

Коин бит

Виртуальные деньги не прошли проверку реальностью

Сначала напомним, о чем идет речь. Биткоин (Bitcoin) - одновременно название виртуальной денежной системы и «монеты», имеющей хождение в этой системе. Эти электронные деньги, в отличие от большинства других, не являются «отражением» реальных общепризнанных денег. Это самостоятельные денежные единицы, которые можно добывать, хранить, передавать другим людям, использовать в расчетах.

Ключевое отличие биткоинов от других денег - отсутствие единого эмиссионного центра. Любой человек может произвести биткоины - по аналогии с тем, что любой человек может добыть золото. Добыча биткоинов происходит случайно, с помощью сложных бессмысленных математических вычислений на компьютерах пользователей. Чем выше вычислительная мощность компьютера (или пула компьютеров), тем выше вероятность появления на счете пользователя биткоинов. Да, и еще одна важная особенность: биткоины внутри системы абсолютно анонимны - как наличные деньги. Кошелек с монетами - это всего лишь набор файлов, никак не привязанный ни к пользователю, ни к компьютеру.

Естественно, на волне роста популярности системы вокруг биткоинов возникла целая инфраструктура. Вы можете купить «монеты» за обычные деньги у тех, кто занимается добычей, или продать, выведя полученные «настоящие» доллары или рубли в «реальный мир». Для этого энтузиастами созданы «обменники» и биржи. Вы можете безопасно проводить платежи с помощью специальных расчетных центров, придерживающих платеж у себя до момента исполнения услуги или поставки товара вашим контрагентом. Вы можете положить честно заработанные или купленные биткоины на счет в специальном онлайн-банке, если не доверяете собственному компьютеру.

Внешняя инфраструктура и «интерфейсы» взаимодействия принципиально виртуальной валюты с реальным миром - это прекрасно. Если бы не одно «но»: преимущества виртуальности разбиваются или даже превращаются в недостатки при контакте с реальными мошенниками и ворами.

Первое событие, которое основательно потрясло мир биткоин-фанатов, - недавняя кража кошелька одного из активных участников системы, накопившего виртуального

богатства на сумму в полмиллиона реальных долларов (около 25 тыс. биткоинов). Впрочем, сумма в долларах в данном случае понятие относительное - курс биткоинов очень волатилен, а рынок - мал, поэтому конвертация даже этого кошелька в реальные деньги могла бы заметно обвалить котировки. Но так или иначе громкая кража заставила пользователей задуматься о «преимуществах» анонимности монет и отсутствия единого центра, который мог бы вернуть украденные деньги. Система принципиально построена так, что даже отследив весь путь монет по кошелькам (а это возможно), заставить их владельцев вернуть ценности не получится.

Второй инцидент произошел буквально на днях. Кто-то взломал базу данных крупнейшей (и почти монопольной) биржи по обмену биткоинов на реальные деньги MtGox, получив доступ к информации о 61 тыс. пользователей. Возможно, столь массивный взлом был лишь прикрытием для другого - более важного действия: взломщик получил доступ к кошельку с очень большим количеством биткоинов (сотни тысяч монет, т. е. миллионы долларов). Этому ему показалось мало, и хакер провел классическую биржевую операцию: начал массивно продавать виртуальные монеты, обрушив их курс с 17,5 доллара до 0,01, после чего «перевернулся» и принялся покупать биткоины у паникующих пользователей. Вполне возможно, что продажа и вовсе шла в основном в пользу «своих» кошельков, т. е. злоумышленник почти ничего не потерял «в монетах», но получил много дополнительных монет «за копейки» во время скупки на волне паники. Наконец, в финале операции прошла сделка по переводу собранных на бирже 432 тыс. биткоинов на некий биткоин-счет.

Биржа закрылась для выяснения подробностей происшествия и построения защиты, вслед за ней закрылись и другие подобные площадки. По идее «виртуальной монеты», базирующейся, фактически, только на доверии пользователей к системе, нанесен мощный удар. Не смертельный - скорее всего, сообщество на этот раз оправится. Но еще несколько таких происшествий, и биткоин можно будет сдавать в архив.

Мне с самого начала идея биткоин-системы чем-то не нравилась. Поэтому я и не писал о ней, несмотря на периодические предложения и просьбы читателей, хотя отслеживаю ее деятельность как минимум несколько месяцев. Теперь смутное сомнение оформилось: виртуальная система, имеющая плотные связи с реальным миром, собрала в себе все недостатки, присущие виртуальности в реальности и реальности - в виртуальности. С одной стороны, полная анонимность и независимость от некоего центра - это замечательно (в виртуальном мире). Но с другой - эта же анонимность превращается в лучшую защиту злоумышленника (в реальном мире). Возможность связывать виртуальную валюту с реальными деньгами и деловыми отношениями - прекрасна и удобна (в реальном мире). Но становится огромной «дырой» для реальных мошенников, которые получают доступ к ценностям (в виртуальном мире).

Возможно, я повторю судьбу советского компьютерщика, который в 1989 году назвал Windows в своей книге «громоздкой и бесполезной надстройкой» над DOS и предостерег читателей от пользования ею. Тем не менее, рискну предположить, что Bitcoin, если и проживет какое-то продолжительное время, то останется игрушкой для компьютерных фриков, получающих удовлетворение от своей «независимости» от реального мира.

С другой стороны, сама идея «добываемых», а не эмитируемых Центробанком денег, безусловно, очень интересна. И со временем эта идея может приобрести намного более разумную и безопасную форму, чем её нынешнее воплощение. Посмотрим.