Департамент образования администрации г. Перми
МБОУ “Лицей №1” г. Перми

Направление:

Информатика**.**

***Тема работы*:**

Исследование атаки на сеть Биткойн и затрат на её проведение.

Выполнил:

Назаров Рустам Мухамадюсуфович, 213 группа.

Научный руководитель:

Батин Сергей Евгеньевич.

Пермь - 2018

Оглавление.

Введение.

Тема данной работы является актуальной, так как криптовалюта - будущее бумажных денег. Цифровые деньги продолжают увеличивать свой спрос каждый год, а курс Биткойна постоянно меняется. Заинтересованность СМИ и других ресурсов показывает, что за криптовалютой стоит будущее и оно уже ближе, чем кажется.

Сеть Биткойн построена на алгоритме, по которому для достижения заработка Вы должны решить задачу, обратную хешированию. Задача решается быстрее при больших количествах мощности сети, подконтрольной пользователю. Майнер, имеющий пятьдесят один процент от мощности всей сети Биткойн, получает возможность перевести себе все деньги, находящиеся в обороте.

Стоит рассмотреть это подробнее и узнать, находится ли сеть Биткойн в безопасности.

Цель:

Оценка средств на проведение атаки пятидесяти одного процента.

Задачи:

- ➔ Изучение теоретической части;
- ➔ Подсчёт нужных мощностей;
- ➔ Подсчёт предполагаемых размеров фермы;
- ➔ Построение вывода на основе проделанной работы.

Глава 1. Устройство криптовалюты.

§ 1. Криптовалюта.

Криптовалюта – это цифровые деньги, существующие в виртуальном мире, которые добываются на вычислительных устройствах.

Биткойн – это новое поколение децентрализованной цифровой валюты, созданной и работающей только в сети интернет. Эмиссия валюты происходит посредством работы миллионов компьютеров по всему миру с использованием программы для вычисления математических алгоритмов.

Биткойн имеет множество отличий от иных электронных денег. Он полностью децентрализован: центральный орган контроля не существует. Вы можете создавать бесконечное количество биткойн-адресов без привязки к имени, адресу или любой другой информации, однако вся история *транзакций*, переводов между счетами, открыта и находится в общем доступе.

Транзакции находятся в цепочке блоков, называемой *блокчейн*. Каждый блок в такой цепи имеет уникальный номер, дату создания, хранит в себе историю о транзакциях и ссылку на предыдущий блок, стоящий позади него.

Зная *биткойн-адрес*, Вы получаете возможность просмотреть все переводы, в которых участвовал этот адрес: суммы, на которые они были произведены, время и дату. Стоит отметить высокую скорость перевода между счетами и отсутствие комиссии за международный перевод. Транзакции, совершённые в сети, нельзя отменить, вернув себе деньги.

§2.Майнинг.

Майнинг – процесс добычи Биткойнов путём решения математической задачи. Задача, которую решают майнеры, владельцы майнинговых ферм, является обратной хешированию, шифрованию информации в интернете. Выгоднее всего для майнинга использовать специально собранные *Интегральные Схемы Специального Назначения* – ИССН (ASIC).

Алгоритм сети Биткойна создаёт некий интервал зашифрованных паролей, *хешей*. Фермы майнеров, используя свои мощности, начинают перебирать зашифрованные файлы с целью найти пароль – координаты следующего блока в цепи. Каждый раз, когда хеш переводится в пароль, он отправляется в сеть. Другие майнеры принимают его и выполняют простую работу – вычисляют пароль по полученному хешу. Когда большинство участников сети, а именно пятьдесят один процент, подтвердит, что пароль подходит, создаётся новый блок, за который майнеры и получают свои Биткойны.

Исходя из этого, можно сделать вывод, что чем больше участников сети, тем больше эта сеть защищена от атак на неё.

Глава 2. Создание фермы для атаки на сеть.

§1.Суть проблемы пятидесяти одного процента.

Как было сказано ранее, чтобы создать новый блок в цепи, надо найти пароль из заданного интервала. Для создания блока нужно подтверждение пятидесяти одного процента мощности всей сети. Возникает вопрос: возможно ли, владея половиной мощности всей сети в мире, совершить атаку на сеть, обманув её и забрав все деньги из оборота себе? Рассмотрим эту проблему внимательнее.

Теоретически, обладая большей частью мощности сети, появляется возможность осуществлять управление Биткойном. Пятьдесят один процент даёт нам возможность создавать новые блоки и собственноручно подтверждать их. В результате, вся сеть начнёт воспринимать этот блок как настоящий, дав нам права на следующее:

- Создание “выдуманных” транзакций внутри этого блока; (возможность переводить деньги со счетов пользователей без их участия).
- Трата одних и тех же монет несколько раз; (возможность приобретения товара с последующим переводом потраченных средств обратно на свой кошелёк).
- Препятствие иным майнерам находить правильные блоки; (не несёт собой цель обогащения, но такая возможность существует).

§2.Подсчёт затрат на атаку.

Для построения мы будем использовать специально созданные модели – ASIC, о которых говорилось ранее. Они обладают самым высоким коэффициентом полезности, который появляется делением суммы модели на её мощность, исчисляемую в хешах.

Необходимо учитывать, что, подключив нашу ферму к питанию, общая мощность сети Биткойн увеличится на мощность нашего сооружения. Таким образом, нужно брать не половину от мощности сети, а почти такое же число, чтобы наша доля от всей сети была минимум пятьдесят один процент.

Для начала необходимо подсчитать нужную нам вычислительную мощность фермы для совершения атаки.

$$N = A \times \frac{51}{49}, \quad (1)$$

где N – необходимый хешрейт для проведения атаки;
A – среднее значение хешрейта сети Биткойн за февраль.

Величина	Хешрейт, х/с
Сеть Биткойн	$20{,}1 \times 10^{18}$
Ферма для атаки	$20{,}9 \times 10^{18}$

Получив необходимый хешрейт, нам следует приступать к подсчётам нужного количества ASIC и их цены. Мною было изучено большое количество ASIC, но самым выгодным оказался Antminer V9. Именно его мы и будем рассматривать как основную модель в ферме.

Чтобы найти нужное количество ASIC, нужно воспользоваться формулой:

$$n = \frac{N}{X}, \quad (2)$$

где n – необходимое количество ASIC; N – необходимый хешрейт для проведения атаки; X – хешрейт одного ASIC.

Стоимость фермы, её объём, масса и общая мощность считаются по формулам:

$$s = d \times n; \quad (3)$$

$$V = v \times n; \quad (4)$$

$$M = m \times n; \quad (5)$$

$$W = w \times n; \quad (6)$$

где n – количество моделей ASIC; s – общая стоимость моделей ASIC; d – стоимость одной модели; V – общий объём фермы; v – объём одной модели; M – масса фермы; m – масса одной модели; W – общая мощность фермы; w – мощность одной модели.

Характеристики	Одна модель ASIC	Вся ферма
Хешрейт, х/с	4×10^{12}	$20{,}9 \times 10^{18}$
Количество, шт	1	5 225 000
Стоимость, $	291	1 520 475 000
Объём, $м^3$	0,005738565	29 984
Масса, кг	5	26 125 000
Мощность, Вт	1 027	$5\,366 \times 10^6$

Общая формула, подсчитывающая стоимость покупки такой фермы, будет выглядеть так:

$$S = \frac{A \times \frac{51}{49}}{X} \times d,$$

где S – общая стоимость полученной фермы; A – средний хешрейт сети; X – хешрейт модели, на которой будет построена ферма; d – цена за одну модель, на которой будет построена ферма.

Заключение:

Таким образом, атака пятидесяти одного процента на сеть Биткойн возможна, но она несла бы собой цель обогащения, только если бы её можно было бы провести незаметно.

Постройка такого большого сооружения и скупка такого количества аппаратуры не может остаться незамеченной. Даже если такую ферму удастся спрятать, после вывода Биткойнов с самого богатого кошелька, атака будет замечена и курс начнёт стремительно падать.

Даже если эта атака не принесёт злоумышленнику выгоды, Биткойн всё ещё уязвим к ней.

Источники:

1. Asic Bitcoin Mining Hardware From Bitmain [Электронный ресурс]. – Режим доступа: https://shop.bitmain.com/productDetail.htm?pid=00020180207154602023j1N1ga6y067C, свободный.
2. Bitstorm.ru – сайт о криптовалюте, заработке и биржах [Электронный ресурс]. – Режим доступа: http://bitstorm.ru/glossary/51-attack, свободный.
3. FB.ru [Электронный ресурс]. – Режим доступа: http://fb.ru/article/356137/chto-takoe-asiki-dlya-mayninga-opisanie-i-osobennosti, свободный.
4. Всё про инвестиции в криптовалюты – ICO, майнинг, кошельки, краны, биржи [Электронный ресурс]. – Режим доступа: https://cryptostate.ru/mayning/chto-eto-takoe, свободный.
5. Как заработать.ру – как заработать и начать свой бизнес [Электронный ресурс]. – Режим доступа: http://kakzarabativat.ru/finansy/chto-takoe-kriptovalyuta, свободный.
6. Накамото С. Биткойн. 2008. 9 с.
7. Нараянан. А. Биткойн и криптовалютные технологии. Редакция №1. 2015. 132 с.
8. Поппер Н. Цифровое золото. Диалектика. 2016. 350 с.
9. Решевский М. Золотая лихорадка XXI века. Мир ПК. 2011. 64 с.
10. Словари и энциклопедии на Академике [Электронный ресурс]. – Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/78851, свободный.
11. Теппер А. Биткойн – деньги для всех. 2015. 59 с.

Annotation.

This research work is devoted to the problem of fifty one percent attack on Bitcoin network. The main task is to find out the possibility of this attach and calculate the costs for it.

To do this work, it was necessary to calculating needed hashrate, the cost of the farm and the time needed for its creation.

It has become obvious that attack is possible, but it still unreasonably in terms of money.

This research work up-to-date because this problem can destroy the biggest digital currency network – Bitcoin.