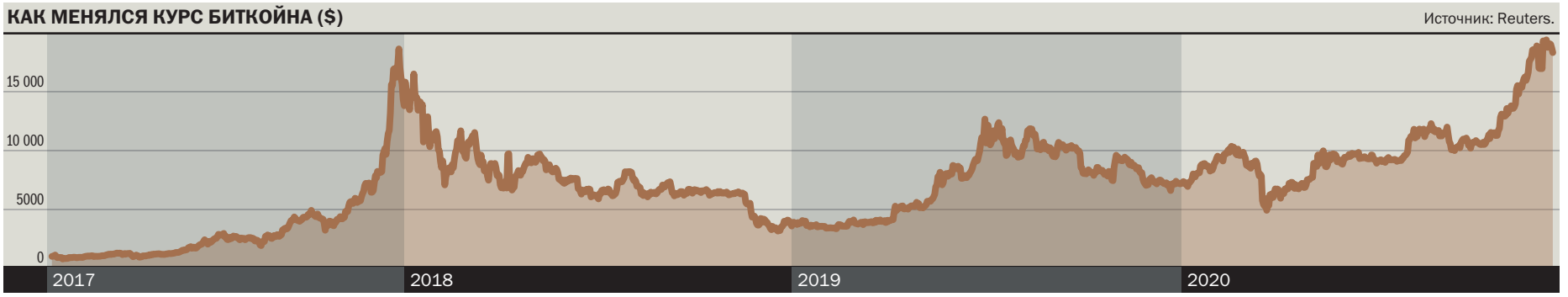

АХИЛЛЕСОВА ПЯТА БИТКОЙНА

МОЖНО ЛИ ПОДДЕЛАТЬ КРИПТОВАЛЮТУ

В биткойн никогда не инвестировал, считая его слишком рискованным активом. И дело здесь совсем не в резких скачках курса, методы алгоритмического трейдинга, которым я занимаюсь, как раз неплохо работают в отношении волатильных активов при наличии трендов в их динамике. Проблема в том, что у криптовалют есть риски совсем другого типа.

Первый, который лежит на поверхности,— этот рынок никем не регулируется и обладает малопонятной инфраструктурой. Условно говоря, если инвестиционная компания собрала средства на покупку акций, а потом присвоила деньги инвесторов, ничего не купив, или брокер не исполнил ваше поручение должным образом, то это повод взыскать ущерб по суду, более того — добиваться уголовного преследования виновных, поскольку речь идет о лицензируемой деятельности, жестко регламентированной законом. В случае с криптовалютами речь зачастую ни о чем таком не идет. Примерно то же самое относится к вопросам манипулирования рынком и организации инфраструктуры и надежности криптовалютных бирж в целом. Впрочем, это можно исправить, приняв соответствующее законодательство и установив единые правила игры. Многие страны пытаются идти по этому пути. Беда в том, что у биткойна есть еще одна черта, которую не исправить нормативными актами.

Что такое криптовалюта с математической точки зрения? Это некий набор цифр (вектор) в памяти вашего компьютера плюс некий алгоритм, позволяющий провести преобразование данного вектора в другой, конечный. Если некий конечный набор цифр удовлетворяет определенным, заранее известным условиям, тогда это и называется биткойном или единицей какой-либо еще криптовалюты. Алгоритм преобразования исходного вектора в конечный у биткойна является открытым — из-за этого и становится возможным производство, или, как говорят, майнинг, криптовалюты широким кругом желающих. С принципиальной точки зрения процесс прост: люди перебирают различные наборы цифр исходного вектора, проводят его преобразование в соответствии с алгоритмом, и, если конечный вектор соответствует заранее заданным условиям, вот оно, рождение биткойна, новый токен начинает жить в распределенной сети пользователей системы. А теперь зададимся вопросом: что будет, если удастся найти алгоритм преобразования, обратный тому, который делает из исходного вектора конечный, правильный? Тогда можно будет по конечному набору требуемых цифр, который, напомню, заранее известен, воспроизводить начальный. Иными словами, печатать новые биткойны или подделывать существующие с минимальными трудозатратами. Причем так, что подделка будет в принципе неотличима от оригинала — при условии, конечно, что оригинал свободно обращается в сети, а не состоит на каком-либо особом учете. Мечта фальшивомонетчика: бумажные деньги подделывать на много порядков сложнее. В таком виде система не сможет существовать — ее придется останавливать, менять алгоритм майнинга, менять все биткойны на новые, запускать заново. Что при этом произойдет с курсом, одному Богу ведомо, непонятно, сколько фальшивых биткойнов, неотличимых от настоящих, успеет оказаться на руках у добросовестных участников сделок.

Можно ли найти этот самый алгоритм обратного преобразования? Сначала чуть-чуть теории. Преобразование, которое используется в биткойне, в принципе является взаимно однозначным. А все взаимно однозначные преобразования обратимы. Другое дело, что в той алгебраической структуре, которая реализована в алгоритме майнинга биткойна, данное преобразование необратимо. Иными словами, вы не можете «вскрыть» систему, находясь в той же алгебраической структуре. Но это не значит, что нельзя решить задачу на другой «платформе» и там генерировать необходимые исходные векторы. При этом почему-то принято считать, что на практике это невозможно. В качестве доказательства обычно приводят невероятное количество вычислений, которые для этого потребуются. Отчасти это так: в лоб задача не решается, биткойн — 256-байтный вектор, искать обратное преобразование, условно говоря, перебором, имея только ключ прямого преобразования,— дело безнадежное. Хотя и существуют механизмы, позволяющие очень существенно ускорить такой поиск, но и они в настоящее время нереализуемы за разумное время.

Главное же в том, что подобного рода задачи — а речь, по сути, идет о поиске механизмов дешифрования — это задачи скорее из теоретической области. Вычислительные мощности здесь ни при чем, для решения подобных задач зачастую хватало листа бумаги с карандашом. После чего можно будет плодить биткойны на дешевом ноутбуке. Сколько времени занимает решение подобных задач, сказать сложно. Это вопрос творчества: открытия совершаются не каждый день. Могу привести пример знаменитой «Энигмы», вскрытой англичанами во время Второй мировой войны. Ее более совершенные «потомки», так называемые дисковые шифраторы, успешно использовались многими странами до конца 1960-х. Найти общее теоретическое решение, позволяющее их вскрывать, удалось, насколько я знаю, только в 1970-х. Чем больше операций с биткойнами вы проводите, тем больше накапливается статистики, которая может помочь при вскрытии системы: появляется возможность задействовать некоторые классы математических методов. Именно поэтому, видимо, американская АНБ рекомендует в коммерческих системах шифрования периодически, через определенное количество трансакций менять ключи этих систем. Причем менять значительно чаще, чем алгоритм майнинга биткойна работает на одном ключе.

Все сказанное, впрочем, вовсе не означает, что я в принципе не доверяю криптовалютам. Наоборот, я думаю, что именно за ними будущее. Но это будут криптовалюты с закрытым ключом и централизованным майнингом, сосредоточенным в руках центральных банков: электронные деньги, которые невозможно подделать, невозможно украсть, и главное — невозможно просто печатать. Некий аналог золота с его ограниченными ресурсами. Возникнет, по сути, новая финансовая система мира ●

ТЕКСТ **Александр Горчаков, руководитель направления алгоритмической торговли АО «Финам», кандидат физико-математических наук, лауреат Государственной премии СССР**

ФОТО **предоставлено АО «Финам»**