – 133 с., http://пниэи.рф/activity/science/BOOK16.pdf.

6. Иванов, А.И. Простейшие оракулы, обученные корректировать ошибки вычисления младших статистических моментов на малых выборках биометрических данных / А.И. Иванов. – Пенза: Издательство АО «ПНИЭИ», 2018. – 34 с., http://пниэи.рф/activity/science/noc/BOOK18.pdf.