Криптовалюты и блокчейн: вопросов много больше, чем ответов

«Я не технический специалист, но начал погружаться в тематику и понял, что это очень надёжно, так как никто не может манипулировать данными», – из одного неназванного интервью.

Популярность биткойна, вызванная стремительным ростом его стоимости в 2017 году, с одной стороны повлекла за собой взрывной рост интереса не только к нему самому и другим криптовалютам, но и к сопутствующим технологиям (прежде всего – к блокчейну), что в целях общего повышения осведомлённости очень даже хорошо, а с другой – породила целый ряд мифов и заблуждений, которые, в свою очередь, создали плодотворную почву для различного рода мошенничества, мелкого и не очень.

Публикаций, новостей, обсуждений по теме КВ и БЧ (криптовалют и блокчейна) уже стало так много, что про них слышали даже и не особо интересующиеся, при этом такое постоянное нахождение на слуху у части аудитории может вызвать ощущение того, что общие основы они себе в целом представляют, а детали не так уж важны.

Однако известно, кто скрывается в деталях, да и мифы, если они не Древней Греции, вряд ли могут доставить хотя бы эстетическое удовольствие и несут в себе хоть какую-то ценность.

В статье рассмотрены некоторые основные вопросы, чаще всего возникающие по поводу биткойна и других криптовалют, а также связанных с ними технологий, таких как блокчейн, смарт-контракты, ICO. При этом, как честно и указано в названии статьи – вопросов много больше, чем ответов.

Вопрос №1 Можно ли заработать на самостоятельном майнинге криптовалют?

Сама логика платформы, на которой построен биткойн и его многочисленные аналоги, иногда называемые альткойнами, казалось бы, позволяет делать деньги из воздуха в процессе так называемого майнинга.

На самом деле майнинг изначально предполагает прежде всего деятельность по поддержанию работоспособности платформы, но за эту деятельность любой желающий (если ему повезёт и он обладает достаточными вычислительными ресурсами) может получить вознаграждение в виде биткойнов, эмитируемых примерно каждые 10 минут (это вообще единственный способ появления новых биткойнов, кстати).

Первоначально вознаграждение составляло 50 биткойнов, с ноября 2012 уже 25 биткойнов, а с июля 2016 только 12,5 биткойна. К слову, следующее уменьшение по прогнозу состоится примерно в середине 2020 года.

Технически упрощённо майнинг выглядит примерно так: все одновременно решают некоторую математическую задачу (получение красивого с математической точки зрения значения хэш-функции для очередного блока с транзакциями) и тот, кто решит её первым, получает вознаграждение.

Такая простая возможность заработка биткойнов сначала привлекала только энтузиастов, но в скором времени были вовлечены и более широкие слои населения: недавний бум «ферм для майнинга» трудно было не заметить. По мере роста числа «майнеров» зарабатывать таким образом становилось всё сложнее.

По мнению многих специалистов, сейчас стоит инвестировать в оборудование для майнинга только в расчёте на очень долгосрочную перспективу или при наличии возможности сразу привлечь существенные вычислительные ресурсы.

Для понимания того, что означает «существенные», можно привести как пример, что, согласно некоторым источникам, КНДР с 2017 года использует майнинг криптовалют для поддержки своей национальной валюты – северокорейской воны.

Другой пример – российский холдинг RMC интернет-омбудсмена Дмитрия Мариничева в ходе первичного размещения монет (ICO) на постройку майнинговой фермы мощностью 20 мегаватт в районе с излишками электроэнергии собрал сумму, эквивалентную 43,2 миллиона долларов (изначально планировалось привлечь 100 миллионов долларов).

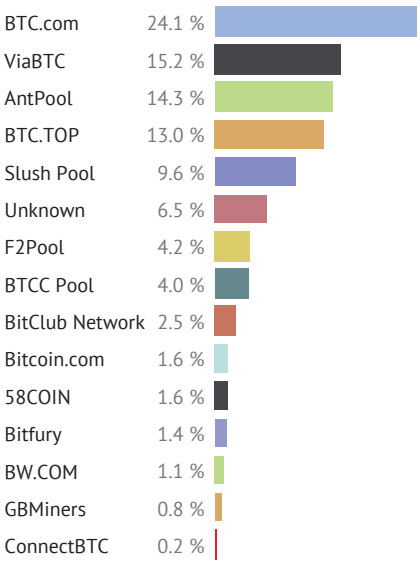
Алексей Колесник, ранее руководивший комитетом природных ресурсов в Минприроды Татарстана, а в конце декабря 2017 года возглавивший ООО «Губахинская энергетическая компания» (ГЭК, в которую входят Кизеловская ГРЭС в Пермском крае мощностью 23,6 МВт и Сарапульская ТЭЦ в Удмуртии мощностью 10 МВт), подтвердил изданию «Коммерсантъ», что рассматривает вариант с майнингом криптовалюты на площадке в Удмуртии.

Думаю, масштабы, при которых сегодня индивидуальный (самостоятельный) майнинг является инвестиционно привлекательным, примерно понятны.

Вопрос №2 Можно ли заработать майнинге криптовалют через пулы?

Решаемая в процессе майнинга математическая задача легко поддаётся распараллеливанию, поэтому отлично зарекомендовали себя так называемые пулы – объединения пользователей, предоставляющих свои вычислительные ресурсы. Пул, действуя как один майнер, получает достаточную производительность для более эффективной работы и существенно увеличивает свои шансы на решение очередной задачи первым.

Крупнейшие пулы и их приблизительные оценки мощности представлены на рисунке ниже.



Так как заработанные пулом биткойны распределяются между всеми его участниками (конкретные схемы распределения могут быть различными), то даже при частом успешном майнинге пула отдельному его участнику достаётся не такая уж крупная сумма. Понятно, что верно и обратное – у пулов с небольшим числом участников доля каждого частника больше, но и шансов на получение биткойнов в ходе майнинга существенно меньше. Не стоит забывать и про комиссию, которую берёт себе пул.

Кроме того, появление в цепочке дополнительно звена в виде пула создаёт дополнительные риски. Например, 6 декабря 2017 года один из

популярных пулов NiceHash подвергся взлому, в результате которого было похищено 4700 биткойнов (64 млн долларов по курсу на тот момент). Справедливости ради стоит сказать, что в конце января NiceHash обязался компенсировать потери всем своим пострадавшим пользователям, правда частями на протяжении нескольких месяцев и, как мы все понимаем, без учёта колебаний курса биткойна к доллару.

Вопрос №3
Можно ли заработать на торговле криптовалютой?

Впрочем, майнинг давно уже не единственный способ для заработка на криптовалютах. Красивые графики динамики роста курса того же биткойна привлекают многих – и профессиональных спекулянтов, и рядовых пользователей.

Вот, например, как выглядел график курса биткойна с января 2017 по январь 2018 (рис 1).

Фантастические проценты годовых вполне могут заглушить даже самый громкий голос разума – и вот уже открыто несколько страниц, найденных через поисковики, с пошаговыми инструкциями о том, как максимально просто и выгодно приобрести немного криптохайпа.

Миллиардер Уоррен Баффетт (инвестор с мировым именем) не так давно в интервью телеканалу CNBC заявил, что не будет инвестировать в криптовалюты: «Я могу почти с уверенностью сказать, что они плохо кончат. Когда это случится или как именно — я не знаю».

Генеральный директор банка JPMorgan Chase Джейми Даймон, в сентябре назвавший биткойн мошенничеством (он сравнил его с тюльпанной лихорадкой в Голландии и предупредил, что если кто-либо из трейдеров JPMorgan решит заняться криптовалютами, то будет уволен за «глупость»), позже заявил, что сожалеет о своих словах о биткойне, но криптовалюта ему по-прежнему неинтересна. Он отметил, что сейчас многие относятся к биткойну «как к чему-то весьма значимому», но у него самого другое мнение.

Заработать на торговле биткойном, несомненно, можно – как и на любой торговле на бирже. Но ровно также можно и потерять свои сбережения. Пожалуй, если учесть сложности с конвертированием криптовалюты в реальные деньги, риски потери денег из-за несовершенства системы в целом (см. следующие вопросы), а также слабое регулирование этой сферы (проблемы «обманутых криптодольщиков» никто точно за них решать не будет), то вполне разумной альтернативой приобретению криптовалюты с целью заработка будет приобретение лотерейного билетика.

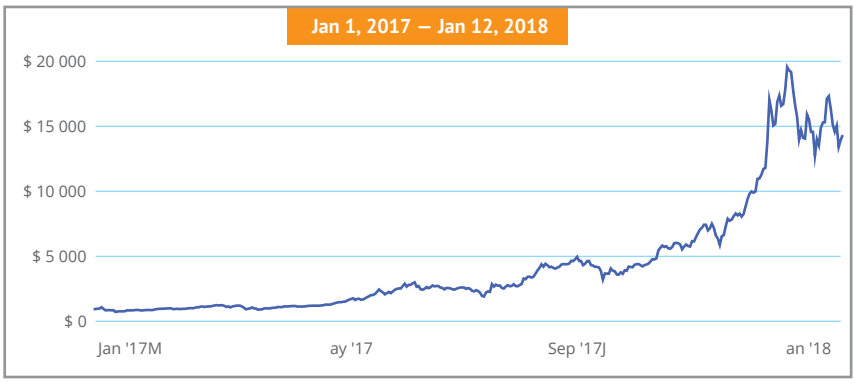


Рисунок 1

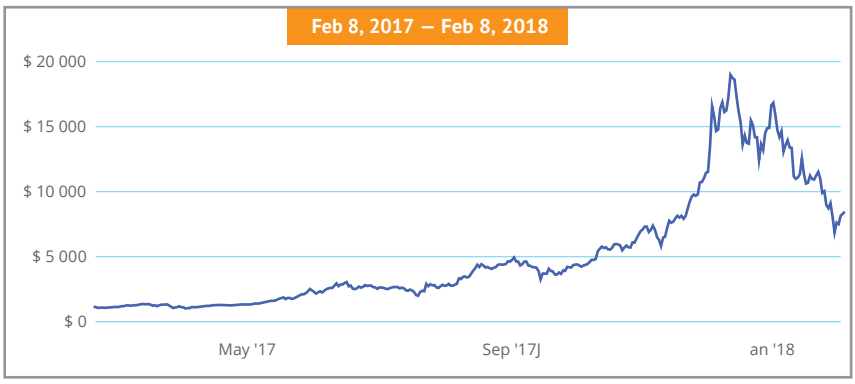


Рисунок 2

Для иллюстрации – вот тот же график курса биткойна, только уже с февраля 2017 по февраль 2018 (рис 2).

Далеко не так привлекательно выглядит. Впрочем, красивое слово волатильность (финансовый показатель, характеризующий изменчивость цены) для кого-то как раз лакмусовая бумажка, показывающая, что при таких резких скачках можно сделать отличные деньги (за счёт тех, кому это слово, например, кажется не красивым, а непонятным).

Вопрос №4
Являются ли криптовалютные технологии безопасными?

Приставка «крипто» легко может ввести в заблуждение. Однако криптография – это лишь часть системы и, пока квантовые компьютеры окончательно не изменили установившийся порядок вещей, – самая, пожалуй, надёжная её часть.

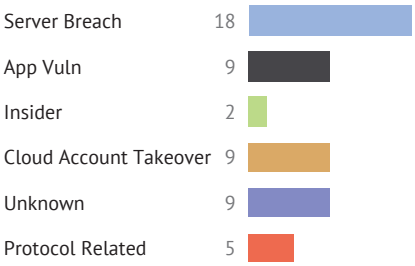
Лежащие в основе большинства криптовалют алгоритмы вычисления электронной подписи на базе асимметричной криптографии и последовательного хэширования сами по себе вполне надёжны, широко применяются (не только на рынке криптовалют) и при необходимости могут быть заменены на аналоги, более стойкие, чем текущие.

Вместе с тем, по некоторым оценкам, менее чем за 10 лет хакерами было похищено только биткойнов и эфира на сумму порядка 1,2 миллиарда долларов.

Компрометация закрытых ключей пользователей (читай – их криптокошельков), взлом криптовалютных бирж, майнинговых пулов – далеко не полный перечень возможных инцидентов. Какие бы надёжные алгоритмы и протоколы ни лежали в основе самой криптовалюты, всё равно неизбежно остаются уязвимости в их практической реализации и в обслуживающих сервисах.

На GitHub есть отдельный репозиторий «Кладбище блокчейна» (Blockchain Graveyard), где собирается информация о различных публичных инцидентах, связанных с

криптовалютами и блокчейном. На момент подготовки статьи был описан 51 такой инцидент. Ниже на диаграмме представлена статистика по причинам инцидентов: взлом сервера, уязвимость приложения, действия инсайдера, кража «облачной» учётной записи, неизвестные причины и причины, связанные с применяемыми протоколами.



Не стоит забывать и про человеческий фактор: фишинговые атаки, ненадёжные пароли, социальная инженерия – всё это повсеместно используется в более традиционном финансовом секторе, где отпор злоумышленникам могут дать те же банки. В мире криптовалют, как уже отмечалось выше, в этом смысле царит первобытная анархия – каждый сам за себя. Думаю, никто не назовёт ущерб, который понесли рядовые пользователи по своей собственной вине, потеряв тем или иным способом доступ к своему криптокошельку.

Наконец, несмотря на общую устойчивость и крайне высокую степень продуманности общей архитектуры (что, к слову, вполне может навести на мысли о причастности к процессу спецслужб), существуют потенциальные возможности для компрометации и основополагающих идей того же биткойна.

Так, в докладе исследователей Института инженеров электротехники и электроники (IEEE – Institute of Electrical and Electronics Engineers) отмечается, что существует возможность использовать одни и те же биткойны дважды, применив так называемую атаку баланса, когда злоумышленники задерживают сетевые коммуникации между группами майнеров, чьи компьютеры проверяют транзакции в цепи, добиваясь тем самым при достаточной длительности такой задержки возможности получить два одновременных подтверждения от двух разных получателей их биткойнов и успеть, например, обменять их на реальные доллары.

Понятно, что в любом случае, как и при так называемой атаке 51% (когда кто-то владеет более чем половиной мощности и может создавать две параллельные цепочки транзакций), злоумышленники могут лишь дважды потратить свои собственные биткойны («двойное расходование»), да и технически такая атака пока выглядит сложно реализуемой на практике, но исследования продолжаются и пока нет гарантий, что не будет найден более простой и менее затратный способ.

Вопрос №5
Является ли криптовалюта анонимным средством платежа?

Пожалуй, это один из самых простых вопросов, на который действительно можно дать однозначный ответ: система анонимна, ровно пока пользователь соблюдает свою анонимность.

Согласитесь, трудно считать систему, в которой все транзакции записываются, доступны абсолютно всем и хранятся вечно, полностью анонимной. Строго говоря, вся анонимность держится на том, что никто не знает, кому какой кошелёк принадлежит, но все история операций открыта и прозрачна. Как только пользователь регистрируется на бирже для, например, перевода криптовалюты в реальные деньги, становится участником майнинг пула, указывая свои регистрационные данные, или любым другим способом даёт возможность связать с собой (например, со своим IP-адресом ил адресом электронной почты) какой-либо кошелёк, в тот же момент все его предыдущие транзакции перестанут быть анонимными.

Вопрос №6
Каков правовой статус криптовалют в России?

Завершить статью логично ответом на вопрос о правовом статусе криптовалют в нашей стране. На сегодняшний день такой статус не определён.

Однако на общественном совете при Минфине РФ 28 декабря был представлен законопроект о регулировании цифровых активов в Российской Федерации. В законопроекте даются определения криптовалюте, майнингу и ICO (процедуре первичного размещения токенов). Финальный вариант законопроекта о регулировании криптовалют в РФ, согласно поручению президента Владимира Путина, должен быть подготовлен в первом полугодии 2018 года.

При этом, как сообщил замминистра финансов Алексей Моисеев, Минфин намерен в феврале внести в Госдуму законопроект о криптовалютах (на момент подготовки статьи этого ещё не произошло). В рамках доработки законопроекта в частности предполагается определить перечень площадок, на которых можно будет совершать сделки с криптовалютами.

А пока Минтруд официально разрешил госслужащим не декларировать сведения о наличии виртуальных валют, как сообщило РИА Новости со ссылкой на заявление ведомства: «Формой справки не предусмотрено указание товаров, услуг, полученных в натуральной форме, а также виртуальных валют».

Пока же с юридической точки зрения согласно сттатье 27 Федерального закона от 10 июля 2002 г. №86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и статье 75 Конституции РФ официальной денежной единицей в стране является рубль, а введение других денежных единиц и выпуск денежных суррогатов запрещено, что не позволяет рассматривать никакую криптовалюту как легальное денежное средство.

Официальные позиции по этому вопросу сформулировали ФНС России в письме от 3 октября 2016 г. № ОА-18-17/1027 и Банк России в релизе «Об использовании частных „ виртуальных валют “ (криптовалют)». И налоговики, и банкиры отметили риски выпуска и обращения криптовалют, а ФНС России в своем письме отдельно напомнила о запрете выпуска денежных суррогатов.

Заключение

За рамками статьи остались такие интересные вопросы, как: заменят ли со временем криптовалюты фиатные деньги, действительно ли биткойн является проектом спецслужб, и, пожалуй, ещё два десятка других. На часть из них ответит время, а какие-то, очевидно, так и останутся без ответа – ровно как и те вопросы, что были рассмотрены в данной статье.

Алексей Комаров
автор блога по информационной безопасности www.zlonov.ru