Упрощенная проверка платежей

Верификация транзакций возможна без запуска полнофункционального узла. Пользователю необходимо лишь хранить заголовки блоков самой длинной цепочки, которую он получил от других узлов, и запрашивать хеш-поддерево для необходимой транзакции. Он не может проверить корректность транзакции самостоятельно, но, получив ссылку на блок, в котором она находится, он может убедиться в том, что этот блок и все последующие приняты и подтверждены сетью.

На такой метод проверки можно полагаться, пока сеть хотя бы наполовину находится под контролем честных участников, то есть пока злоумышленник не завладеет большими ресурсами. Обычные узлы могут проверять транзакции самостоятельно, но если нападающий генерирует самую длинную цепь блоков, то своими сфабрикованными транзакциями он может скомпрометировать упрощенную схему. Одной из стратегий противодействия этому может быть рассылка сигналов тревоги от обычных пиров, которые получают "ложный" блок. Такой сигнал будет заставлять программу-клиент загружать блок полностью, чтобы самостоятельно подтверждать некорректность данных.

Конфиденциальность технологии

Традиционная банковская модель поддерживает необходимый уровень конфиденциальности, предоставляя доступ к информации лишь сторонам-участницам и доверенному третьему лицу. Необходимость открытой публикации транзакций исключает такой подход, однако приватность по-прежнему можно сохранить, если публичные ключи анонимны. Открытой будет информация о том, что кто-то отправил кому-то некоторую сумму, но без привязки к конкретным личностям. Столько же данных раскрывается и на фондовых биржах, которые публикуют время и объем частных сделок, не указывая, между кем именно они были совершены.

Дополнительной защитой будет являться генерация новой пары "открытый/закрытый ключ" для каждой транзакции: это предотвратит связывание различных платежей с их общим отправителем или адресатом. Некоторого публичного связывания все же не избежать: транзакции с несколькими входами доказывают, что эти суммы принадлежат одному лицу. Риск состоит в том, что раскрытие личности владельца ключа может привести к раскрытию и всех принадлежащих ему транзакций.

Оценка вероятности "атаки 51%"

Рассмотрим сценарий, в котором злоумышленник пытается генерировать более длинную цепь блоков, чем честные участники. Даже если он преуспеет, это не приведет к тому, что можно будет создавать деньги из воздуха, присваивать себе чужие монеты или вносить иные произвольные изменения. Узлы никогда не примут некорректную транзакцию или блок, содержащий ее. Атакующий может лишь пытаться изменить одну из своих транзакций, чтобы возвратить отправленные деньги.

Гонку между честными участниками и нападающим можно представить как биномиальное случайное блуждание. Успешное событие, когда "хорошая" цепь удлиняется на один блок, приводит к увеличению отрыва на единицу, а неуспешное, когда очередной блок создает злоумышленник, – к его сокращению. Вероятность атакующего наверстать разницу в несколько блоков такая же, как и в задаче о "разорении игрока". Представим, что игрок имеет неограниченный кредит, начинает с некоторым дефицитом и у него есть бесконечно много попыток, чтобы отыграться. Вероятность того, что он преуспеет, как и вероятность злоумышленника догнать честных участников, вычисляется следующим образом:

p = вероятность появления блока в честной цепочке,

q = вероятность того, что блок создаст атакующий,

q_z = вероятность того, что атакующий наверстает разницу в z блоков.

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

В случае p > q вероятность уменьшается экспоненциально с ростом числа блоков, на которое отстает злоумышленник. Поскольку все ставки против него, без удачного рывка в начале его шансы на успех становятся ничтожно малы.

Рассмотрим теперь, как долго получателю платежа стоит ждать, прежде чем он будет полностью уверен, что бывший владелец не сможет отменить транзакцию. Предположим, что злоумышленник-отправитель позволяет адресату некоторое время верить, что платеж был проведен, после чего возвращает деньги себе. Получатель узнает об этом, но мошенник надеется, что будет уже слишком поздно.

Адресат создает новую пару ключей и сообщает свой публичный ключ отправителю прямо перед подписанием транзакции. Это не позволит отправителю заранее начать работать над цепочкой и провести транзакцию в тот момент, когда он будет достаточно удачлив, чтобы совершить рывок вперед. После отправки платежа мошенник начинает втайне работать над параллельной версией цепочки, содержащей альтернативную транзакцию.

Получатель ждет, пока транзакция не будет добавлена в блок и тот не будет продолжен еще z блоками. Ему неизвестен прогресс злоумышленника, но если средняя скорость генерации честных блоков известная величина, то число блоков атакующего подчиняется распределению Пуассона с математическим ожиданием:

$$\lambda = z\frac{q}{p}$$

Чтобы получить вероятность того, что атакующий обгонит честных участников, необходимо умножить значение случайной величины (число созданных им блоков) на вероятность того, что он сможет наверстать оставшуюся разницу:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Перегруппировав слагаемые и избавляясь от бесконечного ряда, получаем:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Таким образом, разработчики пришли к выводу, что вероятность экспоненциально падает с ростом z. В биткоин-кошельках это было реализовано в виде подтверждения транзакций.

Выводы

При успешной реализации "атаки 51%", если будет иметь место сговор пулов или использование квантовых компьютеров, злоумышленники не смогут получить прибыль, поскольку это подорвет доверие к сети и произойдет крах курса биткоина.

Для поддержания нормальной работы сети необходимо участие честных майнеров с соответствующими распределенными мощностями. Но компаниям, часто принимающим платежи, необходимо подключаться к сети в обычном режиме, а не по упрощенной схеме, для большей независимости, безопасности и быстроты проверки блоков.

Отдельно стоит отметить, что псевдоанонимность биткоина позволяет анализировать транзакции, кластеризовать адреса кошельков и, как следствие, идентифицировать личности злоумышленников в случае инцидентов.

Источники

1. https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf – вайтпейпер биткоина (официальный перевод сообщества).

2. Сейфедин Аммус. Краткая история денег, или Все, что нужно знать о биткоине. Перевод на русский язык, издание на русском языке, оформление. ООО "Манн, Иванов и Фербер", 2019.

Ваше мнение и вопросы присылайте по адресу is@groteck.ru