



# ЭРА КРИПТОВАЛЮТЫ

АЛЕКС ПОЛАНСКИ

## Аннотация

*После случившегося бума на рынке валют в 2018 году слова «криптовалюта», «биткоин», «блокчейн» стали все чаще мелькать в СМИ, новостях и в обычных разговорах людей и бизнесменов.*

*Книга, которую вы держите в руках, простым и понятным языком расскажет:*

- что же такое криптовалюта и зачем она нужна;*
- почему биткоин именуют «электронной наличностью»;*
- как различать такие виды деятельности, как майнинг, форжинг или ICO.*

*Также благодаря книге Алекса Полански вы не только поймете суть современных криптовалютных операций, но и сможете применить эти знания в жизни, начав зарабатывать большие деньги, – технология блокчейн имеет просто огромный потенциал и самые разнообразные сферы применения.*

## Предисловие

Почему я решил осветить тему криптовалют и технологии блокчейн? От друга и партнера поступило предложение поделиться моим опытом участия в этой истории, подключился литературный агент, крупное издательство проявило интерес, и я решил: а почему бы и нет? Я абсолютно не против передать накопленный мною опыт, да и сама технология блокчейн очень занимательна и может многим показаться полезной и многообещающей. Я подумал, что, возможно, заинтересую читателей этим явлением, объясню азы и кому-то даже помогу заработать. Если данная технология все-таки получит взрывной эффект, то тогда она охватит существенную часть нашей жизни – намного бОльшую, чем сейчас. Я верю в то, что она имеет право на существование, может широко распространиться и что у нее огромный потенциал и разнообразные сферы применения. Я надеюсь передать всем частичку своей веры и авторского понимания происходящего глобального процесса, пусть немного упрощенного и, возможно, с нестандартным и даже слегка искаженным видением.

Я получил экономическое образование, но моей страстью всегда были информационные технологии, и, естественно, я не смог пройти мимо криптовалют, как отличного образца IT и финтеха. Я увидел огромные перспективы в криптовалютах и блокчейн-технологиях, начал изучать суть происходящего более углубленно и убедился в том, что не ошибся и это действительно интересно. Благодаря моей маме я с детства увлекаюсь компьютерами, и меня всегда мучил вопрос: почему же их вычислительная мощь простаивает зря? То есть я пользуюсь компьютером максимум два-три часа в день, а все остальное время он стоит в пыли, хотя мог бы проделывать какую-либо полезную вычислительную работу. И технология блокчейн дала мне возможность заставить компьютеры работать круглосуточно, принося пользу не только мне, но и сообществу пользователей криптовалют, а возможно, и обществу в целом. Это лишь маленькая часть того, что несут нам новые технологии, основанные на Blockchain.

Если взглянуть на ряд изученных мною книг о блокчейне и криптовалютах, объемных, сложных и вдумчивых, то даже человеку, знакомому с тематикой блокчейн, будет совсем не просто их понять, а значит, и применить полученные знания на практике. Даже у меня, немного подготовленного читателя, было устойчивое желание бросить чтение некоторых из них после нескольких страниц, потому как приходилось разбираться с большим количеством новых терминов или перепроверять уже усвоенные мною знания на предмет их соответствия описанному автором материалу. Такие книги можно будет воспринять, только прочитав массу статей в Википедии, посетив личные блоги криптоэнтузиастов, ветки профильных форумов и множественные сайты соответствующей тематики, дабы полностью погрузиться в тему... И в конце концов понять, что ничего толком не прояснилось. Именно поэтому я попытаюсь дать читателю упрощенное представление о криптовалюте и помочь в последующем практическом

применении без излишних подробностей. Конечно, без пары десятков новых терминов нам не обойтись, но я очень постараюсь вводить их постепенно и по возможности с примерами. Ведь конечная цель любого знания – сделать так, чтобы как можно больше людей с ним ознакомились, усвоили базовые принципы и начали самостоятельно применять в повседневной жизни. Только с приходом широких масс новых пользователей в блокчейн-экономику вырастет так называемый «сетевой эффект», и мы получим как раз то, о чем мечтали ее создатели и первопроходцы, – простую и понятную всем систему взаимных расчетов, где люди смогут на достаточно честных условиях генерировать собственную цифровую валюту для себя или выпускать ее для других, принимать коллективные решения и проводить голосования, зарабатывать на курсах тех или иных активов, обменивать и дарить, привлекать инвестиции и т. д. Необходимо расширить круг тех, кто поймет, примет и в идеале начнет использовать технологию блокчейн и криптовалюту не только для повседневных нужд, но и для изобретения чего-то нового. Даже среди моих друзей-программистов или специалистов в области информационных технологий все мельком слышали о биткоине и других монетах, причем многие достаточно давно, но единицы знали о том, как работать с криптовалютами и какие перспективы они несут. Сейчас же у большинства много теоретических идей, например, как запустить проект на основе криптовалюты и заработать на этом миллионы долларов, а также идей практических свершений по формированию небольшого собственного портфеля криптовалют. Сегодня существенная часть активного населения России увидела будущие перспективы технологии блокчейн и даже начала использовать криптовалюты для заработка или просто накопления. И это может сделать любой из нас! Любой человек способен придумать полезный проект и привлечь в него инвестиции, банально отложить несколько монет «на черный день» или вклиниться в разнообразную систему сопутствующих сервисов. А для меня станет вознаграждением, если несколько тысяч моих читателей смогут поделиться знанием с тысячами других потенциальных единомышленников из своего круга общения, расширив сообщество криптоэнтузиастов и тем самым дав им возможность реализовать свои идеи и проекты или просто быть в курсе современных технологий.

В первых главах книги я хотел осветить научную подоснову технологии, начав с криптографии и программирования, но понял, что могу отпугнуть большинство читателей, для кого имеет значение общее понимание идеи, а не конкретные точные знания. Чтобы стать настоящим профессионалом, придется углубиться в специальные науки, покорпеть над энциклопедиями, словарями, видеоархивами и специализированными ресурсами в сети Интернет, возможно, даже пройти обучение. Я же хочу избежать этого, донести до читателей суть этой технологии наиболее простыми словами, не с технической стороны, а с концептуальной, и привнести в эту историю социальный и даже немного философский аспект. Ведь для пользования телефоном вам необязательно знать его полное устройство. Чтобы искать информацию в Интернете, не требуется знаний языков программирования. Чтобы управлять автомобилем, не нужно уметь чинить все его узлы и агрегаты. Так же и в сфере криптовалют и блокчейна – достаточно общего понимания принципов и наличия ряда практических навыков именно по применению результатов и достижений научного прогресса, чтобы технология начала работать на вас.

Эта книга поможет вам разобраться в том, как появилась криптовалюта и сколько же монет существует, что такое майнинг и ICO (ай-си-о), как это использовать и применять в повседневной жизни, как это может помочь заработать и реализовать свои идеи. Немного места будет отдано прошлому, немного будущему... Я докажу, что любой человек или сообщество может создать собственную криптовалюту или собрать вычислительный модуль – майнер, провести краудфандинговую кампанию для привлечения инвестиций и сделать ряд простейших операций на криптовалютной бирже. Может быть, у одного читателя откроется талант трейдера, второй придумает собственную монету, третий заработает на своих публикациях, а четвертый скачает на телефон кошелек и просто подарит приятелю один Bitcoin на день рождения. Возможности настолько огромны и разнообразны, что каждый

сможет реализоваться в данной сфере и найти достойное применение своим силам и идеям.

К криптовалютам и технологии блокчейн проявляют интерес такие гиганты информационных технологий, как Microsoft и Google, IBM и Oracle, крупные финансовые институты приобретают криптовалютные биржи и многообещающие блокчейн-проекты, а производители чипов для видеокарт AMD и Nvidia один за другим стараются улучшить вычислительные способности своих устройств именно под индустрию блокчейн. Уже заявлено о внедрении блокчейн в сферы медицины, транспорта, обучения, государственного управления, бизнес-менеджмента, юриспруденции, бухгалтерии, страхования и в прочие отрасли экономики и народного хозяйства. Научные круги не меньше вовлечены в исследование технологии и разработку будущих сфер применения. Такой несправедливый интерес может вылиться во что-то намного большее, чем мы видим сегодня, и я хочу поделиться этой информацией со всеми.

Как бы все радужно и вдохновенно ни звучало, в любой затее существует риск. Традиционно все новые проекты – стартапы – в области блокчейн описывают эти риски одинаково, и самым элементарным риском будет ситуация, когда курс монеты или всего рынка обрушится. Как это не раз происходило в истории биткоина и повторилось в начале 2018 года, в период работы над этой книгой. Централизованная биржа, на которой обращаются валюты, также может обанкротиться, или же группа ее создателей попросту сбежит с деньгами. Например, биржа работала, оказывала услуги, стабильно зарабатывала и вдруг решила, что для безбедного существования достаточно того, что уже есть на счетах пользователей. Владельцы забрали деньги, а в краже обвинили хакеров. Кстати, из-за активности хакеров в этой сфере также существует повышенный риск утраты ваших личных данных, в особенности паролей от электронной почты, к которой привязан аккаунт в криптовалютном проекте или аккаунт самого криптовалютного кошелька, а как итог – исчезновение всех ваших монет. Если вы собираетесь играть на бирже, особенно с кредитным плечом, есть большой риск поставить не на тот актив, который внезапно за день потеряет 100, 200 или даже 300 процентов от стоимости, на которой вы вошли в сделку. Вы считали, что эта монетка сейчас подорожает, но она провалилась. Резкие, глубокие скачки курсов криптовалют принесли немало проблем и состоянию моей нервной системы. Есть риски глобальные, например отключение Интернета и электричества, но тогда многое в жизни будет бессмысленно. Существует юридический риск, что государство примет закон, излишне регулирующий криптовалюту, как это было при первых попытках законодательства в России. Если сейчас посмотреть историю заявлений российских чиновников о том, что такое криптовалюта и как с этим жить, то изначально к новшеству относились очень негативно, предлагали жестко контролировать или даже пресекать любое использование криптовалюты. Со временем отношение улучшилось, законодатели решили, что все же это инновации, а не средство для противозаконной активности. Грядущая весна 2019 года должна стать той вехой, когда появится ряд новых законов и будут внесены поправки в существующие, что позволит индустрии существовать в правовом поле и развиваться без оглядки на возможные негативные последствия. Существуют риски конкуренции со стороны других прогрессивных финансовых технологий, риски сговора влиятельных частных и правительственных структур, риски некомпетентности основателей проектов, которая приведет к массовому неисполнению обязательств. Несмотря на все это, в Америке, Азии и Европе запускают новые биржи, внедряют торговлю фьючерсами, Япония и Корея частично легализуют криптовалюту. Европа выбрала политику невмешательства, а в соседней Белоруссии Александр Лукашенко издал декрет, в котором легализовал криптовалюты и освободил их от налогов до 2023 года. На всем этом фоне хочется лишь вспомнить крылатую фразу: «Кто не рискует – тот не пьет шампанское!» и приступить непосредственно к решению нашей прямой задачи – знакомству с миром криптовалют и технологии блокчейн.

## **Глава 1**

### **Введение в криптовалюту**

## Что такое криптовалюта

Криптовалюта – это совершенно новый вид цифровых денег: электронная наличность. Интернет, цифровые и печатные издания изобилуют пространными объяснениями, но мы помним свою задачу – быть проще. Почему фигурируют слова «цифровые» или «электронные» – не требует объяснения, но почему наличность, если это нельзя пощупать и потрогать? Ведь криптовалюты существуют только в цифровом виде, лишь как запись в распределенной по разным хранилищам информации (децентрализованной) базе данных? Ответ на этот вопрос тоже прост. Наличность в идеальных условиях позволяет вам анонимно осуществлять прямую сделку с кем бы то ни было без посредников и контроля, что невозможно при безналичной форме платежа или использовании существующих форм электронных денег. Когда вы приобретаете не требующий какого-то дополнительного оформления товар, не машину или квартиру, а телевизор или ноутбук у частного лица, вы отдаете ему причитающуюся сумму наличностью, порой не зная ни имени, ни других идентифицирующих данных. Вам они не нужны, как и не нужен посредник, который возьмет деньги из ваших рук и тут же при вас отдаст сумму второй стороне сделки, причем за дополнительную комиссию, еще и сфотографирует ваши паспорта – на всякий случай. Первая из появившихся криптовалют – биткоин – как раз избавляет нас от необходимости привлекать какого-то доверенного посредника для проведения платежа. Сделки проходят напрямую, достаточно быстро, анонимно, с минимальными затратами на транзакцию. Эти сходства с наличными деньгами и позволили включить в описание термина слово «наличность». В целом читателю уже должно быть понятно, почему мы говорим «криптовалюта», за исключением составляющей «крипто» в структуре слова. Греческое слово *κρυπτός* означает тайный, скрытый. Я бы предпочел вариант «зашифрованный» и уточнил, что безопасность системы обеспечена применением надежных алгоритмов шифрования – криптографией. Если читателю необходимы точные детали – лучшим решением будет прочесть перевод «White Paper» создателя биткоина Сатоши Накамото, где сам создатель объясняет, что такое биткоин, для чего он и как функционирует.

Криптовалюта – это платежное средство, которое при этом не обладает полным набором функций денег, если верить Карлу Марксу, поведавшему нам пять этих важных функций в незабвенном «Капитале». Так же твердят высококвалифицированные экономисты, но я вижу, что ситуация стремительно изменилась за считанные пару лет. Для большой группы товаров, особенно цифровых и... товаров, обращающихся на черном рынке, биткоин является мерой стоимости. Стоимость этих товаров уже не выражают ни в долларах, ни в евро, ни в иной фиатной валюте, а только исключительно в биткоинах или еще двух-трех устойчивых криптовалютах. Обращение криптовалют набирает огромные обороты, Интернет содержит массу упоминаний о продаже недвижимости, автомобилей, в конце концов компьютерного оборудования за ту или иную криптовалюту, минуя обмен на фиат. Крупные торговые площадки, такие как eBay и Amazon, принимают оплату в биткоинах. И я сам имел личный опыт приобретения вычислительного оборудования за рубежом за криптовалюту, а также продления регистрации домена при помощи криптовалюты в России. Большинство специалистов, подвизавшихся на поприще технологий блокчейн, выражают стоимость своих услуг в биткоинах или иных популярных криптовалютах. А раз уже есть первые две функции денег, поспекает и третья. Ряд крупных криптовалютных бирж кредитует пользователей в криптовалюте через внутреннюю систему кредитования, есть и монеты, предлагающие учет обязательств в биткоине, Эфире, Риппл и многих других. В последние годы выросло число p2p сервисов кредитования в биткоинах или, наоборот, в фиатах, под залог криптоактивов. Криптовалюта стала средством платежа. Я имел честь общаться с криптоэнтузиастом из США, который часть пенсионных накоплений вложил в биткоины (при его цене на момент покупки около 600 долларов США) и агитировал многих других это сделать. Многие из тех, кто добыл биткоины в эпоху низкой стоимости и сложности добычи, хранят их по сей день – то есть

имеем криптовалюту, как средство накопления. Осталось только выйти на мировую арену и стать мировой валютой, что уже не видится фантастическим сценарием после бума, случившегося на рубеже 2017–2018 годов. Подытоживая, можно констатировать, что криптовалюты – это деньги! Вернее, новый вид денег, без границ и предвзятого контроля третьей стороны, будь то государство или банк.

Вы вполне могли заметить, что биткоин также очень похож на актив, такой как акции компаний Apple, Space X, где помимо стоимости зданий, имущества и патентов есть еще идейная составляющая, то есть некий глобальный посыл, как идеи Илона Маска о покорении космоса, заселении Марса или транспортной системе Гиперлуп, идеи Стива Джобса о лучших цифровых устройствах для всего мира, как разработанный им и покоривший умы миллионов iPod. Я имею в виду, что цена акций компании Маска или Джобса не является стоимостью сухих активов, есть еще и человеческий актив – харизма самого лидера и набор идей, которые он умеет воплощать. Это иногда увеличивает стоимость акций лучше, чем обычные физические активы. Криптовалюта играет схожую роль – это глобальная идея, захватившая как прогрессивные умы, так и маргинальные группы, группы империалистов и приверженцев анархии. Биткоин – это ресурс, в стоимости которого идейная составляющая так же велика, как и в акциях высокотехнологичных компаний.

Многие считают криптовалюты товаром, точнее, «цифровым товаром», и даже в определении биткоина часто фигурирует термин «цифровое золото». Связано это с тем, что себестоимость генерации некоторых криптовалют, в т. ч. и самого биткоина, вполне поддается расчетам. А раз есть стоимость производства, значит, результат производственных усилий вполне может считаться товаром, пусть и существуя лишь в цифровом виде. При этом сложность добычи в последние годы превратила майнинг биткоина в мероприятие, схожее по сложности и затратности с добычей реального золота.

Помимо финансовой и идейной составляющей большую роль играет фактор протеста против действий банков, государственной бюрократии, налоговых органов. Если европеец вложил в криптовалюту, никто не узнает, что он заработал огромные деньги, и при соблюдении определенных условий государство не возьмет с него налог на прибыль. Возможность передавать деньги друг другу на любые расстояния за комиссию, измеряемую в центах, с оборотом в миллионы долларов в день, чтобы купить что угодно, например, в Сингапуре или Гонконге за Bitcoin, будь то завод или копеечный товар, – это открывает широкие возможности, согласитесь! Безусловно, некоторые европейские и азиатские банки могут разменять вам криптовалюту на фиатную валюту, но мы-то рассматриваем такое будущее, где все признают Bitcoin, доверяют ему и согласны с его биржевым курсом. Тогда теряется смысл в долларе или евро, в предоставлении в банк кучи документов, в подтверждении своей личности и источников происхождения денежных средств. Конечно, здесь есть сходство с серой экономикой. Как платежное средство криптовалюту впервые начали использовать именно в серых схемах. Криминальные круги стали использовать биткоин при покупке наркотиков, оружия, других запрещенных товаров или финансировании каких-либо нелегальных операций. Может быть, теневая экономика вообще продвинула вперед эту технологию, уцепившись за ее псевдоанонимность, отсутствие контролирующего органа, быстроту расчетов и надежность. Но этого не могли не заметить более серьезные финансовые институты и отдельные прогрессивные личности, поняв, что незаконный оборот – лишь маленькая часть возможностей и в мире формируется новая социально-экономическая структура, которая может многое поменять, внести существенные коррективы в разные аспекты нашей повседневной жизни.

Радикальные криптоанархисты возлагают на биткоин и некоторые анонимные валюты роль разрушителей устоявшейся ныне финансовой системы во главе с долларом и американскими банкирами, через чьи корреспондентские счета проходит большинство трансграничных валютных операций. Я не думаю, что эта технология обрушит мировую экономику, если действительно пойдет ее скачкообразное бурное развитие. Ведь появление золотых и серебряных монет взамен шкурок, зарождение банков и рынок акций, создание

Интернета и электронной коммерции не обрушили традиционную экономику, а, наоборот, продвинули нас вперед. Поэтому можно ожидать технологического прорыва, и финансовая система лишь видоизменится, приняв в себя новое явление и вписав его в историю как одно из важных событий XXI века. Через одно или несколько поколений люди будут принимать ее как должное. Никто и не представлял в тех же 1990-х, что технологии будут выглядеть так, как сейчас. Многие из привычного сегодня тогда считалось фантастикой, ведь таких технологий попросту не существовало, разве что в фантастических книгах. Развитие Интернета и вычислительных машин и, как результат, сверхскоростные технологии передачи информации за 20 лет изменили мир до неузнаваемости. Так же как эти технологии изменили информационный мир, криптовалюты изменят и финансовый. Блокчейн и криптовалюта, как одна из важных функций технологии, повлияют на экономику, впишутся в нее, и мы к этому привыкнем. Это не приведет к разрушению мирового порядка, потому что старую экономическую и социальную систему мы с вами просто обновим, и человечество продолжит свое существование, как это было сотни раз в истории планеты. К примеру, появилась компания Uber, но она не обрушила рынок такси, хотя изначальной идеей являлся прямой платеж физического лица (клиента) другому физическому лицу (водителю), минуя посредников, сокращая затраты на лицензии и бюрократию, оптимизируя процесс. Клиент получает услугу дешевле, а водитель получает оплату быстрее и не испытывает затруднений с налогами и амортизацией. Однако сегодня Uber продолжает мирно сосуществовать с традиционными службами такси, и в некотором роде он «легализовался», приняв-таки правила игры, навязанные рынком.

С социологической точки зрения криптовалюта – это революционная технология, способная повлиять на все сферы общественной жизни. Например, для людей, которые живут в развивающихся странах, криптовалюты могут стать тихой гаванью для сбережений, с учетом непредсказуемости курса и судьбы национальной валюты в целом. Наличие смартфона и доступа в Интернет позволяет, в теории, обойтись без банковского счета, которого нет у миллионов жителей Азии, Африки, Южной Америки. Посредством же простого смартфона с установленным кошельком для криптовалюты они смогут очень быстро и просто начать пользоваться прогрессивной финансовой системой, сохраняя результат своего труда в активе, более надежном и свободно конвертируемом, в отличие от национальной денежной единицы. Многие социальные группы вполне могут создать свою собственную валюту за считанные минуты, миновав стадию обслуживания в традиционном банковском секторе и отказавшись от традиционных денег. Социальный, экономический и политический эффект от введения простых и надежных методов расчетов при посредничестве технологии блокчейн сложно недооценить.

Делая некоторые выводы, можно считать криптовалюту цифровым активом, топливом для развития цифровой экономики. Но всем ли понравится этот новый вид экономики и новые цифровые деньги? Не встретим ли мы сопротивление влиятельных финансовых и политических кругов? Поживем-увидим!

## **Появление криптовалюты**

Идеи зашифрованной цифровой наличности и анонимных электронных денег давным-давно витали в среде криптоанархистов и шифропанков. Широко известный в узких кругах «Манифест Шифропанка» американца Эрика Хьюза, опубликованный в 1993 году, содержит прямое призывание решить вопрос анонимных платежей, как необходимого элемента защиты личного пространства, во что бы то ни стало. Однако много ранее, в далеком 1983-м еще один американский специалист в области информатики, Дэвид Чаум, начал прорабатывать идею цифровых денег (digital cash) и в 1988-м привлек к доработке своей идеи программиста Амоса Фиата и криптографа Мони Наора, уроженцев Израиля, работавших в США. К сожалению, предложенная офлайн-система проверки отсутствия двойных трат, когда одни и те же цифровые деньги теоретически возможно потратить несколько раз, была несовершенна, и

только в 1991 году силами японских специалистов по криптографии Тацуаки Окамото и Казуо Ота в их труде «Универсальная электронная наличность» она была решена. Но не самостоятельно, а при помощи изобретения Ральфа Меркла, запатентовавшего метод представления цифровых подписей, названный Деревом Меркла (патент US06072363 от 5 сентября 1979 года). Однако Чаум первый, кто создал в 1989 году коммерческую компанию под именем DigiCash для практического внедрения цифровых денег, названных кибербаксами – cyberbucks, в повседневный обиход. Но идея Чаума не включала в свою концепцию прямые peer-to-peer (или кратко p2p) платежи от пользователя пользователю, а только взаимодействие с продавцами товаров (платежными шлюзами) и их пользователями. Также оставалась необходимость иметь обычные деньги для того, чтобы предварительно приобрести кибербаксы. Процесс генерации пользователями стоимости отсутствовал в принципе. Появлению же биткоина, как первой известной широкой общественности криптовалюты, с возможностью печати «своих» денег любым пользователем, помогли работы Адама Бека, предложившего в мае 1997 года на суд публики свой алгоритм HashCash с теоретически реализованной концепцией «доказательства работы», ставшей впоследствии основой для майнинга. Хотя вышеупомянутый Мони Наор в соавторстве с Синтией Дворк изобрел данную концепцию еще в 1993-м, опубликовав совместную научную статью о борьбе со спамом. А сам термин Proof-of-Work (PoW) был впервые упомянут лишь в 1999 году в научной публикации Марка Якобсона и Ари Джюэlsa. Целью Бека также была попытка оградить электронную почту от спама, добавив к процессу отправки каждого письма необходимость проделать небольшую вычислительную работу, тем самым сделав нецелесообразным проведение массовых рассылок. Никто из них не примерял свою идею на проведение финансовых транзакций, как и разработчики алгоритма RSA, ставшего первой описанной в далеком 1977-м системой шифрования на основе открытого ключа. Позднее, в ноябре 1998-го, Вей Дай описал систему b-money, в которой помимо «доказательства работы» предлагался консенсус на основе «доказательства хранения» или Proof-of-Stake, нашедший позднее применение при создании альтернативных биткоину криптовалют – альткоинов. А будущий первый получатель транзакции в Сети Биткоин Хэл Финни доработал концепцию Бека и в августе 2004-го предложил на суд сообщества шифропанков идею многократного доказательства работы Reusable PoW (RPoW) именно для применения в сфере электронных платежей.

Нельзя не упомянуть и о технологии децентрализованного реестра – блокчейн, без которого рождение биткоина вряд ли состоялось бы. Стюарт Хабер и Скотт Сторнетта приложили к этому свою руку, описав принципы меток времени в цифровых документах и комбинирования групп документов в цепочки, за целостностью которых следят пользователи. Доработав и усовершенствовав концепцию цепочки (поместив группы цифровых документов в блоки, а уже их связав в цепочку), Сатоши Накамото пришел к идее создания независимых узлов для хранения и генерации цепочки блоков – майнеров. И именно майнеры и заработок на майнинге, во многом, обеспечат будущий успех биткоину и ряду других криптовалют.

Как мы видим, появлению криптовалют предшествовало множество различных открытий и исследований, огромное количество времени было потрачено на исследования и разработки. Многие проекты преданы забвению, хотя упоминания о них еще можно встретить в сети. После первых успехов биткоина ряды приверженцев пополнились многими профессионалами в своих областях, которые критиковали или восхваляли новое явление. Кто-то слепо копировал идеи, кто-то дорабатывал их, и, возможно, часть имен, задействованных в развитии непосредственно криптовалют второй и третьей волны, мы увидим в «зале славы» криптовалютного сообщества и даже на мировой сцене. Возможно, нас еще ждет явление нового «пророка», чьи идеи и реализованные на их основе решения затмят все, что мы видели до сих пор.

## Как заработать криптовалюту



Каким же образом можно разбогатеть на криптовалюте? Самый простой способ – купить перспективную монету на старте реализации проекта. Например, одна из популярных существующих сегодня монет – монета Dash с быстрыми транзакциями и устойчивой сетью – с момента своего создания заработала 500 тысяч процентов, а это какие-то несколько лет. Я помню время, когда эта монета стоила 400–500 рублей, а в пик конца 2017-го – начала 2018 года достигала отметки более тысячи долларов!

Почему же так выросла цена? Причин этому может быть несколько, и основная – интерес спекулянтов к рынку криптовалют в целом и его «отцу» – биткоину. Бурный рост стоимости биткоина всегда сопровождается ростом всех остальных валют, особенно таких зрелых, как дэш или лайткоин. Это, можно сказать, основной фактор роста. Также нельзя не отметить то, что команда дэш ведет очень активную работу над улучшением своей монеты, иногда опережая других во внедрении усовершенствований. У монеты большое комьюнити, часть которого является владельцами мастернод – специальных узлов сети, которые участвуют в обеспечении безопасности и скорости транзакций, а также в эмиссии новых монет. Запуск мастерноды требует наличия 1000 дэш на вашем кошельке, которые блокируются, если вы хотите запустить полнофункциональный узел. Это ведет к сокращению обращения монет, а также к повышенному спросу из-за желания иметь собственный узел. Также росту поспособствовали позитивные новости о сотрудничестве дэш с крупными IT-компаниями и повышенном интересе национальных групп (например, из Китая) к проекту. И хотя к началу осени 2018-го цена основной массы криптоактивов, включая дэш, демонстрирует очень низкие значения, для первых «ранних последователей» дэш и десятки других монет принесли сверхприбыли.

Включиться в процесс подобного заработка можно и иными способами. Один из самых интересных и относительно безопасных способов, по моему мнению, – майнинг, или процесс создания новой криптовалюты. Если угадать с совсем новой или уже существующей, но «спящей» и не приносящей существенный доход монетой, то в теории, получив большое количество монет как вознаграждение майнера, можно заработать сотни и более процентов годовых. Но может получиться и так, что монета никогда не займет сколько-нибудь заметных позиций и не принесет баснословных барышей. Выбор проекта, в который вы готовы вложиться как майнер, как владелец мастернод или как просто спекулятивный инвестор, – это самая главная проблема существующего рынка криптовалют. Основные критерии выбора вполне очевидны. Во-первых, у проекта должна быть неанонимная команда, состоящая из живых людей, доступных в соцсетях и имеющих профильный опыт на занимаемых позициях в структуре компании. Во-вторых, проработка проекта должна быть серьезной, от маркетинговых материалов до юридической составляющей, и в-третьих, идея должна быть нужной сообществу и нести что-то новое. Например, если у проекта уникальный сайт, есть юридическое лицо в достойной юрисдикции, Вайтпейпер, Рoadмап и другие текстовые материалы подробны и переведены на основные языки, а также профессиональная команда ведет активную работу в социальных сетях и с ними можно контактировать – уже есть за что зацепиться. Проекты же на типовом шаблонном сайте, без вкладки меню «команда» и с невнятной, скопированной 1000 раз идеей не ждет ничего кроме короткого взлета и потом падения до 0 или близких величин. Десятки подобных проектов ежемесячно создаются на основе биткоина, эфириума или дэш, желая повторить их успех. Но имея лишь желание заработать быстрые деньги, реализуют лишь стандартный сценарий Памп-и-Дамп, т. е. искусственно созданный рост и следующее за ним падение биржевого курса. Читателю следует быть очень внимательным в выборе проекта, особенно для инвестиций, которые не связаны с майнингом. Ведь при майнинге вы сохраняете оборудование как некий утешительный приз, а при инвестировании непосредственно в монеты можете потерять все.

О заработке на майнинге мы подробнее остановимся в соответствующем разделе, а также далее осветим такой вариант заработка, как привлечение средств в свой бизнес с помощью криптовалют, получивший название Ай-Си-О (ICO), или первичное предложение монет. Суть его в том, чтобы объявить сбор криптовалюты на новый проект, связанный с блокчейн- или

IT-технологиями, а иногда и относящийся к реальному сектору. Таким образом можно создать как собственную независимую монету, так и внутренний токен на платформах, предлагающих инструменты для проведения такого сбора – краудфандинга, например в сети Ethereum, NEO, Waves и т. д. При этом платформа Waves имеет внутреннюю децентрализованную биржу, на которой без всяких условностей можно сразу торговать созданным активом – токеном. При этом участие в перспективных ICO также является неплохим способом заработка, тем более если войти в хороший проект на самой ранней стадии и вовремя выйти, пусть даже частью вложенных средств, достаточных на покрытие первичных издержек на участие в данном начинании.

Также рынок криптовалют предполагает большое количество обслуживающих его бизнесов – обменных пунктов, бирж, дизайнерских студий и команд разработчиков, маркетологов и советников-эдвайзеров. Продукты, выпущенные для рынка криптовалют, порой могут поспорить по прибыльности с майнингом, трейдингом и привлечением средств в ICO. Например, стоимость услуг консультантов может достигать сотен тысяч долларов, плата за листинг вашей монеты на бирже может составлять от крошечных 0,5 BTC до нескольких десятков BTC, а бюджеты маркетинговых агентств, продвигающих иные многообещающие проекты, могут не идти ни в какое сравнение со стоимостью продвижения традиционных рыночных продуктов. Также и юридическое обеспечение деятельности блокчейн-проектов стоит гораздо выше, нежели решение типовых задач в области корпоративного и международного права. При этом, зарабатывая на подобных услугах, исполнители (как правило) лишены всяких рисков в силу специфики самой отрасли. Вопрос лишь в том, что профессионалов в данной сфере единицы, а чтобы им стать, нужно уделить немало времени, сил и средств на изучение процессов и поиск нужной ниши. Заработать на криптовалюте можно, используя вполне традиционные профессии, расширив свои знания и приобретя ценный опыт именно в этой сфере.

## **Криптовалюта как часть мировой финансовой системы**

Раз уж вокруг криптовалют и технологии блокчейн сформировался рынок различных услуг и сервисов, развилось устойчивое международное сообщество очень разных людей по социальному статусу и уровню доходов, вполне можно утверждать, что криптовалюты стали частью мировой экономики, и какое место они в ней занимают, очень легко выяснить.

Многие десятки исследований проведены и проводятся сегодня с целью выявления текущего влияния криптовалют на мировые финансы, прогноза их поведения и возможных перспектив в будущем. Разные эксперты оперируют разными данными и получают различные результаты. В одном заключении читаются позитивные настроения, в другом в выводах замечен очевидный скепсис. Но сам факт того, что крупнейшие банки, частные и государственные финансовые структуры и именитые институты тратят огромное количество времени и средств на проведение подобных исследований, уже говорит о том, что блокчейн и криптовалюты заняли свое место в мировых финансах и будут в них развиваться дальше. Многие из прочитанных мною документов находятся в свободном доступе в Интернете, некоторые рассылались по закрытым группам. Настойчивому читателю не составит труда найти большую часть необходимых материалов на просторах всемирной паутины. Я же поделюсь с вами небольшими выкладками, без отсылок к источникам.

В период с начала 2016-го по начало 2017-го общая капитализация рынка криптовалют выросла с 10 до 30 млрд долларов США. Существенный рост, однако уже к концу 2017 года общая капитализация выросла в 20 раз и достигла 600 млрд долларов. Несомненно, 2017 год можно смело назвать рекордным по росту капитализации. С первого дня января и значения с 18 млрд до почти 600 в последние дни декабря – это очень существенно. Но первая неделя 2018 года подлила еще масла в огонь энтузиазма, был достигнут абсолютный рекорд капитализации в 900 млрд или 0,9 трлн долларов! Почти триллион долларов США! Т. к. все познается в сравнении, можно привести пример капитализации стран или отдельных крупных

компаний. Например, общая капитализация всей мировой экономики оценивалась экспертами в 2016 году на уровне 65 триллионов долларов, при этом топ-10 стран имели капитализацию 50 трлн долларов. В текущий момент некоторые страны мира имеют капитализацию ниже той, которую показывает рынок криптовалют в начале осени 2018 года (230 млрд долларов США). Если же рассмотреть крупнейшие компании мира, то капитализация лидера рейтинга – американской Apple – достигла 902 млрд долларов в 2018 году, а самая крупная публичная компания России – Сбербанк – не дотягивает в долларовой оценке даже до 100 млрд USD.

Из всего этого напрашивается только один вывод: биткоин (а именно он составляет основу капитализации рынка криптовалют, редко занимая в нем долю ниже 60 %) стал значимой частью мировых финансов, и сложно себе представить, чтобы такой пласт мировой экономики просто перестал существовать... Также и основные преследователи из топ-10 рейтинга криптовалют, такие как Эфир, Рипл, Биткоин-Кэш, Лайткоин, Стеллар и прочие, имеют своих последователей, свое огромное сообщество – комьюнити – и демонстрируют отличные темпы роста и развиваются, несмотря на кризисный для криптовалютного рынка 2018 год. Возможно, нас ждут еще более глубокое «дно» и депрессивные настроения, но так же как и кризисы в традиционной экономике имеют цикличность, кризисы в мире криптовалют сменяются временами небывалого подъема, что может послужить для многих сигналом войти в рынок именно сейчас, на спаде, как завещали великие трейдеры-богачи с Уолл-стрит.

### **Кратко о краудфандинге и ICO**

Одним из новых терминов криптоэкономики, но уже ранее мной упомянутых, является Initial Coin Offering (ICO). В переводе с английского это означает первичное предложение монеты, по аналогии с IPO – первичным публичным предложением (акций) компаний на фондовом рынке. По сути ICO является так называемой краудфандинговой компанией – просьбой ко всем желающим вкладывать деньги в некую идею (чаще новую и тесно связанную с блокчейн, искусственным интеллектом или сопутствующими информационными технологиями и продуктами) для ее реализации. Взамен вложений вы получаете некое количество криптовалюты в виде монет или токенов, отражающее вашу долю в проекте либо долю в продукции, которая будет произведена за счет собранных средств. Отличие от традиционного IPO в том, что для объявления сбора достаточно лишь нескольких незамысловатых действий. Для начала создать некий бизнес-план, или инвестиционный меморандум, или что-то, схожее с форматом ТЭО, технико-экономического обоснования проекта, принятого в российской бизнес-практике. Затем создать сайт, наполнив его необходимым содержанием, в т. ч. опубликовать роадмап – «дорожную карту», и наконец выбрать форму сбора – допустим, смарт-контракт на платформе Эфириум, а то и попросту объявить прямой сбор на кошелек проекта в любой криптовалюте, а учет вести в традиционной базе данных, привязанной к сайту. Именно так многие абсолютно безыдейные или попросту насмешливые проекты собрали значительные суммы. Создается впечатление, что можно просто кое-как что-либо сделать и предложить это миру, а в случае успеха эмигрировать в теплые страны, но сегодня это уже не так. Тем не менее подобные примеры были, есть и будут. Какое-то количество даже очень продуманных и многообещающих проектов не выполнит своих обещаний, что не редкость и в традиционном мире финансов, например на рынке акций. Однако на рынке акций провести подобную манипуляцию нельзя так быстро и относительно недорого. Для размещения бумаг на бирже требуются огромные средства плюс выполнение ряда существенных условий – как минимум наличие юридического лица и штата сотрудников. ICO может провести один человек, не имеющий ни образования, ни фирмы, ни команды, а лишь идею и набор минимальных навыков в IT.

Чтобы не быть голословным, лучше привести конкретные примеры и на них рассмотреть основы процессов, описываемых в текущей части книги. Показательным примером проведения краудфандинговой кампании для реализации блокчейн-проекта является

компания Виталика Бутерина, сына уроженцев СССР, эмигрировавших в Канаду. Будучи человеком, с помощью отца погруженным в программирование и математику, а также получив знания в основах криптографии, Виталик легко впитал историю биткоина и нашел в нем ряд существенных недостатков. Понимая, что одному сделать проект нового улучшенного биткоина ему не под силу, он провел краудфандинговую кампанию, собрав гигантскую сумму в 31 000 биткоинов, что составляло около 18 млн долларов США на тот момент. Естественно, объявлению о сборе предшествовали большая работа, вполне научный труд, а также активное участие в сообществе последователей криптовалют и плотная работа за компьютером. На Эфириуме мы плотнее остановимся далее, но здесь нам важна суть процесса. Идея – упаковка – сбор средств – реализация. Что из этого вышло, знает каждый, даже начинающий энтузиаст блокчейн-технологий. Получилась вторая по капитализации криптовалюта с возможностью создавать собственные монеты-токены внутри платформы и с легкостью проводить свои краудфандинговые кампании. И это лишь одно из многих применений созданной Виталиком технологии.

И уже на базе самого Эфира сейчас проведены тысячи кампаний, от откровенно мошеннических до супервеликолепных и стоящих внимания. Очень ярким примером является проект Дэна Ларимера – известного криптоэнтузиаста, даже примерявшего на себя имя Сатоши Накамото. Проект EOS, грозящий стать очередным «убийцей» биткоина и эфира (со слов самого основателя), проводил сбор все же на площадке Эфириума, отдавая тем самым должное ее удобству и важности для всего сообщества. Сбор проходил целый год, и цена токена выросла за это время в несколько раз. Уже за первые 5 дней сборов проект привлек криптовалюты на 170 млн долларов, а итоговый сбор за весь год превысил 4 млрд долларов. Рецепт успеха были как личность основателя и его опыт в создании проекта BitShares, так и идея об устранении недостатков существующих валют в новом проекте, а также исключительно удачно выбранные время и способ для сборов. Какова будет дальнейшая судьба проекта, покажет время.

## **Сходства и различия пирамиды и криптовалюты**

Самый частый вопрос, возникающий при знакомстве с криптовалютой: является ли она пирамидой? Конечно, есть некоторые сходства с пирамидой, но только лишь при поверхностном анализе. Классическая одноуровневая пирамида представляет собой традиционную «схему Понци». Она получила такое название в честь итальянца Чарльза Понци, который создал одну из самых хитрых финансовых пирамид в истории. Смысл его пирамиды был в том, что выплаты более ранним вкладчикам делаются за счет взносов новых участников. Здесь очень важны харизма лидера, его подход к продвижению проекта, т. к. стоящие за ним участники не играют особо важной роли в привлечении новых игроков, они могут лишь запустить сарафанное радио, получив выплаты в первых рядах. Более продвинутой является многоуровневая пирамида, принявшая на вооружение принципы сетевого маркетинга, где для получения вознаграждения необходимо привлечь несколько последователей и получить некий продвинутый уровень в структуре. Такие проекты часто маскируют деятельность распределением каких-то товаров или услуг, не имеющих реальной потребительской ценности или их характеристики и цена очень сильно завышены. Наиболее совершенным типом можно считать матричную пирамиду, когда заполнение одного сегмента матрицы под вами влечет ее деление на два новых и ваш переход на новый уровень. Здесь уже можно встретить реальные товары и услуги, как базу для мотивации достигать новых уровней и помогать заполнять нижние уровни матрицы. Жизнеспособность таких пирамид, особенно при установлении продуманной системы выплат без чрезмерно завышенных процентов, может быть очень долгой. Общими признаками всех типов пирамид являются необходимость постоянного привлечения новых участников; навязчивая реклама с призывами быстрее вкладываться, при этом цель – лишь личное обогащение; очень высокий гарантированный процент на вклады (гарантии – пустышка); отсутствие реальных активов и бизнеса,

способного генерировать доход, и чаще всего даже юридического лица с необходимыми разрешениями или лицензиями на финансовую деятельность, а соответственно и прозрачной отчетности; закрытый характер получения важной информации о том, как же все-таки работает организация; семинары с элементами секты – восторженные истории успеха и аплодисменты стоя; необходимость оплаты вступительного взноса для получения статуса более высокого, чем рядовой участник.

При инвестировании в криптовалюты можно найти несколько похожих свойств, но больше все-таки различий. Приход новых участников подогревает общий интерес к отрасли, и часто доход первопроходцев зависит от будущего интереса новых инвесторов к той или иной монете, но связан этот доход с ростом стоимости монеты, а не с выплатами из средств новых участников. Многие ранние инвесторы криптопроектов – это энтузиасты, а не дельцы. Их цель – сделать что-то полезное, тогда как пирамида, по сути своей, бесполезна. У хороших, стоящих внимания криптопроектов есть минимальные активы: команда, готовый или будущий продукт, жизнеспособная и нужная обществу идея. Вся информация и код находятся в общем доступе, часто о расходах публично отчитываются или даже голосуют за ту или иную трату. Начальная идея криптопроектов отражается в белой бумаге и дорожной карте, участники осведомлены о рисках, тогда как в пирамиде это старательно замалчивается. Криптовалюты чаще всего свободно конвертируемы в другие монеты или фиатные деньги, стоимость их может упасть до минимума, но торги прекращаются только при отсутствии интереса рынка к торговле. Выход из пирамиды бывает затруднен, а после краха просто невозможен, доли в пирамиде никак не оформлены и не могут быть реализованы за пределами внутреннего сообщества. Неограниченный объем эмиссии ряда монет можно тоже считать сходством, однако для их генерации необходимы определенные усилия: напечатать тот же эфир в неограниченном объеме не могут ни разработчики, ни крупные майнеры, а вот «акции» в пирамиде неограниченно штампуются организаторами. Замечание, что криптовалюта ничем не обеспечена, также имеет не совсем верную окраску. У монет PoW есть себестоимость генерации, есть общественная ценность, есть и стейблкоины, обеспеченные национальными валютами, золотым запасом, драгоценными камнями или будущим объемом производства некой продукции. Криптовалюта децентрализована, тогда как пирамида изначально централизованный проект. В криптовалюте близость к началу цепочки не дает никаких преимуществ в управлении проектом или получении дохода. В конце концов, многие монеты также не имеют ни юридического лица, ни лицензии на деятельность, но это связано лишь с недостатком законодательного регулирования. За создание пирамиды почти повсюду в мире предусмотрена уголовная ответственность, криптовалюты же разрешены многими государствами и признаны цифровыми активами или аналогом иностранных валют. Тем не менее вполне можно организовать криптовалютную пирамиду, даже в момент написания этого материала в СМИ идет волна сообщений о проекте Кэшберри, обвиняемом в организации пирамиды. Подходящей платформой для создания пирамид, с технической точки зрения, сегодня является Ethereum с его системой смарт-контрактов, хотя любая другая платформа по выпуску токенов или самая простейшая монета могут быть базой для запуска пирамиды.

## **Пирамида на смарт-контракте Ethereum**

Как я уже отмечал, смарт-контракт – это неизменяемый программный код договора, который выполняется в случае, если выполнено первичное условие – поступила оплата на адрес кошелька контракта. В смарт-контракт можно легко заложить стандартную схему Понци, например прописать, что новый участник получит две монеты (т. е. 100 % прибыли) взамен одной вложенной, но только если за ним придут три других участника. И неважно, привлек ли их этот самый участник, или организатор, или другие новоприбывшие. Просто число новых «инвесторов» должно расти в геометрической прогрессии. При этом из трех монет, внесенных во вторую и последующие фазы, две идут на выплату более раннему вносителю, а одна монета, за минусом необходимых минимальных комиссий, уходит

владельцу смарт-контракта. Прозрачный код смарт-контракта пирамиды может быть легко проверен на предмет отсутствия завуалированных условий, и в целом можно увидеть относительно «честную» пирамиду, в которой все движения средств и очередность выплат на виду. Если будут прибывать все новые и новые люди, каждый раз в тройном размере, то предыдущие участники будут гарантированно получать две монеты эфира вместо одной, автоматически. Никому не нужно следить за контрактом, никто не может вмешаться, чтобы изъять Ethereum для себя. Каждая транзакция имеет отметку о времени, и, исходя из того, кто был раньше, выстраивается очередь выплат. В Интернете можно легко найти ряд типовых смарт-контрактов на основе схемы Понци, но сам Ethereum от этого не становится пирамидой, он лишь позволяет создать пирамиду внутри себя, причем гораздо более предсказуемую, чем в сфере традиционных финансов. Есть и сложные контракты, с системой выплат по реферальной программе, можно варьировать процент выплат в зависимости от количества привлеченных участников и суммы внесенных средств, присовокупить сюда лотерею и систему рангов участников, вообще играть массой различных параметров. Я не призываю никого бросаться в сферу уголовно наказуемого финансового мошенничества – это лишь пример, позволяющий дифференцировать пирамиду от платформы, на которой ее теоретически можно запустить.

## Пузырь доткомов и пузырь ICO

Я уже упоминал такое событие, как пузырь доткомов (от. com, англ. *dot* – точка и *com* – популярная доменная зона). Блокчейн часто сравнивают с Интернетом, хотя это лишь следствие появления Интернета и всемирной паутины, своеобразная надстройка над ним. Для многих Интернет – это три заветные буквы www, хотя WorldWideWeb – всемирная сеть, это такая же надстройка над Интернетом, сделавшая возможным создание веб-сайтов в привычном нам сегодня виде. Для ранних времен Интернета протокол НТТР как прикладной инструмент его работы, протокол передачи файлов FTP – все это было гигантским технологическим открытием, но никто не предполагал, каких масштабов достигнет развитие Интернета, усиленного дополнительными технологиями. Когда появилась система национальных доменов и началась купля-продажа стандартных доменных имен, многие поверили в то, что любая маломальская идея сайта. com обречена на успех, а уж тем более крупные высокотехнологичные компании. Пузырь доткомов появился из-за того, что многие американские компании и фирмы из высокоразвитых, в технологическом плане, стран начали пытаться придумывать для веб-сайтов и Интернет-технологий всевозможные идеи и применения, регистрировать под это домены и собирать на реализацию проектов деньги через продажу акций. Фактически проводилось то же самое ICO, только вместо создания криптовалют выпускались классические акции. Их продавали людям, надеющимся, что именно эта конкретная идея и созданный под нее домен с сайтом превратятся в крупный бизнес, а в целом наступила «новая экономика» и эпоха Интернет-бизнеса. Как и в Блокчейн, первые энтузиасты Интернет-экономики мечтали сделать что-то большое и общественно-полезное, но следом пришли мошенники с желанием заработать легкие деньги. Нездоровый ажиотаж в обществе, поддержанный хвалебными статьями в СМИ, только раздувал интерес широких масс к супербизнесу на Интернет-сайтах. Огромное количество людей сначала в Америке, а потом и во всем мире, начало вкладываться в любые «грандиозные» проекты, связанные с Интернетом, и пузырь стал расти. Многие обычные компании спешно создавали корпоративные сайты, и их акции уже начинали расти в цене. Начавшись в 1995-м, ажиотаж продлился 6 лет, до 2001 года. Многим казалось, что реально наступила новая эпоха Интернет-экономики, и они были в общем-то правы, только чересчур оптимистичны в прогнозах. Интернет-экономике нужно было еще 10–15 лет для полного становления. Но все больше и больше доменов регистрировалось под самые разные идеи, проводились масштабные рекламные кампании, тратились огромные средства на содержание персонала и офисов, а население покупало все более дорогие акции высоко-, средне- и низкотехнологичных

компаний. Проблемой было лишь то, что люди не понимали, что сами сайты – это лишь инструмент для развития бизнеса, а не сам бизнес. За ним стоит либо реальный производственный процесс, либо компания в сфере услуг. Сам по себе сайт тогда не мог быть источником генерации прибыли.

Среди раздутых проектов были и стоящие, как нынешние Amazon, eBay или Google. Сегодня подобное происходит и в сфере ICO. Волна общественного оптимизма 2017–2018 годов позволила сотням неизвестных команд и проектов привлечь инвестиции под разнообразные, порой заурядные или попросту скопированные у других идеи. Многие из них окажутся мошенниками – умышленно или в силу неизбежного охлаждения рынка и его падения. Но часть компаний, предлагающих именно внедрение инструментария Блокчейн в экономику, развитие инфраструктуры и сообщества, сможет добиться успеха. 2018 год явил нам большую коррекцию рынка криптовалют, очень условно сравнимую с падением индекса NASDAQ в период пузыря доткомов. Кстати, капитализация блокчейн-экономики снизилась с 0,9 млрд до 0,2 млрд долларов за 2018 год, похудев на 80 %, а рынок доткомов сдулся на 5 трлн долларов, потеряв те же 80 %. Проценты одинаковые, но реальная сумма потерь во много раз больше. Можно лишь надеяться, что в это нелегкое время закалятся и выживут по-настоящему нужные проекты, которые своими действиями подтолкнут индустрию вперед и вверх, а несостоятельные замыслы уйдут со сцены и не окажут негативного влияния на будущее развитие. Ведь сегодня мы видим, насколько молодое поколение погружено в Интернет, социальные сети, как много времени они проводят за планшетами, ноутбуками и смартфонами. Для них привычно заказывать товары через Интернет, искать информацию на Википедии, смотреть видеоролики на YouTube и вести прочую сетевую активность. Так же и блокчейн, по моему мнению, переживет период становления, но уже быстрее, чем Интернет-технологии, сможет взрасти на имеющейся благодатной почве и дать плоды. Живущее сегодня поколение миллениалов (также называемое поколением Y), людей, рожденных после 1980 года, легко позволило информатизации войти в свою жизнь, а их дети – так называемое поколение Z, рожденное после 1995 года, уже в новую эпоху, смогут во много раз быстрее и легче принять принципы децентрализованной экономики и государственного управления, если поступательное движение в этом направлении не сбавит обороты. Возможно, они станут свидетелями и появления государственных блокчейн- и криптопроектов как в нашей стране, так и в отдельных странах, и даже в глобальном мировом масштабе.

## Глава 2

### От зарождения криптовалют до наших дней

#### Зарождение Bitcoin

31 октября 2008 года в электронной рассылке для криптографов и шифропанков на сайте gmane.org анонимный человек или группа людей под псевдонимом Сатоши Накамото опубликовал так называемую «white paper» – «белую бумагу» – документ с описанием общей концепции новой платежной системы. Как мы уже писали выше, это был некий сконцентрированный посыл в виде технико-экономического обоснования идеи, которую пытается предложить автор или коллектив авторов сообществу. Это первичный манифест о том, как все будет работать и что для этого нужно сделать, доказательная база, формулы, математические расчеты. Список литературы вполне позволяет разобраться в некоторых источниках зарождения биткоина, что я и описал в предисловии к своей книге.

Сам исторический документ до сих пор хранится в открытом доступе и переведен на разные языки, он публичен, но с автором все не так прозрачно. В США живет однофамилец Дориан Сатоши Накамото, однако многие исследователи не смогли на 100 % связать данного господина с создателем биткоина. Возможно, ныне покойный Хэл Финни – получатель первой транзакции биткоина – законспирировался настолько, что придумал себе вымышленного

напарника. Есть версия, что один из первых девелоперов биткоина – Марти Малми, тот самый автор проекта. Кто-то считает, что создатель второй по популярности криптовалюты – лайткоина – Чарли Ли и есть Сатоши. Многие приписывают авторство известному американскому криптографу Нику Сабо, развивавшему проект «цифрового золота» – Bit Gold. Есть версия, что авторы поданной 15.08.2008 патентной заявки № 20100042841 A1 на систему обновления и распределения ключей шифрования Нил Кинг, Владимир Оксман и Чарльз Брай имеют непосредственное отношение к созданию биткоина из-за совпадения редкого сочетания слов в их заявке и «белой бумаге» Сатоши. Существует несколько псевдо-Накамото, ведь из-за того, что личность создателя биткоина не раскрыта, любой может представиться Сатоши Накамото. И такие ребята, естественно, нашлись, делая себе пиар и продвигая личные интересы. Как бы то ни было, следы Сатоши потеряны, он отошел от дел, и теперь проект развивается сообществом, как это и должно было случиться.

В том же 2008 году, а именно 18 августа, регистрируется домен bitcoin.org, на котором будет размещаться вся информация касательно проекта Биткоин, в ноябре создается одноименная ветка с форумом и хранилищем на ресурсе sourceforge.net, а уже через год, в ноябре 2009 года, появляется приветственное сообщение от satoshi на ресурсе bitcointalk.org, где в дальнейшем будет обсуждаться большинство значимых событий сообщества криптоэнтузиастов со всего мира. Сам же satoshi последний раз проявит свою активность на форуме 13 декабря 2010 года и с тех пор ни разу не посетит данный ресурс под этим именем.

Первый узел сети Биткоин, принадлежащий Сатоши Накамото, начал работать 09.01.2009, и создатель в первый же день сгенерировал цепочку из 14 первых блоков, создав таким образом 700 биткоинов. Это заняло всего лишь несколько часов, т. к. первоначальная награда за блок составляла 50 биткоинов, а сложность добычи была равна 1, что позволяло находить блоки на обычном процессоре домашнего компьютера.

Идея биткоина и способ ее претворения в жизнь довольно быстро нашли отклик в среде шифропанков, криптографов и программистов. Первым известным помощником Сатоши стал Хэл Финни, который скачал клиентское приложение на свой компьютер и первым из сторонних пользователей вычислил блок в сети, предположительно за номером 78, а затем сгенерировал еще ряд блоков. Он несколько дней искал недочеты в коде и давал советы по оптимизации самому Сатоши, а тот вносил правки в код. Также считается, что первая транзакция в 10 BTC была сделана 12.01.2009 с адреса Сатоши в адрес Хэла, однако в тот же день было проведено еще 4 транзакции на анонимные адреса... Некоторое время спустя Хэл забыл о проекте, но в 2010 году был приятно удивлен, что проект живет и развивается, во многом благодаря ему самому и нескольким таким же активным энтузиастам, как вышеупомянутый Марти Малми.

Итак, идея Сатоши стала реальностью, произошел переход от концепции на бумаге к тестовой версии программного обеспечения и к первичному блоку, а от него к следующему и следующему. Цепь начала расти, а идея – захватывать все больше умов. Все, что существовало до Bitcoin, было достойно реализации, но именно он появился в нужное время и в нужном месте. Почему же именно биткоин стал успешным и до сих пор сохраняет лидирующие позиции, несмотря на давление тысяч конкурирующих монет со своими новшествами, доработками, усовершенствованиями? Возможно, уровень развития вычислительных технологий достиг необходимого минимума (как в плане производительности, так и распространенности в мире), плюс средний уровень знаний в определенной группе потенциальных пользователей позволил семенам технологии дать бурные побеги. Как бы то ни было, биткоин был первым и останется первым навсегда, что бы ни случилось на рынке в ближайшие годы.

## **Эволюция майнинга**

Я уже описал в предыдущей главе, как Сатоши сгенерировал первичный блок – genesis block – и еще 13 последующих блоков в первый день работы своей системы. Процесс



генерации блоков получил название майнинг (от англ. *mining* – добыча). Наградой майнеру – человеку, производящему на своем оборудовании вычисления, – становятся новые монеты, а также комиссии за транзакции, включенные в этот блок. Если транзакций нет – то и дополнительного вознаграждения с комиссий тоже нет. В первое время награда составляла 50 монет за каждый найденный блок. Легко посчитать, что Сатоши заработал 700 монет за несколько часов работы простого процессора. Однако в силу невысокой сложности вычислений и отсутствия какого-либо признания технологии в массах стоимость этих монет была близка к нулю. Последующие несколько месяцев генерация шла вяло, и сложность майнинга не росла до декабря 2009-го, когда в канун нового 2010 года на блоке № 32256 произошел пересчет сложности, и вместо единицы этот показатель составил 1,18 хеша в секунду. Теперь каждый добытый биткоин становится ценнее. Пересчет сложности происходит каждые 2016 блоков, следовательно, за первый календарный год майнинга прошло 16 циклов без пересчета сложности, было сгенерировано более 1 600 000 биткоинов из 21 000 000 возможных, что составило около 8 % всей возможной эмиссии. Но уже через полгода, благодаря распространению информации в сети Интернет, на блоке № 68544 сложность скакнула в 4 раза – с 45,39 до 181,54 хеша/сек. Несложно посчитать, что уже за первое полугодие 2010 года было добыто больше монет, чем за весь предшествующий год. И с тех пор сложность вычислений, а следовательно, количество вычислительной мощности, которое необходимо для генерации нового блока, только растет. Очень редко этот показатель снижается – например, в период уполовинивания награды за блок или выхода очередного форка (ответвления блокчейна) биткоина. Майнинг – это непрерывный поиск решения усложняющейся задачи. В реальной жизни можно провести параллель с математической олимпиадой с призами за решенную задачу, где всем участникам раздали одинаковые задачи, а после их решения одним из участников немного усложнили условия, а затем еще и еще. Возможно, участникам сначала выдают счета, затем калькуляторы, потом маломощные компьютеры, потом суперкомпьютеры... Чем больше вычислительных ресурсов вы используете, тем больше решаете задач и зарабатываете. И в процессе вычисления блоков биткоина реализовался подобный сценарий. Все производили вычисления на процессорах, пока некто с псевдонимом ArtForz не написал специализированное программное обеспечение, позволявшее использовать графические ускорители (видеокарты) в параллельных вычислениях и в несколько раз эффективнее вычислять хеш-функции для генерации блоков биткоина. Собрав несколько видеокарт в один вычислительный модуль, была реализована первая «ферма» на видеокартах, и в небольшой промежуток времени один человек смог кратковременно завладеть 25 % вычислительных мощностей сети Биткоин. Речь идет о середине 2010 года, но уже в 2011 году использование видеокарт стало более массовым, как и выбор программного обеспечения, появившегося в публичном доступе. Здесь затронут один важный момент – понятие «атаки 51», когда майнер или группа майнеров, владеющих 51 % мощности сети, могут игнорировать решения других 49 % майнеров и выстраивать свою цепочку, отвергая ненужные варианты блоков. Такая группа может очень долго иметь повышенный уровень генерации, но своими действиями также может навредить всей системе, скомпрометировав ее и оттолкнув честных участников.

В это время биткоин уже обрел некоторую реальную стоимость, и усилия по внедрению новых аппаратных и программных решений окупались в сравнительно небольшой срок. И вот уже в июне 2011-го на рынок вышли майнеры на основе FPGA (ПЛИС) – вычислительных чипов, которые могли быть запрограммированы пользователями под конкретные задачи. Правильная архитектура и ПО позволили добиться намного более высокой производительности. Но и у этой технологии был век недолог. Компания Butterfly Labs (BFL), достигшая хороших показателей в разработке и внедрении (а следовательно и продажах) FPGA-майнеров, уже через год, в июне 2012-го, начала прием предзаказов на ASIC-майнер на микрочипах специального назначения, сконструированных и оптимизированных только для целей вычисления хеш-функций алгоритма SHA-256, на котором, собственно, и работает биткоин. Не все прошло гладко, и не растерялись конкуренты в лице ASICMINER и Avalon,

бросившие силы на разработку своих микросхем. Сейчас добывать биткоин можно только на последних поколениях ASIC-майнеров, которые демонстрируют низкое потребление электроэнергии при приемлемой стоимости в \$ за 1 Th/s вычислительной мощности.

Первоначально майнинг даже не преследовал цель покрыть издержки на электроэнергию и амортизацию вычислительного оборудования, а больше походил на попытку заработать побольше очков в новой интересной игре. Никто не придавал такой ценности Bitcoin, как сегодня, никто даже не предполагал, что он будет стоить десятки тысяч долларов. Ведь изначально речь шла о цене в несколько центов за один биткоин. Благая цель Сатоши по наделению каждого ядра процессора одним голосом в сети начала разрушаться, как только ценность монеты позволила зарабатывать хорошие деньги на создании крупных вычислительных центров. Такова человеческая сущность – мы хотим больше и больше...

В силу того, что майнинг перестал быть способом достижения консенсуса в сети и стал способом заработка, ведь фактически майнер – это печатная машинка для денег, изменился и состав сообщества майнеров. Место талантливых программистов, математиков, специалистов по криптографии заняли матерые финансисты и бизнесмены, почуявшие золотую жилу как в производстве оборудования для майнинга, так и в строительстве крупных дата-центров для собственной генерации криптовалют. Из чего же складывается награда майнера? Рассмотрим чуть подробнее.

Первая часть – фиксированное вознаграждение, заложенное в алгоритм создателем, которое получает пользователь, первым вычисливший новый блок. Изначально награда составляла 50 BTC за блок. Но для борьбы с инфляцией Сатоши придумал механизм уполовинивания награды через каждые найденные 210 000 блоков. Первое уполовинивание до 25 BTC за блок произошло именно на блоке № 210000 в конце ноября 2012 года, второе случилось в начале июля 2016 года. Следующее снижение награды предстоит в апреле-мае 2020 года. Предполагается, что чем меньше награда за блок, тем ценнее должна становиться каждая следующая добытая монета. Если в начале 2010 года кто-то мог получить дневное вознаграждение в 50 монет за найденный блок, пользуясь мощным, но доступным для всех ноутбуком, то сейчас придется купить тысячу(!) дорогостоящих специализированных устройств типа Antminer s9, чтобы заработать лишь 1 Bitcoin, и не за несколько часов, а за сутки. При этом потребив примерно 1,5 мВт электроэнергии, что сравнимо с потреблением энергии 15 000 ноутбуков! Получается, что в 2020 году можно ожидать очередного роста цены биткоина, потому что оставшееся количество монет будет еще более ценным, так как их добыча становится невероятно сложной и затратной. Обычному пользователю в сегодняшних условиях сгенерировать блок просто невозможно, либо он должен обладать магической удачей, чтобы его не очень функциональное устройство вдруг нашло верное решение раньше других. Кстати, существует такой фактор в майнинге, как luck – удача. То есть вы можете найти блок за час, а можете за одну минуту. Однако на долгом отрезке времени теория вероятности сделает свое дело, и шансы будут стремиться уравниваться. На некоторых специализированных форумах даже предлагаются к продаже асики, которые сильно выбились из средней статистики по количеству найденных блоков, работая в соло-майнинге, т. е. пытаясь решить задачу единолично, вне сообщества (пула) таких же вычислительных модулей. Однако это лишь маркетинговый ход, не имеющий под собой математической подосновы.

Вторая часть награды майнера – это награда за проведенные транзакции. То есть помимо награды за блок он также получает всю сумму комиссий, которые заплатили пользователи за осуществление своих платежей. Если майнер нашел блок – это пустой контейнер, в который можно поместить определенный максимальный объем транзакций. Сейчас идет работа над увеличением объема информации, хранимой в блоке, и следовательно, над увеличением совокупной награды за транзакции, включенные в блок. Не так давно, в 2017 году, было время, когда транзакции перестали помещаться в блоки, очередь была огромной и платеж в сети Биткоин мог идти сутками, хотя система криптовалютных платежей позиционирует себя как способ сделать перевод быстро, анонимно и децентрализованно. В итоге сложилась ситуация,

в которой огромные вычислительные центры, созданные в основном производителями специализированных чипов, смогли выбирать, какие транзакции включать в блок из всего мем-пула (списка транзакций к исполнению). Если какая-то транзакция предполагала бОльшую оплату, майнер предпочитал включить в блок ее, а не ту, что была более дешевой. В данном случае ситуация в чем-то похожа на железную дорогу, только вагоны подгоняют каждые 10 минут, а на станции уже ждет множество грузовых машин, которые хотят отправить что-то в соседний город. Машин уже намного больше, чем вагонов, и мы не можем поместить все грузы в один вагон. Естественно, возникает ситуация, когда некоторые водители начинают платить более высокую цену, лишь бы поместить свой груз именно в этот вагон. Естественно, машинист поезда выберет тех, кто предложил больше других. Майнер работает так же: из всех поступивших в базу запросов на обработку транзакций он выберет только те, которые заплатят больше. В итоге сумма комиссий с упакованных в блок транзакций могла составлять более 1 BTC, помимо фиксированной награды за блок. А «дешевые» транзакции никто не хотел обрабатывать.

Сегодня все борются за награду за блок, т. к. эта цифра очень существенна, даже несмотря на два ее состоявшихся уполовинивания – 12,5 Bitcoin. Это более 100 тысяч долларов за один найденный блок (на дату 01.05.2018). А объем транзакций, которые может включить майнер, в спокойное время менее 1 Bitcoin. В среднесрочной перспективе, примерно к весне 2024 года, когда награда за блок упадет до 3,125 Bitcoin, а количество транзакций в одном блоке будет в несколько раз больше, чем сейчас, мы можем увидеть ситуацию, когда размер комиссий приблизится к вознаграждению за блок, а вот в 2028 году и превысит этот размер. Тогда будет важно, сколько и каких транзакций вы добавили в блок. Поэтому майнинг в будущем – это не охота за наградой за блок, а кропотливая работа оператора по проведению платежей, который постоянно обрабатывает транзакции и зарабатывает на них.

## **Накопление криптовалюты и первые транзакции**

Остановлюсь чуть подробнее на теме накопления первых активов на биткоин-кошельках. Сейчас с помощью различных сервисов можно проанализировать некое количество самых первых кошельков и увидеть, что в них лежит огромное по сегодняшним значениям количество Bitcoin, которые ни разу не перемещались с самого момента создания. Были либо получены награды за генерацию одного или нескольких блоков, либо тестовый перевод, а далее кошельки замерли. Монеты накапливали и старались сохранить доступ к кошельку лишь единицы, которые прочитали «white paper Bitcoin» либо услышали компетентное мнение специалиста или восторженный отзыв друга и увидели перспективу. Некоторые просто оставили кошелек «на авось». Кто-то поигрался неделю, кто-то месяц, но, не получив азарта, который присутствует в карточных играх или лотереях, решил прекратить эксперименты.

Однако, когда уже начали проходить реальные сделки и в системе затеплилась жизнь, гораздо большее количество людей начало копить Bitcoin. Они понимали, что как средство платежа он еще отстает от Visa, MasterCard и традиционных банковских инструментов. Но они чувствовали потенциал технологии, и при условии, что разработчики будут продолжать ее совершенствовать и развивать, когда-то Bitcoin будет стоить один доллар вместо одного цента. Кто-то просто решил сохранить круглую сумму, например в 1000 биткоинов. Появились пулы совместной добычи монет, чтобы несколько слабых компьютеров смогли совместными усилиями увеличить шанс на поиск блока. Если кому-то одному везло, то награда делилась на всех, пропорционально объему вычислительной мощности, которую каждый участник совместного пула вложил в него. Например, у одного человека компьютер слабый, и он может дать только 15 процентов от общей вычислительной мощности пула, у двоих компьютеры мощнее – они дадут по 25 процентов, а у четвертого участника будет суперкомпьютер, дающий 35 процентов. Таким образом, если пользователь с самым мощным компьютером найдет блок, то он должен будет справедливо поделить его на всех: забрать себе 35 процентов,

а остальным раздать по мере их вложения в мощность. Если блок нашел участник с меньшей мощностью, он также делит награду на всех. Со временем люди, объединившиеся в пулы и сгенерировавшие какое-то количество совместных монет, разошлись: кто-то продал компьютер, а кто-то просто отключился, но монеты все равно никуда не делись.

Были и такие участники экосистемы, которые не копили полученные монеты, а сразу пускали их в оборот, обменивая на доллар (либо на другую криптовалюту) или на какие-то услуги. Что надежнее и практичнее: сразу обменять и получить услугу или деньги или все-таки их приберечь? Ответ, конечно, зависел от времени. До сегодняшнего дня их явно стоило хранить. Было эффективно покупать оборудование и монеты год, два, три назад и накапливать биткоины и другие криптовалюты, чтобы сейчас потратить лишь малую часть, получив огромную прибыль.

В пользу того, что стоит накапливать криптовалюту, говорит и тот известный случай, благодаря которому 22 мая мы отмечаем Bitcoin Pizza Day – день биткоин-пиццы. Речь идет о 2010 году, когда Bitcoin стоил очень мало и программист из Лас-Вегаса Ласло Ханеч предложил на Интернет-форуме оплатить доставку 2 пицц с помощью биткоинов, намереваясь потратить на это 10 000 биткоинов. Тогда это было лишь 25\$. Кто-то поверил, что проделанная вычислительная работа для накопления десяти тысяч Bitcoin была существенной – несколько дней работы, не выключая компьютер. А пекарь потратил 15–20 минут на то, чтобы сделать и испечь пиццу. В принципе, это неплохо обменять: получасовой труд, себестоимость которого десять долларов, на труд профессионального вычислительного устройства и человека с более ценной профессией. Кто-то из пользователей форума принял правильное решение – обменять достаточно дешевый, массовый продукт на что-то уникальное и, возможно, перспективное. Не думаю, что тот, кто оплатил своими наличными деньгами доставку пиццы в Papa John's, свято верил, что когда-то причитающиеся ему Bitcoin будут стоить десятки миллионов долларов! Никто не предполагал, во что превратились те две пиццы сегодня. Если же представить, что получатель транзакции принял правильное решение – сохранить хоть 1/10 часть тех монет, то у него все хорошо. Спустя много лет, в 2018 году, Ласло опять повторил свой эксперимент и заплатил за две точно таких же пиццы уже 0,00649 биткоина (что-то около 60 долларов). При этом Ласло использовал для последнего платежа усовершенствованную технологию Lightning Network.

Если говорить про транзакции, когда нужно заплатить Bitcoin человеку, который сталкивается с криптовалютами впервые, но готов их принять, то ему первоначально нужны будут кошелек и адрес, на который он получит свои Bitcoin. Вы вводите в нужное приложение адрес кошелька, как номер карты или счета, вводите сумму, которую нужно отправить, у некоторых клиентов можно регулировать комиссию – повысить ее, чтобы ускорить транзакцию, или наоборот. Если сеть не перегружена, то можно поставить комиссию поменьше, все равно она пройдет в те же сроки, что и дорогая. Причем размер комиссии не зависит от суммы отправки, а лишь от состояния пула транзакций – есть ли очередь на их проведение или нет. После определения суммы и комиссии вы нажимаете «отправить». Ввели пароль, если он установлен, нажали «ОК» – остается ждать, когда майнер, как узел обработки транзакций, включит транзакцию в блок и будет получено не менее трех подтверждений от других узлов сети. В любое время в открытом реестре вы можете посмотреть судьбу вашей транзакции. Программа-кошелек сообщит ваш Transaction ID, то есть идентификатор транзакции. Вы можете контролировать исполнение платежа с помощью обозревателя блоков, специального веб-сервиса, как «Яндекс» для блокчейна. Сегодня такие обозреватели блоков, как blockchain.info, уже не просто сайты, хранящие реестр, – на них собирают аналитику, полезную информацию по количеству кошельков и распределению их по странам: какова общая вычислительная мощность и сложность сети, среди каких пулов и в каком процентном соотношении распределена эта мощность, сколько есть брошенных адресов с ненулевыми балансами и какие из них самые дорогие. Итак, введя в поле поиска свой адрес, или адрес получателя, или идентификатор транзакции, вы видите ее статус – передана в сеть или нет, не подтверждена или уже имеет несколько подтверждений. Как только майнер найдет блок и

включит именно вашу транзакцию в этот блок, статус обновится до одного подтверждения. Когда ближайшие по доступу в Интернет узлы от этого майнера также включили в свою цепочку этот блок, то есть подтвердили его валидность, то появляются второе, третье и следующие подтверждения. Тогда и продавец, например, которому вы отправили оплату, может спокойно передать вам товар. В среднем проведение транзакции происходит в течение получаса. Транзакция может пройти и раньше, а при установлении низкого размера комиссии, наоборот, зависнуть на многие часы.

Помимо рядовых энтузиастов первыми начали принимать Bitcoin не банки или бизнесы «у дома». В первую очередь оплата криптовалютой принималась сервисами, продававшими цифровые товары и услуги, может быть, даже не очень приличного содержания. Например, порнографические ресурсы, сайты по продаже нелегальных товаров, для которых важна анонимность. Затем это, конечно же, работники IT-сферы, которые продавали товары на досках объявлений или подобных торговых площадках. Также компании, предоставляющие сервисы хостинга и регистрации доменов, достаточно активно внедрились в эту историю. В России впервые возможность оплаты Bitcoin я увидел как раз на сайте хостинг-провайдера. У него я мог продлить домен, купить дисковое пространство, оплатить хостинг сайта или арендовать сервер за Bitcoin.

Сейчас я храню немного биткоинов, хотя это не единственная криптовалюта, которая у меня есть. Bitcoin в моем портфеле занимает примерно 10–20 %, затем от 30 % до 50 % в валюте Ethereum, а остаток в различных проектах меньшего масштаба. В силу того, что в молодости увлеченно копался в устройстве компьютера, я участвую в майнинге криптовалют с помощью процессоров и видеокарт, а не с использованием специализированных ASIC-майнеров. Для меня понятнее собственная сборка реального сервера с помощью общедоступных компонентов, которые при возможном падении рынка не превратятся в дорогостоящий цифровой мусор. Иногда, когда я хочу почувствовать, что криптовалюта что-то мне приносит, я меняю часть монет на фиатные деньги, чтобы покрыть ежемесячные издержки или купить новое оборудование для майнинга. В основном я делаю это в маленьком объеме, т. к. верю в еще больший рост криптовалютных активов в будущем, хотя падение 2018 года больно ударило по моему карману.

Гуляют в сети и курьезные случаи, связанные с потерей Bitcoin. Например, парень поспорил с подругой, она разбила ноутбук и выкинула его в помойку, а спустя три года этот человек пошел искать, не найдется ли где-нибудь на свалке жесткий диск от этого ноутбука. На самом деле жесткий диск не важен, главное, чтобы сохранился файл резервной копии кошелька, пароль или закрытый ключ. Ведь если они у вас есть, восстановить доступ к кошельку на другом устройстве не составит проблем. Это все равно что сейчас потерять смартфон с приложением «Сбербанк онлайн», но при этом свой банковский счет вы не потеряете. Вы купили новый, скачали и вошли в приложение, ввели логин и пароль – все ваши деньги остались на счету. Так же и криптовалютные монеты никуда не денутся с потерей оборудования, если вы позаботитесь о резервных копиях и паролях. Поэтому очень важно не только иметь монеты, но и знать, как их не потерять.

## **Черный рынок как катализатор роста популярности криптовалюты**

Понимая специфику сделок на черном рынке, можно предположить, что именно он помог биткоину вырасти до тех масштабов, когда и традиционные предприниматели, и инвесторы решили применять технологию в сфере платежей. Почему черный рынок? Предположим, кто-то захотел купить запрещенный к обороту товар. Естественно, покупатель не может отправить на карточку или на счет какого-то юридического лица средства и написать, что это «оплата за оружие». Даже если покупатель замаскирует назначение платежа, ему не хотелось бы раскрывать свою личность, если вдруг продавца поймают и он все расскажет правоохранительным органам. Самому продавцу также не хотелось бы, чтобы попавшийся полицейским покупатель сказал, что приобрел товар именно у него. Встал вопрос

анонимности сторон сделки и платежей между ними. Традиционным способом в подобных сделках всегда выступали наличные, но был риск, что купюры будут мечеными или номера будут записаны при контрольной закупке. Тем не менее идеальным сценарием незаконной сделки остается покупка товара под вымышленным именем и осуществление оплаты наличными. Стороны знают лишь минимум необходимой информации друг о друге, деньги и товар передаются быстро, в некоем условном месте – возможно, публичном. Это считается анонимной сделкой, несмотря на то, что стороны видели лица друг друга. Существует огромная вероятность, что продавец и покупатель никогда больше не встретятся и не появятся в этом месте, поэтому можно считать такую сделку условно безопасной, при этом понимая, что все-таки нарушен закон и сторонам грозит за это ответственность. Однажды кто-то из дельцов, так или иначе задействованный в незаконном бизнесе, понял, что с помощью биткоина достаточно легко добиться анонимности при первоначальном отсутствии доверия. Тогда уже существовали первые обменные пункты, и, ко всему прочему, в августе 2010 года вышла памятная статья о биткоинах на сайте Slashdot, подогревшая и без того растущий интерес к блокчейну и биткоину. Уже существовала возможность посмотреть котировку Bitcoin на определенный день, чтобы привязать ее к какой-то стоимости в долларах. Тогда, соответственно, и начал развиваться черный рынок.

Надо оговориться, что черный онлайн-рынок был бы невозможен без создания в начале 2000-х годов проекта DarkNet – темной стороны Интернета, в который можно попасть через анонимизированные прокси-серверы и так называемую луковую маршрутизацию – Tor. Программное обеспечение Tor позволяет передавать информацию в зашифрованном виде по сети виртуальных тоннелей, делая соединения сторон полностью анонимными. В феврале 2011 года, объединив технологии Tor и Биткоин, американский предприниматель Уильям Росс Ульбрихт создал анонимную торговую площадку Silk Road – Шелковый Путь – для покупки изменяющих сознание веществ, ставшую впоследствии синонимом успеха на поприще незаконной торговли психотропными веществами и пиратским контентом. Площадка просуществовала по октябрь 2013-го. Конец был предсказуем: организатор арестован, как и его активы. Но необходимо обратить внимание на цифры, которые стали достоянием публики в результате расследования ФБР. Страшный пират Робертс (Dread Pirate Roberts) – именно таков был псевдоним Ульбрихта в ДаркНет – провел 1,2 миллиона сделок на общую сумму 9,5 млн биткоинов, получив в качестве комиссий 600 тыс. биткоинов, что приближалось к круглой сумме в 50 млн долларов на начало 2013 года, однако уже к концу того же 2013-го она перевалила за полмиллиарда долларов, но ими наш антигерой воспользоваться не успел. Чем важны эти цифры? Давайте посмотрим на общий объем выпущенных биткоинов в обороте на начало 2013 года – он составлял около 12 млн единиц, 80 % из которых никогда не участвовали в транзакциях. Часть рынка, занятая легальными инвесторами и теми же простыми пользователями Биткоин, коих насчитывалось уже несколько сотен тысяч, принадлежала бирже MtGox, и наверняка обороты биржи и пиратской площадки сильно пересекались. Различные источники сообщают о доле рынка Биткоин, обслуживаемой MtGox, не менее 50 %. Можно предположить, что несколько миллионов «активных» биткоинов курсировали между этими двумя площадками, создавая самый главный плюс биткоину – распространение его в массы. Сотни тысяч покупателей на Шелковом Пути, которых в реальности могло быть меньше в разы, из-за возможности одного пользователя создавать неограниченное количество кошельков Биткоин, и всего не более 10 тысяч пользователей с ненулевым балансом на крупнейшей на тот момент бирже MtGox – показатель важности ресурса Silk Road в становлении биткоина. И сегодня последователи Ульбрихта не сдают свои позиции, достоверных данных о доле глобального рынка, занятой ими, нет, однако можно с уверенностью сказать, что эта доля весьма существенна.

## Появление новых монет

Так как Bitcoin реализовывался как проект с открытым кодом, любому желающему

можно создать свои монеты на его основе, скопировав исходный код и внося в него свои правки. Изменить название, модифицировать алгоритм добычи монет, настроить свои сетевые узлы, собрать сообщество пользователей и команду разработчиков... В самом начале эта задача была под силу только небольшому числу профессионалов, но сейчас существует множество подробных иллюстрированных инструкций, как можно сделать форк (от англ. *fork* – вилка, ответвление) той или иной монеты или даже заказать его практически моментальное изготовление на специализированном сайте. Можно сделать и последующий форк предыдущего удачного форка. Другое дело, что в сегодняшнее время количество монет огромно и полезность минимум 90 % из них вызывает сомнения. Такие «дочерние» монеты принято называть альткоинами – альтернативными монетами. Например, первым задокументированным форком был namescoin – монета, из названия которой видна связь с английским словом «имя» – name, что вкратце отражает ее суть. Namescoin предлагает пользователям доменные имена в зоне .bit и систему альтернативных традиционным DNS (domain name servers) – систему адресации доменных имен. Выход монеты датируется сентябрем 2009-го, спустя чуть более полугода после биткоина. Следом появляется «облегченный» биткоин, что также нашло отражение в названии монеты – litecoin – от англ. *lite* – облегченный, упрощенный. Создатель лайткоина Чарли Ли анонсировал ее в октябре 2011 года, спустя целых 2 года после появления первого форка. Как мы помним, на начало 2011 года пришлось множество значимых событий в мире криптовалют. Появление лайткоина также, несомненно, является таковым. И если неймкоин по общей капитализации занимает место в начале четвертой сотни популярного ресурса CoinMarketCap (рейтинг монет по рыночной капитализации и не только), то лайткоин уверенно держится в десятке лидеров.

Сегодня альткоинов, со своим доработанным, собственным уникальным кодом и даже структурой блокчейна, уже несколько сотен. Но необходимо понимать, что некоторые платформы, такие как Ethereum – Эфириум или просто Эфир, созданный нашим бывшим соотечественником Виталиком Бутериным, предлагают создать собственный токен, как бы дочернюю монету внутри проекта, не создавая свой блокчейн и соответствующую инфраструктуру. Уже тысячи монет-токенов являются составной частью платформы Ethereum. Существует также платформа BitShares (цифровые акции или доли), где можно превратить в цифровой актив что угодно, например, долевое участие в пляжной недвижимости или доходы от рекламы на Интернет-сайте. Можно в этом же ключе упомянуть платформу Waves (волны) от российских разработчиков, возглавляемую Сашей Ивановым, которая позволяет создать внутренний токен и начать торговать им на внутренней бирже за считанные минуты.

Одной из уникальных и популярных на сегодняшний момент криптовалют является монета Dash, созданная в 2014 году известным криптоэнтузиастом Эваном Даффилдом. Ранее монета называлась Darkcoin (а при создании носила имя Xcoin) и позиционировалась как монета для полностью анонимных и по-настоящему моментальных транзакций, которые проходят лишь за пару секунд. Эван объединил 11 алгоритмов хеширования в комбинированный алгоритм x11, что должно было спасти блокчейн Dash от вездесущих ASIC-устройств, угрожавших децентрализации криптовалют, что уже настигло биткоин и лайткоин. Также ставку на анонимность сделали создатели монеты monero (с эсперанто – монета), появившейся как форк монеты ByteCoin (байткоин). В 2017-м мир узрел еще одну монету, с упором на анонимность и быстроту – Zcash, которая обеспечивает приватность отправителя, получателя и суммы транзакции. В названии буква Z – от словосочетания zero knowledge (доказательство с нулевым разглашением), намек на возможность подтверждения верности транзакций, не имея никакого представления о другой стороне. Если в Bitcoin и большинстве других монет по адресу кошелька или идентификатору транзакции можно узнать всю информацию о получателе и отправителе, то благодаря ZK узнать эти данные нельзя.

Также Dash отличается от собратьев тем, что имеет гибридную систему консенсуса. То есть для подтверждения транзакций нужны не только майнеры – физические вычислительные устройства, но и стейкхолдеры (хранители монет), имеющие минимум по тысяче монет в

кошельке и установившие на сервере специальное программное обеспечение, именуемое MasterNode или «главный узел». Это узел, который также помогает обрабатывать транзакции, получая вознаграждение за свою работу. Случайно выбранные мастерноды участвуют в генерации блоков и обеспечивают дополнительную стабильность и анонимность. Одна беда – стоимость дэша выросла настолько стремительно, что владение 1000 монет вам обойдется в четверть миллиона долларов (по состоянию на середину 2018 года).

По ценности, естественно, все монеты отличаются друг от друга, причем иногда сложно соотнести, почему одна монета стоит дороже другой, хотя технологически и идейно она гораздо хуже. На цену сильно влияет фактор сообщества. Например, вокруг Dash сформировалась определенная группа разработчиков, которым верят, они известны в своей среде и их профессионализм и идейная составляющая не вызывают сомнений. Планы команды грандиозны и многообещающи. Пользователи Dash активно помогают команде разработчиков в достижении этой цели, приобретая и храня монеты, вводя их в ежедневный обиход. В максимальных значениях января 2018 года стоимость одного дэша доходила до 1,5 тысяч долларов.

Существуют утилитарные монеты, например, EmerCoin, созданный по типу криптовалюты № 2 неймкойн для того, чтобы можно было покупать и оплачивать услуги компании, оперирующей доменами в нескольких зонах, таких как. coin,lib,emc и. bazar, также выдающей SSL-сертификаты, подтверждающие безопасность и действительность владеющего им сайта, работающие на технологии блокчейн, а также DNS-серверы, системы хранения, учета авторских прав и прочих полезных задач в сфере IT-технологий. Все эти услуги можно приобрести за эмеркойн. Наличие утилитарной ценности является очень большим подспорьем для монеты и привлекает в ее экосистему не просто спекулянтов и дельцов, а целевую аудиторию, гарантируя проекту последовательный рост и развитие.

На рынке существует проект Augur, токен которой позволяет пользоваться оракулом. В криптовалютах оракул – программно-аппаратный комплекс, позволяющий производить миграцию данных из блокчейн в традиционные централизованные базы данных или обмен информацией между разнотипными проектами.

Хотелось бы упомянуть монету Gamecredits, форк Litecoin, которая пыталась стать одной из первых внутриигровых криптовалют для сетевых, браузерных игр и игр для смартфонов. Она интересна как пример хорошей идеи внедрения криптовалюты в индустрию игрового бизнеса. В большинстве игрушек, которые вы скачаете в приложениях Google Play и Apple Store, существует понятие «донат», когда вы финансируете разработчика путем покупки внутриигровых товаров и ресурсов за реальные деньги. Например, играете вы в какую-либо игру, и вам нужно повышать способности своего персонажа путем покупки либо навыков, либо брони и оружия, что даст вам преимущество над другими игроками. Зачастую такие улучшения можно купить только за самый дорогой ресурс в игре (например, некие кристаллы), который нужно либо очень долго искать и копить, либо проще приобрести за реальные деньги. В каждой игре за донат предлагают приобрести не только обмундирование и косметические улучшения для вашего персонажа, но и различные постройки, виртуальных животных и многое другое. Для оплаты таких внутриигровых покупок и могли существовать монеты наподобие Gamecredits, которые обеспечили бы меньшую комиссию, быстроту транзакций для игроков, а также упрощенную интеграцию в уже созданную игру для сторонних разработчиков. Т. е. один и тот же ресурс может вводиться и выводиться из разных игр, делая возможным и продажу игровых вещей, и даже целиком аккаунта со всем игровым имуществом. Проблема лишь в том, что проект до сих пор остается на уровне идеи, в сообществе поползли слухи о том, что за время с момента привлечения проектом средств и до осени 2018 года ничего толком не сделано. Но монета Gamecredits не единственная в своем роде, сегодня существует ряд уже внедренных в игры блокчейн-активов, чей функционал вполне реализован и применим.

## **Обменные пункты и криптовалютные биржи**



Свершению первой обменной операции в сети Биткоин способствовал один очень важный момент, а именно появление у Сатоши Накамото одного важного сторонника в лице финского студента Университета технологий в Хельсинки – Марти Малми (Martti Malmi). Марти заинтересовался идеей биткоина и поздней весной 2009 года связался с Сатоши, предложив ему помощь в продвижении проекта, при этом уже опубликовав несколько сообщений о нем на сторонних ресурсах, связанных с анархическими воззрениями и борьбой с диктатурой государств в лице их центробанков. Сатоши предложил Марти взять на себя функцию редактора сайта bitcoin.org, и за короткое время ресурс преобразился до неузнаваемости – конечно, в лучшую сторону. Далее совместными усилиями был создан форум bitcointalk.org, где Марти выступает под ником Sirius. В одном из обсуждений некто под ником NewLibertyStandarts (Новые Стандарты Свободы) поднял вопрос о необходимости создания площадки для обмена биткоина на фиат. Тогда, 12 октября 2009 года, Sirius переслал, а NLS получил 5050 биткоинов и взамен перечислил 5,02 долларов США через платежную систему PayPal. Упоминание об этом событии есть в Твиттере Марти. Итого первый официальный обмен биткоинов на фиатные деньги состоялся по цене 0,00099 доллара США за BTC! Уже немногим позже NLS запустил обменник по адресу newlibertystandard.wetpaint.com, а Марти в том же 2009 году не поленился создать собственный ресурс bitcoinexchange.com.

В это же время появляется сервис по внебиржевому обмену, построенный на базе чата IRC, по функционалу похожего на привычные нам мессенджеры. В старейшем канале Bitcoin-otc была создана площадка для торговли биткоином, позднее получившая дополнительный функционал в виде бота gribble, следящего за созданием книги заявок, авторизацией и рейтингом доверия пользователей. Сейчас канал находится в упадке, т. к. сам IRC-чат малопопулярен, а количество более удобных сервисов возросло в разы.

Вышеописанные операции можно назвать p2p-обменом или ручным обменом, когда сделка происходит между двумя участниками без посредника. До сих пор многие обменники действуют по такому принципу и функционируют лишь как площадка, позволяющая сторонам найти друг друга. Ярким примером служит ресурс localbitcoins.com, ныне заблокированный Роскомнадзором в РФ на основании решения Приморского районного суда Санкт-Петербурга. На нем было возможно купить и продать криптовалюту «с рук», при этом были нередки случаи мошенничества, что является основной проблемой прямых сделок. Для жителей других стран ресурс продолжает работать и не теряет свою популярность поныне.

Биржа, как централизованный посредник, появилась в сфере криптовалют почти сразу, как только цена биткоина выросла до значений, схожих с рынком акций. Наиболее известной биржей тех времен остается MtGox, начавшая операции в 2010 году. История биржи полна трагических моментов, и ее финал в виде банкротства в 2014 году стал апогеем этой трагедии. Более подробная информация содержится в открытых источниках, и нет смысла останавливаться на судьбе отдельно взятой биржи. Нам же важно, что уже через два года количество бирж исчислялось десятками, а через пять лет уже сотнями. Шли годы, менялись интересы и требования сообщества, также менялся рейтинг криптовалютных бирж. Золотой 2017 год принес рынку новых героев, при этом старая гвардия не потеряла бойцов. Сегодня в листинге популярного инструмента coinmarketcap содержатся данные об обороте криптовалют на более чем 200 биржах. Из них только 5-10 я использую как инструмент. Не все из них работают как централизованный посредник, многие являются децентрализованными биржами, где обмен происходит непосредственно в блокчейне, например на платформе Bitshares.

Еще больше существует обменных сервисов, которые растут как грибы и так же часто исчезают в небытии. Сложно предположить количество электронных площадок по обмену криптовалют. Наверняка я не совру, если назову цифру в десятки тысяч в мировом масштабе. Живых же обменников не так много, особенно в России. Только в 2016 году начали появляться публичные точки, а также биткоин-банкоматы, пока позволяющие только односторонний

обмен рублей на биткоин или на некоторые другие популярные криптовалюты. В этом плане лидируют Европа и США, впрочем, не отстает и Азия, особенно индустриально развитые страны.

Надеюсь, с принятием законодательства, закрепляющего базовые понятия и отношения в сфере криптовалют, и наша страна догонит и перегонит мировых лидеров – с учетом наличия интеллектуального ресурса, большого комьюнити и ряда других позитивных факторов это вполне возможно.

## Формирование стоимости криптовалюты

Как же формировался курс обмена на первых порах? Как и ожидалось, за основу был взят расчет средней стоимости электроэнергии в США, потребленной одним процессором (хорошего уровня, работающего у самого NLS) в год, что составляло 1331,5 кВт/ч. При средней цене электроэнергии в 0,1136 доллара выходило, что работа процессора будет стоить 151,2584 доллара в год. Далее эта сумма делилась на 12 месяцев, а затем на количество биткоинов, сгенерированных этим процессором за предшествующие 30 дней. В то время с помощью хорошего процессора легко было сгенерировать 11 блоков в день по 50 монет в каждом, что давало 330 блоков или 16 500 биткоинов в месяц. Теперь эти цифры легко подставить в расчеты и получить стоимость 1 биткоина на уровне 0,000764 доллара США, итого на 1 доллар можно было приобрести 1308,9 биткоина. Нужно признать, что сделка между NLS и Sirius прошла по несколько иному курсу, и уже через несколько недель курс биткоина вырос и составлял 700–800 монет за 1 доллар США. Да, тогда считали именно количество биткоинов, необходимых для покупки 1 доллара США, а теперь мы считаем количество долларов США, необходимых для покупки 1 биткоина.

В дальнейшем формула расчета стоимости добычи 1 биткоина изменилась в связи с ростом интереса к майнингу и включению в добычу разного типа процессоров. Брался в расчет средний объем генерации блоков в день за предшествующий год и делился на среднюю стоимость электричества и Интернета в день. Цифра все равно оставалась условной, т. к. существовала большая разница между тарифами на Интернет и электроэнергию, стоимость разного типа процессоров и компьютера в целом в разных странах и регионах. Позднее в расчет стали включать стоимость амортизации оборудования, тариф на Интернет и аренду помещения, т. е. расчет приобрел более реальный экономический базис.

Сегодня в формировании стоимости биткоина большое значение играют спекулятивные факторы. С приходом трейдеров из мира Форекс в криптовалюты и появлением бирж, позволяющих торговать с плечом, стало заметно влияние крупных капиталов на стоимость биткоина и других монет. Трейдеру неважно, растет монета или падает, важно сделать верную ставку. Майнерам же, особенно пришедшим на рынок достаточно поздно, не имеющим старых запасов монет и сгенерированных по дешевой себестоимости, такой подход в корне не подходит. Для них важны именно рост актива и как минимум превышение цены продажи над себестоимостью генерации. Трейдеры же могут манипулировать рынком, заставляя цену ползти то вверх, то вниз. Это приводит к высокой волатильности курса и повышает риски участия в процессе для людей, не обладающих должными знаниями и морально-волевыми качествами.

А что же другие криптовалюты, особенно те, которые не создаются путем майнинга, а печатаются сразу в полном объеме эмиссии или же генерируются с помощью алгоритма PoS или узлами обработки транзакций – Мастернодами? Как формируется их стоимость? Здесь многое зависит от того, как себя ведет команда разработчиков монеты. При запуске проекта цена монеты, имеющая ограниченную эмиссию, может принимать значение, равное себестоимости реализации проекта, деленной на общее количество монет, выпущенных в первую фазу реализации проекта. Например, всего монет 21 млн, из них 1 миллион поступает в предпродажу, и смета реализации проекта также равна 1 миллиону. Легко привязать стартовую стоимость монеты к 1 доллару, рублю или иной валюте. Дальнейшая реализация

проекта будет способствовать росту монеты, а если объем дополнительной эмиссии рассчитан правильно, прирост денежной массы за счет генерации новых блоков не даст цене монеты снижаться. Например, за год будет сгенерировано еще 0,5 млн монет, а оценочная капитализация компании вырастет до 3 млн, значит, цена монеты составит уже 2 доллара. Пример очень простой и утрированный, но нужно понимать, что сейчас на рынок выходят сотни новых проектов ежемесячно, они сами формируют первичную цену размещения, порой без какого-то экономического моделирования будущих процессов и без привязки к микро- и макроэкономике. Хватает и откровенно мошеннических проектов, когда под светлую идею собираются средства, делаются минимальные шаги по выводу монеты на биржу и запуску минимального среднестатистического функционала, далее монеты организаторов проекта распродают, цена монеты падает и продолжает снижаться до нуля. Все. Никакие действия сообщества или крупных игроков не спасут такую монету от краха. Стоит также упомянуть, что рынок альткоинов очень зависим от биткоина. Растет он – растет большинство альткоинов, курс падает – за ним катятся и остальные.

Хочется еще кратко описать так называемые «стабильные монеты» – StableCoins, которые привязаны к традиционным активам, например к золоту. Здесь цена монеты или токена напрямую связана с биржевым курсом актива. Если монета привязана к грамму золота, т. е. вы можете обменять ее на реальный металл, находящийся в хранилище оператора, то никакие факторы, влияющие на обычные криптовалюты, не смогут обрушить цену в 2, 5 или даже в 10 раз, что наблюдается в некоторых неудачных криптопроектах. Однако не каждый StableCoin настолько стабилен. И вопрос здесь опять же в способе организации проекта. Возьмем очень известный и популярный проект Tether или TUSD – эквивалент 1 доллара США. Стабильность его курса должна обеспечиваться наличием на счетах или в хранилищах равного количества американских долларов. Вполне может быть, что вначале так и было. Однако позднее компания-оператор стала проводить бесконтрольную эмиссию, а уровень обеспечения реальными долларами никому не известен. Гуляли слухи о том, что аудит активов выявил отсутствие какого-либо обеспечения вообще. Хотя чему удивляться, сам американский доллар и большинство мировых валют – это только обещание, ничем не подкрепленное, по сути – цветной фантик.

## **Первые сообщества криптоэнтузиастов**

Основной проблемой в России является непопулярность криптовалют в официальном деловом обороте, возможно, некий страх перед публичным применением, основанный на несовершенстве текущего законодательства РФ в сфере обращения криптовалют. Если открыть приложение для смартфонов Bitmapp, которое показывает точки на карте, где можно потратить, купить или продать Bitcoin, то вся Европа и США будут покрыты геометками с описанием типа сервиса, будь то магазин, бар, банкомат и прочее. В то время как на всю Россию наберется чуть более десятка точек. На огромную карту, составляющую одну седьмую территории суши, приходится всего несколько зафиксированных магазинов, которые готовы рассказать, что они работают с Bitcoin или другой криптовалютой, а также единичные обменные пункты или банкоматы. Конечно, реальное количество сервисов гораздо больше, но ведь та же картина и за рубежом. Сервисы, добавленные в приложение, едва ли составляют четверть от общего их количества на территории того или иного региона. На какой вывод это наталкивает? Меня только на один – наше общество пока не готово широко принять криптовалюты публично, частично из-за проблем с законодательством, но в основном из-за недоверия, которое, в свою очередь, зиждется на банальном непонимании сути криптовалют и их перспектив. Для большинства людей это пирамида и пузырь, криминальные деньги и прочее. В других же странах приятие на всех уровнях гораздо шире, от рядовых граждан до элит и политических кругов. И это приятие случилось не в один короткий период, а постепенно.

Я уже упоминал о сообществе шифропанков, в среде которых зародилась часть технологий, примененных в Биткоине, и где обсуждалась «White Paper», написанная Сатоши Накамото и

распространенная через подписной лист рассылки шифропанков. Нельзя не согласиться, что многие из них были не просто людьми, а учеными, лидерами мнений, преподавателями в университетах. На такой благодатной почве зерна знания не могли не прорасти. К шифропанкам подключились математики и программисты, для кого было просто увлекательным разобраться в новинке. Многие программисты, как активные участники IT-сообщества, заинтересовали своих друзей, не относящихся к профессиональной касте программистов, но разбирающихся в «железе» – компьютерах и их устройстве. И здесь уже начался рост аудитории по нарастающей – компьютерщик привлек финансиста и бизнесмена, трейдеры с валютных рынков разглядели новые возможности, а где-то в параллельном потоке росла армия людей, использовавших криптовалюту в нелегальных схемах. Я уже упоминал об объеме торгов на площадке Шелковый Путь и вероятном количестве ее пользователей. Как-никак это огромная часть сообщества, своими действиями популяризовавшая биткоин. Где же формировались сообщества и до сего времени можно найти исторические записи и посты? Конечно, первый открытый источник – это [bitcointalk.org](http://bitcointalk.org), где до сих пор обсуждается львиная доля проектов в области блокчейн и криптовалют, а количество зарегистрированных пользователей превышает 2 млн. Нельзя не упомянуть площадку [reddit.com/r/Bitcoin](http://reddit.com/r/Bitcoin), где уже в декабре 2010-го началось обсуждение биткоина. Сегодня в канале 1 млн подписчиков. И таких больших и маленьких групп тысячи. Более продвинутые пользователи пишут инструкции и разъяснения для новичков, новички высказывают свои мнения и идеи, обсуждаются новости и перспективы...

Сложно сказать, когда произошел переломный момент и ранее фантастическая идея созрела и начала давать плоды в виде перехода от сотен последователей к тысячам и миллионам. Для России это, несомненно, 2017 год, когда бурный рост рынка заставил даже скептиков проявить осторожный интерес к происходящим процессам, а некоторых даже кардинально изменить свою точку зрения на криптовалюты или как минимум технологию блокчейн, стоящую за ними. В 2016 году конференции по криптовалютам не собирали порой и половины арендованного зала. В 2017-м все залы были переполнены, что также привело к махинациям на так называемом «хайпе» – всеобщем интересе к предмету. Появились посредственные спикеры и организаторы, мусолившие одни и те же постулаты по 10 раз, рассказывающие чужими словами совсем уж базовые понятия и не дававшие никакой практической пользы посетителям. Однако сегодня каналы обсуждения криптовалют в мессенджерах, группы в социальных сетях и другие средства коммуникаций насчитывают сотни тысяч подписчиков из русскоязычной аудитории. На Западе новостной фон в сфере криптовалют на телеканалах и иных глобальных СМИ сформировался гораздо ранее, и уже в далеком январе 2012-го биткоин был удостоен отдельной серии под названием «Биткоин для тупиц» в сериале «Хорошая жена», где в авторском видении представлен процесс поиска Сатоши Накамото и где обсуждалась сущность самого биткоина с очень импонирующими мне выводами. Этот сериал, а также традиционные сообщения в СМИ увидели и поняли миллионы человек. Нужно ли говорить, что сегодня жители США – это самые крупные игроки на рынке криптовалют?...

В конце главы хотелось бы упомянуть, что часть криптовалютного сообщества создала и приняла симбиоз криптовалют и социальных сетей в виде новой формы социальных медиаплатформ. Такие проекты, как Стимит ([steemit.com](http://steemit.com)) и условно российский Голос ([golos.io](http://golos.io)), предлагают вознаграждение в криптовалюте за создание постов, лайки, комментарии... На системе блокчейн развивается и социальная сеть Nimses, где внутренняя криптовалюта может быть также заработана за оценки ваших постов, передана любому пользователю или сгенерирована за счет банального участия в системе – просто за проведенное в ней время. Можно сказать, что раньше сообщество было двигателем криптовалют, а теперь некоторые монеты становятся базисом, топливом для развития сообществ.

## Бурный рост числа монет и токенов

Токен – это транслитерация английского слова *token*, которое означает «жетон». Многие считают, что понятия «токен», «монета» и «криптовалюта» – это одно и то же, но это не совсем так. Я бы сказал, что это почти одно и то же в общем смысле, но разные субстанции в деталях. И токен, и монету, несомненно, можно назвать криптовалютой. Между ними можно провести черту, если обозначить, что монета – это отдельная экосистема, платформа со своим протоколом и

программным обеспечением, в конце концов своим уникальным блокчейном, а токен – это подвалюта внутри этой платформы, как некий субсчет в бухгалтерском учете. Это можно сравнить с наличием у вас основного счета, который привязан к пластиковой карте, и дополнительных счетов: пенсионного или валютного. Проще всего разница видна на примере Эфириума. Изначально есть сама монета Ethereum со своей экосистемой, но с помощью определенного кода (смарт-контракта), загружаемого в блокчейн Эфириум, вы можете создать токен внутри Ethereum. То есть для отправки и получения этих токенов будет использоваться функционал блокчейна и, конечно, расчетные финансовые единицы Ethereum. Токен в данном понимании никогда не станет самостоятельной платформой и без Ethereum существовать не сможет. Обязательно должна быть базовая среда – виртуальная машина Ethereum, в которой будут производиться транзакции и учет всех созданных токенов. Чтобы вы могли расплатиться токенами с другим пользователем, у обеих сторон должен быть кошелек Ethereum, который поддерживает токены. При этом на один и тот же адрес Ethereum в поддерживающем токены кошельке могут поступать токены из различных проектов в неограниченном количестве, как по объему, так и по номенклатуре. Вы также можете без проблем покупать и продавать токены на биржах, вообще не имея локального кошелька Ethereum. Биржевые аккаунты позволяют вам генерировать неограниченное количество Ethereum-адресов, и у вас будет отдельный адрес конкретно под каждый токен и абсолютно уникальный для монет ETC. Использовать биржевой адрес Ethereum для перевода на него токенов нельзя, так же как нельзя посылать ETC на адрес, сгенерированный под отдельный токен. При участии в ICO часто можно увидеть предупреждение, что вы не должны переводить Эфир на адрес смарт-контракта ICO с биржевого аккаунта, т. к. токены в данном случае будут попросту потеряны.

Количество монет со своей платформой для выпуска токенов не так уж велико: уже упомянутые проекты Ethereum и Waves, молодой EOS, ориентированный на Китай NEO, старый, но не нашедший широкого распространения блокчейн Bitshares также можно отнести к площадкам для выпуска криптоактивов. Есть ряд старичков и новичков – всего же, по данным ресурса coindata.vc, их общее число сегодня составляет восемнадцать. Широкое применение токены получили, когда на арену вышел Ethereum, ставший неоспоримым лидером среди площадок для коллективного финансирования проектов через криптовалюты. До появления платформы Ethereum сборы проводились по различным сценариям, а Виталик Бутерин ввел некий простой унифицированный вариант, задав стандарты для индустрии краудфандинга в криптоэкономике. Если верить исследованиям различных команд, объем средств, привлеченных с помощью краудфандинга в 2013 году, не превысил 0,8 млн долларов, а количество сколько-нибудь заметных проектов можно было сосчитать по пальцам одной руки. В основном это были проекты по созданию улучшений для биткоина или новых монет на основе биткоина, хотя платформа NXT представляла из себя программу, код которой был написан с нуля. Судя по информации из Википедии, NXT привлекла 71 биткоин, т. е. не более 10 тыс. долларов на тот момент. Однако платформа-таки появилась. Более удачлив был проект MasterCoin, ныне носящий имя OMNI Layer. Разработчики анонсировали надстройку над блокчейном Биткоин для решения массы задач, в т. ч. выпуска токенов, и привлекли для ее создания 5000 BTC, или рекордные на тот момент 0,5 миллиона долларов. В этом же году был представлен проект ProtoShares. Следующий, 2014 год принес урожай около 30 млн долларов, из которых больше половины пришлось на ICO-Ethereum, а общее число проектов было чуть больше десятка. Интересно отметить, что именно в 2014 году также стартовала менее удачливая платформа по выпуску цифровых активов Counterparty, на которой состоялся выпуск токена StorJ X – проекта децентрализованного хранилища информации, а также детище Дэна Ларимера – Bitshares как продолжение проекта ProtoShares, ставшее в будущем наиболее жизнеспособным конкурентом Ethereum. Также 6 млн долларов собирает первый токен на базе MasterCoin – MaidSafeCoin, призванный создать безопасную автономную распределенную сеть – децентрализованный Интернет. Кризисный для биткоина 2015 год стал не таким урожайным на ICO и принес лишь около 15 млн долларов, причем данные популярных агрегаторов ICO сообщают лишь о трех ICO за год – уникальный проект ЮТА для Интернета вещей (IoT), первый успешный токен на платформе Ethereum – рынок предсказаний (оракул) Augur, а также актив на платформе Counterparty – игровая валюта BitCrystals. Год начала бурного роста числа монет и проектов – 2016-й, он позволил собрать трем десяткам заметных проектов сумму более четверти миллиона долларов, 2017-й запомнился сборами в 6 млрд, а 2018-й перешагнул 10-миллиардный рубеж уже к середине года. Сборы ICO напрямую связаны с

появлением новых монет. Если до 2016 года появилось лишь несколько стоящих токенов OMNI, CounterParty и Bitshares, сегодня общее количество функциональных «живых» токенов или цифровых активов на трех вышеперечисленных платформах, плюс более-менее активных Waves и NEO, а также менее популярных NXT, NEM, Stellar и ряде молодых платформ не превышает сотни или едва перевалило за сотню, тогда как количество ликвидных токенов Ethereum уже гораздо больше тысячи, даже одной тысячи ста. Я не учитываю спам-токены, мошеннические токены-клоны имеющихся валют и активы, которые созданы ради смеха или эксперимента и не имели целью выход в массы с расчетом на долгую и успешную историю. Этот бурный рост произошел буквально за два года, с середины 2016-го по середину 2018-го, но именно 2013–2015 годы заложили его основу, явив миру платформы для создания цифровых активов, существующих поверх поддерживающих их функционал блокчейн-решений.

Также нельзя упустить из виду и моду на форки, появившуюся в том же 2016 году и набравшую гигантские обороты в 2017–2018 годах. Одних только форков монет на основе Dash и Pivx появились сотни благодаря необъяснимому интересу публики к монетам на основе алгоритма PoS, предлагающих минтинг с помощью мастернод. Также активно копировались Monero, разветвлялся отец-основатель биткойн и сегодняшняя валюта № 2 – эфир. Большой интерес к блокчейн и криптовалютам породил и большой спрос на новшества, соответственно – расширилось предложение. Не всегда качественное, но несомненно разнообразное и не без креатива.

Приведу упрощенный пример, как может появиться очередной токен. Допустим, мы с вами решаем, что хотим открыть издательство, которое готово напечатать книгу тиражом от 1 экземпляра любого автора и на любую тематику, а также издавать и распространять книги в цифровом виде. Для запуска необходим миллион долларов. Мы называем наш проект Publishing (издание) и называем наш токен New Publishing Token с тикером NPT. Начинаем кампанию по сбору средств, ведь мы понимаем, что не можем профинансировать вновь созданную фирму своими силами, но считаем, что это стоящая идея для того, чтобы продать ее некому сообществу. Мы заявляем, что нужно собрать миллион долларов, и выпускаем в свободное обращение миллион токенов, то есть один токен будет продаваться по одному доллару. Напомню, что технически это не будет отдельная монета, мы не запускаем свой блокчейн: мы не создаем отдельных кошельков для нашей монеты, не призываем владельцев вычислительных ресурсов поддерживать нашу сеть. Каждому, кто перевел эквивалент одного доллара, выдается цифровая акция проекта. Продажа акций и размещение токенов – это самая явная параллель, которую можно провести между традиционной экономикой и криптовалютой. Для того чтобы гарантировать собственное участие в прибылях, часть выпущенных токенов создается для нужд команды. То есть в продажу поступает 1 млн токенов, а 300 тыс., например, остается команде. Значит, изначально нужно предусмотреть в смарт-контракте генерацию именно 1,3 млн токенов, из которых 1 млн будет распродан. Если все пройдет успешно, можно ожидать и выполнения основателями бизнес-плана по созданию издательства, а мир увидит очередной токен NPT. Пользуясь такой простой логикой, самые разные люди с самыми разными проектами создают все новые и новые токены или отдельные монеты. Сегодня ресурсы, отслеживающие статистику по криптовалютам, содержат более 2500 наименований монет и токенов, а в будущем их будут десятки тысяч.

## Платформа Ethereum

Раз мы затронули тему Ethereum, я бы хотел вкратце рассказать и о ней, хотя тема вполне достойна отдельной книги. Как я уже писал выше, придумал и реализовал платформу Виталик Бутерин, сын российских экспатов, которые переехали в Канаду. Его отец занимался высокими технологиями и как-то раз рассказал сыну про Bitcoin. Виталик, с детства увлекавшийся компьютерами и математикой, сначала посомневавшись, все же с интересом взглянул на технологию, найдя в ней не только достоинства, но и недостатки. Первый деятельный интерес проявился в соавторстве и издании электронного журнала Bitcoin Magazine, выпускавшегося им при содействии румынского программиста Михая Алиси. Результатом погружения в суть процессов и переосмысления концепции биткойна стала своя white paper революционной платформы Ethereum, которая давала более широкий простор для творчества и раздвигала границы сфер применения криптовалюты.

Основное новшество платформы – это реализация предложенной Ником Сабо концепции смарт-контрактов или умных контрактов, представляющих из себя программный код для автоматического исполнения договоров, алгоритм переноса коммерческих контрактов с бумаги на язык кода (при наличии подготовленной среды, в которой возможно исполнение кода). Кстати, Java-подобный язык программирования Solidity, применяемый для написания смарт-контрактов, является тьюринг-полным языком, а значит, при правильном применении способен реализовать любую вычислительную функцию. Язык был предложен соратником Виталика Гэвином Вудом и доработан командой Solidity для использования в виртуальной машине Ethereum – среде исполнения смарт-контрактов и децентрализованных приложений. Смарт-контракт, однажды выложенный в сеть, нельзя изменить. Это важное свойство, дающее и достоинства, и недостатки. При обнаружении ошибок в коде изменить их не удастся. Придется создавать новый контракт. Также важным свойством смарт-контракта является неукоснительное выполнение условий сторонами, особенно обязательства внесения оплаты плательщиком. Только факт поступления средств от плательщика на адрес смарт-контракта может запустить механизм его реализации. Опять же, если речь идет об исключительно виртуальном, цифровом взаимодействии, плательщик может быть уверен, что при своевременной и полной оплате он получит то, за что платил.

Самым распространенным смарт-контрактом на сегодня является контракт создания токена, и это неудивительно. Эфир позиционировался как площадка для проведения краудсейлов – массовых продаж для сбора средств на реализацию проектов и идей. Простейший контракт токена был описан Виталиком сразу при выпуске платформы и включал минимум программного кода. Упрощенно это выглядит так: вы выбираете название токена, объем эмиссии, количество знаков после запятой, курс обмена эфира на свой токен и ряд других значений, далее загружаете контракт в блокчейн Эфира, при этом оплатив небольшую комиссию и оставив немного средств на исполнение контракта. Теперь любой желающий, пославший эфир на адрес смарт-контракта (аналогичный адресу кошелька), получит взамен N-ное количество токенов, исходя из ранее заданных параметров. Если все токены распределены – контракт перестает функционировать, но при этом он никогда не исчезнет из блокчейна Эфира. Далее собранные в Эфире средства идут на реализацию проекта, под который велся сбор. При определенных навыках программирования контракт можно усложнить дополнительным функционалом – сжиганием непроданных токенов, добавить возможность дополнительной эмиссии, предусмотреть дивиденды на токен, заблокировать часть из них на какое-то время и т. д. При всем при этом контракт создания токена и контракт краудсейла могут быть разными сущностями. В сети существуют коллекции подобных смарт-контрактов и даже конструкторы, позволяющие новичку создать свой контракт за несколько минут – как платно, так и абсолютно бесплатно. Следует учесть аспекты безопасности при использовании сторонних библиотек смарт-контрактов. Код может содержать уязвимости, сделанные неумышленно либо специально, с помощью коих злоумышленник может похитить средства, находящиеся на адресе смарт-контракта. То же касается и приватных цифровых ключей адреса-владельца контракта. Их компрометация может также привести к потере средств.

Но сфера применения смарт-контрактов не ограничивается созданием токенов. В одной из последующих глав мы пофантазируем на тему недалекого будущего, в котором массово применяются смарт-контракты. Однако уже сейчас мы можем встретить десятки примеров применения технологии в реальной жизни. Первый пример – это контракт-нотариус. Может использоваться для удостоверения прав владения текстами, фото или видео путем проставления временной метки на загруженном в специальное хранилище файле и также выдавать цифровой сертификат. Есть примеры реализации завещаний на смарт-контракте, верности копий документа или подтверждения неких фактов. Необходимо учесть, что зачастую работа таких контрактов невозможна без участия третьей стороны – Оракула, программы, человека или устройства, контактирующего с внешним миром и проверяющего или поставляющего данные для одной из сторон смарт-контракта. Это может быть сайт с информацией о курсах валют, компьютер с датчиками, судья на соревнованиях. Вторым ярким примером применения смарт-контрактов является игровая индустрия – прием ставок на события, лотереи, казино, а также создание компьютерных игр. Третьей сферой применения нельзя гордиться, но тем не менее смарт-контракты используют для создания финансовых пирамид на основе схемы Понци. Пока есть новые участники, схема будет работать, независимо от воли первоначального автора. Часто такую пирамиду называют честной, не забывая добавить оговорку «возможно». Четвертой, но первой по

обороту криптовалюты среди проектов можно назвать нишу биржевой торговли. Существуют десятки обменников и бирж, работающих на некоей совокупности смарт-контрактов. Такие комбинированные контракты принято называть децентрализованными приложениями Dapps. Популярный сайт-библиотека смарт-контрактов и Dapps [stateofthedapps.com](http://stateofthedapps.com) содержит почти 2000 записей децентрализованных приложений и управляющих ими смарт-контрактов. Пятый пример – инвестиционный пул для участия в некоем проекте. Проводится сбор для выкупа минимальной доли недвижимости или вклада в перспективное ICO.

В Ethereum существует понятие «газ» (англ. *gas*) – это внутреннее топливо для осуществления транзакций внутри этой системы. Это не токен, его нельзя отдельно купить и хранить на кошельке, но при переводах монет или исполнении смарт-контрактов эфир, находящийся на кошельке, тратится на закупку газа внутри системы. Цена газа формируется исходя из загруженности сети. Чем более загружена виртуальная машина, тем дороже газ для последующих транзакций.

Хочется упомянуть, что мой личный интерес к криптовалюте был подпитан идеями, реализованными на платформе Эфир. Именно широкий простор для применения в различных сферах, помимо просто перевода неких цифровых активов с кошелька на кошелек, сделал меня приверженцем идей Бутерина. Многие называют Ethereum криптовалютой 2.0, тогда как биткоин был криптовалютой 1.0. Следуя этой логике, нас ждет еще много поколений новых проектов криптовалют от 3.0 и до бесконечности.

## Реакция государства на появление цифровых денег

Если я и многие криптоэнтузиасты восторженно отреагировали на появление биткоина, эфира и дарованные ими возможности, правительства многих стран отнеслись к появлению криптовалют неоднозначно. Первая реакция большинства правящих кругов была негативной, в основном из-за анонимности системы и невозможности отследить большинство транзакций, что могло способствовать использованию ее в криминальных и террористических целях. Естественно, государства стали считать, что эта система создана только для отмывания денег, продажи нелегального товара и финансирования терроризма. При этом политические круги тесно связаны с банковским сектором, а уж банкирам конкуренция в их поле деятельности также не нужна. Против криптовалют в нашей стране выступали некоторые политики, министры, главы государственных органов, финансисты и даже президент. С появлением открытых и полезных проектов количество обычных пользователей значительно увеличилось, и они стали активно пользоваться криптовалютой в быту. Политическое мнение также стало меняться в положительную сторону. Первые прогрессивные государства не стали туго закручивать гайки. Они не вводили ее жесткое регулирование и приняли политику наблюдения без явного вмешательства, при этом присвоив некий статус имущества или иностранной валюты криптоактивам для целей их налогообложения, ведь именно эта сфера должна волновать чиновников в первую очередь.

Есть страны, которые официально в той или иной степени признали криптовалюту. Впереди планеты всей оказались США, выпустившие ряд документов, направленных на некую систематизацию отношений в сфере криптовалют. Одной из первых из стран, полностью легализовавших биткоин, стала Япония, где утвердили ряд законопроектов, в том числе по лицензированию участников рынка – бирж и обменных пунктов. При этом некоторые монеты существуют и используются только в Японии.

В Республике Беларусь также была легализована криптовалюта в рамках так называемого бизнес-инкубатора. Это особая экономическая зона, расположенная на закрытой территории, резидентам которой позволено заниматься предпринимательством без налогов и ограничений, кроме обязательного содержания гарантированного депозита в банке на случай провала для защиты прав вкладчиков.

Страны, в которых полностью или частично запретили криптовалюту, – это Китай, Индия, Бангладеш, Боливия, Таиланд, Вьетнам, Эквадор. Во Вьетнаме сначала она имела полулегальный статус, но, видимо, правительство узрело для себя большие риски и поспешило обезопаситься. При этом жители продолжают пользоваться криптовалютой в обход закона. Китай то разрешает, то запрещает своим гражданам майнить криптовалюту, но однозначно запретил ICO как способ сбора денег у населения под непонятные активы, некую нелегальную инвестиционную



деятельность. Нужно понимать, что полностью запретить криптовалюту сложно, ведь привязать обезличенный кошелек, некую многобуквенную строчку, к конкретному человеку без его согласия невозможно. В этом плане запрет криптовалюты условный, потому что большинство криптовалют предполагают тот или иной уровень анонимности, а закрыть все выходы в Интернет, убрать с компьютеров все приложения и программы попросту невозможно. Отсутствие центрального контролирующего органа, на который можно было бы оказать влияние, также мешает ее запрету. Конечно, некоторые элементы контроля можно ввести. Например, отследить майнинг смогут по повышенному круглосуточному потреблению электроэнергии, особенно в ночное время. Ведь оборудованию нужно работать круглосуточно, поэтому и потребление майнеров заметно выше среднего. С помощью Интернет-провайдеров зачастую можно вычислить объем и тип получаемой и отправляемой информации, если майнер не позаботится о более тонкой настройке безопасных каналов. Но даже при успешном запрете майнинга добывать криптовалюты можно с помощью мастернод или по алгоритму Proof-of-Stake или его разновидностей, когда монеты могут начисляться за владение некой минимальной долей в определенном проекте. Уже упоминавшаяся платформа Waves, признанная улучшить и даже обогнать Ethereum, предлагает именно способ добычи новых монет на основе делегирования баланса одному кошельку-оператору. Работа происходит удаленно, вы только получаете долю в выработке узла обработки транзакций. Соответственно, никаких затрат электроэнергии и сетевого трафика нет. Невозможно выяснить, откуда берется монета и отследить ее прирост. Заставить платить за нее налог или каким-то образом заблокировать использование невозможно, исключая только лишь силовой метод и физическое ограничение свободы и запрет на использование смартфона или компьютера.

Сегодня в России ведется работа по созданию законодательной базы для использования криптовалют. Жаль, что на момент написания мною книги рассмотрение законопроекта перенесено на осеннюю сессию, однако движение все-таки идет вперед и вверх. Я рад тому, что в нашей стране и во многих странах СНГ потеплело отношение к криптовалюте, многие настроены позитивно. Глупо было бы отрицать полезность технологии блокчейн и созданных на ее основе решений. Не за горами широкое общественное приятие криптовалют, и освоенные сферы применения будут только расширяться. Будем надеяться, что законодательство будет живым, а не мертворожденным, загоняющим молодую и неоформившуюся отрасль в некий юридическо-бухгалтерский тупик.

Как я уже говорил, совсем немного государств высказались в пользу безусловного запрета криптовалют. Все остальные государства либо заняли наблюдательно-выжидательную позицию, либо ввели слабое регулирование, обозначив криптовалюту либо цифровым активом, либо цифровом товаром, либо иностранной валютой. Некоторые страны ввели лицензирование криптовалютной отрасли либо обязали проводить некие регистрационные процедуры при проведении ICO и выпуске токенов – например, как в Гонконге. В ряде штатов США также есть так называемая BitLicense. В Европе также существует ряд локальных государственных и общеевропейских инициатив на эту тему. Все остальные страны либо частично отрегулировали закон для целей налогообложения криптовалютных активов, либо остаются нейтральными.

Сегодня неофициальное звание столицы криптовалют занимает кантон Цуг в Швейцарии, где расположены офисы многих крупных криптовалютных компаний. Не отстает и Гонконг, где расположено минимум 1/2 из топ-10 рейтинга криптовалютных бирж. Штат Калифорния и город Сан-Франциско являются центрами притяжения криптовалютного сообщества в США. Это означает, что при желании запустить свой криптопроект можно очень сильно увеличить его презентабельность и повысить шансы на успех, если разместить его в одной из правильных юрисдикций. При этом нельзя сбрасывать со счетов традиционно теплое отношение офшорных юрисдикций к новым экономическим течениям. Уже в 2014 году на острове Мэн была зарегистрирована компания, уставный капитал которой был выражен в биткоинах, а в 2015 году юридическая компания Aхon Partners из Украины внесла 1 биткоин в качестве вклада в уставный капитал, скорее всего отразив его как имущественный вклад. У регистратора вопросов и претензий не возникло. На роль криптовалютной гавани претендует и соседняя Эстония, а множество первичных регистраций компаний под будущие криптопроекты приходится на Великобританию и Кипр.

# Глава 3

## Майнинг и его разновидности

### Майнинг на центральных процессорах

Еще раз остановимся на понятии «майнинг» и на примере эволюции майнинга Bitcoin разберем принцип его работы. Мы говорили упрощенно, что майнинг – это перебор вариантов решения условно нескончаемой задачи. Допустим, по соседству с вами находится большой склад мелких предметов, который постоянно пополняется новыми вещами с разным весом и стоимостью. Вещи нужно перенести через висячий мост, на который в ширину помещается лишь один человек, соответственно люди должны идти цепочкой, держа за руку предыдущего и следующего носильщика. Хозяин склада платит 12,5 рублей фиксированной платы человеку, который приведет к нему носильщика, плюс 1 % от стоимости перенесенных товаров. Есть бесконечное число потенциальных носильщиков с одинаковыми корзинами, готовых загрузить в корзину одинаковый вес предметов, но рассчитывающие, что цена предметов, помещенных в их корзину, будет максимальной, дабы их процент комиссии был также максимальным. Но вот хозяин склада – странный человек – хочет, чтобы каждый следующий носильщик имел день, месяц и год рождения, отличающийся лишь на один день от предыдущего. Например, предыдущий носильщик был рожден 01.01.2001, соответственно следующим взять груз имеет право носильщик с датой рождения 02.01.2001, далее 03.01.2001 и так далее. Носильщики толпятся на площади перед складом и молчат. Ваша задача опрашивать одного за другим в хаотичном порядке, чтобы найти нужного носильщика, с нужной датой рождения в паспорте. Таких же людей, ищущих нужного носильщика, – сотни и тысячи. Кто первый найдет нужного человека – ставит его в цепочку и нагружает его корзину самыми дорогими товарами под завязку. Если кто-то другой нашел второго носильщика с идентичной датой рождения, но пришел позже вас – его носильщик отвергается. Задача наполнения корзины при этом схожа с классической задачей о рюкзаке, известной математикам.

Очевидно, что найти подходящего носильщика очень сложно, особенно если желающих это сделать очень и очень много. Можно искать носильщика сообща, объединившись в пул, и, если один из команды нашел подходящего, награда делится на всех, исходя из времени, потраченного каждым на поиски. Кому-то из поисковиков может повезти, и он найдет нужного носильщика с 1-й попытки, а в следующий раз просмотрит сотни дат рождения, пока найдет нужного. Здесь в дело вступает параметр удачи. Также важно, насколько быстр поисковик. Бабушка с плохим зрением, но хорошим аппетитом за 8 рабочих часов проверит лишь 8 носильщиков, а молодая девушка, сидящая на диете, – проверит 16 носильщиков и съест в два раза меньше пищи на обеде. В случае с майнингом биткойна мы ищем блок, некоего цифрового носильщика корзины, у которого очень редкие параметры, соответствующие предыдущему блоку, и при его успешном нахождении получаем награду – это 12,5 BTC на сегодняшний день. Также мы можем загрузить блок под завязку транзакциями, выбрав самые дорогие из мем-пула (склада транзакций), и получить комиссию за их включение в блок. В нашем случае команда поисковиков – это пул совместного майнинга, а каждый из них – это майнинг-устройство старого или нового поколения со своей вычислительной мощностью и энергопотреблением. Необходимость выбора людей с конкретной датой рождения можно назвать алгоритмом поиска.

Майнинг биткойна и других монет, построенных на алгоритме PoW – Proof-of-Work (с англ. – доказательства работы), – это постоянный перебор данных по определенному алгоритму, вычислительная работа, производимая компьютерным оборудованием. И чем мощнее и экономичнее вычислительное устройство, тем больше шансов на успех. Вычислительное оборудование для майнинга прошло несколько стадий развития, которые я опишу ниже.

CPU (англ. *Central Processing Unit* – **Центральный процессор**) – это самый маломощный вычислительный элемент, который сейчас может быть использован в майнинге. Для определенных типов алгоритмов майнинга он вполне может справиться с поставленными задачами, особенно если это современная мощная модель. Сам процессор – это вычислительный модуль, состоящий из одного или нескольких ядер, каждое из которых может обрабатывать несколько потоков информации одновременно. В случае со среднестатистическим процессором эффективность его работы в сети Bitcoin была продуктивной только на заре становления криптовалюты в 2009–2011

годах. Сегодня добыча биткоина и многих других монет, начинавших свой путь с помощью майнинга на процессорах, просто экономически нецелесообразна.

В рассмотрении параметров мощности и производительности любого майнингового оборудования важен термин **хешрейт** (*hashrate* – «рейтинг хеширования»), который отображает скорость вычисления значений хеш-функции за единицу времени, в основном в секунду. Допустим, вы включили на 1 минуту процессор, и он нашел 60 решений, следовательно, хешрейт вашего оборудования 1 хеш в секунду, записывается как 1 х/с. Однако важен и параметр энергоэффективности – сколько джоулей или ватт электроэнергии на 1 единицу хешрейта потребит вычислительный модуль. В основном он применяется в описаниях ASIC-устройств, о которых речь пойдет ниже. В сети Интернет можно встретить множество ресурсов, наполняемых пользователями, где они сообщают о полученных значениях хешрейта при тестировании майнинга на том или ином алгоритме с использованием конкретного устройства. Важно учесть, что более старое оборудование почти всегда потребляет больше энергии на выполнение одной и той же задачи.

Энергоэффективность процессоров почти всегда проигрывает более производительным устройствам, таким как графические ускорители – видеокарты, FPGA- или ASIC-устройства. Именно поэтому выбор монет для майнинга на процессорах сегодня сильно ограничен. Энтузиасты криптоиндустрии из года в год пытаются создать алгоритм, который будет подходить только для процессоров, и использование видеоускорителей или специальных интегральных микросхем будет просто нецелесообразным ввиду более высокой стоимости подобных устройств. Сегодня такие алгоритмы, как HODL, и одноименная монета пытаются что-то повернуть в утраченной нише, однако уровень притяжения данного проекта массами сложно назвать высоким. Традиционно алгоритмы серии *cryptonight* в различных вариациях *v7*, *light* и *heavy* также доступны для майнинга на современных многоядерных процессорах, показывая вполне понятную экономическую ситуацию – доходность от майнинга превышает затраты на электроэнергию (как минимум) и на амортизацию в течение 2–3 лет. Но при росте монеты в несколько раз и при условии оплаты счета за электричество из своего кармана или наличии условно «бесплатной розетки» вы можете окупить затраты моментально, как это произошло со многими приверженцами монеты монеро. Известны редкие случаи построения ферм (большого количества компьютеров для майнинга, расположенных в одном месте) для майнинга на процессорах. Единственным преимуществом таких ферм может быть относительная компактность размещения и высокая ликвидационная стоимость оборудования. Сегодняшние процессоры и материнские платы уже настолько совершенны, что не устаревают и не теряют в цене столь же быстро, сколько их собратья начала XXI века.

Такой ресурс, как *cryptunit.com*, позволяет выбрать ряд современных процессоров для добавления в риг (от англ. *rig* – установка, снаряжение). У майнеров ригом принято называть единичный элемент фермы – материнская плата, процессор, память, жесткий диск и несколько видеокарт, соответствующие количеству доступных физических портов для их подключения. Так, на сентябрь 2018 года один из популярных процессоров от AMD модели Ryzen 1700 демонстрирует потенциальную доходность в районе 30 центов, или около 20 рублей в день. При стоимости одного процессора 14 500 рублей и среднего набора сопутствующих компонентов для запуска ПК в районе 15 500 рублей выходит, что компьютер стоимостью 30 000 рублей будет окупаться 1500 дней, более 4 лет. Негусто. Все было лучше зимой 2017–2018 года, когда уровень дохода с 1 процессора достигал 2 долларов, минимум 100 рублей. В таком формате окупаемость достигалась максимум за 1 год, что является достаточно хорошим показателем по сравнению с некоторыми видами традиционного бизнеса, либо вложением в недвижимость или размещением средств на депозит. Тем более если устройство можно 1–2 часа использовать как компьютер, по прямому назначению. Гораздо более низкий срок окупаемости демонстрируют процессоры предыдущего поколения, такие как AMD FX с восемью физическими ядрами. Их стоимость сегодня крайне низка, так же как и стоимость комплектующих. При этом функционал процессора позволяет решать большинство сегодняшних прикладных задач, будь то графические программы либо игры. При стоимости в три раза ниже такая сборка продемонстрирует доходность в 1,5–2 раза ниже, что существенно сократит срок окупаемости.

Основной проблемой майнинга криптовалют на процессорах является зараженность сетей таких монет так называемыми ботнетами (*botnet* от англ. *bot* – робот, бот и *net* – сеть). В руках

злоумышленников находятся тысячи (если не миллионы) зараженных компьютеров, на которых может быть установлена программа-майнер, соответственно злоумышленник способен без затрат средств на оборудование и электроэнергию производить вычислительные операции, получая большое преимущество перед честными майнерами и не имея при этом заинтересованности в сохранении монет на будущее. Естественно, добывая множество «дешевых» монет, такой человек тут же избавляется от них по любой цене, сбивая биржевой курс и подрывая доверие к монете в целом. Также это идет вразрез с идеей Сатоши Накамото, представлявшего 1 процессорное ядро как 1 сущность в экосистеме Биткоин, 1 голос при голосовании... Получается, что равномерного распределения ресурса между всеми людьми не достичь, а возможности более обеспеченных людей по включению сотен ядер в майнинг делают идею децентрализации несостоятельной.

### **Майнинг на видеокартах**

В 2011–2012 годах состоялся массовый переход с процессоров на графические ускорители – видеокарты, или GPU (англ. *Graphic Processing Unit* – графический процессор). Связано это с тем, что видеоускорители способны обрабатывать в тысячи раз больше операций на 1 такт, нежели процессор. Встала задача по оптимизации программ для майнинга под данный тип вычислительных устройств, и первые, кто догадался это сделать, протестировать и запустить на собственном оборудовании, получили огромное преимущество перед майнерами, построенными на CPU – центральных процессорах. Есть мнение, что в середине-конце 2010 года, определенный человек или небольшая группа людей могли получить более 50 % мощности сети Биткоин, что позволяло провести злонамеренные действия по проведению атаки 51, при которой владелец более чем 51 % мощности сети может манипулировать цепочкой блоков для организации «двойной траты». Однако децентрализованный характер Биткоин изначально предполагал общедоступное программное обеспечение с открытым кодом, поэтому более поздние разработчики майнингового софта для видеокарт поделились им с сообществом, уже в сентябре-октябре 2010 года появились первые версии программ как для Nvidia CUDA, так и для AMD OpenCL. Естественно и то, что развитие технологии всегда идет в сторону оптимизации. Кто-то покопался в коде общедоступных программ, заметил какие-то несовершенства – некоторые функции нужно было бы убрать или улучшить, – как результат явил миру криптоэнтузиастов майнер, который максимально использовал ресурсы видеоускорителей, при этом отчисляя часть дохода разработчикам. В то время гораздо больше, чем сейчас, майнинг на видеоускорителях зависел и от программно-аппаратного обеспечения компьютера в целом. Версия операционной системы и набора драйверов, тип жесткого диска и оперативной памяти, мощность блока питания – все это влияло на итоговый результат. Когда же конкуренция сделала программное обеспечение максимально удобным и производительным, были подобраны наиболее стабильные и экономически оправданные наборы аппаратного обеспечения, произошел первый бум 2013 года, и люди стали скупать видеокарты в огромном количестве. Основным виновником был лайткоин, чей алгоритм хеширования Scrypt был пока еще недоступен асикам, а рост цены биткоина подтолкнул вверх и его облегченного собрата.

На этом заработали те, кто первыми успели купить несколько десятков достойных видеокарт, собрать их в риги, а риги объединить в фермы. Жаль, что период всплеска продлился недолго, и уже в 2014 году резкое падение биткоина спровоцировало выброс на рынок большого количества видеокарт, ставших попросту ненужными. Ситуация изменилась только в 2015 году с появлением новых монет, алгоритмов и общим оживлением рынка. Середина-конец 2017 года стали периодом второго, во много раз более крупного бума закупки видеокарт. Скупалось абсолютно все, даже маломощные ускорители, годами лежавшие на полках. Сеть наводнили сводки о значениях производительности той или иной карты на разных алгоритмах, появились рекомендации по «разгону» параметров видеокарт, в т. ч. с помощью изменения значений таймингов памяти в заводской прошивке микросхем управления BIOS, на фоне общего подъема энтузиазма производители видеокарт значительно увеличили объемы своих продаж. Но, как и в предыдущий бум, все закончилось весной 2018 года, при стагнации рынка, резким – до 5 и даже 10 раз – падением курсов основных монет, пригодных для майнинга. В некоторых случаях – при наличии видеокарт предыдущего поколения, а также использовании коммерческого тарифа электроснабжения – доходность от майнинга перестала покрывать затраты на содержание ферм. А наиболее удачные и энергоэффективные видеокарты, размещенные в недорогом домашнем

тарифе, стали приносить лишь 30 % рентабельности, тогда как в декабре 2018 демонстрировали уровень рентабельности 150–200 % и даже более.

2017 год явил миру даже специальные видеоускорители, выпущенные производителями конкретно для работы в майнинге. Для этого были немного оптимизированы элементная база и программное обеспечение, улучшена система теплоотвода, созданы специализированные драйверы. Такие карты оказались существенно производительнее и энергоэффективнее своих стандартных собратьев. При этом часть карт от компании Nvidia лишилась видеовыхода, что исключает ее дальнейшее применение в традиционном виде – как графический ускоритель для настольного ПК.

Сегодняшняя (на сентябрь 2018 года) доходность видеокарт в майнинге далека от наивысших значений предыдущих лет. В 2016 году можно было окупить вложения в видеокарты и даже процессоры за три месяца, сегодня же при самой профессиональной оптимизации вряд ли срок окупаемости будет менее 1 года. В периоды бума даже не важно, какой у вас тариф на электроэнергию, но в период застоя разница в 1–2 рубля делает майнинг на некоторых видеоускорителях просто нецелесообразным. Заработать на этом можно, но придется более плотно вникнуть в то, какие алгоритмы наиболее энергоэффективны, какие монеты на этих алгоритмах имеют потенциал роста, изучить самый оптимизированный софт, произвести прошивку BIOS видеокарты под майнинг на конкретном алгоритме и, возможно даже, перевести видеокарты на жидкостное охлаждение и дополнительно использовать их тепло в быту для достижения максимальной прибыли от майнинга. В настоящий момент рынок предлагает десятки вариантов хороших видеокарт, бывших в употреблении, по отличным ценам, отдельные образцы еще долго сохранят свою актуальность и в сфере майнинга, и в быту, и в профессиональных сферах. При наличии веры в определенные блокчейн-проекты, технических знаний, помещений с необходимой электрической мощностью и конкурентной ценой, ну и, конечно, материальных ресурсов на воплощение проекта возможно получать прибыль большую, чем от многих традиционных видов бизнеса и инвестиций.

## Майнинг на микросхемах FPGA и ASIC

В сфере вычислений существует еще один тип оборудования на основе ПЛИС – **Программируемой логической интегральной схемы**, – включающий два типа вычислительных устройств, подходящих для задач майнинга – интегральные микросхемы FPGA (ППВМ) и ASIC (*Application-Specific Integrated Circuit*, или интегральная схема специального назначения). Это специальный тип чипов, имеющих существенные отличия. Так, *FPGA (field-programmable gate array*, или программируемая пользователем вентильная матрица) – это микросхема, которую пользователь может запрограммировать на выполнение какой-либо вычислительной работы, а впоследствии перепрограммировать для других задач. *ASIC (application-specific integrated circuit)* – специализированные чипы, изначально спроектированные и запрограммированные в заводских условиях так, что они подходят исключительно для одной конкретной задачи – например, хеширования по алгоритму SHA256, используемому в майнинге Биткоин. Удобство данных микросхем заключается в их энергоэффективности и возможности объединения вплоть до сотен чипов на одной плате, что удешевляет конструкцию и делает устройство более надежным. Напомню, что видеокарта имеет на плате максимум два ядра, при этом такие видеокарты более подходят для профессиональной графики, нежели для майнинга. Единственное преимущество FPGA в том, что они сделали видеокарты в пять раз менее энергоэффективными при схожей производительности, позволив создавать компактные и экономичные фермы, но вот ASIC-устройства достигли комбо-эффекта – снизилось потребление энергии и существенно выросла вычислительная мощность. Давайте взглянем на цифры: мощный процессор тех времен Intel core i7 990x мог выдавать хешрейт до 30 Mh/s (мегахеш в секунду) при потреблении 200 Ватт, наиболее производительная видеокарта от AMD ATI Radeon HD5970 (с двумя графическими ядрами) выдавала уже 600 Mh/s при потреблении 350 Ватт, появившиеся в 2011 году первые решения на базе FPGA выдавали 850 Mh/s при потреблении 80 Ватт, а вот самое первое устройство от компании с говорящим названием ASICminer, анонсированное летом 2012 года, имело производительность 10 000 Mh/s, или 10 Gh/s,

при потреблении 100 Вт на одну плату Blade Block Erupter, причем платы можно было объединять, создавая дата-центры промышленного формата.

Для описания разницы между устройствами для майнинга в голову приходит сравнение со спортом. Например, один спортсмен занимается триатлоном: плаванием, велоспортом и бегом. Он занимается всем понемногу, поэтому не сравнится ни с бегуном, который занимается исключительно бегом, ни с профессиональным пловцом, ни с велосипедистом. Зато он может быть универсальным и участвовать во всех спортивных сферах, как видеокарта. Отдельный профессиональный бегун – это ASIC, он не умеет быстро плавать или часами кататься на велосипеде, вообще не думает ни о чем, кроме бега. Бегун наверняка пробежит свои коронные дистанции гораздо быстрее, чем триатлонщик. При этом он пробежит в разы лучше, чем обычный человек – в нашем случае процессор. Среднестатистический человек, не увлекающийся спортом, проиграет любому из этих спортсменов на их поле. Ну а микросхемы FPGA – это профессиональный спортсмен, который несколько раз в карьере менял вид спорта. То был конькобежец, то пошел в борьбу – и везде он выше среднего.

Проблема ASIC, как и профессионального бегуна, что в определенном возрасте он достигнет пика и не сможет перестроиться на другой вид спорта. Он больше ни для чего не предназначен. Перепрограммировать ASIC на другие задачи невозможно. Все остальные устройства могут в любой момент времени быть применены в не связанных с майнингом вычислениях. В меньшей мере FPGA, представляющая все-таки профессиональное и узкоспециализированное оборудование, и в гораздо большей мере видеокарты и процессоры, обладающие самой высокой остаточной ликвидностью, не теряющие своих качеств годами (если говорить именно про «топовые» модели).

Для более детального понимания ASIC необходимо также понимать, что конкуренция на рынке продаж ASIC-оборудования спровоцировала технологическую гонку вооружения – борьбу за уменьшение размера кристалла, используемого при создании конкретного чипа. Начав с размера 130 нанометров, технология дошла до 10 нанометров и стремится уже к 7 нм техпроцессу. Первые значимые скачки с 65 нм на 28 нм, а затем на 16 нм техпроцесса позволили повысить производительность и снизить энергопотребление чипов в разы. Сегодня же, например, переход с 16 нм на 14 нм дает лишь 30 %-ный прирост производительности при 10 %-ном снижении энергопотребления. И даже существующие 10 нм чипы не дают такой заметной разницы с лучшими образцами 16 нм чипов. Так же, как и в производстве процессоров для ПК и графических чипов, уменьшение размера кристалла имеет некий предел. Стоимость внедрения нового техпроцесса может составлять от нескольких сотен тысяч до миллионов долларов США. Если ранее новые устройства выбивали с рынка старые модели, делая инвестиции в асики очень рискованными, то в ближайшее время могут появиться устройства на 5 нм или 7 нм чипах, чьи срок жизни и эксплуатация будут ожидаемо дольше, чем у их предшественников. На это указывает то, что пресловутый закон Мура (об удвоении числа транзисторов на кристалле чипа каждые 2 года), действовавший до сих пор, многими теперь ставится под сомнение. Технологии достигли таких высот, что требуют чего-то кардинально нового – например, внедрения квантовых технологий в вычислениях.

Что касается меня, то я, конечно, имею опыт эксплуатации АСИК-устройств. Их основной недостаток – сильный шум, исключая установку в домашних условиях без специальных шумоподавляющих камер или искусственного занижения производительности чипов, что уменьшает нагрев и тем самым позволяет снизить скорость вращения вентиляторов. Мне довелось экспериментировать с первыми асиками для алгоритма x11, считавшегося неприступным бастионом для ASIC и тихой гаванью для GPU-майнеров. Однако уже упомянутая гонка вооружений заставила меня через полгода распродать устройства за 1/3 цены (это позволяло окупить его в ближайшие три месяца при профессиональном подходе). Причем на тот момент оно окупилось лишь на 50 %. Почему же так? Я знал, что появится устройство в два или более раза эффективнее, чем текущее. И я добывал монету Dash, от которой я ожидал иксов (икс от англ. X – умножение, чаще употребляется кратное x2, x3 и т. д.). С продажей я не ошибся, а вот с производительностью нового оборудования прогадал. Новая модель была производительнее в 30 раз, чем первый батч (от англ. *batch* – партия продукции), а через месяц после ее анонса конкуренты уже предлагали предзаказ образцов еще в 2 или 3 раза мощнее! Из этой ситуации можно сделать несколько выводов, и, возможно, я кого-то уберегу от опрометчивых шагов. Во-

первых, важно быть покупателем самых первых партий оборудования от производителя (по цене завода-изготовителя) и следить за новыми партиями, чтобы вовремя продать старые. Во-вторых, необходимо правильно эксплуатировать устройство с мощным блоком питания, в подходящих условиях температуры и влажности. В-третьих, правильно выбрать монету или монеты для добычи и, в-четвертых, не бояться потерять все вложения. Именно так произошло с покупателями биткоин-асика Antminer s9, приобретавшими его у спекулянтов по 300–350 тыс. рублей в начале 2018 года и майнившими дешевающий биткоин. Уже через полгода цена устройства упала в 10 раз, а цена биткоина снизилась в 3 раза. В условиях дорогого тарифа на электроснабжение, в ожидании прихода новых поколений асиков такая инвестиция, к великому сожалению, не окупится никогда. Хотя это и печатный станок для денег, печатает он слишком мелкие монеты и по высокой себестоимости.

Совсем недавно майнинговый мир всколыхнула новость о выходе нового поколения FPGA-процессоров от компании Xilinx, которые могут потеснить асики и видеокарты, особенно в некоторых нестандартных алгоритмах хеширования. Расчетные цифры поражают, впрочем, как и цена устройств. По слухам, весь первый батч был раскуплен за считанные часы. Реальных видеоили фотоотчетов на момент написания этой главы я не видел, но, думаю, они скоро появятся и покажут, на что способны.

## Майнинг на жестких дисках

Этот вид майнинга появился гораздо позже всех основных вариантов заработка монет, которые добывались на видеокартах, процессорах и ASIC, и пока принят на уровне энтузиастов. Его смысл в следующем: у любого пользователя, особенно у пользователей, которые покупают новые компьютеры, зачастую есть свободное место на жестком диске. Очень часто у других людей или определенных компаний наблюдается нехватка места на жестком диске или в массиве жестких дисков, чтобы хранить определенные объемы информации в виде статического архива с редким к нему обращением или с постоянным дополнением и перезаписыванием информации. Простым примером является ваша общедомовая система видеонаблюдения, которая хранит в записи только несколько последних дней или недель, а потом постепенно стирает самый дальний из прошедших дней в цепочке и записывает на его место сегодняшней. Стоимость установки и обслуживания хранилищ бывает несоразмерно высока, из чего родилась идея, почему бы не сделать децентрализованное хранилище и платить пользователям деньги за их свободное место в виде криптовалюты? В общем-то идея простая, понятная и, в принципе, успешная, потому как аренда этих мощностей у централизованных провайдеров – дата-центров – стоит минимум пять долларов, а чаще в районе десяти долларов за Tb (терабайт) хранилища в месяц. Тогда как обычный пользователь, имея специальную программу, мог бы определить в ней количество незанятого пространства, которое он может выделить на диске для аренды, и запросить за аренду 2 доллара за 1 Tb. В таком случае арендатор существенно сэкономит по сравнению с крупным провайдером типа Amazon или «Яндекс. Диск». Незанятое, неиспользуемое дисковое пространство начинает приносить доход. Ну а компания, которая даст возможность соединить спрос на массивы хранения информации и предложение свободных емкостей, тоже заработает свою комиссию на этом. Достаточно понятная бизнес-схема, тем более если к ней добавлены фишки в виде блокчейн, смарт-контрактов, одновременного хранения частей файлов на разных дисках и возможность восстановить файл даже при отказе большинства узлов сети хранилищ. Естественно, что смельчакам, взявшимся за такой проект, предстояло решить кучу технических вопросов, но в итоге такие нашлись. И не один – попыток организовать подобный сервис было несколько, и еще не один стартап попробует свои силы в будущем. При этом мне лично известна команда проекта Storj.io, которая успешно реализовала подобный сервис, работающий по принципу децентрализованного приложения dApp на основе смарт-контрактов и со своим утилити-токеном, т. е. внутренней монетой проекта, в которой можно вести расчеты в системе. Я даже участвовал в тестировании ранней версии системы, но не уделил достаточно времени и усилий для получения вознаграждения. Вспоминая публично обнародованные выплаты других тестеров, я рассчитывал, что покупка самого недорогого, но объемного жесткого диска на 8 Tb окупалась за один год. Для многих видов бизнеса за год вернуть вложения – это недостижимый показатель. Например, в сфере строительства и эксплуатации дата-центров один год может уйти на запуск, один год для выхода

на операционную прибыль и еще годы, чтобы окупить первоначальные вложения. Сегодня, в период написания мною книги, рынок криптовалют переживает смутные времена, и, вполне вероятно, доходность майнинга storj не позволяет окупить оборудование даже за 3 года.

В целом идея проста и понятна: «отдай свободное место, получи за это деньги» для продавца и «купи дешевле, чем у конкурентов» для покупателя. Но есть и ряд аспектов, которые могут разрушить идиллию. Понятно, что нельзя выключать компьютер, дабы хранилище было постоянно доступно для пользователей. Опять же, в системе Storj применен принцип децентрализации. То есть на вашем диске не хранится полностью файл, его разбивают на множество частей, и эти части дублируются по многим независимым хранилищам. Программа, которая управляет процессом, в любой момент может собрать файл заново из множества доступных хранилищ. Сделано это для случаев, когда жесткий диск арендодателя отключился от системы, потому что данному пользователю больше не хочется сдавать место в аренду или попросту сломался компьютер, и это не повлекло бы потерю информации заказчика услуги – арендатора дискового пространства.

Однако Storj не были инноваторами в области майнинга на жестких дисках. Гораздо ранее, еще в 2014 году, международная команда исследователей предложила научно обоснованную концепцию PoSpace (Proof-of-Space, или доказательство пространства), иногда также именуемую PoC (Proof-of-Capacity, или доказательство емкости), где емкость и пространство как раз означают свободное место на жестком диске. Результатом работы команды воспользовался проект Burstcoin (от англ. *burst* – взрыв), который был построен как форк платформы NXT, но с существенными отличиями. В Burst гораздо раньше, чем в Ethereum, были разработаны и внедрены смарт-контракты и тьюринг-полный язык программирования для них. Работоспособность была показана на примере смарт-лотереи и проекта контракта для краудфандинга. Не менее важным отличием стала возможность проведения торговых операций между двумя разными блокчейн-монетами или токенами без привлечения третьей стороны посредника, что было названо Atomic swap, или атомарным обменом. Сегодня эта технология только-только находит применение в сфере обменных операций на рынке криптовалют. В сети есть ряд актуальных калькуляторов, на которых можно рассчитать доходность майнинга Burst, которая нарастает в долгосрочном периоде. На момент написания этой главы калькуляторы показывают доходность 300 Burst за 1 месяц, что при цене 0,01 USD за монету дает всего 3 доллара и не мотивирует на данный вид деятельности. В пиковые месяцы 2018 года цена монеты была в 8 раз выше, именно тогда был смысл ее добывать и выводить в доллар, но этот период был очень коротким и не дал бы возможности окупить вложения. Опять же, традиционный жесткий диск постоянно потребляет некое количество электроэнергии, как и компьютер в целом, где он установлен. Затраты на обеспечение работоспособности хранилища могут не покрываться доходом.

Что в майнинге Storj, что в Burst ситуация может измениться с приходом на рынок арендаторов, желающих арендовать децентрализованные зашифрованные хранилища в большом объеме. В целом, учитывая темпы создания и накопления информации мировым сообществом, такое время может наступить в ближайшие пару лет. Тогда цена на монеты, являющиеся единственным возможным вариантом оплаты услуг децентрализованных хранилищ, должна существенно вырасти.

Стоит упомянуть, что два вышеописанных проекта не единственные, кто занялся проблемой утилизации незадействованного пространства жестких дисков. Также достаточно давно на рынке существует проект Siacoin, правда, майнить эту монету нужно было с помощью GPU, а ныне ASIC. В 2017 году достаточно успешное ICO провело проект Filecoin, однако до текущего момента нет сведений о возможностях добычи монеты каким-либо вычислительным оборудованием.

## Майнинг на смартфонах

Одними из наиболее распространенных и понятных пользователю устройств в наши дни являются смартфоны на базе операционной системы Android. Зачастую в них встроен очень мощный процессор, но с урезанным функционалом. Сделано это для того, чтобы ваш смартфон не перегревался и не опустошал емкость аккумулятора очень быстро. В процессор также встроен видеоускоритель, который позволяет пользователю, имеющему модель телефона с хорошим экраном, получить разрешение формата 4K и даже использовать специальные шлемы виртуальной



реальности для своих устройств. Таким образом, ваш смартфон – это тоже небольшой компьютер. В магазине Google Play вы можете найти парочку неплохих профессиональных программ, благодаря которым можно осуществлять майнинг. Например, программа MinerGate, то есть «Ворота майнера», установив которую можно начать добывать монеты на алгоритме cryptonight. По сообщениям пользователей большой производительности смартфоны не демонстрируют, и здесь проблема не только в урезанном функционале процессоров телефонов, но и в том, что, возможно, программа MinerGate также занижает ваш хешрейт для увеличения собственных прибылей.

Конечно, если взять средний телефон с 4-ядерным процессором предыдущего поколения и использовать не самую лучшую программу для майнинга, ожидать внятных финансовых результатов с одного устройства не стоит. Но есть все-таки возможность улучшить показатели майнинга при определенных условиях. Предположим, у вас есть некоторое количество материнских плат телефонов. Путем некоторых манипуляций возможно заставить плату работать от внешнего источника питания и без экрана, при этом раскрыв весь потенциал установленного на плате процессора и даже задействовав в майнинге графическое ядро. Я принимал участие в эксперименте, проделанном командой энтузиастов, суть которого была в следующем: необходимо было удалить систему Android и установить вместо нее ARM Linux, затем запустить стандартные майнеры, созданные для настольного компьютера. При этом стояла задача использовать процессор без тех ограничений, которые встроены в операционную систему Android. Для тестовой системы были использованы дешевые платы от смартфонов предыдущих поколений со сломанными экранами и неработающими батареями, главное для нас – рабочий процессор. Конечно, пришлось доработать систему отвода тепла и настроить удаленный доступ к плате через Wi-Fi модуль. Также требовалась некоторая работа программиста. В результате получился тестовый майнер, в 5 раз превосходящий возможности смартфона, которым он был в прошлой жизни. И еще осталось место для оптимизации. Применение такой технологии могло бы быть эффективным, если бы не падение рынка 2018 года, которое сделало проект нерентабельным. Сегодня если вы купили телефон в магазине, то майнинг с телефона вряд ли окупит всю его стоимость из-за его небольшой мощности и огромной нагрузки на батарею телефона. Но если бы вы начали майнить монету со смартфона несколько лет назад и не прекращали до зимы 2017–2018 года, то стоимость даже топового смартфона или планшетного ПК вполне могла окупиться.

В программе MinerGate есть полезная функция «Включать майнинг, когда телефон находится на зарядке». Когда вы ночью ставите свой смартфон на зарядку, он начинает выполнять вычислительную работу, и это правильно, ибо майнинг нецелесообразен, когда устройство лежит у вас в кармане: посадить батарею можно за считанные минуты. Но почему бы ему что-то не майнить, когда вы включаете его в розетку? В целом идея достаточно интересная и очень хорошо ложится на концепцию децентрализации.

В рамках работы над проектом cryptonight-майнера на основе плат от смартфонов мы пытались приспособить стандартный майнер для компьютера под чуждую ему среду. Возникла идея создать специализированный майнер для смартфона, учитывающий логику работы его процессора и видеокарты, а также подключить функционал SD-карты, обладающей возможностью быстрого чтения и записи информации. Можно было бы создать отдельное решение, спроектированное специально для телефонов, новую блокчейн-историю с собственной монетой и получить потенциальный миллиард независимых узлов по обработке и подтверждению транзакций. Если бы такие корпорации, как Samsung или Huawei, обратили внимание на возможности смартфонов в блокчейн, могла бы появиться самая отказоустойчивая сеть с возможностями гигантского облачного суперкомпьютера, которая решила бы массу вопросов, стоящих перед блокчейн-проектами и научными кругами сегодня.

Конечно, майнинговый кластер из телефонов, наподобие того, который демонстрировали специалисты Samsung, приходил в голову многим майнерам. Инженеры Samsung, заинтересованные в блокчейн, взяли готовые телефоны и объединили их в некую ферму. Задачей было лишь показать слаженную совместную работу нескольких вполне новых и функционирующих смартфонов по решению определенного алгоритма, что было абсолютно неэффективно экономически. А вот повторно использовать оставшиеся материнские платы с чипами вместо утилизации вполне даже возможно. Средняя стоимость одной платы может быть в районе 10 долларов, а доход от майнинга на ней составит около 1 доллара в месяц. В теории за

один год можно полностью вернуть вложенные в оборудование деньги. Другое дело, что все модели процессоров и разработанных под них плат очень разные и, чтобы собрать 1000 штук для получения чего-то, сопоставимого с хорошей зарплатой, придется изрядно попотеть. Да еще и вложить первоначальный вклад в размере не менее 10 000 долларов США. Перспектива остается весьма туманной...

## Майнинг на игровых консолях

PlayStation4 – это небольшой персональный компьютер, оптимизированный для игровой индустрии. В нем установлен графический процессор (аналог видеокарты AMD Radeon HD 7850), то есть оборудование, вполне подходящее для майнинга. На консоль вы можете устанавливать не только игры, но и программы, поэтому ничто не мешает установить туда программу-майнер и пустить ресурсы на добычу криптовалюты. Когда майнинг был в основном делом энтузиастов, так и поступали. Всегда есть очень погруженные в процесс люди, которые все что угодно заставят работать ради поставленной цели. Производители консолей вполне могли бы сделать свою программу для майнинга и продавать ее в своем цифровом магазине. Я пользовался такой видеокарткой и знаю, что она до сих пор может работать на благо блокчейн и приносить небольшой доход. Возвращаясь к тучным временам бума конца 2017 – начала 2018 годов, б/у консоль стоимостью в 15 тысяч рублей могла приносить одну тысячу рублей в месяц. У многих людей консоли лежали и продолжают лежать без дела, и самое лучшее, что можно было с ней сделать, – это выложить устройство на доску объявлений и продать за достаточно низкую цену.

Обладая возможностями, имеющимися у компании Sony, вполне можно было создать собственный блокчейн-проект с игровой монетой для внутренних целей. По идее достаточно было лишь заинтересовать своих пользователей оставлять консоль включенной, при этом запустив специальное приложение. Взамен отданной вычислительной мощности корпорация выплачивала бы токены. Эти монеты можно было бы потратить в магазинах Sony, оплачивая игры, дополнения к ним, а также приобретать любые товары, производимые корпорацией и ее партнерами.

Производитель мог бы получить огромный вычислительный кластер, пригодный для решения различных задач, а не только для майнинга. Если предположить, что Sony продала миллион устройств и половина из них установила специальное приложение для распределенных вычислений, то такой облачный вычислительный узел мог занять конкурентную нишу даже среди уже существующих блокчейн-проектов и традиционных суперкомпьютеров. Даже если бы идейные руководители Sony заставили работать часть клиентских игровых консолей на половине своей мощности, чтобы она практически не потребляла электроэнергию и не грелась, то это все равно был бы огромный вычислительный ресурс, который сегодня попросту простаивает.

## Proof-of-Stake форжинг, минтинг и харвестинг

Все ранее описанные способы майнинга работают на алгоритме Proof-of-Work, когда участнику системы требуется представить доказательство работы над достаточно бесполезной, в научном смысле, задачей. При этом тратятся электроэнергия и ресурс вычислительных устройств. Но в мире блокчейн есть абсолютно иной алгоритм достижения консенсуса, получивший наименование PoS или Proof-of-Stake (от англ. *stake* – доля, пай) – доказательство доли владения. Для генерации новых монет в блокчейн-системах, построенных на данном алгоритме, нужно лишь иметь некоторое количество монет на своем кошельке и активировать функцию блокировки баланса, чтобы заблокированные монеты начали участвовать в майнинге. Считается, что монеты, основанные на консенсусе PoS, более защищены от возможной атаки 51 % и проведения с ее помощью двойной траты средств. Аккумулировать на одном кошельке 51 % всех монет системы будет либо очень дорого, либо вообще физически невозможно, а ряд дополнительных инструментов позволяет защитить блокчейн от злонамеренных действий даже такого участника, который владеет 90 % всех монет в обращении.

Первая реализация рабочего блокчейн на основе комбинированного консенсуса PoS + PoW была предложена летом 2012 года в PPCoin, сейчас известной под именем Peercoin. Для эмиссии новых монет используется как традиционный SHA-256 майнинг, так и PoS-форжинг (от англ. *forging* – ковка). Также создание PoS-блоков принято называть минтингом (от англ. *minting* – чеканка). Первым на 100 % основанным на механизме достижения консенсуса PoS стал блокчейн NXT (от англ. *next* – следующий). NXT не является форком какой-то предшествующей монеты,

это созданный с нуля продукт, новая платформа, наметившая свой вектор в развитии криптовалют. В PoS-форжинге монет очень важно, какой баланс у вашего кошелька и как долго монеты лежат на балансе. Чем больше монет вы храните и чем дольше не используете, тем больше шансов сгенерировать новый блок и получить за него вознаграждение. Со временем появились дополнительные вариации PoS-консенсуса, которые расширили его функционал и добавили безопасности и надежности системе.

LPoS – Leased Proof-of-Stake (от англ. *leasing* – сдача в наем, аренда) – предполагает возможность сдать свой баланс в аренду более крупному узлу взамен на пропорциональную долю в доходе такого узла. Ведь более крупный узел будет иметь больше шансов на генерацию новых блоков и сможет чаще вознаграждать арендодателей, чем при попытке каждого отдельного маленького узла бороться за право генерации блока в условиях большой конкуренции узлов. Примером работающего механизма LPoS можно назвать платформу Waves, при этом, имея 1000 Waves, вполне можно создать свой узел и при определенной удаче сгенерировать блок, забрав всю награду себе. Шансы невелики, но все же они есть. Технически сдача баланса в аренду не предполагает фактической передачи монет другому пользователю, а лишь блокирует их на вашем балансе. Заработать на подобных проектах вполне можно, особенно если войти в них на ранней стадии и с достаточно большим стартовым балансом.

DPoS – Delegated Proof-of-Stake (от англ. *delegate* – делегировать, поручать) – отличается тем, что владельцы монет обладают неким количеством голосов, которые они вправе отдать доверенному узлу – свидетелю или Witness, при этом не рассчитывая на долю вознаграждения от доходов узла-свидетеля, но коллегиально избирая сеть надежных узлов для поддержки бесперебойности и чистоты работы всей сети. Такой подход, например, использован в работе известной платформы Bitshares (с англ. – цифровые доли), в рамках которой также можно создавать собственные активы и обменивать их на другие. На основе системы Bitshares функционирует ряд децентрализованных криптовалютных бирж. Т. к. комиссии за обработку транзакций получают доверенные узлы, получить доход от участия в подобной системе можно, лишь став доверенным узлом.

MN – MasterNodes (от англ. *master* – главный и *node* – узел) – вариант, при котором вам необходимо не только иметь на балансе некое минимальное количество монет – например, 1000, но и запустить отдельный сервер с полностью рабочим узлом – нодой, на которой имеется достаточно вычислительных ресурсов, а также дискового пространства для хранения полной версии блокчейна данной монеты. Это можно сделать либо на базе собственного ПК или даже мини-ПК типа Raspberry PI, либо арендовав виртуальный сервер у провайдеров хостинг-услуг. Сегодня существуют и специализированные хостинги, созданные специально для развертывания мастернод. Запустив мастерноду, вы через некоторое время начинаете получать награду за генерацию блоков. Считается, что выбор мастернод-победителей происходит хаотично, но справедливо. Т. е. на длинном отрезке времени все мастерноды в сети сгенерируют в среднем одинаковое количество блоков. Однако есть мнение, что ноды, размещенные на плохих хостинг-площадках с низкой сетевой доступностью от центрального узла и других узлов сети, могут быть доминированы. Чем больше активных мастернод находится в сети, тем меньшее вознаграждение достается каждому отдельному узлу. Бывает и так, что разработчики монет (называемые, кстати, «дэвами» от сокращенного англ. *dev* – *developer* – разработчик) делают несколько уровней мастернод, например в 1000, 3000 и 5000 монет. Соответственно, при меньшем количестве больших нод их шансы на генерацию блоков и вознаграждение будут большими. Также дорожная карта монеты может предполагать увеличение коллатерального баланса (от англ. *collateral* – залог, обеспечение) в будущем с 1000 до 2000 монет и так далее. Это делается для борьбы с инфляцией и обесцениванием монет. Одной из самых популярных монет, использующих мастерноды, является дэш – Dash. На сегодняшний день годовая доходность составляет от 7 до 10 %, но это ничто по сравнению с тем, как вырос курс самой монеты за период с 2015 по 2017 год. Для многих 2018 год стал годом мастернод. Количество монет, предлагающих заработок на мастернодах, выросло экспоненциально, однако большинство из этих проектов – мошенничество. Цена монеты падает так быстро, что даже 10000 % годовых заявленной первоначальной доходности не покрывают обесценивание ноды. Целью разработчиков являются только кратковременный, чаще искусственный, рост курса и следующий за ним сброс принадлежащих команде монет. Убедиться в этом просто, вычислив монеты с ценой в несколько Сатоши (минимальная неделимая часть

биткойна) и мизерным объемом торгов на недорогих для первичного листинга площадках [crupto-brige.org](http://crupto-brige.org) или [cruptopia.co.nz](http://cruptopia.co.nz).

PoI – Proof-of-Importance (от англ. *importance* – важность) – предполагает не только наличие баланса на счету, но и подразумевает минимальный срок хранения баланса, а также активное участие в операциях отправки и получения монет. Исходя из этих и некоторых других параметров формируется значение репутации, той самой важности отдельного узла. Такой принцип применен в блокчейне NEM. Чтобы активировался харвестинг (от англ. *harvest* – собирать урожай), необходимо, чтобы минимальные 10 000 монет на балансе созрели, а кошелек получил минимальную важность для начала получения вознаграждений. По сообщениям на профильных форумах, доходность харвестинга NEM трудно назвать достойной, она находится на уровне 3–5 % годовых. Но перспективность самого проекта и ожидание роста стоимости каждой отдельной монеты могут стать бОльшим стимулом для покупки 10 000 монет, нежели мизерный доход от харвестинга.

## Появление пулов в майнинге

Сложность добычи PoW-монет, имеющих широкое распространение, как, например, биткойн или лайткойн, постоянно растет. Понимая, что одному человеку с небольшой вычислительной мощностью может оказаться непосильной задачей найти блок в одиночку, майнеры начали объединяться в пулы, то есть создавать один общий узел совместного майнинга. Направляя свою мощность в пул, майнер может рассчитывать на часть награды пропорционально переданной мощности. Кому-то одному повезло найти блок – награда делится между всеми. Первым известным сообществу и старейшим пулом является Slush pool, ранее располагавшийся на домене [bitcoin.cz](http://bitcoin.cz) и базировавшийся в Чехии. Публично анонсированный поздней осенью 2010 года, пул занял лидирующие позиции и сохраняет высокий рейтинг до сих пор. Всего стараниями майнеров Slush-пула было добыто более 1 000 000 биткойнов и огромное количество других монет, добавленных в пул позднее. Любой пул берет комиссию за свои услуги, в среднем 1,5–2 % от награды за блок. Сегодня существуют тысячи пулов, как для совместного майнинга одной или нескольких монет, так и для одиночного соло-майнинга (доступного владельцам крупных мощностей), а также для мульти-алгоритмического майнинга, например с помощью программного обеспечения NiceHash miner. Большинство крупнейших пулов находится в Китае, как и большинство крупнейших ферм или большинство производителей майнингового оборудования. Значение пулов для экосистемы блокчейн очень велико, однако не стоит забывать, что пул может быть атакован хакерами и средства пользователей будут похищены. Наиболее простым способом избежать потерь является автоматический вывод средств с баланса пула при достижении минимального порога на вывод. Это может вылиться в более высокие затраты на комиссии, но точно не даст потерять все заработанные монеты. Существуют и мошенничества со стороны владельцев пулов, но предсказать такое их поведение изначально невозможно. Специализированные сайты и форумы содержат массу отзывов о работе пулов, что может помочь майнерам избежать проблем. Также существует гипотетическая вероятность захвата одним из пулов более 51 % мощности сети какой-то монеты и проведение соответствующей атаки на нее.

Принципов распределения наград между участниками пула существует несколько, и очень важно выбрать соответствующий пул, чтобы максимизировать свою прибыль. Но сначала нужно ввести в обиход понятие шáры. (от англ. *share* – доля). Так как время появления новых блоков в сети должно быть усредненным, допустим, до 1 блока раз в 10 минут, существует механизм увеличения или уменьшения сложности сети, призванный контролировать данный процесс. Чем выше сложность сети, тем более сложная задача стоит перед майнером. Найти решение задачи с высокой сложностью одному майнеру не под силу. Но он может найти решение задачи с более низкой сложностью (но не ниже определенного минимума), которое может случайно оказаться подходящим решением и для сложной задачи – тогда шáра превращается в блок. Решения мелких задач, которые мы посылаем пулу совместного майнинга, называются шáрами и служат для оценки нашего личного вклада в процесс поиска текущего блока – раунда.

PPS – (англ. *Pay Per Share* – плата за долю, шáру). Пул вознаграждает майнера за каждую валидную шáру, соответствующую заданным параметрам, вне зависимости от успешности пула в нахождении блока. Для того чтобы компенсировать периоды возможных неудач, пул должен

иметь запас средств на выплаты майнерам. Данный метод невыгоден в долгосрочном периоде на пуле, имеющем короткие раунды. Существуют варианты системы PPS с доработками – например, RBPPS – PPS на основе раунда, HBPPS – PPS с ежечасной оценкой, PPSW с усредненной наградой за N блоков и еще минимум пять вариаций.

Prop (англ. *Proportional* – пропорциональный). Награда за каждый найденный блок делится пропорционально вкладу (количеству шар) каждого участника.

PPLNS (Pay Per Last N Shares – плата за последние N шар). Вознаграждаются либо конкретно последние N шар (например, N=10 000), либо N шар за определенный временной интервал.

Score (англ. *score* – баллы, соревновательные очки). Каждой шаре присваиваются очки, согласно ее возрасту. Распределение награды происходит согласно накопленным очкам.

В основном пулы создаются под конкретный алгоритм определенной монеты, как было с вышеупомянутым первенцем bitcoin.cz, при этом самими пользователями используются разные программы-майнеры, установленные на своей ферме. Но в сфере криптовалют есть проект, стоящий особняком.

## Майнинг с помощью NiceHash Miner

В середине 2014 года команда энтузиастов из Словении создала уникальную систему nicehash.com, которая решила одну из главных проблем майнеров – переключение оборудования на наиболее прибыльный алгоритм и, соответственно, монету. NiceHash Miner – приложение, которое выбирает для майнинга альткоин с наибольшей доходностью, при этом производя автоматическую конвертацию выплат в Bitcoin. То есть вы получите не набор разных монет, а их эквивалент в BTC. Перед первым запуском программа производит тестирование вашей системы для определения производительности в различных алгоритмах и, исходя из этих данных, подбирает наиболее выгодную монету для майнинга. Если же в какой-то момент доходность другой монеты возрастает, программа останавливает текущий процесс майнинга и запускает новый, более выгодный. Программа состоит из нескольких независимых приложений для майнинга, которые запускаются по запросу, поэтому ее можно назвать мульти-алгоритмичным майнером. Один отдельный компьютер, или ферма, или АСИК-устройство называются воркером (от англ. *worker* – работник). На сегодняшний день в системе ежедневно присутствуют до 0,5 млн воркеров разного типа и мощности, а также сотни тысяч заказчиков мощностей майнинга, что делает NiceHash крупнейшим рынком купли-продажи майнинговых мощностей в мире. Следует отметить, что Найсхеш лишь stratum-сервер, сервер-посредник между пулами, которые выбрали покупатели хеш-мощности, и ее продавцами. Каждый пользователь системы может быть как продавцом мощности, так и покупателем. Исходя из выбранной роли, так же формируется стратегия работы с сервисом. Выбор действий у продавца мощности совсем невелик, а вот покупатель имеет бОльшую свободу действий. Многие операторы пулов заявляют, что майнинг на NiceHash менее выгоден, чем на традиционных пулах, особенно на их собственных... Судя по моим наблюдениям, это не так. Многие монеты, которые добываются с помощью сервиса, очень волатильны и зачастую имеют непродолжительный период роста. То, что они конвертируются сервисом NiceHash в более устойчивый биткоин, может оказаться большим плюсом на долгом промежутке. Также управление десятками кошельков с разными монетами требует гораздо больше сил и времени: нужно отслеживать их курсы, оперировать учетными записями на разных биржах, синхронизировать несколько блокчейнов на локальном компьютере. Если нет других занятий или это уж очень нравится – тогда пожалуйста, но если ваша задача – иметь некую более простую и предсказуемую схему работы, стоит обратить внимание на возможности Найсхеш. Если же вы решили попробовать себя в качестве покупателя мощностей, вам сначала необходимо иметь биткоины для зачисления на свой внутренний кошелек в системе, а затем ввести данные пула, на который вы хотите направить арендованную мощность. Это может быть обычный или соло-пул, важно лишь то, что вы должны постоянно мониторить состояние сети той монеты, на которую нацеливаете мощности. Например, сложность сети монеты Zcash уменьшилась, а на некоем пуле была череда «долгих» блоков с очень большим эффортом (от англ. *effort* – усилие, попытка). Вполне вероятно, что пул сможет найти несколько «счастливых блоков» в ближайшее время с большей вероятностью. Если вы направите арендованную мощность на него и ваш прогноз оправдается, выплаты от пула покроют стоимость аренды мощностей. Конечно, это своеобразная лотерея, но при вдумчивом, даже научном подходе можно оставаться в плюсе. При этом

обязательно нужно учесть систему выплат, принятую на пуле, – в системе PPLNS есть защита от так называемых пул-хопперов, людей, заходящих в пул как раз в такой момент, когда это наиболее выгодно, и выходящих при изменении ситуации в худшую сторону. На Найсхеш принята система PPS, значит, и вам следует выбирать аналогичную систему либо рисковать в соло-майнинге. В данном случае можно примерно посчитать ваши шансы на успех. Например, вы решили добывать ETC – Ethereum Classic. Награда за блок составляет 4 ETC + комиссии, или около 43 долларов США на сегодняшний момент. Необходимое количество хеш-мощности для нахождения 1 блока в сутки можно взять из калькуляторов соло-майнинга, оно составляет примерно 2,5 Gh/s. Стоимость аренды 1 гх/с на Найсхеш составляет 0,0025 BTC за Gh в сутки. Итого нам потребуется 0,00625 BTC, или 41 доллар США, для аренды требуемой мощности. Гипотетически получаем 2 доллара прибыли. Но есть еще комиссии за ввод/вывод и конвертацию средств. В итоге выходит, что затраты равны прибыли. Именно здесь и появляется простор для размышлений. Например, при должном везении можно найти блок за 12 часов, а ордер на покупку мощности отменить, получив назад половину средств. А можно не найти ничего, и тогда придется вносить еще 0,00625 BTC в надежде найти уже два блока... Можно увеличить мощность в 2 раза, при этом сократив в 2 раза время аренды. Получится, что мы арендуем 5 Gh/s на 12 часов. Возможно, именно такой расклад будет более удачным. Именно параметр удачи в нахождении блока будет решающим в такой лотерее. Но по заявлению бывалых майнеров существуют способы минимизации рисков и максимизации прибыли. Важно лишь выбрать правильную стратегию майнинга, рассчитанную на более долгосрочный период и учитывающую бОльшее количество факторов, кроме неподвластной нам удачи.

## Некоторые стратегии майнинга

Самая простая, на первый взгляд, стратегия – определиться с монетой, в которую вы верите, и добывать только ее, как в соло-режиме или на публичном пуле с применением собственного оборудования, так и с помощью арендованных вычислительных мощностей. В конце 2015 года тысячи энтузиастов поверили в проект Ethereum. Вера эта не была слепой, а основывалась на ряде проверенных фактов. Личность основателя, методическое обеспечение проекта, наличие опыта в сфере криптовалют, проявленный первичный интерес сообщества, отличная, пусть и не совсем новая идея, множество планируемых к реализации новшеств, проделанная за два года предварительная работа – все эти признаки указывали на то, что проект, при должном приложении сил, будет успешен. Сегодня мы видим, что расчет был верен, однако скептики могут напомнить о более чем пятикратном снижении цены монеты в 2018 году. Мне лишь стоит напомнить, что по сравнению с сегодняшней ценой в районе 200 долларов США курс монеты вырос более чем в 1000 раз с мизерных 0,2 USD за 1 монету ETH. При этом многие вошли в проект, когда монета стоила уже 3 или 5 и более долларов США. Несомненно, майнинг Ethereum на первых порах мог не казаться таким выгодным, т. к. стоимость добытых монет приносила чуть больше, чем затраты на покупку и содержание майнингового оборудования. Впрочем, уже в начале 2016 года рост стоимости ETH позволил зарабатывать на майнинге в 15 раз больше фактических затрат на электроэнергию. Но многие заработали больше. Суть заключалась в оплате электроэнергии собственными средствами, а не за счет проданных монет. Например, если ваш счет за электроэнергию составлял 9000 рублей в месяц при цене монеты 300 рублей, вам необходимо было выплатить 30 эфиров сетевой компании. Даже при сегодняшней цене в 15 000 рублей за монету эфира это обошлось бы лишь в 0,6 монеты. Фактически можно было выкупать эфир у себя самого по себестоимости и сегодня увеличить размер вложений в 50 раз. На промежутке двух лет ни один банковский вклад или традиционный инвестиционный пакет не дал бы такой доходности. Еще одной стратегией, которую исповедовали умудренные опытом майнеры, была конвертация части добытых средств в BTC. Курс эфира по отношению к BTC одно время был на уровне 0,15 BTC за 1 ETH, порой опускаясь до 0,1 и даже 0,05. Сегодня 1 эфир стоит 0,035 BTC, а значит, подобное хеджирование рисков, как конвертация какой-то части средств в более стабильную валюту, имело все основания для применения. Посчитать возможную доходность от такой страховки легко. Если вы имели 100 ETH при его цене 120 долларов и стоимости биткоина 1200 долларов, можно было на 50 ETH получить 5 BTC, а 50 оставить в ETH. Сегодня 100 ETH стоят около 23 000 долларов США, а вот портфель из 50 ETH + 5 BTC стоит уже 11 500 + 33 000 = 44 500 USD. Гораздо более

приятная цифра. И держать яйца в разных криптовалютных корзинах вполне уместно, как и в случае с традиционными валютами.

Из предыдущего абзаца также можно сделать вывод, что добывать эфир в начале его развития было во много раз выгоднее, чем сегодня. И это чистая правда. Еще одной популярной стратегией майнинга является поиск молодых монет, пусть даже не очень подходящих для хранения в долгой перспективе, но которые демонстрируют хорошие показатели в текущем моменте. Основной проблемой владения такими монетами является выбор времени и объема монет для продажи. Я считаю целесообразным продажу 50 % монет в момент такого роста, когда 50 % проданных монет покрыли издержки на их добычу. Остальные 50 % можно либо хранить в надежде на «иксы», либо также частично конвертировать в более зрелые монеты либо токены многообещающих проектов (которые нельзя заработать прямым майнингом). Стратегия поиска таких монет в узких кругах получила название «shithunting» – охота за отбросами, так как молодые бесполезные монеты зачастую называют «shitcoins» – бросовые монеты. Но среди массы мусорных монет иногда мелькают вполне достойные экземпляры.

Читатель может возразить, что гораздо эффективнее была бы такая инвестиционно-спекулятивная стратегия, как просто достать из своего кармана 1000 долларов на заре становления эфира, получить 5000 монет, а сегодня продать их за 1 млн долларов. Конечно, он будет прав, такая стратегия получила название HODL (от видоизмененного англ. *hold* – держать). Однако многие майнеры уже имели некоторое количество готовых мощностей для майнинга ETH, которые уже окупались на майнинге биткоина и лайткоина, ничего не стоило включиться в новый проект без затрат. Тем более майнинг происходил на видеокартах, остаточная стоимость которых сохраняется на очень продолжительном интервале времени. Для человека, умеющего обращаться с оборудованием и анализировать новшества в сфере блокчейн, найти применение оборудованию не составит труда. Даже доходность на уровне 30 % годовых, которую сегодня демонстрирует майнинг ETH, невозможно найти даже в самом дружественном банковском учреждении, разве что в не менее рискованных проектах по вложению в микрофинансовые организации и кредитные кооперативы. При этом майнинг, как поддержка защищенности сети и как система эмиссии стоимости, признается делом общественно полезным и уважаемым.

Помимо «законных» стратегий в майнинге присутствуют и «читерские» – надувательские – методы майнинга. К ним относится так называемый пул-хоппинг (от англ. *pool* – бассейн и *hop* – скакать). Термин произошел от американского сленга, когда ближайший сосед не брезговал пользоваться вашим бассейном в период отсутствия хозяев дома. В майнинге пул-хопперы используют возможность программного анализа пулов, основанных на методе выплат Prop, на которых можно вычислить начало очередного раунда и эффективно продать пулу свои шары, особенно на коротком удачном раунде. Сегодня таких пулов очень мало, и их суммарная мощность невелика, тем не менее при должном техническом оснащении переключение пулов может дать экономический эффект. Особенно хорошо это работало в период форков – изменения алгоритма добычи, связанного с защитой от ASIC-устройств. Сложность сети очень сильно падала из-за выключения ASIC из процесса майнинга, и на некоторый короткий период становилось в два-три раза выгоднее майнить такую монету, нежели что-то стабильное. Многие владельцы ферм внимательно следили за объявлениями об очередном анти-асик-форке монет на основе алгоритма scryptonight, переключаясь с пула на пул в периоды падения сложности. Сегодня все больше алгоритмов захватывают асики, и такая ситуация будет повторяться вновь и вновь.

Также считаю целесообразным упомянуть здесь о таком явлении, как облачный майнинг. Оно заключается в возможности купить контракт на некий размер вычислительной мощности у крупного провайдера. Чаще всего тариф включает в себя все затраты – и на электроэнергию, и на амортизацию оборудования, и на персонал, и на аренду площадей. Иногда помимо цены контракта, соразмерной со стоимостью вычислительного устройства, сверху начисляется комиссия за обслуживание, включающая вышеприведенные затраты. В целом, учитывая широкое распространение облачных хранилищ и облачных серверов в традиционной нише обработки информации, вполне закономерным является и существование облачных сервисов в майнинге. Беда лишь в том, что многие «провайдеры» облачного майнинга являются банальными пирамидами и не имеют никаких реальных мощностей. Наиболее крупной и разрекламированной компанией, с которой я имел опыт сотрудничества, является Genesis Mining. Я лично знаком с основателями компании и по общению с ними на профильной конференции, сделал для себя вывод

в неплохих перспективах такой индустрии применительно к началу 2016 года. Вложенные мною 1700 долларов в контракт майнинга эфира принесли около 120 монет, из которых 100 я храню до сих пор. Выгоду может посчитать любой школьник. Сегодня в связи со снижением доходности майнинга облачные контракты не являются такой золотой жилой, хотя позволяют вам избавиться от бремени содержания и обслуживания оборудования, потеряв часть прибыли. По моим расчетам осенью 2018 года гораздо выгоднее приобрести сами монеты ETH или BTC, нежели вкладываться в облачный майнинг. По похожей схеме сегодня работают так называемые майнинг-отели, предлагающие вам временно разместить у них свое оборудование на колокацию, оплачивая аренду полки и тариф на электроэнергию. Разница лишь в том, что вы покупаете свое собственное устройство, а не его часть, и размещаете его временно, с возможностью получить оборудование назад в любой момент. В случае с облачным майнингом при истечении контракта вы ничего не получаете назад.

Каждый может найти подходящий для себя вариант добычи криптовалюты, вы даже можете комбинировать все стратегии. Но, какой бы ни была стратегия майнинга, важным остаются еще два фактора – эффективность оборудования и стоимость электроэнергии. Последний фактор приобретает очень большое значение в периоды медвежьих настроений на рынке, когда цена криптовалюты идет вниз, как в период работы над этой книгой. Низкопроизводительные устройства и дорогой тариф на электроэнергию могут свести на нет все ваши попытки заработать на майнинге в таких условиях.

## Выбор оборудования для майнинга

Основная функция любого оборудования для майнинга, которая интересует любого бизнесмена, – это создание новых монет, эмиссия. По сути вы получаете печатный станок для денег. Но не все они одинаковы. Какие-то устройства живут долго, век некоторых очень короток, как в силу технического несовершенства, так и из-за влияния рыночных факторов. При этом помимо генерации криптовалюты майнер принимает участие в консенсусе, целью которого является подтверждение транзакций, как бы работа мини-процессингового центра. В предыдущих главах мы немного затронули возможные типы оборудования для блокчейн-вычислений, попробуем рассмотреть их более детально.

Самым легкодоступным устройством, пригодным для майнинга, является игровой компьютер. Как правило, такое устройство обладает очень мощным центральным процессором и высококлассной видеокартой. Современные модели обязательно оснащаются быстродействующими твердотельными накопителями SSD, что тоже является большим плюсом в работе майнера. Даже игровой компьютер предыдущего поколения может продемонстрировать хорошие параметры производительности в некоторых алгоритмах хеширования. Чаще всего это алгоритм `cryptonight` и его защищенные от воздействия ASIC-устройств вариации. Для запуска майнинга на домашнем ПК необходимо установить специальное программное обеспечение, программу-майнер, а также наиболее подходящие драйверы для вашей конкретной видеокарты. Легким стартом может быть выбор вышеупомянутого майнера `NiceHash`, который поможет вам быстро и без особых сложностей войти в процесс майнинга. Если же вы задались целью выжать из своего оборудования максимум, придется провести ряд экспериментов по подбору наиболее подходящего вам софта, в сочетании с тонкими настройками «разгона» оборудования или, наоборот, искусственного занижения его энергопотребления (не в ущерб средней производительности). Необходимо учесть, что есть очень энергоемкие алгоритмы, называемые в среде майнеров «горячими», при запуске которых ваше оборудование потребляет максимальное количество энергии и сильно греется. Есть же более щадящие, особенно если не гнаться за моментальным повышением параметров производительности, но сосредоточиться на долговременной стабильности работы устройства и экономии его ресурса. Если же ваш компьютер имеет несколько свободных портов типа `pci-express`, в него можно добавить еще несколько видеокарт, получив таким образом риг – мини-ферму по добыче криптовалют. Любой профессиональный майнер начинал именно с этого, как и автор этих строк. К имеющейся в наличии видеокарте была приобретена еще одна, бывшая в употреблении, заменен процессор на максимально мощный для данного типа материнских плат, добавлена оперативная память. Бюджет мероприятия был невысок, но полученный опыт позволил перейти к построению



следующего типа устройств – мультикарточных ригов, состоящих из 5–6 мощных видеокарт, расположенных на открытом каркасе. Такие риги также называют фермами, хотя более правильным было бы сказать, что ферма – это несколько отдельных ригов. А промышленная ферма может состоять из тысяч ригов или асиков.

Вплоть до 2017 года специализированных материнских плат и графических ускорителей, спроектированных под майнинг, не существовало, за исключением материнских плат некоторых производителей, в названии моделей которых присутствовал индекс BTC. Тогда не было нужды в размещении более четырех видеоускорителей на одной материнской плате, поэтому майнерам приходилось экспериментировать с тем, что есть, задействуя и те порты, что изначально не предназначались для графических ускорителей, с помощью специальных переходников – рейзеров. В сети Интернет можно найти огромное количество обзоров, какие материнские платы хороши для майнинга и без проблем позволяют слаженно работать всем подключенным видеокартам. Популярность же темы криптовалют и майнинга заставила производителей компьютерного «железа» выпустить на рынок материнские платы, полностью адаптированные под майнинг, содержащие до 20 дополнительных портов для подключения видеокарт, а также специализированные видеоускорители для тех же целей. Но даже некоторые обычные видеокарты, имеющие лишь одну особенность в виде установленных на них чипов памяти от компании Samsung, демонстрировали более чем 10 %-ное преимущество в майнинге перед своими аналогичными собратьями, оснащенными другими микросхемами видеопамати.

Сегодня при построении фермы необходимо ориентироваться на максимально изученное и проверенное оборудование. Не стоит гнаться за материнскими платами с огромным количеством портов или наиболее дорогими видеоускорителями, которые выпущены для игр или профессиональных приложений по обработке графики. На момент написания этой главы моим базовым выбором стала материнская плата от компании Onda модели b250-d12p с простейшим процессором, диском SSD на 64 Gb и двумя модулями оперативной памяти по 4 Gb каждый. Материнская плата не нуждается в использовании рейзеров при подключении видеокарт, применение которых часто приводит к проблемам с питанием и даже поломке оборудования. Проверенные видеокарты AMD rx570-580 с 8 mb памяти Samsung стали бы основным вычислительным элементом системы. Конечно, в такой компоновке необходим специализированный высокоэффективный блок питания стандарта 80+ (желательно уровня gold как минимум), и лучше все это упаковать в корпус с принудительной вентиляцией. При этом вполне можно найти готовые решения из подобных ферм, уже помещенных в специальные корпуса для шести, восьми или двенадцати видеокарт, собранных и протестированных, с заранее известными параметрами. В текущих ценах октября 2018 года стоимость сборки такого сервера обошлась бы в сумму около 240 000 рублей при покупке всех комплектующих, кроме видеокарт, в Китае, а приобретении GPU уже в России, с должной гарантией и сервисным обслуживанием. Дневная доходность в текущем моменте, за вычетом стоимости стандартного домашнего тарифа на электроснабжение, согласно расчетам сервиса [whattomine.com](http://whattomine.com), составляет 300 рублей в день, что предполагает 800 дней до момента полной окупаемости фермы. В начале 2018 года даже при цене такой фермы в 350 000 рублей тот же самый калькулятор показал бы в 3–4 раза меньший ROI (англ. аббр. *ROI* – *return on investment* – срок возврата инвестиций). Следует учесть, что рост стоимости монеты в два или три раза пропорционально уменьшает срок окупаемости оборудования и, выбрав правильную монету для добычи, можно сократить этот срок и в 5, и в 10 раз. Но даже при сроке окупаемости, близком к 2,5 годам, проект, возвращающий вам более ½ вложений за 1 год, можно считать вполне достойным. Вложения в жилую недвижимость порой не окупаются и на промежутке в 15 лет.

Чтобы снизить объем вложений и минимизировать риск потерь, а также уменьшить расчетный срок окупаемости, можно приобрести недорогое бывшее в употреблении оборудование на доске объявлений, типа Avito, или в специализированных разделах профильных форумов. Некоторые энтузиасты заходят в своем стремлении сэкономить уж очень далеко, что получило шуточное название «некромайнинг», а построенные из совсем уж старинного оборудование фермы ласково нарекли «бомжефермами». То есть собрать из достаточно неактуального для игр или профессиональной графики материала работоспособную единицу – не очень простой, но иногда достаточно выгодный путь. Особенно это актуально при наличии недорогого электричества и некоторых готовых компонентов системы под рукой. Если есть минимальный навык обращения с

компьютерами, то майнить можно даже на обычном wi-fi роутере, хотя у компании Antminer имеются и роутеры со встроенными майнинговыми ASIC-чипами. Да, сейчас наступила эпоха промышленного майнинга, когда компании используют для добычи криптовалют сотни и тысячи видеокарт или такие же объемы асиков, размещенных в специально спроектированных помещениях. У большинства же людей нет огромных свободных средств, но нет никаких препятствий для того, чтобы начать с малого. Например, самая дешевая материнская плата для трех видеокарт может стоить не более 1000 рублей в комплекте с процессором и памятью. В качестве жесткого диска подойдет и старый диск, наверняка имеющийся в наличии у всех, приобрести три вполне достойные видеокарты уровня rx 550 4 gb можно за 4500 руб./шт. Итого в сумму 15 000 рублей обойдется устройство, приносящее на начало октября 2018 года до 1500 рублей в месяц, без учета небольших затрат на электроэнергию. ROI такой мини-фермы составит в районе одного года. Цифра, конечно, невелика, но ведь таких ферм может быть 10 штук, и цена добытой криптовалюты может расти...

Я не призываю каждого читателя потратить все силы и средства на подобные эксперименты, но, может быть, кто-то, имеющий доступ к компьютерным комплектующим или обладающий навыками ремонта, откроет для себя путь заставить работать компьютеры на пользу блокчейн-индустрии и приносить небольшую финансовую выгоду. Кто знает, какая монета станет очередным биткоином, дэш или эфиrom и вырастет в цене в сотни и тысячи раз в ближайшие несколько лет. Мой совет для начала майнинга – недорогие модели, которые могут быть проданы на вторичном рынке без потерь. Например, сегодня распространенная материнская плата Gigabyte GA-970 и процессор AMD FX 8100–8320 (желательно с потреблением 95 ватт) могут стать отличной недорогой базой для пяти видеоускорителей, а для начала даже двух, которые можно подключить напрямую к материнской плате. Блок питания уровня 80+ Bronze, мощность которого в идеале должна в два раза превышать мощность установленного оборудования, также стал бы уместным. Важно лишь учесть наличие на нем нужного количества разъемов питания PCI-E на 6 или 8 контактов для подключения видеоускорителей. Вот выбор GPU – дело более специфическое и часто зависит от того, какой алгоритм и монету вы предпочтете добывать. Наиболее подходящей под широкий спектр алгоритмов является продукция AMD, модели rx 570–580 с 8Gb видеопамью и старшие модели Vega 56 и 64 с новейшим типом памяти HBM. Конец 2018 года может явить миру новые модели ускорителей, которые продемонстрируют лучшие показатели, например модель rx-590 вполне может потеснить предыдущие модели в майнинге. Компания Nvidia также имеет несколько моделей, пригодных для майнинга. В силу изменчивости ситуации и частым выходом асиков, занимающих именно те ниши, где традиционно была сильна продукция Nvidia, в текущем моменте, кроме бывших в употреблении ускорителей 1080ti, сложно что-то выбрать из модельного ряда компании. Новинка rtx 2080 пока не стала прорывом в майнинге, при этом текущая цена видеоускорителя очень высока.

Мы уже упоминали об основных конкурентах видеоускорителей и центральных процессоров на ниве майнинга – микросхемах FPGA и ASIC и построенных на их базе устройствах. Ниша FPGA настолько узкая, что есть лишь 2–3 хороших производителя, и лишь один из них предлагает сегодняшнему рынку что-то достойное, в плане производительности в интересующей нас области. Если кому-то непременно хочется покопаться и в этом вопросе, советую обратить внимание на отладочную плату от компании Xilinx модели VCU1525, которая подает гипотетические надежды в майнинге на некоторых алгоритмах. Опять же, это профессиональное оборудование, требующее более высокой квалификации, нежели базовый уровень.

Гораздо более широкий выбор демонстрируют ASIC-устройства, выпущенные уже под многие популярные алгоритмы. Многие монеты заявлялись как обладающие ASIC-устойчивыми алгоритмами хеширования, однако время показало, что индустрия настолько развилась, что разрушила надежды создателей подобных монет в прах. Сегодня при выборе ASIC-устройства важно учесть ряд критических моментов.

Во-первых, асики пригодны только для блокчейн-вычислений, и срок актуальности этих устройств очень короток. Например, лидер продаж и хит 2015 года Antminer s5 сегодня может работать «в плюс» только в условиях тарифа для сельского населения Иркутской области, равного 0,01 USD за кВт/ч. Да и год назад появление сегодняшнего лидера Биткоин – асиков Antminer s9 – уже сделало старичка s5 малоперспективным вложением. Единственную дополнительную выгоду, которую гипотетически можно извлечь из этого устройства, – тепло. Тепловыделение и шум

асиков для жаркого климата и жилых помещений являются отдельными проблемами, и это второй момент, который нужно учесть. Асик необходимо размещать в специализированных помещениях, и это факт. В-третьих, отсутствуют четкие гарантийные отношения со многими производителями, а также мастерские по оперативному ремонту вышедших из строя деталей. В-четвертых, программное обеспечение майнеров может быть уязвимым, позволяя несанкционированный доступ к устройству. Хотя это же касается и обычных ПК и майнинг-ригов на GPU. А в-пятых, вокруг торговли ASIC-устройствами сформировалась огромная армия спекулянтов-посредников, которые задирают цены в 1,5–2, а то и в 10 раз, как это было с предзаказом майнера на алгоритм x11 модели Antminer d3 или iBelink 10g.

Рассмотрим сегодняшний рынок асиков более подробно, и попытаемся понять, какие модели выбирать и где их приобретать. Выбор асиков на момент написания этого текста уже настолько широк, что начинающему майнеру будет не просто разобраться с ним. Чтобы как-то упростить задачу, необходимо сделать небольшой экскурс в технологический аспект устройства асиков, а также алгоритмы хеширования, под которые они созданы.

Начнем, пожалуй, с перечисления алгоритмов для майнинга и основных монет, использующих эти алгоритмы. Естественно, самый распространенный алгоритм – это SHA-256 и его король – Биткоин. Хотя с какой-то периодичностью в доходности майнинга он проигрывает той или иной монете. Второй по популярности алгоритм, облюбованный асиками, – это Scrypt, где властвует Litecoin. Третьим лег под асики алгоритм x11 во главе с монетой Dash, и именно в гонке производителей асиков x11 было много примеров, когда и что НЕ следует покупать и как себя нельзя вести. Далее были захвачены редкие алгоритмы x13 и x15, к ним же присоединились Quark и Qubit, а также x11ghost. Не успел рынок опомниться, как варианты алгоритма Blake для монет SiaCoin и Decred тоже пали перед вездесущими ASIC, и уже стало не так фантастично звучать появление подобных устройств для майнинга эфира на алго DaggerHashimoto или Ethash. Но перед тем как вышел асик для эфира, GPU-майнеры вздрогнули от появления cryptonight-майнеров для Монего, более нескольких месяцев находившихся в тени и добывавших тысячи монет для своих владельцев. Также не устоял и алгоритм хеширования Equihash с монетой Zcash, который проектировали изначально для защиты от ASIC. К чести команд разработчиков монет вызов, брошенный производителями ASIC, был принят, и алгоритмы хеширования были видоизменены, сделав устройства менее функциональными.

Основным элементом конструкции асика являются так называемые «лезвия» – платы, с размещенными на них асик-чипами, а также иными электронными компонентами. Платы устанавливаются вертикально, они соединены проводами – шинами, на них есть разъемы для питания, а также установлены алюминиевые радиаторы для отвода тепла. Корпуса делаются в форме куба или параллелепипеда, где сверху устанавливается плата управления (чаще готовый мини-ПК типа Orange Pi), а по бокам мощные вентиляторы для сквозного продува устройств воздухом. Схема сборки устройств мало отличается от производителя к производителю, но главным отличительным элементом является чип – сама ASIC-микросхема. Важное значение сегодня имеет технологический процесс (или техпроцесс), на котором построен чип, и указывается это значение в нанометрах – нм. Большинство лидеров сегодняшнего дня используют при производстве чипов 16 нм техпроцесс. Попадают остатки устройств, созданных на 28 нм техпроцессе. В горячую пору зимы 2017-2018-го некоторые производители выпустили несколько моделей таких устройств в надежде на большие продажи. Примером является Antminer V9 (по сути реинкарнация модели antminer s7) от компании Bitmain Tech. Стоивший в феврале 2018 года 20 000 рублей на заводе в Китае, сегодня он продается по 5000 рублей уже в России. Кому-то, как, например, компании Bitfury, также удалось избавиться от старых запасов 28 нм чипов и отработавших свое лезвий с 28 нм чипами. Сегодня такие устройства могут работать лишь в условиях бесплатного размещения и недорогой, очень недорогой электроэнергии. Кстати, буквально несколько дней назад компания Bitfury анонсировала свои новейшие 14 нм чипы Clarke и профессиональные майнеры в форм-факторе 19 серверов на их основе под именем Tardis. Следовательно, предыдущая модель сервера Bitfury B8 (на чипах 16 нм) уже теряет свою актуальность. Также Bitmain анонсировал ASIC по 7 нм технологии, ранее партнеры компании «Самсунг» – производитель асиков DragonMint и новичок рынка Halong Mining – заявили о производстве 10 нм чипов для майнинга, а еще ранее японская компания GMO объявила о скором выпуске майнеров на основе 7 нм чипов. Напомним, что чипы на более совершенном техпроцессе

имеют бОльшую производительность и гораздо меньшее энергопотребление в отличие от своих предшественников. Исходя из этого утверждения, покупка асик-устройства на основе техпроцесса 16 нм уже не имеет смысла и является рискованным вложением. Прошу учесть, что речь идет именно о майнерах под алгоритм SHA-256. В производстве устройств для других алгоритмов первые модели вполне могут выходить на дешевом в запуске 28 нм техпроцессе, а сегодняшние новинки только встают на 16 нм рельсы. Вернемся к конкретике. До бума 2017–2018 годов основными производителями ASIC числились компании Bitfury (промышленный сегмент), Bitmain, Innosilicon и Canaan с брендом Avalon. В период небывалого роста рынка в процесс производства активно включились в бренды Baikal, iBelink, Pinidea, WhatsMiner, DragonMint, позже также заявили о себе Ffminer, Bitfily, Dayun, причем Dayun выпустили майнер в алгоритме Lyra2REv2, пока единственный в своем роде. Именно такие новейшие асики, приобретенные в самом начале производства и демонстрирующие максимальную доходность, можно посоветовать к приобретению, но не по спекулятивной цене. Все основные производители оборудования расположены в Китае. Тем не менее в России также появилось несколько проектов по производству АСИК-майнеров. Первым широкой публике стал известен проект Sunrise Сергея Бобылева, также продемонстрировала возможность сборки майнеров в РФ компания «Фейсмен технолоджи», как и «Санрайз», стартовавшая со сборки устройств на основе старых хеш-бордов (лезвий) компании Bitfury с чипами 28 нм. Сегодня обе компании ведут сборку, используя 16 нм чипы, и готовятся к переходу на 14 нм технологию. Также не могу не упомянуть проект combiner.pro по выпуску единственного в своем роде промышленного майнера с жидкостным охлаждением на основе тех же чипов Bitfury, в котором мне довелось выступить сооснователем на этапе концептуализации проекта и выпуска первого тестового майнера. К сожалению, я не смог принять дальнейшего участия в реализации идеи и вынужден был покинуть команду еще до выхода промышленных образцов на рынок, получив лишь огромный опыт работы в инновационной сфере и массу полезных знакомств и новых друзей из криптосообщества. Как же разобраться в марках и моделях майнеров, как сделать выбор?

Ресурс [whattomine.com/asic](http://whattomine.com/asic) как раз демонстрирует нам более 10 популярных алгоритмов и их вариаций, в которых присутствуют асики и позволяет рассчитать текущий доход от их эксплуатации. Для получения расчета необходимо ввести параметры своего устройства – хешрейт и потребление, а также стоимость электроэнергии в пересчете на USD и нажать на кнопку калькуляции. В таблице результатов можно выбрать, что наиболее выгодно для майнинга сегодня. Также можно сравнить разные ASIC между собой, но так как цена их разная, придется сначала вывести значения, какую мощность и потребление вы получите на 1000 долларов вложений в тот или иной АСИК. Кстати, при покупке устройств многие учитывают такой параметр, как стоимость в USD за 1 Th/s вычислительной мощности. Этот параметр позволяет оценить эффективность начальных вложений в то или иное устройство. Чем меньше вы потратите на 1 Th мощности, тем выгоднее закупка. Например, при сегодняшней цене в 2500 USD и мощности 50 Th майнер Bitfury B8 имеет показатель 50 USD/Th. Лидер же рынка Antminer s9 стоит 500 USD и выдает 14,5 Th/s, что дает значение 35 USD за Th. При этом Bitfury потребит порядка 120 Ватт на террахеш, а Antminer 100 Ватт. Для розничного покупателя выбор очевиден, однако при промышленном использовании Bitfury может оказаться более грамотным выбором, т. к., сконструированные для дата-центров, они продемонстрируют большую надежность, плюсом станет возможность управления потреблением в зависимости от времени суток (учитывая дневной и ночной тариф на электроэнергию), что в конечном счете приведет к снижению операционных издержек в долгосрочном периоде. Для крупных проектов представители компании Bitfury предоставляют финансовую модель, с помощью которой можно сделать точные расчеты и прогнозы прибыли. При этом я не противник экспериментов и имел у себя не один АСИК разных производителей и разных моделей. В общем, все они заслуживают внимания и занимают свою нишу.

Проделав расчеты на сегодня, взяв за основу розничные цены крупнейшего оптово-розничного рынка SEG-market в Шенчжэне (Китай), я получил такой результат, основанный на гипотетическом наличии у меня 1000 долларов для входа в рынок. Тариф на электроэнергию взят в размере 0,05 USD за kWh, или около 3 рублей 30 копеек в национальной валюте. При этом значения доходности и сложности вычислений взяты средние за 7 дней.

Модель	Алгоритм	Цена \$	Шт. на 1000 \$	Мощ-ть на 1000 \$	\$/ед. мощ-ти	Ватт общ.	Ватт на ед.	Доход на 1000\$/дн.	ROI дней
Antminer s9i	Sha-256	500	2	29 Th	35	2900	100	3	334
Bitfury B9 Tardis	Sha-256	4680	0,21	16,5 Th	60	1350	82	2,1	476
Avalon A9	Sha-256	1000	1	20 Th	50	1800	90	2,5	400
Whatsminer m10	Sha-256	1900	0,53	17,5 Th	57	1160	66	2,5	400
Bitfily B1	Sha-256	1000	1	24,5 Th	41	2200	90	2,9	345
Innosilicon T2Turbo+	Sha-256	1900	0,53	17 Th	59	1200	70,5	2,4	416
DragonMint T1	Sha-256	600	1,67	26,5 Th	38	2500	94	2,95	339
Sunrise s13i	Sha-256	3800	0,26	12 Th	83	865	72	1,65	606

Аналогично можно рассчитать параметры для всех других алгоритмов, при этом раздел для GPU позволяет рассчитать и прибыльность некоторых видеокарт. Анализируя же таблицу, получается, что самыми быстро окупаемыми АСИК-устройствами для алгоритма SHA-256 из всех вышеперечисленных стали Antminer s9, Bitfily B1 и DragonMint T1, при этом самым энергоэффективным оказался WhatsMiner M10, что может легко сделать его лидером рейтинга при резком снижении курса BTC или росте сложности вычислений.

Ведя расчеты, мы не можем с точностью учесть массу важных показателей – как тот же рост сложности вычислений, непосредственно влияющий на доходность, объемы выпуска устройств заводами, перспективы роста или падения стоимости BTC, операционные издержки на содержание фермы из нескольких устройств и многие другие факторы. Покупая АСИК, легко можно стать заложником таких вот расчетов «в моменте». Допустим, завод выпускает новый тип микросхем ASIC. Он выводит на открытый рынок 100 единиц продукции и отправляет их по всем уголкам нашей планеты. Появляются обзоры на YouTube, специализированных форумах, в социальных сетях и блогах. Из уст в уста передается, что новый ASIC приносит по 150 долларов в день при его стоимости в 3 тысячи USD. За 20 дней можно окупить вложения: представьте, как круто! Что же происходит на самом деле? На ASIC делают предзаказы до Нового года, завод обещает, что выпустит три тысячи штук в феврале и еще пять тысяч в марте. Тут же спекулянты выкупают все имеющиеся места в очереди на предзаказ и начинают продавать еще несуществующие устройства по пять тысяч долларов. Однако, когда устройство будет фактически отгружено вам, доходность упадет до 20 долларов в день, и, соответственно, ваш ROI в момент получения товара составит уже 150 дней. При этом ведь предстоит еще следующий батч, гораздо больший, чем первый, значит, конкуренция возрастет в два раза! Имеем 10 долларов доходности в день через месяц после получения устройства. Ждать возврата инвестиций придется уже год, если не случится чудо. Такое может случиться именно с новейшими моделями асиков для новых, ранее не освоенных алгоритмов. Любой человек «в теме» сразу вспомнит ситуацию с майнером Antminer d3 и созданным вокруг нее ажиотажем. Конспиративные версии же гласят, что все это время, пока собирались деньги на предзаказ и якобы велась работа по сборке-отправке продукции, майнеры были уже готовы и установлены в дата-центре завода-изготовителя или близких к нему лиц, снимая самые сливки. Когда же доходность начала резко снижаться, в т. ч. из-за действий конкурентов, устройства почистили и отдали покупателям, вынужденным смириться с финансовыми потерями.

Несколько выводов, которые я сделал для себя, при работе с асиками. Покупать стоит только новейшие модели, желательно напрямую у завода-изготовителя, благо у всех есть сайты. Иначе, наценка посредника просто съест всю возможную прибыль. В период «хайпа» или «бума» цены

растут в 2–3 раза, а при последующей коррекции снижаются в 5 раз. Приобретая самый первый батч ранее производившегося устройства, которое демонстрирует просто сумасшедшую доходность, важно учесть, что устройство может быть «сырым». Приобретя один из первых в мире x11 асиков модели Pinidea DR1, я столкнулся с необходимостью отправки его в Китай для ремонта, назад мне прислали уже усовершенствованную модель DR2. Два месяца суперприбыльного майнинга были потеряны, и новый образец был продан мною, так и не окупив первоначальных вложений. Именно своевременная продажа является вторым ключевым фактором при работе с асиками. Срок доставки и возможность быстрого включения в работу не менее важны. Зачастую выгоднее организовать размещение устройства прямо в Китае, сразу после отгрузки с завода, либо использовать ускоренный вид авиадоставки в РФ. Чем раньше новейшее устройство включено в сеть, тем больше шансов захватить наиболее тучный период майнинга и выйти на самоокупаемость. Наличие возможности быстрого размещения в правильных условиях с бесперебойным электроснабжением, грамотной вентиляцией и обслуживанием – еще один немаловажный фактор.

## Вопросы электропитания

Для организации домашнего майнинга вам нужно немного понимать, как устроены системы электроснабжения в вашем доме. Если вы включите одну небольшую ферму из трех маломощных GPU, которую я описал чуть выше, максимальное потребление составит около 300 Ватт. С такой нагрузкой справится любая розетка, даже в старых домах советского периода на алюминиевой проводке и с неплотно прилегающими контактами. Нагрузка на сеть в этом случае будет минимальной. Но если вы включите в эту розетку пять компьютеров или даже пару мощных асиков, линия попросту не справится. Начнется излишний нагрев проводника, особенно в местах наличия соединений типа «скрутка» – распаячных коробках или при плохом монтаже кабеля к розеткам. Ко всему прочему, номинальная мощность автомата, который установлен у вас в щитке, тоже может оказаться не подходящей для такой постоянной нагрузки. В конце концов, суммарная максимальная мощность, выделенная на квартиру, может быть очень низкой и ограничиваться как сечением подводящего кабеля, так и установленными в щитке устройствами автоматики. Правильная дистрибуция питания, то есть организация электроснабжения в вашей домашней или промышленной ферме, – очень важная задача. Бывает так, что к одному автоматическому выключателю подключено несколько розеток, часть из которых занята энергоемкими устройствами типа чайника, микроволновки, утюга. Пока домашняя техника не работает – все будет хорошо. Но как только вся она включится и начнет давать нагрузку на сеть – может произойти срабатывание автомата, следовательно, отключение электроснабжения вычислительных устройств – равно простой и даже выход из строя некоторых элементов при неправильном возобновлении питания. Учитывая вышесказанное, необходимо соблюдать и требования пожарной безопасности. Интернет пестрит фотографиями сгоревших ферм из видеокарт и асиков, которые были неправильно собраны или содержали заводской брак.

Столкнувшись с необходимостью подключения даже пяти мощных ферм у себя дома, я стал в два раза внимательнее относиться к некоторым вопросам, которые мы часто считаем мелочами. Маркировка тройников и пилотов всегда содержит значение максимальной силы тока, с которой справится удлинитель. Зная эту цифру, можно учесть мощность, которую он способен выдержать. Например тройник-пилот на 10 Ампер способен выдерживать кратковременно 2,2 кВт нагрузки, а 16А – уже 3,5 кВт. Эти цифры легко получить, пользуясь базовыми школьными знаниями с уроков физики. Соответственно, включить более двух ригов по 1 кВт в один слабый тройник – существенный риск. Важно подумать не только о доходе с майнинга, но и о собственной безопасности и безопасности членов семьи, особенно в ваше отсутствие. Учтите, что укрупнять свою домашнюю ферму вы можете только до определенного предела: пока вы не упретесь либо в установленную электрическую мощность, либо в размер помещения и возможность его вентиляции для отвода излишнего тепла. Что-то наступит ранее, и, скорее всего, это будет вопрос вентиляции. Если читатель не обладает соответствующими навыками и знаниями, целесообразно проконсультироваться с профессиональным электриком, прежде чем устанавливать более трех средней мощности вычислительных устройств в своем жилище. Ведь случаи крупных возгораний ферм уже были: например, в ноябре 2017 года в Новороссийске случился пожар, в результате

которого полностью сгорела квартира владельца майнинговой фермы и сильно пострадала квартира соседей. Жилец съемной квартиры не соблюдал технику безопасности, включив в сеть слишком много энергоемких устройств без должной проработки схемы электропитания и вентиляции. Результат такой небрежности оказался весьма плачевным. Обычно выделенная мощность на одну квартиру или частный дом составляет от 10 до 15 кВт. Это значит, что при потреблении асика Antminer s9i в 1,5 кВт невозможно установить более 6 или 10 устройств у себя в квартире. При этом не получится пользоваться никакой другой бытовой техникой, а все лампочки придется заменить на светодиодные. Еще раз выражу свое мнение, что для домашнего майнинга можно использовать не более 5–6 средних ферм на видеоускорителях, грамотно распределенных по комнатам и соответственно запитанных электричеством. Единственный способ объединить все в одном небольшом пространстве – протянуть отдельный кабель с большим сечением от главного щитка и перевести риги на жидкостное охлаждение. Именно к такому выводу я пришел, эксплуатируя домашнюю ферму.

Хочу также еще раз вернуться к вопросу стоимости электроэнергии в данном разделе. Очень большим преимуществом домашнего майнинга является двух- или трехтарифная система учета, когда за энергию, потребленную вне пиковой нагрузки – в ночное время суток, вам придется платить в три раза меньше, чем днем. Используя возможности тонких настроек своих устройств, можно сделать так, что в период с 23:00 до 07:00 они будут работать на полную мощность, не учитывая возросшее энергопотребление, а в дневное время на максимально энергосберегающих настройках. В таком случае можно сэкономить на ежемесячном счете за электроэнергию до двух раз. Но все это будет работать лишь до тех пор, пока в нашей стране не заработает система нормативов предельного потребления электроэнергии домохозяйствами. Коротко: если вы потребите больше средних нормативов на одного проживающего, включится повышенный тариф. Сэкономить тогда точно не удастся. А при введении налога на майнинг квартира с круглосуточным повышенным потреблением станет легкой мишенью для контролирующих органов при выявлении нерадивых домашних майнеров.

Для правильного размещения ферм, состоящих из нескольких сотен устройств, необходимо специальное помещение. Ажиотаж 2017–2018 годов спровоцировал появление на рынке контейнерных решений эконом-класса, в которых правильно организованы электроснабжение и вентиляция. Установлены датчики и автоматизированная система управления майнингом. Первым наиболее известным решением такого рода является мобильный дата-центр на базе 40-футового морского контейнера BlockBox AC от компании Bitfury, вмещающий до 176 серверов. Весной 2017 года мне довелось быть гостем компании на одном из их дата-центров в Грузии, я оценил качество исполнения, но слишком большой уровень шума существенно сужает выбор места для установки контейнера. При этом из имевшихся на тот момент решений контейнерный дата-центр Bitfury был вне конкуренции. Уже в 2018 году мне довелось эксплуатировать собранный в России контейнерный ДЦ от компании Bitferra, исполнение которого также оставило только лучшие впечатления. Сегодня и крупнейший производитель ASIC – компания Bitmain – предложила рынку свой вариант контейнера AntBox на 324 стандартных юнита собственного производства. При стоимости около 900 000 рублей на заводе и учитывая доставку, имеем стоимость места для одного юнита, равную примерно 3000 рублей. Это лишь около 10 % от первоначальной стоимости нового устройства типа Antminer s9 и сравнимо с двумя месяцами аренды полки в майнинг-отеле. Для более дорогих моделей ASIC цена внедрения контейнерного решения в пересчете на 1 юнит будет еще меньше. Контейнерное решение хорошо именно тем, что основной упор в нем сделан на правильную дистрибуцию электропитания.

## Программное обеспечение

Как в промышленном масштабе майнинга, так и в домашних условиях очень важно программное обеспечение, которое позволяло бы наиболее комфортно управлять всем комплексом стоящих задач. В первую очередь важно, какой операционной системой вы умеете пользоваться. В общем случае вполне подойдет Windows последних поколений. В этой системе всегда есть выбор версий драйверов для установки оборудования (видеоускорителей), большой выбор программ-майнеров и сопутствующих приложений, таких как программы мониторинга оборудования или те же кошельки криптовалют. Речь, конечно, идет об эксплуатации GPU-ферм.

В случае с ASIC и множественными GPU-фермами опцией выбора являются системы на базе ОС Linux. Именно на ней построены специализированные операционки для майнеров, такие как HiveOS, EthOS, MinerOs, Awesomeminer и ряд других. В них уже «защиты» самые проверенные версии драйверов-устройств, есть возможность мониторинга и настройки «на лету», переключения пулов различных монет и алгоритмов. Есть возможность управления разноплановыми устройствами – и асиками, и GPU-фермами. Крупные провайдеры облачного майнинга или производители оборудования имеют собственные решения для управления майнингом и облачными контрактами: так, у компании Genesis mining есть продукт Genesis-Hive для управления собственными дата-центрами. Нужно отметить, что производители асиков зачастую устанавливают свою, основанную на том же Linux оболочку и встраивают в нее модифицированный под конкретные задачи майнерский софт. Такая прошивка чаще всего не подлежит изменению, хотя в среде профессионалов гуляют пользовательские версии ПО, позволяющие оптимизировать работу устройств для разгона или снижения шума.

Безусловным лидером среди программ-майнеров для видеокарт является софт от Claymore, имеющий версии для большинства популярных алгоритмов, а также dual-версии для одновременной добычи двух разных монет. В среде почитателей алгоритма cryptonight распространены майнеры XMR-stak и SRB, JCE и даже малоизвестные частные версии с ограниченным распространением. В большинстве случаев в майнер встроена комиссия разработчиков, составляющая от 1 % до 5 %. На определенное количество минут в сутки майнер переключает свою работу на кошелек разработчика. Для ASIC-устройств используются версии SGminer или CGminer или собственные разработки на основе публичного кода программ-майнеров. Управлять фермами из асиков также позволяет специальный софт, например упомянутый Awesomeminer. Сегодня активно ведется разработка новых софтверных решений, как для конкретного управления ригом, так и для объединения множества устройств под одной оболочкой, внедряются модули по управлению электропитанием на объекте, климат-контроль и улучшенные параметры сетевого взаимодействия и безопасности. Большинство таких профессиональных решений являются платными, с разовой или ежемесячной оплатой, и чаще всего одна лицензия распространяется лишь на одно устройство. При большом количестве видеокарт в обороте имеет смысл более плотная установка карт на материнскую плату, ведь за риг из 4 или 20 карт придется платить одинаково.

Выбор подходящего именно вам и вашему оборудованию софта для майнинга – не всегда простая задача. В условиях падающего рынка стали важны и процент отчисления разработчикам, и максимальная скорость хеширования, которую может показать программа в требуемом алгоритме, и демонстрируемый при этом уровень энергопотребления. Зачастую приходится перепробовать 3–4 решения, прежде чем добиться максимальной скорости и стабильности работы. Разница в значениях хешрейта может достигать 20 %, при том же потреблении энергии, что напрямую отразится на финансовых результатах, особенно при майнинге в промышленном масштабе. При этом майнер, подходящий к одному типу видеокарт, может плохо себя показать на других, но как бонус готов заставить и ваш центральный процессор работать в одной упряжке с видеокартами. Операционная система HiveOS позволяет вам выбирать из большого списка существующих майнеров, а служба поддержки готова добавить в систему новый достойный вариант за считанные дни. Для меня эта система на сегодня – лидер сегмента.

При погружении в майнинг пользователь непременно столкнется с вопросом увеличения производительности своих устройств за счет разгона, и для этого существуют как стандартные, так и специализированные решения. Например, известный геймерам и продвинутым пользователям софт для графических ускорителей MSI Afterburner имеет в себе множество полезных функций. Можно увеличить тактовую частоту работы памяти и понизить частоту ядра, когда это позволяет тот алгоритм, на который настроен майнер. Вполне реально снизить потребление карт, поигравшись с напряжением графического ядра и занизив параметр, устанавливающий общий лимит мощности для устройства, плюс тонкая настройка вентилятора поможет избежать перегрева устройств или снизить шум, когда система охлаждения работает вхолостую. Продукт Wattman как раз создан для управления питанием видеокарт. В специальных программах для майнинга этими параметрами также можно управлять, используя соответствующие команды в конфигурационном файле, но применение графического интерфейса всегда проще и понятнее, особенно начинающим. Ряд программ создан только для целей



увеличения параметров майнинга – это специальные редакторы BIOS видеокарт, позволяющие изменить заводские параметры с целью увеличения производительности GPU. К таким можно отнести Polaris Bios Editor для видеокарт компании AMD с одноименным чипом Polaris или программу OhGodAnETHlargementPill для разгона почти в 1,5 раза видеокарт от Nvidia, имеющих на борту память типа GDDR5x, на других картах этого производителя с более старым типом памяти GDDR5 (без X) модификация не сработает. Налицо узкоспециализированные решения для конкретных моделей видеокарт, позволяющие их владельцам получить существенные преимущества от владения именно такими графическими ускорителями. Существуют программы, вносящие изменения в Windows, оптимизируя его для майнинга, есть программы мониторинга (иногда совмещенные с аппаратной частью) и программы управления драйверами, программы оптимизации электропитания компонентов ПК и даже программы по подключению вашего ПК в сеть облачных вычислений и получению наград в криптовалюте, созданной для осуществления проекта.

## Глава 4

# Криптовалюта в реальной жизни

### Кошельки для цифровых денег

Для повседневного использования цифровых денег важно не только то, чтобы биткоин или другие монеты принимались торговыми точками, но и наличие у пользователя удобного способа потратить имеющуюся криптовалюту. Для хранения и переводов цифровых активов используют программы-кошельки, которые обладают различным функционалом и особенностями.

Холодный кошелек – это обычно аппаратный кошелек, который не имеет постоянного доступа в Интернет. Это либо флешка с чувствительными файлами для программного кошелька, который установлен на вашем компьютере, либо USB-устройство, на котором находится программный модуль управления этим аппаратным кошельком. Такой способ – наиболее защищенный вариант хранения Bitcoin или иных криптовалют, т. к. получить к нему доступ невозможно, не завладев им физически. Да и при этом доступ к аппаратному кошельку может быть дополнительно зашифрован. Наиболее известными представителями являются продукты Trezor и Ledger разных моделей. Например, модель Ledger Nano S поддерживает более 30 криптовалют, и перечень продолжает расширяться. Наличие дополнительных приложений, доступных к установке на ваш кошелек, сильно расширяет его функционал. Но помимо таких достоинств, как мультивалютность, компактность и безопасность, холодные кошельки имеют и свои недостатки. Некоторые из них сложны в использовании, отсутствует внятная русификация, некоторым требуется наличие полного блокчейна монеты на ПК для осуществления транзакций, да и в принципе нужен ПК для операций с кошельком, к тому же пользователь может потерять секретную фразу для восстановления кошелька, состоящую из 24 слов, которую просто неудобно хранить и сложно запомнить. Держать эту фразу на бумаге – почти то же самое, что перейти к формату бумажного кошелька, который можно сгенерировать в Интернет бесплатно. Именно бумажный кошелек, который можно создать на таких сайтах, как [bitaddress.org](http://bitaddress.org), [bitcoinpaperwallet.com](http://bitcoinpaperwallet.com) или [myetherwallet.com](http://myetherwallet.com) (MEW) что для биткоина, что для эфира и других криптовалют, является наиболее дешевым способом холодного хранения криптовалюты. Я бы все-таки посоветовал сохранять резервную копию файла кошелька или ключевого файла MEW на USB-флеш в надежном месте. Ведь если Ledger стоит более 100 долларов США, что также сложно отнести к разряду достоинств, то бумажный кошелек не стоит ничего, ну или может быть приравнен к стоимости недорогой флешки. Однако есть случаи фишинговых атак на владельцев MEW-кошельков, когда в письме вам подсовывают ссылку на похожий сайт и просят ввести пароль и загрузить ключевой файл под предлогом каких-то важных изменений в системе. В данном случае всегда важно проверять адрес сайта и наличие защищенного протокола <https://> в адресной строке и верного SSL-сертификата рядом с адресом сайта. Случай такой кражи имел место в кругу знакомых мне майнеров.

Новинкой мира криптовалют можно назвать смартфон FINNEY на базе модифицированной специально под блокчейн и dApps системы Android, который можно заказать у израильской компании [sirinlabs.com](http://sirinlabs.com). Помимо своей блокчейн-направленности и даже возможности майнинга

внутренней валюты проекта SRN реализован и весь стандартный функционал смартфона. Поводом помещения его в данный раздел является тот факт, что в него также встроено холодное хранилище для криптовалют. Судя по сообщениям на новостных ресурсах, ориентировочная цена устройства составит 999\$, которые необходимо оплатить с помощью токена SRN.

Горячий кошелек – это программный кошелек на вашем ПК, аккаунт на бирже или любом Интернет-сайте, который предлагает вам генерацию кошелька и имеет постоянный доступ в Интернет. Отличие программного кошелька на компьютере от онлайн-собрата в том, что вы владеете всем функционалом кошелька – закрытым ключом, ключевой фразой, резервными копиями, а также всеми возможностями программы-кошелька, которые она предоставляет. Это могут быть функции по запуску мастернод, приватной отправки и перемешивания монет, осуществление запросов к блокчейну и так далее. Кошелек может быть комбинирован со специальной блокчейн-версией Интернет-браузера с возможностью загрузки dApps и другими специальными опциями, как в проекте Mist для Ethereum. В данном случае вы и только вы отвечаете за сохранность собственных средств. Если вы не зашифровали файл кошелька wallet.dat или оставили пароль или ключевую фразу в той же папке в текстовом файле, а кто-то получил доступ к вашему компьютеру и похитил средства – это полностью ваша вина. Я лично знаю историю, когда взлом электронной почты дал возможность злоумышленнику получить доступ к нескольким кошелькам валют и нанести существенный финансовый ущерб команде криптоэнтузиастов, не позаботившихся о безопасности.

Кошелек, размещенный на вашем ПК, может быть также «легким» или «тяжелым», в зависимости от того, скачивает ли он полную цепочку блоков на жесткий диск или нет. Встречаются и варианты названия «тонкий» и «толстый» кошельки по той же аналогии. Основным кошельком для биткоина является bitcoin-core wallet с официального сайта bitcoincore.org, а для любой другой валюты доступны для скачивания версии кошельков с их официальных сайтов. Существуют и кошельки сторонних разработчиков, например, мультивалютный Jaxx или ориентированный на эфир Parity. Последний содержал в себе уязвимость, с помощью которой летом 2017-го было похищено 82 000 эфиров у проекта Aeternity. Поэтому выбор кошелька и соблюдение правил его безопасного использования – это очень серьезная и важная задача.

Горячий кошелек на онлайн-сервисах, таких как Coinbase, или blockchain.info, или аккаунт на криптовалютной бирже, не дает вам больших возможностей по управлению средствами, обычно выполняя функцию временного хранения небольших объемов криптовалюты и последующей траты внутри самого сервиса. Нередки случаи краж средств пользователей с таких кошельков. С сервиса NiceHash в декабре 2017 года было украдено, по разным сведениям, около 5000 биткоинов. Соответственно хранение больших сумм на горячих кошельках может привести к их полной потере. К чести компании NiceHash они смогли возместить похищенное с помощью внутренней программы поощрения пользователей. В любом случае, что при использовании холодным кошельком, что при установке горячего вам нужно помнить три главных правила: безопасность, безопасность и безопасность!

Есть программные кошельки, которые работают на смартфонах и их можно синхронизировать с горячим кошельком на сайте сервиса или своем ПК, получая возможность управлять своими цифровыми наличными отовсюду. Зачастую мобильные приложения для биржевой торговли таких площадок, как, например, СЕХ.Ю, используются в качестве кошелька криптовалюты. И раз уж мы затронули тему обмена, рассмотрим случаи, когда пользователь не может потратить криптовалюту напрямую, и требуется конвертация цифровых активов в фиатные, традиционные деньги.

## **Обмен криптовалют на фиатные деньги**

Первый способ – личная сделка. Существуют сервисы и форумы, на которых можно найти объявления о купле-продаже криптовалюты напрямую, без биржевого посредника. Один из старейших подобных сервисов – localbitcoins.net – существует с 2012 года и представлен в 246 странах и 16 406 городах. Это огромная доска объявлений с системой рейтингов, проверкой регистрационных данных участников и возможностью проведения как сделок с помощью переводов средств с карты на карту, так и за наличные при личной встрече. Касательно России – был инцидент, когда основной домен localbitcoins.com был внесен в реестр запрещенных ресурсов

на основании решения 2-10224/16 от 05.07.2016 Приморского районного суда города Санкт-Петербурга. Но даже несмотря на это, пользователи продолжали работать с площадкой, используя VPN-сервисы и анонимайзеры, а количество объявлений для обмена в одной только Москве превышает 7500, всего же по России их более 10 000. Вам достаточно выбрать свой город и провести P2P-сделку лично либо довериться проверенному продавцу/покупателю и задействовать кредитную карту для платежа, без необходимости встречи со второй стороной. Отсутствие посредника – самый идеальный способ превращения криптовалюты в фиатные деньги и наоборот, это именно то, что является одной из основ ее существования и глобальных преимуществ. Важно учесть вопрос доверия сторон друг другу и не забывать, что мошенники могут встретиться везде. Такой уж это рынок, на котором много кто хочет поживиться за счет других.

Второй способ – обменный пункт. Обменники представляют из себя более автоматизированную платформу по проведению транзакций с отдельным сайтом и даже мобильными приложениями. Функционируют обменные пункты так же, как и личный обмен, и еще не факт, что подобная сделка безопаснее, чем p2p-сценарий. Автоматизация может быть достигнута лишь при обмене на электронные деньги (Яндекс. Деньги или Webmoney), но курс обмена и комиссия, взимаемая при дальнейшем снятии в банкоматах, могут отбить желание проводить сделку. Такие сервисы, как bestchange.ru, ведут мониторинг обменных пунктов, есть система отзывов и рейтингов, но кто находится на той стороне, не всегда понятно. Чаще всего разница между отдельным менялой с localbitcoins, профильного раздела популярного криптовалютного форума, и неким сервисом, называемым обменным пунктом, абсолютно отсутствует. Часть обменных пунктов имеет сервис по личному обмену, но минимально требуемая сумма сделки для организации встречи может быть высокой. Конечно, наиболее открытые сервисы имеют и офисы, и некоторое подобие обменных касс, при этом случаи мошенничества происходят и в стенах подобных заведений. Мой опыт обмена мелких сумм с помощью автоматически выбранного варианта сервисом bestchange.ru только положительный: из десятка операций ни одна не вызвала проблем, деньги в полном объеме зачислялись на мой счет пластиковой карты, перечисление всегда происходило от физического лица. Для того чтобы воспользоваться обменом, в правой колонке сайта нужно лишь выбрать, что и на что вы хотите поменять, а сервис выведет в таблицу все варианты, начиная с самого выгодного, в ней можно увидеть и имеющиеся в распоряжении обменника резервы, и рейтинг, и отзывы клиентов.

Третий способ – финансовые учреждения, предлагающие выпуск пластиковых карт с привязкой к ним криптовалютного кошелька. Большой проблемой является размер разовых минимальных комиссий за осуществление единичной операции. Она может взиматься и при покупке в точке продаж, и в банкомате. При этом при снятии наличных к базовой комиссии еще прибавляется процент, а дневной и месячный лимиты на снятие бывают слишком небольшими. Такие продукты, как Wirex, Coinsbank, BitPay и другие, предлагают карты в валюте, а значит, при снятии рублей вы потеряете еще и на конвертации из иностранной валюты в рубль. При этом не всегда заказ подобных карт доступен для россиян. Более-менее подходящим для РФ можно считать продукт компании Харо, позволяющей выбрать рубли в качестве основной валюты. При желании обладать самым подходящим вариантом дебетовой криптовалютной карты просторы Интернета, содержащие массу обзоров и сравнений подобных продуктов, помогут определиться с выбором.

Четвертый способ – использовать специализированный банкомат. На сайте coinatmradar.com можно найти точки их размещения даже в России. Разные модели банкоматов демонстрируют разную степень удобства в обращении с ними, а также разный уровень жадности операторов в установлении комиссии за обмен. При небольших суммах вряд ли вы почувствуете удар по своему кошельку, но при крупных сделках разница может стать ощутимой. К слову сказать, установка биткоин-банкоматов и терминалов является одним из достаточно простых и прозрачных способов заработка на криптовалюте.

## **Возможности применения криптовалют в России**

Несмотря на разнонаправленные векторы заявлений крупных и мелких чиновников и политических деятелей России о судьбе криптовалют, сегодня риторику властей можно назвать скорее положительной, чем отрицательной. Хотя нужно признать, что у тех, кто занимается законотворческой, управленческой, государственной деятельностью у нас в стране, нет

достаточного количества времени на углубленное изучение обсуждаемой нами тематики. Красной тряпкой для чиновников, силовиков и банкиров остается возможность применения криптовалют в нелегальной деятельности, хотя и до появления криптовалют криминалитет как-то справлялся со своими задачами, используя вполне традиционные инструменты. Объявленный в 2017 году курс на регулирование криптоиндустрии и создание профильного законодательства вселил надежды, что не за горами новая страница для деятельности криптовалютных компаний в нашей стране. Многие зарубежные финтех-компании из профильного сектора просто боятся заходить на российский рынок, не зная, чего от него ожидать. Меня лишь волнует перенос принятия законопроектов о криптовалютах с весенней сессии Государственной Думы на осеннюю и опять на новую весеннюю... В таких условиях как раз проще развиваться серому сектору бизнеса, нежели цивилизованным бизнесам. Однако даже в период правового вакуума, криптосообщество не дремлет, и применение цифровой наличности и блокчейн в нашей стране набирают обороты.

Самое широчайшее развитие в нашей стране приобрела индустрия майнинга криптовалют. Наличие огромных полуразрушенных производственных и пустующих складских площадей, дешевой рабочей силы и очень выгодных тарифов на электроснабжение в некоторых регионах РФ сделали майнинг в России очень выгодным, а город Иркутск с минимальными тарифами на электроэнергию – лидером и даже «Столицей майнинга». Домашние тарифы на электроэнергию также позволяют частным небольшим фермам конкурировать с Китаем, США и Европой, где стоимость киловатта в 1,5–2 и даже 3 раза дороже по сравнению со средним тарифом по регионам России. И если ранее большинство оборудования для майнинга было по сути нелегальным, сегодня в реестре криптографических средств числятся десятки устройств, разрешенных к ввозу в страну, что дает возможность крупным инвесторам развивать промышленный майнинг, строить специализированные дата-центры и даже крупные производственно-ремонтные базы.

Для малого и среднего бизнеса существенным подспорьем стал бы разрешенный легальный оборот криптовалют, который позволил бы увеличить объем продаж своих товаров на экспорт, т. к. существенно сократились бы организационные издержки, связанные с проведением валютных операций. Многие небольшие бизнесы, ориентированные на туристов, смогли бы привлечь дополнительную аудиторию за счет приема к оплате основных криптовалют. Также возможность привлечения инвестиций в криптовалюту могла бы дать большой толчок для многих предприятий, в том числе крупных, и бизнесов, не совсем связанных с IT и финтех-индустрией. Одним из наиболее частых вопросов, которые я слышу: как провести небольшое ICO, то есть организовать привлечение инвестиций в бизнес, уже существующий или находящийся на низком старте?

Есть возможность перенять американский опыт пенсионных накоплений в зрелых криптовалютах. На одной из конференций, организованной Coinsbank, я общался с американцем, который еще в начале 2015 года приобрел Bitcoin по цене чуть выше 400 долларов. Сообщив в своем блоге, что сделал таким образом инвестицию для выхода на пенсию, он получил шквал критических комментариев. Особенно шквал критики и язвительных замечаний обострился в середине того же года при падении курса до средних 250 USD. Сейчас даже при упавшей по сравнению с январем 2018-го цене его инвестиция принесла огромный плюс. В США при традиционном консервативном мышлении на своем капитале можно заработать максимум несколько процентов годовых, и это еще считается очень достойно. Если вы положите деньги в банк на депозит, вам вряд ли дадут больше двух процентов годовых. Даже если вы рискнете и войдете в некий инвестиционный портфель, вряд ли вам повезет заработать более 30 % в год. А мой собеседник увеличил свою свободную часть пенсионных накоплений в 15–17 раз с учетом текущего курса биткоина в диапазоне значений от 6000 до 6800 долларов США. Надеюсь, он продал их зимой 2018 года в три раза дороже, а летом купил снова, оставив себе солидный куш. Сегодня в США работает официальный криптовалютный пенсионный страховой фонд BitCoinIRA, возглавляемый не кем-то неизвестным, а бывшим директором монетного двора США Эдмундом Мойем. Раз история вполне работоспособна, значит, она применима и в России. Пенсионные накопления стремительно дешевеют из-за ослабления национальной валюты. Перевод их даже малой части в перспективные криптовалюты или надежные фонды криптовалют позволил бы сохранять и приумножать пенсионный капитал. Опять же, без законодательной базы невозможно создать юридическое лицо с инновационной стратегией инвестирования, которое

имело бы право само управлять пенсионными накоплениями граждан либо дало возможность существующим управляющим компаниям участвовать в блокчейн-проектах.

Если говорить о возможностях технологии блокчейн в России в отрыве от биткоина или криптовалют, то ее сфера применения достаточно обширна. Блокчейн – это реестр, база данных, которая может в некоторых случаях показать бОльшую эффективность, чем традиционные базы данных, которыми пользуются наши государственные органы. Блокчейн неизменяем, децентрализован, прозрачен и гибок. Он лишен внешнего контролирующего фактора, который может каким-либо образом вмешаться в реестр. Имея огромный интеллектуальный потенциал, наша страна может экспортировать решения, основанные на блокчейн, по всему миру. Логистика, фармацевтика, недвижимость, инвестиционная деятельность – сфер, где применим блокчейн, очень много. Создав обучающие, внедренческие центры, особые зоны с государственной поддержкой, можно вывести Россию в число лидеров новой криптоэкономики и привлечь большой объем валюты в экономику страны.

Некоторое время назад ходили слухи о крипторубле, как о перспективе развития экономики страны. С одной стороны, правительство не может принимать в этом участие, т. к. криптовалюта должна быть децентрализованной. И все же на рынке существуют централизованные блокчейн-активы, управляемые группой лиц, компаниями, а не сообществом. Такими примерами являются Ripple и стейблкоин Tether – USDT. Стейблкоином он является условно, о чем я писал раньше. В теории ничто не мешало бы создать и стейблкоин, привязанный к обеспеченному нефтью или золотом рублю и легко конвертируемый в любую другую криптовалюту. Как минимум поднялся бы престиж национальной валюты, расширились бы возможности для международного сотрудничества, уменьшилась бы привязка к доллару (как, впрочем, и с ростом свободного оборота криптовалют в целом). Есть все предпосылки для появления в 2019 году целого ряда обеспеченных национальными валютами стейблкоинов, и мы имеем все шансы иметь свой, и не деревянный, а золотой, с цифровым отливом рубль.

Упомянув о привлечении инвестиций в экономику страны, считаю важным уделить еще раз внимание теме ICO и попытаться наложить ее на существующую бизнес-реальность, оценить перспективы применения такой схемы финансирования в масштабе страны.

## **ICO-инвестиции в России**

Initial Coin Offering – первичное предложение монет (также иногда с заменой слова Coin на Token) – сейчас является неплохим способом создания некоего подобия децентрализованного акционерного общества и получения инвестиционного акционерного капитала на реализацию нового проекта. Многие помнят так называемые «народные IPO» Сбербанка и ВТБ, прошедшие не совсем вовремя и не совсем удачно для инвесторов, но нам важна именно суть процесса. Этими банками были затрачены колоссальные средства и силы для реализации проектов, отличие ICO же в том, что процесс подготовки и реализации гораздо проще и дешевле. Мне кажется, не зря в Беларуси в первую очередь разрешили именно ICO помимо обменных операций с криптовалютами, хотя и в рамках единственного «парка высоких технологий» процедура привлечения инвестиций путем ICO способна значительно увеличить приток иностранного капитала в страну и в какой-то мере открыть доступ к инвестициям гражданам тех стран, на кого действуют различные санкционные ограничения, введенные против России. По оценке многих успешных ICO большинство криптовалютных инвесторов были жителями Северной Америки, Европы, Азии, но не России и стран СНГ. По уровню вложений россияне и граждане ЕАЭС занимают не более 15 процентов для международных проектов. Естественно, этот процент существенно больше в российских локальных проектах, из них достойных внимания и неуличенных в мошенничестве или его признаках можно отметить лишь несколько. Сегодня только набирают обороты расследования сборов в мошеннических ICO, Генпрокуратура и ЦБ РФ обвинили проект Cashberry в создании массовой финансовой пирамиды, специализированные каналы в мессенджере Telegram, как и канал «ICO-крипто-мужик» и сайты наподобие cryptokompromat.ru, ведут разбор потенциально мошеннических проектов, порой с убедительными доказательствами, и наверняка дальше громких дел будет больше, в т. ч. в публичной сфере и с привлечением правоохранительных органов. По некоторым исследованиям до 80 % сегодняшних ICO – мошенничество. Введение законодательного регулирования отрасли очень помогло бы в

обелении процесса ICO и дало понятные инструменты для реального бизнеса в привлечении инвестиций и развития большого числа проектов в различных отраслях экономики.

Большой интеллектуальный и творческий потенциал, направленный в нужное русло, смог бы помочь развитию бизнеса в нашей стране в период неблагоприятных внешних геополитических факторов. У нас достаточно профессионалов в области юриспруденции, финансов, маркетинга, бизнес-администрирования, программирования и других необходимых компетенциях, требуемых для реализации ICO.

Рассмотрим небольшой пример, как можно было бы совместить множество идей в одном ICO-проекте на благо страны. Сейчас в списке top500.org 500 лучших суперкомпьютеров, самая мощная российская машина «Ломоносов-2» занимает всего лишь 72-ю строчку, уступив за год 13 позиций, а еще два известных представителя давно ушли ниже первой сотни рейтинга. В 2016 году этих компьютеров в топ-100 было семь, в 2017-м осталось лишь три, сегодня один. Второй суперкомпьютер в локальном российском рейтинге top50.supercomputers.ru, установленный в Росгидромете, едва удержался в конце второй сотни мирового рейтинга. Еще в 2012 году было заявлено об инвестициях в размере 1 миллиарда долларов для создания в России суперкомпьютера или экзаккомпьютера мощностью более 1 эксафлопса, при том что сегодняшний мировой лидер «Саммит» из США обладает лишь примерно 1/9 долей эксафлопса, потребляя 9 мегаватт электроэнергии, да и весь топ-100 рейтинга суммарно едва дотягивает до 0,8 эксафлопса. А в начале 2017 года некоторыми сайтами сообщалось, что в ядерном центре в Сарове этот экзаккомпьютер уже есть. Почему такая новость не стала мировой и почему так мало внимания уделено работе такого гиганта, непонятно, возможно, это была лишь фантазия единичных журналистов. А вот новость о том, что инженеры из Сарова пытались майнить криптовалюту на секретном суперкомпьютере, облетела все мировые средства массовой информации. Вернемся же к сути. Россия обладает самым важным ресурсом для создания подобного компьютера, пусть даже на импортных компонентах – это избыточная и недорогая электроэнергия. Потребление одного лишь китайского «Гяньхе», занимающего 4-ю строчку мирового рейтинга, составляет 15 мегаватт, а суммарное потребление топ-100 мировых лидеров составляет цифру, близкую к 300 МВт. Если учесть, что достаточно современные «Саммит» и «Сиерра» потребляют вдвоем около 20 мегаватт и производительность их составляет 0,2 эксафлопса, то мы легко подсчитаем, что современный экзаккомпьютер должен потреблять не более 100 МВт на 1 EFLOPS. Чтобы понять, что такое 100 МВт, давайте вспомним простой масляный электрообогреватель, способный обогреть небольшую комнату, который потребляет 1 кВт. На 1 Мвт их нужно 1000, а на 100 мегаватт уже 100 000, непрерывно работающих. Пользуясь этим примером, легко представить и количество тепловой энергии, которое выделится этим мега-котлом. Задавшись целью построить такой компьютер, вполне реально задействовать незагруженные мощности атомных или гидроэлектростанций, например в холодном климате Сибири. По разным оценкам Иркутская область обладает более чем 1 гигаваттом свободных электрических мощностей, при этом тарифы на нее одни из самых низких в мире. Выделяемое тепло можно было бы утилизировать с помощью систем жидкостного охлаждения, произведенных из местного алюминиевого сырья (оказавшегося под санкциями Запада), и отапливать им круглогодичные теплицы, жилые и нежилые строения. Сколько бы стоил такой проект и сколько бы он заработал? По очень условным расчетам при затратах в 200 000 000 долларов проект мог бы быть реализован за 1 год и принести массу плюсов научной сфере и экономике государства. Такой проект мог бы поддерживать огромное множество инновационных начинаний, молодых ученых, объединить тысячи людей для реализации масштабного проекта. Идея реализации могла бы быть следующей: за основу берется гражданское, но высокоуровневое Hi-End-оборудование, как, например, улучшенные материнские платы, имеющие возможность установки от двух до четырех видеоускорителей с максимальной пропускной способностью шины, а также хороший многоядерный процессор, быструю оперативную память плюс топовые «игровые» графические ускорители уровня Nvidia gtx 1080ti или новейшие rtx 2080ti. Почему не профессиональное оборудование? Первая причина – стоимость таких решений ниже в разы по сравнению с профессиональными решениями, но при этом производительность падает максимум на 1/3. При аренде мощностей для рендеринга вы легко можете найти предложения, основанные на серверах с установленными там видеоускорителями 1080ti. Индустрия давно применяет стандартные комплектующие для организации облачных хранилищ, проведения коллективных научных изысканий, серверов удаленного гейминга и рендеринга. При необходимости апгрейда

оборудования гражданские компоненты могут быть гораздо легче реализованы на вторичном рынке или распределены между участниками. Продать или как-то пристроить устаревшие серверные решения в разы сложнее. По сути такой суперкомпьютер мог бы быть объединением разного уровня компьютеров, что сейчас пытаются реализовать такие проекты как iExes, Golem, Sonm, Iagon, IOTA и ряд других. При этом идея облачных, или «туманных», вычислений за счет объединения массы обычных компьютеров в кластеры настолько популярна, что iExes, имеющий за плечами многолетний опыт постройки крупных дата-центров, завершил сборы хард-капа (максимальной планки финансирования) буквально за несколько минут, а это ни много ни мало 12 млн долларов США. Sonm, о котором, впрочем, можно найти очень разнонаправленные отзывы, собрал 42 млн долларов. Iagon, вышедший на арену в кризисный 2018-й, смог собрать софт-кап (минимальную планку финансирования для запуска проекта) более 1 млн долларов. Самый ранний из перечисленных проектов – Golem – был в десятке лидеров 2016 года с 8,2 млн долларов США. И это частные проекты, токены которых будут обеспечены лишь работой команды и реализацией идеи. Собственной физической вычислительной инфраструктуры, способной претендовать хоть на какое-то место в топ-100 суперкомпьютеров, не будет. Представьте себе проект с государственной поддержкой (в виде недорогой атомной или гидроэлектроэнергии и земельного участка) при содействии научного сообщества, помощи блокчейн-комьюнити и финансировании за счет краудфандинга в виде «народного ICO». Вы скажете, зачем тогда строить дата-центр, возведение которого при уровне Tier2-Tier3 обойдется от 15 до 25 тыс. USD за квадратный метр, когда можно использовать имеющиеся ресурсы жителей не только нашей страны, но и всей планеты? Я отвечу, что это может стать второй частью задачи. Централизованный вычислительный кластер с научными и испытательными лабораториями, собственным образовательным учреждением, юридической службой, площадями для стартапов и конференций смог бы принести гораздо больше пользы и создать максимум предпосылок для завоевания лидерства РФ в блокчейн-индустрии. Объединив сотни проектов, можно было коллективными усилиями и с помощью находящейся под рукой полностью развитой инфраструктуры сделать шаг к научному прорыву, так желаемому политиками, экономистами и прогрессивными членами общества. Даже на одних оборонных исследованиях, изучении проблем ядерной физики, фармакологии и химии, можно было получить существенный экономический эффект. А если просто включить все имеющиеся мощности на майнинг, в т. ч. собственной внутренней криптовалюты, только это способно окупить вложения за срок от 3 до 5 лет, с учетом плановой замены устаревшего оборудования на новое. Если взять все 70 миллионов официально работающих граждан страны, то для построения с их помощью лучшего в мире экзакомпьютера может понадобиться лишь по 3 доллара с человека. Это всего 200 рублей, стоимость одного простого бизнес-ланча в кафе. Даже если каждый 5-й рискнет и выделит по 1000 рублей, сумма невелика, зато наша страна могла бы стать лидером блокчейн-индустрии в мире. Для скептиков, считающих сбор в 200 млн долларов чем-то космическим, могу лишь привести данные о сборах трех самых успешных ICO за 2018 год. Hdac, проект Hyundai для Интернета вещей – 258 млн долларов. Filecoin – проект облачного хранилища (опять же на компьютерах пользователей) – 257 млн долларов, из них 200 за первые полчаса с момента публичного старта, и проекты Tezos и EOS Stage1 (именно первая стадия) – очередные «убийцы Ethereum» с собственными блокчейнами и смарт-контрактами – собрали по 230 млн долларов каждый. Все, кроме Hdac, – это проекты по созданию программных платформ. Вдумайтесь, миллиард долларов США на четверых, в основном для написания и внедрения программ... Какие же еще проекты востребованы на рынке криптовалют и блокчейн? Обратившись к любому ICO-агрегатору, можно с легкостью выяснить категории, в которые группируются ICO. Номенклатура отраслей очень большая, и количество проектов в каждой из них – десятки. Справедливости ради скажу, что иногда один проект попадает в разные категории, и тем не менее вот какие ICO могут проводиться в России, исходя из мирового опыта: в области искусства, в сфере банковского дела и финансов, искусственного интеллекта и Биг Дата, игорного бизнеса и развлечений, спорта и туризма, образования и бизнес-сервисов, медицины и торговли, интернета и виртуальной реальности, юриспруденции и страхования, энергетики и коммуникаций, социальной сферы и благотворительности, производства товаров, в т. ч. электроники и робототехники, – в общем, практически везде. Любой бизнес может рассчитывать на привлечение средств.

## Рынок криптовалюты и блокчейн

Я уже приводил цифры капитализации рынка криптовалют. Нельзя сказать, что это реальное голое отображение происходящего. Сегодняшнее состояние рынка я бы оценил как позу бегуна, застывшего на низком старте перед рывком вперед. До сих пор спортсмены лишь разминались, и судья еще только готовится произвести стартовый выстрел. Кризис рынка криптовалют 2018 года – лишь затишье перед бурей, идет масса кажущихся невидимыми процессов и работы, которые рано или поздно станут явными и прорвутся вовне. Я бы охарактеризовал перспективы ближайших двух лет как растущий рынок, рынок возможностей. Если сравнить развитие отраслевых рынков России, Запада и Азии, то впереди всех шагают США и развитые страны Азии: Япония, Южная Корея, Сингапур. Некоторые европейские государства не отстают. В производстве майнеров, чипов, всего оборудования для майнинга впереди всех Китай, рынок специализированного майнингового оборудования захвачен компаниями из КНР, и пока повлиять на это невозможно. Объемы продаж гигантов индустрии графических ускорителей составляют сотни миллионов долларов в квартал только для нужд майнинга, о чем в середине 2018 года сообщала компания Nvidia. Объемы продаж ASIC-устройств вряд ли ниже, а вероятнее, в разы выше. Финансовые криптовалютные институты широко распространены в Гонконге, Швейцарии и США. Суточный объем торговли криптовалютами, который регистрирует популярная аналитическая площадка [coinmarketcap.com](https://coinmarketcap.com), составляет более 10 млрд долларов. Для примера: объем торгов на московской бирже ММВБ лишь не более двух десятков раз за весь 2018 год превышал значение в 1 млрд долларов США, единожды преодолев показатель в 2,5 млрд долларов, чаще демонстрируя средние значения чуть выше 0,5 млрд USD в сутки. А если сравнить акции российских компаний с токенами и монетами в криптоиндустрии, напрашиваются печальные выводы, и ситуацию нужно менять! Рынок услуг в области блокчейн составляет миллиарды долларов уже сегодня – такой вывод можно сделать из сборов инфраструктурных проектов, проводивших ICO в 2018 году. Только крупнейшие 10 проектов привлекли инвестиций на 1,7 млрд долларов США. В сотни миллионов оценивается и рекламный рынок сферы блокчейн, что заставило компанию Google частично отказаться от ранее введенного запрета на рекламу ICO и криптовалютных проектов. Рынок юридических и консалтинговых услуг может также составлять цифры с шестью нулями. При этом многие так называемые эдвайзеры – советники – берут десятки тысяч долларов лишь за упоминание своего имени в составе команды очередного криптостартапа, не участвуя в делах фактически, а стоимость профильных юридических услуг завышена в разы в силу отсутствия большого числа профессионалов, разбирающихся в тонкостях международного законодательства в области блокчейн и криптовалют. По моему мнению, как и по мнению многих энтузиастов, развитие рынка будет продолжаться, и его ждет светлое будущее, хотя делать какие-то публичные прогнозы на столь непредсказуемом поле я считаю делом неблагодарным.

## Будущее криптовалют и блокчейн

Реально представить себе развитие технологий и движения индустрии блокчейн мне представляется вероятным лишь на коротком отрезке, а долгосрочные перспективы проще назвать смелыми личными фантазиями, нежели строгими научными заключениями. При этом, оглянувшись в прошлое, можно сделать некоторые выводы о будущем. Те амбициозные проекты, которые уже собрали инвестиции на решение вопросов по глобализации, упрощению, унификации и внедрению разных блокчейн-проектов, должны через полгода-год показать результат своей деятельности. Учитывая исследования о мошенническом характере 80 % ICO-проектов 2017–2018 годов, рисуется не самая радужная картина. Массовый отказ от обязательств, падение стоимости отдельных токенов, исчезновение разработчиков и следующие за этим долгие судебные тяжбы и следственные действия могут подорвать доверие широких масс ко всем проектам рыночного сегмента финтех и IT-инноваций поголовно. Какое-то количество замыслов, несомненно, будет реализовано, но достаточно ли для перевеса чаши общественного признания, а не чаши порицания? Наделение государствами официальным статусом криптовалюты, выпуск отдельными странами своих стейблкоинов, расширение международной юридической базы станут явным сигналом для прихода в отрасль консервативных инвесторов, не чувствующих себя защищенными сегодня, а это повлечет за собой волну среднего и мелкого капитала. Тема прихода в криптовалюты и блокчейн институциональных инвесторов часто поднимается на разных уровнях, и если мы увидим грамотное поведение политиков и законодателей – они точно придут. Введение



же массовых запретительных мер и избыточного регулирования из-за превышения критической массы плохих криптоактивов над проверенными и доверенными спровоцирует отток осторожных инвесторов с рынка. Здесь стоит упомянуть и о возможном влиянии крупных держателей криптоактивов на биржевые курсы и их способности манипулировать рынком. Существуют «живые» кошельки биткоинов с крупными суммами на них, и сброс таких сумм на биржах может создать панику. Неясна и судьба «заброшенных» кошельков, многие из которых поражают размером своего баланса и текущей оценкой в фиатной валюте. Если интересно, вы можете найти их по поисковому запросу «Dormant Bitcoin Addresses» в Google или Яндекс. Если вдруг появится способ заполучить такие сокровища или объявится владелец, рынок может существенно встряхнуть.

Огромный рост ожидает индустрию блокчейн в случае, если будут успешно внедрены и протестированы механизмы управления производственными процессами и цепочками поставок, запущены решения для государственного управления и голосования, сектор медицины и управления авторскими правами перейдет на распределенные реестры, укоренятся в головах людей принципы децентрализованной экономики и войдет в привычку применение криптовалют в быту, настанет эпоха IoT (от англ. *Internet of Things* – Интернет вещей) с повальным применением смарт-контрактов, уже не требующих оракулов для взаимодействия с внешним миром. Развитие необязательно должно быть связано с криптовалютами, но широкое внедрение блокчейн-решений будет сильно способствовать укреплению их статуса, как важного элемента экосистемы. Решение стоящих перед криптовалютами задач, таких как увеличение значения TPS (англ. *transactions per second* – транзакций в секунду) за счет запуска сайд-чейнов – дочерних или боковых цепочек, упрощения обмена криптоактивов при помощи процесса Atomic Swap, появление новых или комбинированных алгоритмов консенсуса, развитие майнинговой индустрии и прочие новшества и идеи, рождающиеся каждый день, могут создать накопительный эффект и спровоцировать очередной всплеск интереса широких масс. А может быть, общество, СМИ и государства совсем охладели к блокчейн-индустрии, и этот пузырь сдуется или лопнет по аналогии с пузырем доткомов. Да и пузырь ли это вообще? Признаки сходства есть, и это факт. Но в отличие от пузыря доткомов, который разросся до сотен триллионов долларов, размер пузыря криптовалют (если это на самом деле пузырь) составляет сегодня лишь четверть триллиона долларов, «раздуваясь» максимум до одного триллиона в пик роста 2018 года. Это совсем не гигантская цифра. Даже если сегодня криптовалюта исчезнет полностью, разрушительного воздействия на мировую экономику не случится. Также хочется вспомнить, что на волне интереса к доткомам появилось множество процветающих и поныне компаний: не все проекты оказались пустышками. Пусть 90 % сегодняшних криптовалют и одиозных ICO не оправдают ожиданий – оставшиеся 10 % смогут вытащить на себе идею блокчейн и криптовалют. Конечно, я имею в виду количественное соотношение проектов, а не стоимостное.

## Государственный блокчейн и криптовалюта

Имеет ли право на существование государственная криптовалюта? Нужен ли государствам блокчейн? Запустить в стране государственную криптовалюту и перевести на рельсы блокчейн государственные реестры вполне реально, особенно в небольших государствах. Многие страны уже сегодня внедряют блокчейн в процесс государственного администрирования, а особо прыткие даже создают отдельные децентрализованные государства (пока виртуальные) с собственной национальной криптовалютой и естественным признанием других подобных валют в качестве официального средства платежа. Я встречал упоминание о ряде виртуальных государств, планирующих в дальнейшем получить мировое признание, обзаведясь собственной территорией, государственным аппаратом и, конечно, гражданами. Самым занимательным мне показалось виртуальное государство Романовская империя, созданное российским политиком-монархистом Антоном Алексеевичем Баковым. Новое государство возглавил принц Карл-Эмих Лейнингенский, являющийся потомком Романовых и коронованный как Николай III, а Баков, получивший титул «светлейшего князя», стал эрцканцлером – главой имперской канцелярии и по сути вторым лицом после государя. Заявлялось о скором выпуске паспортов и признании государства на международном уровне, при этом страна имеет шансы обзавестись собственной территорией, состоящей из приобретенных или созданных под эти цели земель в Черногории, островов в

республике Кирибати и искусственных насыпных островов близ столицы Гамбии. Сайт [romanovempire.com](http://romanovempire.com) содержит ряд документов, таких как конституция, указ № 10 о формировании правительства, копия меморандума о дружбе и сотрудничестве с Гамбией и пара документов, касающихся проекта Атлантис в Гамбии. Заявлялось, что национальной валютой Романовской империи может стать биткоин, а госуправление будет вестись на блокчейн. В кризисный 2018 год существенных новостей от проекта нет, 20 подписчиков канала в telegram почти не общаются, а ICO для создания стартового капитала государства было отменено. Похожая история творится с либерлендом, также уповавшим на биткоин и блокчейн. Существует и ряд других подобных государств, таких как Децентурион, уже выдавший 1500 паспортов и выведший в августе 2018 года свой государственный токен DCNT на криптовалютную биржу. Правда, его цена за последующие 2,5 месяца снизилась с 1000 долларов США до 35, а в цифровых СМИ появились неоднозначные отзывы. Идея также базируется на покупке или строительстве острова с децентрализованным управлением и инновационной моделью развития. Зарегистрироваться и подробнее ознакомиться с проектом мне не удалось: сайт сообщал о технических работах. Есть упоминания и о покупке участков для криптокоммун, а также попытках создания подобных государств в полностью виртуальном мире. Без привязки к территории пытаются функционировать эстонский проект цифровой нации e-residency, а также подобный проект BitNation. Это, возможно, будущее, а что происходит сейчас?

Украина заявляет о проведении аукционов по продаже государственного имущества на блокчейн. Грузия переводит реестр недвижимости на эту технологию. Эстония давно имеет проект электронного гражданства на блокчейн и позволяет зарегистрировать брак на смарт-контракте между e-резидентами. Развитые страны выделяют огромные средства на изучение блокчейн, как технологии для государственных нужд. Об этом заявили и Китай, и США, и Великобритания. Вектор российской политики также нацелен на изучение и внедрение блокчейн в некоторые отрасли народного хозяйства. Можно ожидать, что часть реестров и простых функций исполнительной власти будут переведены на распределенные реестры и базы данных уже совсем скоро. Наверняка появятся признанные государством аналоги описанных Виталиком Бутериным децентрализованных автономных организаций – DAO, как замена нынешних коммерческих и некоммерческих компаний, часть финансового сектора сама перейдет на блокчейн и заставит правительства подстраиваться под бурно изменяющуюся среду. По моим оценкам, еще до истечения 2020 года некоторые небольшие государства смогут перевести до 50 % государственных функций на блокчейн и смарт-контракты, и уже в 2019 году мы увидим настоящую государственную криптовалюту, а не провальный El Petro, который пытались запустить власти Венесуэлы в пику американцам, или условно одобренные государствами белорусский талер и эстонский EstCoin.

Существуют и целые платформы, наподобие eGaas.org, что расшифровывается как electronic Government as a service – электронное правительство как сервис, позиционирующийся как база смарт-контрактов и их связки в смарт-законы для любых государственных областей применения.

## Глава 5

# Краудфандинг и ICO

### Что такое краудфандинг?

**Краудфандинг** (от англ. *crowdfunding* – народное финансирование) – это способ финансирования проекта за счет взносов неограниченного числа инвесторов, в основном частных. Примером самого раннего краудфандинга можно считать сбор на строительство храма. Стоит ящик, и каждый кидает столько денег, сколько может. Однако, в отличие от краудфандинга, спонсоры не получают взамен ничего кроме подпитки религиозных чувств, морального удовлетворения и чувства сопричастности.

Централизованный краудфандинг через стандартные централизованные ресурсы происходит следующим образом. Допустим, у меня есть модель какого-то нужного мне устройства или его проект. Я заявляю, что хочу выпустить сотню таких устройств и это обойдется мне по 100 долларов за каждое устройство. Затем я объявляю сбор по 100 долларов, намереваясь привлечь 100 человек, которым также нужно это устройство. Мне необходимо собрать десять тысяч долларов, чтобы заплатить их подрядчику, который возьмется изготовить продукцию. Если сбор

прошел успешно и устройства готовы, каждый участник, заявивший о желании получить опытный образец, получит его. Бывает и так, что сбор идет и в мелких масштабах: не обязательно вносить 100 долларов и претендовать на товар, можно просто перевести 3-5-10 долларов в поддержку интересной идеи. Или же другой пример. Человек хочет написать книгу, работа над ней и публикация труда обойдутся в существенную сумму денег. Автор объявляет общественный сбор и дает обещание, что за вклад в пять долларов пришлет спонсору электронную версию книги, за пятнадцать долларов добавит бумажную копию, а за пятьдесят долларов – бумажную копию с автографом и благодарственным письмом. Самым известным ресурсом с тысячами активных проектов является платформа Kikstarter.com, с помощью которой было реализовано более 150 000 кампаний силами 15 млн жертвователей. Платформа появилась в 2009 году и стала своеобразным экономическим явлением, новым способом реализовать проект без сложных согласований с венчурными инвесторами, которые просят кучу бумаг и затратных подготовительных работ. Если проект понравился людям и его профинансировали, то организатор сможет реализовывать свою идею. Если же не собрал минимум, необходимый для запуска, значит, средства спонсоров вернутся им на счет в системе.

Я уже упоминал два таких понятия, как *soft cap* и *hard cap*. *Soft cap* – это минимальная планка, которая необходима для реализации проекта. *Hard cap* – это максимальная планка, которая даст возможность сделать расширенную версию продукта с улучшенными потребительскими свойствами. Многие проекты стартуют без *hard cap* и *soft cap*, рассчитывая, что любой сбор поспособствует развитию идеи. Если же проекты ставят эти планки, значит, у команды есть, как минимум, финансовый план или бизнес-модель, и они понимают, сколько средств нужно минимально и сколько максимально. Эти термины очень часто применяются и в децентрализованной модели краудфандинга с помощью процесса, названного ICO.

## Реализация проекта с помощью ICO

По информации в Википедии первое криптовалютное ICO было проведено в 2013 году проектом Mastercoin и принесло организаторам 0,5 млн долларов США. Далее, с 2014 по 2015 год, началось поступательное движение вверх, а первым годом массовых ICO стал 2016-й, когда количество ICO и объем их сборов увеличились в несколько десятков раз. За 2017 год было привлечено инвестиций на более чем шесть миллиардов долларов, а за первое полугодие 2018 года – свыше 17 миллиардов долларов. Всего на сегодняшний день по данным сайтов-агрегаторов ICO проведено более 6000 ICO-кампаний, из которых минимум половина стала успешной, собрав *soft cap*. Большинство из ранних ICO проводились очень простым способом, не заботясь о детальной проработке проекта и организационных моментах. Целью было лишь попасть на пик волны и урвать хоть что-то. Первые компании были такими: одностраничный сайт (англ. *landing*), страница с адресами кошельков, ссылка на белую бумагу (англ. *white paper*), коротенькая дорожная карта (англ. *roadmap*) и, возможно, состав команды. Информация дублировалась на форуме [bitcointalk.org](http://bitcointalk.org) и рекламировалась на профильных ресурсах. Но чем дальше, тем больше начала усложняться система, сегодня все больше внимания уделяется юридическому оформлению проекта, более детальной проработке белой бумаги и дорожной карты, формированию команды, маркетинговым мероприятиям и созданию первичного сообщества. Ожидать, что «повзрослевшая» публика просто так осыпет вас криптовалютой, уже не стоит, хотя и такие случаи продолжают происходить. Итак, задача первичного размещения монет – собрать какое-то количество средств для реализации проекта, выдав взамен цифровой аналог акции, его называют монетой или токеном, который в будущем можно продать или обменять на централизованных и децентрализованных биржах, а также потратить на услугу или продукт, предлагаемый создателями проекта. Цель создателей – привлечь инвестиции, цель участников – банально заработать на росте монеты или получить будущую услугу/продукт по минимальной цене за счет раннего участия. С помощью ICO реализуются не только блокчейн-проекты, хотя они и занимают существенную долю в общем их количестве, но и проекты традиционной экономики, понявшие относительную простоту организации финансирования подобным способом. В целом план по проведению ICO состоит из нескольких больших блоков: концептуализация и оформление идеи, далее сбор первичной команды, подготовка необходимой юридической документации, создание сайта и смарт-контракта, после этого проведение массы маркетинговых мероприятий, и в итоге

выход на стадии продаж. При этом продажи могут быть разделены на несколько этапов, с разными условиями участия в них. В случае успеха начинается реализация согласно первоначальному плану и дорожной карте. Сегодня практически у любого человека или группы единомышленников есть возможность реализовать свой проект с помощью ICO. Мне хотелось бы уделить некоторое внимание удачным реализациям амбиций и идей.

### **Самые успешные ICO-проекты**

Виталик Бутерин создал свой Ethereum как раз в качестве инструмента для краудфандинга в криптовалютах. Это лишь малая часть функционала платформы, но именно она активно эксплуатируется и используется участниками криптовалютного сообщества. Сам Бутерин провел первичный сбор средств с помощью краудфандинга и привлек 31,5 тыс. биткоинов, раздав взамен более 60 млн монет Ethereum. Сейчас более 80 процентов новых проектов проводят сбор средств именно на платформе Ethereum.

Самая успешная кампания, запомнившаяся мне лично по скорости сбора средств, – это уже упоминавшийся проект iExes с их токеном RLC. Его организовала профессиональная команда, которая более 15 лет занимается строительством суперкомпьютеров. Сборы должны были начаться в определенный день и час, и я планировал перевести часть Эфира в токены RLC, но задержался и смог сесть за компьютер гораздо позже. Каково же было мое удивление, когда к моменту входа на сайт проекта кампания уже была завершена! Рынок отлично встретил очередную идею облачного суперкомпьютера, и iExes собрал нужную сумму в 15 млн долларов всего лишь за несколько часов. Также необычайно быстро завершилось ICO проекта внедрения искусственного интеллекта SingularityNet – еще до выхода на ICO подписной лист содержал десятки тысяч заявок на 360 млн долларов, тогда как проекту требовалась лишь десятая часть этих средств для проведения разработок. В итоге с помощью искусственного интеллекта были отобраны 5000 потенциальных инвесторов и собрана сумма в 36 млн долларов США. Еще одним запомнившимся скоростным проектом был Decentraland, который почти мгновенно собрал hard cap. Целью проекта является создание виртуального мира, которым бы владели сами пользователи. Виртуальные участки земли со строениями, виртуальные магазины одежды и продуктов, впрочем, с возможностью приобрести их реальную версию, аватары пользователей, соответствующие действительности или фантазийные, – все это породило неподдельный интерес широкой публики. В целом понять, о чем идет речь, можно из фрагмента фантастического фильма Люка Бессона «Валериан и город тысячи планет», где действие разворачивается на виртуальном рынке. Люди надевают специальные очки и гуляют по виртуальному рынку, выбирая товары. Они могут даже покупать товары, которые потом с помощью специального устройства можно материализовать в нашем мире. Это фантастическая версия, но уже сегодня развитие VR способно изменить процесс выбора товаров, особенно верхней одежды, с примеркой на виртуальном аватаре – собственной копии и последующей доставкой традиционными способами.

Самым дорогим на сегодняшний день считается проект EOS, проводивший необычное ICO длительностью, без малого, в календарный год и разбитое на стадии. Лишь за начальную неделю первой стадии проект собрал более 200 млн долларов, а по итогам всех стадий привлек более 4 млрд долларов. Идея создателей состоит в разработке новейшей блокчейн-платформы, объединяющей достоинства существующих решений и устраняющей их недостатки, а также во внедрении ряда новшеств, ранее не применявшихся никем. Вопрос состоит лишь в том, насколько созданное решение позволит поддерживать капитализацию проекта и не захотят ли ранние инвесторы поскорее распродать свои токены в поиске лишь спекулятивной выгоды. По мнению многих аналитиков, такая крупная сумма не нужна для создания описанного решения и создает благодатную почву для растрат, нецелевого использования сборов и удовлетворения личных нужд создателей. Недалеко от EOS ушел и проект создателя социальной сети vkontakte и мессенджера Telegram Павла Дурова – TON, также предложившего идею революционного блокчейна, который будет интегрирован в Telegram и позволит почти 200 млн его пользователей безопасно хранить, переводить и обменивать криптовалюту, названную Gram. Блокчейн TON должен появиться на рубеже 2018–2019 годов и стать самым массовым за всю историю. Сборы на проект велись не в криптовалюте, а в долларах США, минимальный платеж составлял 100 тыс. американских долларов, но многие инвесторы обходили данное ограничение, создавая коллективные инвестиционные пулы. По результатам пре-сейла, или по-русски предпродажи, оценочные сборы

составили около 2 млрд долларов США, при этом точные цифры остаются загадкой. Дуров отменил публичную стадию сборов, когда возможность приобрести токены должна была появиться у всех желающих, мотивировав это тем, что собранных средств вполне достаточно для проведения разработок и содержания команды и инфраструктуры. Выйди Gram на ICO, наверняка побил бы рекорд EOS.

Успешность ICO нельзя охарактеризовать только размером или скоростью сбора *hard cap*. Важное значение имеет дальнейшая судьба проекта, напрямую зависящая от разработчиков. Если в результате действий команды планы, заложенные в дорожную карту проекта, реализуются – это поспособствует росту стоимости токена и позитивно отразится на настроениях сообщества последователей идеи. Одним из важных моментов является листинг токена или монеты на бирже, и чем солиднее биржа, тем большее влияние на цену актива имеет данный фактор. Выпуск собственного кошелька, запуск собственного блокчейна без сбоев, проведение других заявленных работ в срок и с должным качеством также толкают цену токена вверх. Соответственно можно оценить успешность того или иного ICO по росту цены его акции – токена, по доходности вложений в данное ICO. Одним из лидеров роста доходности, запомнившихся рынку, стал токен STRAT стартапа Stratis. Стоивший 0,01-0,02 USD на старте в середине 2016 года, токен за неполный год достиг стоимости 10 USD к июню 2017-го, а затем, после непродолжительного отката к уровню 3–5 USD, пробил планку в 20 долларов США на пиковых значениях рынка рубежа 2017–2018 годов. На сегодняшний момент его цена не превышает 1,5 долларов, что говорит нам о необходимости выбора правильного времени не только для входа в ICO, но и выхода из него. Выход на первом пампе цены токена (от англ. *pump* – надувать, накачивать) мог принести от 50 000 % до 100 000 % доходности, а в первые две недели января 2018-го до 200 000 %. Даже избавившись от токенов сегодня по 1,4 USD, ранние инвесторы, приобретавшие их по 0,007 USD, могут зафиксировать прибыль на уровне 20 000 %. Каждый вложенный доллар принес бы 200 к моменту работы над этой книгой. При этом краудсейл эфира при начальной цене 0,2 за монету также можно считать мегадоходным. Сегодняшняя цена в 200 USD за 1 эфир дает доходность в 100 000 % за 3 года, а продажа его в том же январе 2018 года за максимальные 1400 USD могло принести 700 000 % доходности. Просто безумные цифры, но это исторический факт. Но не все ICO такие полезные и перспективные, а их команды открытые и честные. В бочке меда легко может оказаться и ложка дегтя, а порой и целое ведро.

## Бесполезные и мошеннические проекты

Существуют такие ICO-проекты, разработчики которых собирали деньги, но не планировали ничего делать. Хорошо, если об этом сразу заявлено честно. Например, Useless Ethereum Token (с англ. – бесполезный токен Ethereum) был выпущен анонимным автором абсолютно бесцельно. Сайт [u token.com](http://u token.com) содержал честное уведомление, что ничего делать не планируется, даже выводить токен на биржу. Белая бумага оправдывала свое название – это был пустой чистый белый лист. Сообщество оценило юмор по достоинству, переведя на смарт-контракт создателя более 300 ETH, что при грамотном распоряжении средствами могло подарить организатору почти полмиллиона долларов к Новому 2018 году. Однако те, кто вложил в бесполезный токен по начальной цене примерно в 1 цент за токен, имели все шансы продать его на бирже HitBTC, причем в феврале 2018-го цена токена достигала 0,25 доллара, а объем торгов превышал четверть миллиона долларов в сутки! Сегодня торги токеном закрыты в связи с обнаружением уязвимости в смарт-контракте токена, позволяющей красть все токены, находящиеся на кошельке пользователя. Видимо, разработчик не был до конца честен, а его заявление о том, что он хочет отыграться за потерю своих средств на бирже GDAX, наполняется дополнительным смыслом.

Еще в самом начале роста моего интереса к криптовалютам мне попался проект Elastic, разработчики которого одними из первых заявили об идее облачных – или туманных – суперкомпьютерных технологий, инновационной среды для смарт-приложений и т. д. Они провели сбор средств, получив 0,2 Bitcoin и от меня. Это отразилось в таблице участников, и на этом я успокоился. Через некоторое время главный разработчик растворился со всеми деньгами, оставив прощальное письмо с сообщением, что он переоценил свои силы. Однако основное сообщество не бросило проект и попыталось провести повторный сбор, нанять разработчиков и все-таки реализовать идею. Другое дело, что те, кто вложил повторно, получили токены нового

ICO, а все, кто остался в стороне, в итоге потеряли свои деньги, переданные первичной команде. Я уже не стал вкладываться повторно, решив зафиксировать убыток. Тем не менее проект вышел в публичную фазу, провел листинг на крупной бирже Bittrex и выпустил кошелек, а также программу-майнер с функцией программной среды для создания децентрализованных приложений. Сегодня токен XEL, как и многие другие криптовалютные активы, находится на минимумах как по цене токена, так и по объему торгов на двух им поддерживающих торговлю биржах.

Есть на моей памяти проекты, у которых была хорошая идея, с великолепной белой бумагой и сопутствующей документацией, красивым сайтом и известным в криптовалютном сообществе лидером команды, но почему-то публика не стала инвестировать средства в данное начинание. Например, стартап Ронни Бесинга, бывшего топ-менеджера CoinsBank, называется AppTrade (от англ. *app* – «приложение», *trade* – «торговля»), и его первоначальная идея заключалась в поиске потенциально «взрывных» приложений для смартфонов и планшетов на ранней стадии их разработки, дальнейшем их финансировании из первично собранного венчурного фонда, а затем участия в прибылях от продаж ставших успешными и популярными приложений. Все мы знаем о мессенджерах Viber, WhatsApp, играх наподобие Angry Birds или утилитарных приложений, как TripAdvisor или сервис такси Uber, которые завоевали популярность и стали стоить миллионы долларов. AppTrade должна была поддерживать новые прогрессивные идеи и создавать свои, дабы занять свободные перспективные ниши. Отличная идея, но сбор первой фазы ICO не достиг даже минимальной планки в один миллион долларов. Может быть, Ронни неправильно подавал свой проект, не так активно рекламировал, надеялся на сарафанное радио и определенную известность среди криптообщества или вышел с ним не в то время. После него появлялись подобные проекты и все-таки получали финансирование. С точностью узнать, что же пошло не так, невозможно. Сегодня сайт [apptrade.io](http://apptrade.io) предлагает иной формат взаимодействия, но я рад, что все-таки проект не заглох и развивается в выбранном направлении.

Случаются в сфере ICO и печальные истории, связанные не столько с умышленным мошенничеством команды, сколько с простой ошибкой в их работе. Примером может послужить уже описанный проект Aeternity. Средства от сборов во вторую фазу ICO в размере 82 000 ETH были размещены на кошельке Parity, имевшем критическую уязвимость, что позволило мошенникам похитить большую часть собранных средств. Ряд других проектов также сообщал об исчезновении средств по вине хакеров.

Примеров умышленного мошенничества сегодня хоть отбавляй. Простота организации ICO сыграла не только на руку честным разработчикам, мечтающим о реализации общественно-полезных идей, но и банальным аферистам, грезящим лишь о личном обогащении и неразборчивым в методах достижения своих целей. Иногда сложно понять, является ли проект мошенническим, пока это не объявят во всеуслышание официальные власти. Например, техасский проект AriseBank привлек около 600 млн долларов США, чему очень способствовал и нанятый ими в рекламных целях знаменитый и популярный боксер Эвандер Холифилд. Но комиссия по ценным бумагам США прервала развитие истории, подав на организаторов иск в федеральный суд. Прославилась гигантскими сборами и вьетнамская компания ModernTech, организовавшая ICO-проекты PinCoin и iFan, оказавшиеся банальной пирамидой. Мошенники заработали, по разным данным, до 660 млн долларов. Множество мошенников паразитировало на закрытом ICO блокчейна TON, о котором я писал выше. Например, создатели проекта Seele похитили более 2 млн долларов под видом сборов инвесторского пула для участия в покупке токенов Gram. В сети вы можете найти сотни упоминаний о мошеннических ICO, многие из которых рекламировались известными людьми и имели хорошие рейтинги среди сайтов, собирающих аналитику. Именно поэтому очень важно все тщательно проверить и изучить, прежде чем отдавать свои средства неизвестно кому. По мнению многих экспертов и рядовых членов сообщества, привлечение звезд и знаменитостей к рекламе ICO является косвенным признаком мошенничества. Сегодня существуют проверочные листы, с помощью которых можно отсеять потенциально мошеннические проекты. Их можно найти в свободном доступе в сети и использовать как дополнительный инструмент при оценке того или иного криптовалютного замысла.

Надеюсь, никто из моих читателей не собирается идти на сделку с совестью и при желании провести собственное ICO сделает это ради благих целей, а не ради наживы на чужом горе. Попробую рассказать, как же провести собственную кампанию по краудфандингу на блокчейн.

## Запуск ICO: вначале была идея

Привлечь средства через ICO могут абсолютно любые проекты, но среди успешных сборов наметилась определенная тенденция: упоминание в описании будущего внедрения AI (от англ. *Artificial Intellect* – искусственный интеллект), облачных вычислений и облачного хранения, нового типа блокчейн с фантастическими параметрами или же просто передового блокчейн-сервиса повышают статус проекта и позволяют ему собрать больше конкурентов. Акцент на FinTech (от англ. *Financial Technologies* – финансовые технологии), как инновационной отрасли, в связке с передовыми IT-решениями (от англ. *Information Technology* – информационная технология) также способствует успеху сборов ICO. Тем не менее даже проекты, никак не связанные с новомодными технологиями, могут проводить ICO, причем вполне успешно.

Допустим, у вас есть кафе. Вы уже три года им занимаетесь и знаете, как работает этот бизнес. Вы понимаете, что за место подходит для его размещения, как взаимодействовать с персоналом, какое оборудование качественное и надежное, где закупать продукты и т. д. В общем, вся бизнес-модель у вас на ладони. Но у вас не хватает средств, чтобы создать сеть из подобных заведений. Организовав ICO, можно собрать средства в криптовалюте на реализацию подобной идеи взамен выдав токены, с помощью которых можно расплачиваться за услуги сети кофеен или получать прибыль от их перепродажи. Существует очень известный проект фермы Колионово, привлекший более 400 BTC для развития своего хозяйства посредством ICO на платформе Waves. На момент сборов это было более 500 000 долларов США. По замыслу создателя токены можно потратить на экологически чистые фермерские продукты. К слову, токены KLN с момента создания не потеряли в стоимости так сильно, как многие другие криптоактивы. Сегодня токен стоит чуть меньше полудоллара, тогда как изначально продавался за один доллар. У ранних инвесторов также был шанс продать токены по 8 долларов в момент зимнего криптовалютного бума 2018 года. Важно отметить, что проект Колионово оказался под прессом правоохранительных органов, оценка краудфандинговой кампании обществом и властями была очень разной. Это не помешало множеству других российских проектов попытаться счастья на ниве организации ICO, при этом выбрав в качестве платформы для размещения российский же проект Waves со своей внутренней биржей и простым механизмом создания токенов в несколько кликов мышью.

ICO в России проводилось для постройки заводов – проект ZrCoin, создания майнинговых дата-центров с майнерами собственной сборки и собственным «чипом будущего» для майнинга – проект RMC.ONE, выпуска игры для смартфонов – Lordmancer II, запуска ICO-агрегатора – Wings, создания блогосферы на блокчейн – Golos, инвестиционной криптовалютной платформы – Genesis Vision, рекламной сети – AdEx, децентрализованной криптовалютной биржи – DEEX, платформы этичного хакинга и кибербезопасности – Hacken, трейдинговой платформы с искусственным интеллектом – Cindicator и многих других различных сфер. По разным причинам часть из вышеперечисленных названий можно встретить в списках сайта [cryptokompromat.ru](http://cryptokompromat.ru). Насколько оправданно, покажет только время. Нас же больше интересуют собственные потенциальные возможности.

Решив организовать ICO, организатору придется пройти несколько важных этапов на пути от идеи к реализации. Я попытаюсь полнее описать важные шаги в последующих разделах книги, при этом сейчас обозначу их поверхностно и нескрупулезно.

Первый этап – сформулировать идею, описать ее в первичном виде, создать черновик white paper. Для многих ранних сторонников Биткойн была важна именно идея независимой децентрализованной платежной системы, и мало кто пытался на нем заработать в первые годы. Девятистраничный документ Сатоши Накамото взбудоражил умы и заставил многих ранних приверженцев тратить свое время и силы на помощь в реализации проекта. Здесь важно довести идею до оформленного состояния, чтобы возникало желание ее реализовать, появились сторонники и наметились дальнейшие шаги по развитию концепции. Именно законченность идеи Накамото, ее оформленность и готовность к подаче – пример того, как может зародиться и ваша идея для ICO. Конечно, как только все готово, идею нужно обязательно анонсировать в узкой целевой группе. Это могут быть как родные и друзья, так и члены некоего профессионального сообщества или социальной группы, а можно адресовать идею сразу неограниченному кругу лиц, при наличии соответствующих ресурсов. Объем вложений на данном этапе сложно оценить

адекватно, но в общем случае их можно приравнять к нулю. Здесь важно иметь лишь ресурс времени и средств для обеспечения минимальных личных потребностей.

### **Упаковка идеи и команда**

Второй этап – упаковать идею. Термин «упаковка» появился в маркетинге и бизнес-администрировании не так давно, но он достаточно хорошо отражает суть необходимых действий. После обсуждения идеи в узких кругах вы примерно понимаете, что нужно сделать и какие ресурсы вам для этого потребуются. При дальнейшей проработке белой бумаги и дорожной карты формируется более четкое видение бюджета проекта в разрезе разных сегментов, будь то состав команды и фонд оплаты труда или вид и стоимость планируемых маркетинговых мероприятий. Нужно отметить, что здесь уже возникают вполне конкретные затраты, а популярным способом для их сбора является проведение закрытой стадии сборов, так называемой предпродажи – presale. Ранним инвесторам, зачастую членам команды и их близкому окружению, предлагается приобрести токены или даже обязательство об их начислении по более низкой цене, чем планируется в будущем. Иногда для этого создаются отдельный смарт-контракт и токен. Если смарт-контракт пресейла не планируется, то при традиционном личном финансировании первых стадий важно закрепить договоренности между основателями на бумаге, иначе при успешной реализации этапа продаж проблем с дележкой долей будет не избежать. При упаковке продукта важную роль играет выбор юридического статуса проекта и юрисдикции для размещения юридического лица. Нужно обязательно учитывать особенности регулирования ICO в разных странах, например в США и Гонконге есть отличие utility token (внутренней монеты проекта, не предполагающей доли в компании и начисления дивидендов, нужной именно для покупки товаров/услуг внутри платформы) от security token (монеты, имеющей основные свойства ценной бумаги, акции или доли в компании, с правом голоса и получения прибыли от участия в бизнесе). В большинстве случаев можно избежать крупных проблем и внимания регуляторов, если исключить слова «инвестиции и доходность, долевого капитал и прибыль, акции и пассивный доход» и ряд других из своего лексикона при упаковке и продвижении ICO. Тогда можно рассчитывать, что токен будет утилитарным и не будет приравнен к акциям. Большой упор придется сделать на продвижение идеи в массы, и один из самых затратных и сложных элементов – маркетинговый план. Выбор рекламных площадок, авторов для написания статей и текстов рассылок, формирование сообщества с поддержкой групп в социальных сетях и мессенджерах, создание баунти-компании, привлечение статусных советников и подбор спикеров для конференций. Для реализации масштабного плана понадобится большая команда, о чем я попробую рассказать подробнее.

Чем смелее план, тем более многочисленной и профессиональной будет команда. Для успеха нужны такие люди, кто скажет: «Да, мы справимся за этот срок, привлечем дополнительные аутсорсинговые ресурсы, мы сделаем свою работу». В зависимости от технической составляющей проекта вам потребуется команда разработчиков. Это могут быть один человек и наемная компания ему в помощь или 2–3 штатных специалиста с возможностью привлечь фрилансеров на некоторые объемы задач. Фронт-энд разработчик отвечает за лицо вашего проекта – сайт. Бэк-энд разработчик – за сердце проекта, код продукта, необходимое техническое обеспечение для его работоспособности, а также смарт-контракты всех стадий продаж токена. Для продвижения проекта понадобятся копирайтеры, контент-менеджеры, операторы службы поддержки, интернет-маркетологи, экономисты... Понадобятся и юристы, штатные или внештатные, которые учтут все риски, связанные как с размещением проекта в России, так и при выходе на международную арену. Нелишним будет обзавестись набором документации, такой как уведомление о рисках, соглашение о неразглашении конфиденциальной информации, трудовыми договорами с сотрудниками и контрактами с подрядчиками, учитывающими вопросы владения созданной интеллектуальной собственностью и пр. Всем процессом кому-то придется управлять, и личность руководителя имеет немалое значение в успехе или провале начинания. Конечно, в рамках бюджетного стартапа возможно совмещение разного функционала в одном лице, особенно в рамках дружеской команды основателей, имеющих соответствующие компетенции. Разработчики сайтов зачастую владеют инструментами для их продвижения и ресурсами для привлечения копирайтеров, контент-менеджеров на сдельной основе, им проще освоить программирование смарт-контрактов, и они знакомы с основами дизайна и нейминга. Маркетолог вполне может



закрыть вопросы ведения рекламной кампании и кампании поощрения (bounty-кампании), взять на себя вопросы внешних коммуникаций и часть функций экономиста. Юристы зачастую обладают руководящими навыками или как минимум видением последовательности шагов для достижения конкретной цели, им не чужды представительские функции – будь то переговоры или выступление перед аудиторией. А все вместе участники могут осуществлять поддержку групп в социальных сетях и распределить нагрузку по проведению конференций, видеопрезентаций или встреч с ранними инвесторами. Таким образом, у нас получается четыре главных звена: идейно-управленческое, техническое, юридическое и маркетинговое. Эти четыре составляющие в правильной комбинации помогут проекту ожить и выйти в ту стадию, когда первоначальный интерес публики принесет первые плоды и позволит расширить команду требуемыми сотрудниками. Стоимость данного этапа, несомненно, будет очень высокой по сравнению с фазой идейного оформления проекта. Два месяца работы профессиональной наемной команды из программиста, маркетолога и юриста, при вашем общем руководстве проектом, может стоить до 1 млн рублей с учетом заработной платы, аренды помещения и текущих организационных затрат. Но справедливости ради скажу, что множество проектов запускаются силами двух-трех человек, и большинство процессов можно автоматизировать или отдать на откуп профессиональным командам, не вкладывая собственные средства. Сегодня существует немало компаний, которые за долю в будущих сборах возьмут на себя все, что связано с упаковкой идеи и дальнейшей поддержкой на этапе сбора средств. Также практикуется формат оплаты труда членов команды долей в будущем проекте. Если идея обладает потенциалом, вполне возможно замотивировать потенциальных членов команды премией в виде будущих токенов или монет за их трудовой вклад на благо проекта. Так работают и многие эдвайзеры – советники в области блокчейн, чье опосредованное участие в проекте может усилить его позиции. Стоит, правда, избегать услуг «массовых» советников, мелькающих в любых начинаниях, готовых оплатить гонорар, – такое участие может отвратить взоры думающих людей от вашего бизнеса. Некоторые публичные и именитые персоны в криптоиндустрии часто выступают в роли гарантов или эскроу (от англ. *escrow* – условное депонирование), их функция – держать средства крупных инвесторов на личном кошельке до завершения фазы продаж и распределения токенов. Это делается, дабы обезопасить участников от потери средств в случае каких-то проблем. Такие посредники берут небольшой процент за свои услуги, но нам главное, чтобы сбор средств прошел успешно!

## Этап сбора средств

Для меня этап подготовки к сбору видится наиболее сложной стадией, и если на ней все проработано и отточено – фаза непосредственно проведения ICO не должна быть какой-то проблемой, но расслабляться не стоит. У нас есть сайт с условиями участия и продуманной системой скидок для ранних инвесторов, протестированы личные кабинеты участников и работоспособность кошельков различных криптовалют. Возможно, подключен и платежный шлюз по приему фиатной валюты. Вся документация в порядке, социальные сети уже работают, и результат их действий уже может быть зафиксирован в предварительном подписном листе, охвачены разные языковые группы и страны. Есть escrow-агент и именитые советники, потенциальные партнеры и члены команды, проведен аудит смарт-контракта и общей безопасности сайта. Что ж, можно начинать? Осталось лишь сделать финальный рывок и добиться цели.

Сколько времени должен максимально длиться сбор и на какие этапы он разделен – решается заранее. Обычно существует закрытая фаза пресейла, длящаяся не более 1 месяца – еще до запуска основной кампании, а затем наступает публичная фаза, разбитая на этапы. Первый из них часто называют этапом «ранних пташек» – *early birds*. Суть легко раскрывается известной поговоркой: «Кто рано встает, тому Бог подает», и ее англоязычной версией: «*early bird gets the worm*» – ранняя пташка получает червячка. Всем, кто произведет оплату в первые 2–3 дня краудсейла, обещаются существенные бонусы в токенах, например на 10 % больше, чем в последующие дни. Также в период падения рынка получил распространение вариант искусственного завышения курса криптовалют, в которых идет сбор. Например, курс эфира фиксируется на уровне 500 USD при его реальной сегодняшней стоимости в 200. Такой маркетинговый ход позволяет тем держателям эфира, кто жалеет об упущенной возможности, продать свои монеты по 500-1000 долларов в

период роста, легче расстаться со своими подешевевшими активами. Кстати, для такого психологического состояния существует термин FOMO – «fear of missing opportunities» – страх упущенных возможностей, который часто фигурирует в период кризиса криптовалют середины-конца 2018 года. За этапом ранних пташек идет основной этап, когда цена токена фиксирована и курс криптовалют, принимаемых к оплате, также равен биржевому. В последнюю неделю или несколько дней продаж курс токена может быть повышен на какую-то величину. Дело даже не в том, что планируется увеличение сборов на последнем этапе, необходимо замотивировать колеблющихся потенциальных инвесторов произвести оплату до повышения цены. Весь процесс сборов должен быть прозрачен, статистика поступлений должна отображаться на главной странице сайта, а пользователям должно быть видно, достигнут ли soft cap, далеко ли до hard cap и ряд других параметров – сборы в каждой отдельной валюте, число проданных и оставшихся токенов, общее количество участников, время до окончания ICO. В период активной фазы сборов необходимо сделать акцент на безопасности протекающих процессов. Сайт должен быть защищен от любых возможных кибератак, команда – быть готовой отразить черные PR-акции завистников и конкурентов, юридическая служба – следить за отсутствием возможных внезапных проблем с законом или действиями чиновников, а кошельки, на которых аккумулируются средства, защищены мультиподписью, дабы невозможно было физическое воздействие на кого-то из основателей с целью грабежа полученных средств.

На каждом этапе и в каждую фазу должны максимально работать все маркетинговые инструменты: проводиться заготовленные электронные рассылки, публиковаться сообщения и ответы в социальных каналах коммуникации, отслеживаться и по возможности корректироваться публичные рейтинги, задействоваться любые рекламные возможности с прогнозируемой положительной конверсией. На этап сбора средств может потребоваться самый большой бюджет из всех стадий до непосредственной реализации. Если у проекта маленький soft cap, при его достижении вполне допустимо использовать часть собранных средств на дальнейшее продвижение проекта и задействовать дополнительные рекламные возможности, т. к. в описании проекта всегда есть раздел о будущем расходовании собственных средств и выделенная строка бюджета на рекламу и продвижение. Если минимальная планка достигнута за короткое время, можно не дожидаться окончания сборов и начинать реализацию проекта, исходя из минималистичного сценария.

## Реализация проекта

Все мы стараемся верить в лучшее и стремимся к совершенству, но зачастую объективная реальность вносит свои коррективы в наши, казалось бы, идеальные планы. С какими препятствиями может столкнуться проект на стадии реализации? Кто может помешать планам создателей?

Как ни странно, в первую очередь проблемой может стать сама команда – как ее банальная профессиональная некомпетентность, так и разные психологические факторы. Если сбор прошел успешно или проект получил признание еще на стадии пресейла, у некоторых членов команды могут разыграться личные амбиции. Их могут специально настроить таким образом, что они – ключевые фигуры, все зависит от них, остальные лишь приатки. Один из моих друзей отказался от участия в перспективном проекте именно из-за возросших амбиций ключевых фигур в период стадии пресейла. Обратная ситуация – выгорание команды. Напряженная работа на подготовительных стадиях, появление огромного объема новой информации, возможно, осознание ответственности перед тысячами людей – все это может сыграть дурную шутку с некоторыми людьми, не привыкшими к высоким нагрузкам. Может появиться ложное чувство, что все уже и так случилось, цель достигнута, а работу как-нибудь сделаем. На моей памяти не менее 10 крупных проектов почти полностью меняли состав команды, причем неоднократно, т. к. основатели, получив свою долю, предпочли личное общественному. Найти новую команду – полбеда. Ввести их в курс дела и передать компетенции – вот основная проблема, выливающаяся в потерю времени и средств, срыв сроков и как итог – в репутационные потери и финансовые риски. Избежать этого можно, лишь имея в запасе план Б, который может предполагать наличие у ключевых персон помощников, частично обладающих навыками и компетенциями своих руководителей; предусмотрительное создание базы данных потенциальных сотрудников, например путем проведения хакатонов и конкурсов; сформированный фонд на оплату услуг

профессионалов со стороны. Да и вообще, наличие резервного фонда может помочь избежать многих проблем при претворении идеи в жизнь.

Самая распространенная на сегодняшний день юридическая проблема, с которой можно столкнуться уже после ICO, – неблагоприятные действия чиновников как в собственной юрисдикции, так и в юрисдикции, к которой относятся инвесторы вашего ICO. Для участия граждан США в ICO важно учесть массу нюансов, а пренебрежительное отношение к таким, казалось бы, мелочам может сыграть дурную шутку. На большое число проектов были поданы иски такими органами, как SEC в США или SFC в Гонконге, итогом которых может стать прекращение деятельности компаний не только в зоне влияния этих стран, но и личная ответственность создателей в виде крупных штрафов или заочных тюремных сроков. Именно поэтому при отсутствии должной юридической проработки проекта рекомендуется запретить гражданам США, Гонконга и государств, напрямую запретивших криптовалюты или находящихся в «черных списках», участие в ICO путем размещения соответствующего уведомления на сайте. Даже размещение головной компании в благоприятных для криптобизнеса юрисдикциях, таких как Швейцария, Сингапур, Белоруссия, или классических оффшорах не гарантирует защиты от форс-мажорных обстоятельств в виде запретительных действий властей или резкой смены налогового климата.

Нельзя упускать из виду и воздействие таких внешних факторов, как криминалитет, недобросовестная конкуренция, промышленный шпионаж. Немало криптовалют и блокчейн-проектов закрываются из-за кражи средств с кошельков компании или пользователей, не один проект пал жертвой более активных конкурентов, скопировавших идею и вышедших на рынок раньше жертвы подобных недобросовестных действий.

Если же вернуться к сухим фактам и рассмотреть типовой пример реализации проекта, достаточно ознакомиться с типовой дорожной картой большинства ICO. В ней можно выделить несколько вех, повторяющихся с небольшими изменениями. Сначала идет взгляд в прошлое, декларируются уже достигнутые отсечки на дорожной карте, например оформление патентов, какой-то документации или время появления идеи и сбора команды основателей. Далее следует текущий период – отсечка стоит на пункте плана о проведении ICO. Дальше, казалось бы, должны быть десятки шагов и статус их выполнения, но лишь единичные проекты раскрывают свою дорожную карту так широко. Обычно же следом за ICO идет важный пункт «листинг на биржах», и он действительно важен: токен должен торговаться на бирже, а лучше на нескольких приличных. Потом стоит задача выпуска программного продукта, будь то кошелек для криптовалюты, личный кабинет сайта по инвестициям, программа для майнинга/форжинга/минтинга, программно-аппаратный комплекс для машинного обучения, инновационная блокчейн-платформа или готовый веб-сайт со всем сопутствующим функционалом криптовалютной биржи. Достойные проекты разбивают процесс создания продукта на некоторые важные составные части и дают возможность пользователям видеть, какой процент работ по каждой конкретной части завершен. По итогу основных работ может быть анонсирован промежуточный этап тестирования, а после него следует запуск готовой версии продукта. Затем обычно идет пункт о достижении некоей планки по капитализации проекта, или план по привлечению N-ного числа пользователей в систему, либо другой показатель, который свидетельствовал бы о росте проекта и его развитии. Конечным пунктом может являться вопрос об актуализации белой бумаги и формировании новой дорожной карты на будущий период. В принципе, все так, как и должно быть, и для реализации проекта самое главное – хорошо подготовиться, привлечь необходимое финансирование, вывести монету на биржу, выпустить заявленный продукт, внедрить его в массы и затем двигаться дальше. На словах все просто, а на деле может быть не очень. Но все-таки главное – это работать над проектом до победного конца.

Учитывая все вышперечисленное, остается лишь добавить, что для успешной реализации проекта очень важна личность лидера, который будет все время держать руку на пульсе происходящих событий, знать и решать существующие проблемы, будет готов к потенциальным вызовам, станет мотиватором для команды и всего сообщества, не перестанет генерировать идеи и вести за собой проект. Надеюсь, в России предостаточно таких людей, и мы имеем все шансы занять свою нишу в столь перспективной индустрии, как блокчейн и криптовалюты.

## Оценка российского рынка ICO

Я уже упоминал, что мировой рынок ICO развивался сумасшедшими темпами с 2015 по 2018 год. Оценочный объем инвестиций через ICO может составить более 30 млрд долларов на конец 2018 года. За 2017-й эта цифра была примерно в 5 раз меньше. Проекты с российскими корнями привлекли в 2017 году сумму до полумиллиарда долларов, что не дотягивает и до 10 % общемирового рынка. Если бы тенденция сохранилась, можно было бы ожидать привлечения от 2 до 3 млрд долларов в экономику России в нынешнем 2018 году, но, к сожалению, вести с полей не так радужны. Если считать проект блокчейна TON российским, то привлеченные им минимум 1,7 млрд долларов вроде как поддерживают статистику, однако проект Дурова не российский. Инвестиций в экономику России с этих денег можно не ждать, все прекрасно знают почему. Новостные ресурсы, публикующие рейтинги ICO, не особо любят разделять их по странам, откуда растут корни команд, но нам важно участие именно нашей страны в глобальном процессе. Именно привлечение средств внутрь страны и развитие российского сегмента имеют значение для развития экономики нашего государства. Проанализировав ряд аналитических ресурсов, я сделал вывод, что в 2018 году не будет побита даже прошлогодняя планка сборов. Что же является причиной такого явления и как исправить ситуацию?

Основополагающих факторов несколько. Во-первых, влияние глобальных факторов, таких как неблагоприятная конъюнктура рынка криптовалют в целом, пусть это и не помешало многим зарубежным проектам достичь рекордных сборов за все время существования криптовалют и проведения ICO. Политическая нестабильность во внешней политике и санкционные действия западных стран также можно отнести к глобальным причинам низкого интереса инвесторов к развитию проектов в России. Отсутствие законодательного регулирования и понятных правил игры вполне могут быть сдерживающим фактором для массового развития института краудфандинга в нашей стране наряду с вышеописанными. Вывод – скорейшее принятие мягких законодательных актов и введение инструментов поддержки бизнес-проектов в сфере блокчейн смогли бы дать толчок для развития индустрии и увеличения числа внутренних проектов, пусть без ориентации на западных инвесторов. Многие стартапы из России сегодня предпочитают реализовывать свои проекты в США, Европе, Азии, внося вклад в экономику других государств – эту тенденцию однозначно нужно менять. Широкая программа внедрения блокчейн и соответствующий этому новостной фон вполне могли бы позитивно отразиться на всем мировом рынке криптовалют и блокчейн-технологий.

Во-вторых, проблема заключается во внутренних факторах, например негативной оценке многими экспертами результатов исполнения обязательств большинством российских проектов. Часть из них уже открыто обвиняют в мошенничестве как на локальных информационных ресурсах, так и в иностранных СМИ. Несоответствие проделанной работы уровню сборов и изначальной дорожной карте, обвинения организаторов в растратах – не редкость и за рубежом, но полное невыполнение обязательств по дорожной карте двух из топ-5 российских ICO 2017 года – это серьезно. Утрата доверия иностранного капитала к российским ICO с таким подходом неизбежна. На сайте [vc.ru](http://vc.ru) содержится краткий, но содержательный разбор полетов с названием: «Год спустя. Что сделали топ-5 российских ICO-проектов за год после сбора средств?» Из него видно, что все совсем не хорошо, даже у компаний, формально следующих пунктам дорожной карты. Почти по всем участникам этого рейтинга можно найти негативную информацию на ресурсах наподобие [sputnik.com](http://sputnik.com). Что же делать с этими факторами? По моему мнению, необходимо увеличить число небольших, более приземленных ICO, привязанных к реалиям, а не слишком футуристическим идеям. Уже упомянутый проект Колионово – вполне подходящий пример. Вместо гонений на фермера, обвинений в создании суррогатных денег ему следовало помочь. Создание инкубаторов, акселераторов, обучающих программ – минимум того, что нужно сделать для мотивации предпринимателей на использование схемы ICO для привлечения средств в бизнес. Опять же, упираемся в вопрос регулирования рынка. Установление правил игры и ответственности за их нарушение способствовало бы увеличению притока честных игроков и уходу с рынка откровенных аферистов, чувствующих безнаказанность в сложившемся правовом вакууме.

При устранении основных внутренних препятствий, влияющих на рынок ICO и криптовалют, вполне можно было ожидать взрывного роста объемов иностранного капитала, привлеченного в

экономику страны через криптовалюты и ICO. Одна только отрасль добычи полезных ископаемых, зачастую страдающая от нехватки средств на реализацию проектов, могла бы привлечь сотни миллионов долларов инвестиций. Использование криптовалют, с их относительной анонимностью, могло бы открыть доступ многим иностранным инвесторам – например из США, боящимся санкций или негативной реакции правительственных органов их стран на такие действия, – а также устранило бы проблемы несовместимости бизнес-ментальности российских и китайских партнеров, сделав правила игры одинаковыми и общепризнанными, дало шанс территориально удаленным инвесторам участвовать в российских проектах в упрощенном порядке без долгих перелетов, переговоров, согласовательных и бюрократических процедур.

Высокий профессиональный уровень российских программистов и математиков, специалистов любых других сопутствующих сфер, наличие большого сырьевого, энергетического, потенциала и больших территорий вполне могут стать поводом для интереса массовых мелких инвесторов в участии в проектах российских ICO разного масштаба. При пессимистичных оценках и сохранении общего восходящего тренда в развитии блокчейн-технологий захват от 5 до 10 % общего объема инвестиций в новые ICO-проекты не выглядит чем-то несбыточным. Если же предположить, что объем общемировых инвестиций в ICO будет расти лишь на скромные 100 % в год, а не 500 %-1000 %, как за период 2015–2018 годов, то Россия сможет претендовать на несколько миллиардов долларов инвестиций ежегодно. При том, что приток прямых иностранных инвестиций в Россию составлял 32,5 млрд долларов в 2016 году и уже «скромные» 28 млрд в 2017-м, по итогам 2018 года этот приток может стать еще меньше. Подспорье в виде притока криптовалют будет только плюсом для нашей страны. Свершению такого сценария могло бы способствовать создание в стране крупных криптовалютных бирж, биржевых посредников, различного типа фондов и иных финансовых учреждений, возможно, даже банков или как минимум платежных систем.

## Глава 6

### Биржи и биржевая торговля

#### Сходства и различия традиционных и криптовалютных бирж

В принципе, привычные нам товарно-сырьевые, фондовые и валютные биржи работают точно так же, как и большинство криптовалютных. Имеется некоторое количество торговых пар, есть универсальное средство обмена – например, доллар, есть котировки и биржевые индикаторы, ведут торговлю трейдеры, а биржа выступает универсальным посредником по обмену ценностями. Функция посредничества при исполнении заявок характерна именно для централизованных бирж, многие из которых должным образом зарегистрированы в респектабельных юрисдикциях с оформлением всей требуемой документации. В отличие от централизованных децентрализованные биржи работают как площадка для встречи продавца и покупателя, не проводят сделки через свои счета, а контроль за процессами осуществляют валидаторы или свидетели – специальные узлы обработки транзакций на блокчейн. Если работа традиционных бирж разделена на сессии, то криптовалютные биржи работают круглосуточно семь дней в неделю. Для участия в торгах на большинстве традиционных бирж требуются не только существенный капитал, но и оформление лицензий, наличие профильного образования или специальной сертификации для прохождения процедуры соответствия требованиям. В случае с криптовалютными биржами все проще. Большинство из них позволяет анонимную торговлю небольшими объемами активов, а при необходимости расширения лимитов нужно лишь предоставить копию какого-либо документа, удостоверяющего личность, и небольшой объем дополнительных данных. Любое физическое лицо имеет возможность торговать на бирже криптовалют напрямую, без брокеров или каких-то специальных посредников. Чуть сложнее процедура для юридических лиц, но и она существенно проще и быстрее, чем, например, на фондовой бирже. Вывести свой актив на традиционную биржу – задача долгая, сложная и дорогая. Стоимость проведения аналогичной ICO-процедуры на традиционной бирже и именуемой IPO может составлять десятки и сотни тысяч долларов, а листинг на криптовалютной бирже для ICO может обойтись в лишь несколько тысяч долларов, а порой он и вовсе бесплатен. Количество новых ICO исчисляется сотнями в месяц, тогда как количество новых IPO в США не дотягивает

до сотни в год. И там, и здесь присутствуют комиссии, но на криптовалютных биржах их размер существенно меньше.

Важным отличием традиционных бирж является защита от инсайдерской торговли – когда владелец компании или лицо, осведомленное о будущих вероятных движениях курса акции, делает соответствующие ставки через подставные компании. В США инсайдерская торговля уголовно наказуема. При этом депозиты инвесторов страхуются на суммы до 500 000 долларов, что делает торговлю более цивилизованной и безопасной. На криптовалютной бирже инсайдерская торговля не запрещена, манипулирование рынком крупными игроками происходит постоянно, а вклады рядовых участников никак не застрахованы. Все компании, чьи акции торгуются на фондовых биржах, имеют прозрачную отчетность по определенным стандартам, тогда как токены ICO-проектов невозможно адекватно оценить, т. к. отсутствуют реальные сведения о компании, ее активах, патентах и прочих важных моментах для оценки состояния бизнеса. Зачастую нет даже никакой компании – юридического лица, которое было бы связано с токеном или монетой. Во многом именно это приводит к большой волатильности на криптовалютных биржах. Цена на традиционные акции, товары или валюты не изменяется на несколько десятков или сотен процентов за торговую сессию. Колебания курса обычно укладываются в 10 %-ный предел. А криптовалюты могут демонстрировать рост и падение на сотни и тысячи процентов в коротком временном интервале. С другой стороны, при торговле криптовалютой с большим кредитным плечом, сделав верную ставку, можно заработать сотни и тысячи процентов доходности в день.

Инструменты, применяемые при биржевой торговле, также вполне одинаковые на обоих типах площадок. Различные типы графиков и инструментов технического анализа для построения стратегий – общее явление для всех бирж. При этом, имея некую стратегию торговли, гораздо проще привлечь к ее реализации робота – торгового бота – именно на криптовалютных биржах. На некоторых площадках это запрещено, но в большинстве случаев вполне допустимо.

Главным и наиболее важным выводом по всей совокупности различий между традиционными и криптовалютными биржами является тот факт, что криптовалютные биржи представляют очень большой риск для работы. Это большой минус, но есть и плюсы. Попытаемся их обозначить.

### **Плюсы и минусы криптовалютных бирж**

Главным плюсом криптовалютной биржи я считаю возможность быстрого листинга – вывода токенов своего проекта на международную торговую площадку за считанные дни, при этом к нему не предъявляется заоблачных требований. Крупные биржи, конечно, взимают за это плату, достигающую 500 000 долларов, но в среднем около 250–300 тыс. USD в BTC, токенах проекта или американских долларах, но если начать со средних площадок, можно обойтись суммой в 1–5 BTC и достичь одной из важных целей при реализации проекта – придать токenu ликвидность и получить официальные биржевые котировки. Быстрота входа инвесторов на биржу – также несомненный плюс. Криптовалютных бирж огромное количество, более двух сотен, что заставляет их больше конкурировать и развиваться, снижать комиссии и тарифы на листинг. При этом сегодня многие биржи имеют свои токены, покупка которых может принести доход от операций биржи, а также дает возможность получить скидку на размер комиссий биржи до 90 %. Обычно такую возможность дают децентрализованные биржи, и если биржа децентрализована – это также отдельный плюс. Одной из очень популярных функций биржи является возможность иметь мультивалютный кошелек в виде биржевого аккаунта. Это может быть рискованно, но очень удобно. Доступ к бирже и такому кошельку возможен из любого места и с любого устройства, круглосуточно и без выходных. Огромное преимущество криптовалютных бирж – это скорость ввода/вывода активов, которой не достичь на традиционных биржах. Получить свои монеты можно за считанные минуты, тут же обменять на фиат и потратить. Конвертация фондовых или товарных ценностей в живые деньги на обычной бирже может длиться неделями. При этом обычно ограничения на ввод/вывод средств с бирж очень лояльные, минимумы очень низкие, а максимумов или нет совсем, или при прохождении идентификации они расширяются до очень больших значений.

Теперь поговорим о некоторых явных минусах криптовалютных бирж. Во-первых, они имеют непонятный юридический статус. Только единицы из сотен бирж работают по правилам SEC – комиссии по ценным бумагам и биржам США, чуть больше соответствуют требованиям

гонконгского аналога – SFC. При этом большинство бирж зарегистрировано в офшорных юрисдикциях или вообще не имеют аффилированного юридического лица, соответственно, конечные владельцы и ответственные лица неизвестны. Действия властей или преступников могут легко уничтожить биржу за считанные дни. Хранение больших сумм на бирже – это риск, можно запросто потерять все свои средства, как по вине хакеров, так и при внезапном исчезновении владельцев биржи. Большой интерес киберпреступников к криптовалюте и биржам, как месту консолидации крупных ее объемов, делает многие средние и мелкие биржи очень ненадежным вариантом размещения активов.

Уже обозначенная волатильность может сыграть дурную шутку с вашими инвестициями. Возможное резкое воздействие внешних факторов на курсы и непредсказуемость, хаотичность поведения рынка в целом – существенный недостаток площадок торговли криптовалютами. Если не проявлять должной аккуратности и внимательности, есть риск потерять большую часть своих средств за считанные часы. Огромное влияние новостного фона и действий крупных игроков-манипуляторов на курсы – также явный минус криптовалютных бирж.

## Самые крупные биржи

Биржу принято считать крупной, если по объему торгов она опережает своих конкурентов. При этом несомненные лидеры прошлых лет – биржи Bitfinex, Poloniex, Bittrex – уступают место новичкам, хотя одна из старейших площадок – Bitfinex – сохраняет место в топ-10 и по сей день. Лидеры же первой волны плавно смещаются во вторую и третью десятки рейтинга. В 2017 году появилась биржа Binance, которая буквально за один год перетянула на себя одеяло и стала крупнейшей торговой площадкой для криптовалют. Суточный объем торгов на Binance сегодня приближается к 1 млрд долларов. Также сегодня в топ-5, по версии Coinmarketcap, входят OKEx, ZB.COM, Huobi и LBank: их среднесуточный оборот составляет от 300 до 500 млн долларов. Однако рейтинг постоянно меняется, так как на рынок выходят все новые и новые биржи.

В основном биржи расположены в офшорах с либеральным налоговым и финансовым законодательством, таких как Гибралтар, Белиз или Сейшелы, либо в надежных юрисдикциях, например, Гонконг, Мальта, Сингапур, США. Существует даже проект IDAX из Монголии, стремящийся в первую десятку рейтингов. Лицензирование в этих странах происходит по аналогии с традиционными финансовыми компаниями. Официальное лицензирование именно криптовалютных бирж ввели Япония и Филиппины. К большому сожалению, пока не существует официальных российских бирж, зарегистрированных на территории страны. И снова вся проблема в законодательстве. Организация финансовых компаний в РФ требует очень больших временных и финансовых затрат на лицензирование, требования к лицензиатам достаточно жесткие, а контроль Центрального банка, как мегарегулятора, чересчур бдительный. При этом существует несколько бирж, организованных нашими согражданами, таких как скандально известная BTC-E, ставшая называться WEX после ареста одного из ее предполагаемых сооснователей американскими властями по подозрению в отмывании средств. При этом WEX в октябре 2017 года также приостановила операции, а ряд российских пользователей подали коллективное заявление в МВД с просьбой привлечь площадку к ответственности.

Если анализировать юрисдикции, в которых сконцентрирован самый крупный биржевой капитал, несомненным лидером станет Гонконг. Не будет преувеличением сказать, что каждая вторая из бирж топ-10 находится в Гонконге. Для каждой страны, где деятельность криптовалютных бирж разрешена, существует свой локальный лидер. Например, в Южной Корее это UPbit, в Японии – Coincheck (испытывавшая проблемы с хакерской атакой и находящаяся под ударом), в Великобритании – Bitstamp.

## Листинг монет на бирже

Листинг (от англ. *list* – список) криптовалюты – это внесение определенной монеты в список торгуемых активов на бирже. Как я уже отмечал, для многих монет или токенов этот шаг – одна из важнейших ступеней в реализации проекта. Вывод актива на биржу из топ-10 мирового рейтинга – мечта большинства разработчиков. Есть несколько способов вывести монету или токен на биржу.

Первый способ – создать такой проект, который получит широкое общественное признание, и тогда биржа сама захочет провести листинг перспективной монеты. Если руководство площадки

увидит основу для роста объема торгов за счет ввода нового инструмента и получение временной монополии на получение комиссий с оборота молодого криптоактива – можно считать, что всем повезло, ситуация выигрышная для обеих сторон.

Второй способ – заплатить за листинг. Причем платная услуга может быть в двух вариациях. Либо биржа сама организует вам ICO и сразу добавит торговую пару в листинг, либо после самостоятельного проведения ICO биржа добавит актив по факту оплаты и завершения этапа сборов. Стоимость такой услуги очень разнится от площадки к площадке и может составлять от минимальных 0,5 BTC до 50 BTC на площадках, расположенных на вершине рейтингов и гарантирующих солидный объем торгов.

Третий способ – голосование. Биржи регулярно проводят голосования по добавлению новых монет. Монеты, собравшие нужное количество голосов, допускаются к торгам. Здесь приобретает значение, насколько хорошо ведется работа с сообществом, комьюнити проекта. Если команда разработчиков способна активизировать своих последователей и их ближайшее окружение, вполне реально получить доступ к крупной бирже без прямых финансовых затрат.

Четвертый способ – создать токен на платформе, внутри которой встроена собственная биржа, или существуют биржи, предлагающие бесплатный листинг токенов. Примером может послужить не раз упомянутый проект Waves. Создавая токен внутри платформы, вы сразу можете торговать им на внутренней бирже Waves DAX. Также такие проекты, как Etherdelta, созданные для обмена токенов на Ethereum, могут бесплатно допустить достойный актив к торгам.

В случае если токен и монета прошли листинг на популярной площадке, это может стать стимулом для роста стоимости актива и привлечения дополнительных инвесторов в торги. Но иногда листинг на неправильной бирже может сыграть злую шутку. Например, биржа с весьма неоднозначной репутацией YoBit – не лучший вариант для первичного листинга. Хуже, что площадка может и не спросить вашего желания и начать торги самостоятельно. Чтобы этого избежать, желательно как можно скорее провести первичный листинг одним из вышеописанных способов.

## Инструменты трейдинга на криптовалютных биржах

Один из основных инструментов, используемых трейдерами, – это графики, которые могут быть в виде линии – линейные, в виде горизонтальных отрезков – баров, а также в форме японских свечей. Разные графики обладают разной информативностью, а степень удобства каждый трейдер выбирает себе сам. Обычно графики выстраиваются за какой-то определенный интервал, и пользователь может его изменять для аналитических целей. Обработка графиков с помощью различных индикаторов называется техническим анализом. Индикаторы разделены на два основных класса: трендовые, соответственно, следящие за трендом (от англ. *trend* – курс, направление), и осцилляторы. Также выделяют объемные и информационные индикаторы. Не буду вдаваться в глубины, лишь скажу, что все необходимые индикаторы доступны для применения на большинстве криптовалютных бирж и располагаются в том же окне, где и графики. Применение технического анализа в торговле – вопрос уже не любительской сферы. Требуется минимальный опыт и профессиональные навыки, чтобы данный инструмент приносил пользу. В сфере традиционной торговли активами существуют аналитические агентства, которые проводят анализ самостоятельно и предоставляют доступ к результатам бесплатно либо на основании закрытой подписки. Такая отборная информация часто называется торговыми сигналами и сейчас есть множество поставщиков торговых сигналов для криптовалют, однако верить им или нет – большой вопрос, особенно если монета неизвестная, с маленьким объемом торгов. Возможно, вас просто пытаются сделать трейдером-инвестором для схемы памп и дампа.

Большинство трейдеров на традиционных биржах применяют в работе такой инструмент, как экономический календарь, содержащий даты появления различной важной для рынка информации из множества официальных источников. В торговле криптовалютами крупные информационные поводы также могут быть занесены в календарь, и в дату появления той или иной информации рынок в целом или отдельные активы проявят большую волатильность, что может стать отличным поводом для начала рискованных торгов либо, наоборот, для временной приостановки операций при консервативном стиле работы. И если для трейдеров Форекс есть готовые календари с собранными воедино различными датами появления важной информации, то для криптовалют таких универсальных календарей нет. Возможно, в будущем какое-то подобие общего календаря



появится на свет, а сейчас каждому трейдеру придется составлять свой собственный вариант. Также важно хранить историю сделок, для чего существуют инструмент [coinsharbor.com](http://coinsharbor.com) – дневник криптотрейдера.

Специализированное программное обеспечение – не редкость на фондовых и валютных рынках. Объединяя в себе все необходимое, оно может стать универсальным инструментом для сферы традиционной биржевой торговли. Например, торговый терминал MetaTrader 4, созданный в основном для Форекс, позволяет добавить через API (от англ. *Application Programming Interface* – интерфейс программирования приложения) различные криптовалютные биржи, а энтузиасты мира криптовалют создали свой аналог под названием Qt Bitcoin Trader. Часть из программного обеспечения позволяет осуществлять торговлю не только самостоятельно, так сказать «живую», но и подключить к процессу торговых ботов. Бот (сокр. от слова «робот») – это программа, осуществляющая автоматическую торговлю по заранее заданному алгоритму, торговой стратегии. Создать идеального бота невозможно, как не бывает и идеальных торговых стратегий. Самая успешная стратегия перестает быть суперприбыльной, как только ее влияние на рынок становится более или менее заметным, а число трейдеров и ботов, применяющих такую стратегию, очень сильно растет. Именно поэтому я не верю в рекламные кампании по продаже неких эксклюзивных ботов с уникальной стратегией либо паев инвестиционных фондов, владеющих подобными чудорешениями. Один простой вопрос: зачем продавать курицу, несущую золотые яйца? Одним из видов ботов является арбитражный бот – это программа, которая реализует возможности покупать и продавать валюту на разных площадках, зарабатывая на разнице курса между биржами. Эта очень простая и понятная схема, но чаще всего трудно реализуемая с одним и тем же объемом депозита. Суть проста: купить, например, 30 эфиров за 1 биткойн на бирже А, перевести эфир на биржу Б и продать за 1,05 биткойна, заработав на сделке 5 % прибыли. Но важно учитывать, что время проведения транзакций может сыграть негативную роль – ордер на покупку эфира по высокой цене может быть закрыт на бирже Б, и курс сравняется или даже снизится. Гораздо более простой представляется торговля по классическим стратегиям, например, торговля интрадей – в рамках одного торгового дня, либо стратегия долгосрочного и среднесрочного инвестирования с горизонтом от нескольких месяцев до нескольких лет. Моей целью не является посвящать читателя во все тонкости трейдинга, стратегии и знакомить со всей терминологией, могу лишь сказать, что многие из моих знакомых вполне успешно применяют имеющийся инструментарий для реализации собственных торговых стратегий и очень неплохо зарабатывают на движениях криптовалют, хотя примеры потерь средств тоже есть.

## Bitcoin-фьючерсы и паевые фонды

Фьючерсы – (от англ. *future* – будущее) – это производный финансовый инструмент, позволяющий вам через определенное время купить некий актив по фиксированной цене. Это биржевой инструмент, известный рынку сотни лет. До декабря 2017 года не было ни одной биржи, предлагающей организованную торговлю фьючерсами на биткойн, но вдруг сразу две чикагских товарно-сырьевых биржи выпустили такой инструмент в обращение. Фьючерс предполагает, что в определенную дату одна сторона обязуется продать, а вторая купить определенное количество товара по определенной цене. Соответственно, одна из сторон заведомо окажется в проигрыше, и вот почему: если цена актива к моменту наступления момента исполнения обязательств вырастет – в выигрыше окажется покупатель, если же цена упадет – то выиграет продавец. Нужно понимать, что те, кто покупал за 18 тысяч долларов январский фьючерс на Bitcoin в декабре 2017 года, рассчитывали на его дальнейший рост и заработали. Те же, кто покупал мартовский фьючерс по той же цене – проиграли, т. к. курс монеты существенно снизился. Если копнуть глубже, то на самом деле Bitcoin участникам торгов не нужен. Это возможность играть именно на курсе Bitcoin и вместо настоящих монет выпустить на рынок суррогатный актив в виде фьючерсов – ничего не значащих обязательств. Ведь фактически никто не собирается поставлять вам монеты в срок, а лишь получить прибыль или зафиксировать убыток с курсовой разницы. Это называется «расчетный фьючерсный контракт», когда фактическая поставка актива не предполагается в принципе. Все операции открываются и закрываются в долларах США, как только заканчивается срок действия одного фьючерса, вам тут же открывают другой на новый срок или закрывают сделку в основной валюте баланса. Происходит просто перекачивание денег из одной корзины в

другую. При этом еще раз напомню, никакой реальной продажи биткоина за всем этим нет, транзакции при покупке и продаже фьючерсов в блокчейне Биткоин не проводятся, никто не резервирует монеты или хеш-мощность под данную сделку. Если разобраться, на рынке просто появилось огромное количество неких фантомных биткоинов на бумаге, что в итоге не лучшим образом отразилось на курсе. Однако появление фьючерсов открыло новую страницу в признании биткоина и других криптовалют реальным активом, привлекло в индустрию дополнительные инвестиции, расширило способы заработка на криптовалютах. Сегодня существуют фьючерсы на десятки различных монет на множестве криптовалютных и традиционных бирж. Многие прогрессивные криптовалютные биржи планируют введение и других производных финансовых инструментов в деловой оборот. Чаще всего лидером в данном сегменте называют биржу Bitmex, также предлагающую торговлю с плечом до x100, что является абсолютным рекордом для существующих криптовалютных площадок.

Еще одним инструментом, который очень ждут и криптоэнтузиасты, и традиционные инвесторы, является ETF (от англ. *Exchange Traded Fund* – фонд, торгуемый на бирже). По сути это аналог паевого фонда, и продаются/покупаются на бирже именно паи этого фонда. Сам же фонд может вкладывать средства в один конкретный инструмент, например, в товар (золото), в голубые фишки (акции крупных компаний США), или в несколько разных товаров, или в акции различных компаний. Акции могут быть сгруппированы по отраслям, тогда фонд называется отраслевым. Сегодня рынок ждет появления отраслевых криптовалютных фондов, где капитал фонда будет распределен между некоторыми криптовалютами, образуя сбалансированную корзину. В неофициальном виде они существуют давно, примером является российский Cyber.fund, а вот официально зарегистрироваться пока не удается ни одному из претендентов, подававших заявки в SEC США. Новости об отказе в регистрации криптовалютных ETF негативно сказываются на курсе криптовалют, т. к. именно через паи ETF рынок ожидал привлечь основную массу так называемых институциональных инвесторов.

### **Волатильность криптовалют, пампы и дампы**

Волатильность (от англ. *volatility*) – изменчивость цен на рынке. Криптовалюты настолько нестабильны, что внушают ужас трейдерам, привыкшим торговать на фондовом или валютном рынке, где волатильность может достигать лишь нескольких процентов в день. В криптовалютах же скачки курсов настолько большие, что могут достигать тысяч процентов в день. Для многих игроков на бирже это не недостаток, а огромный шанс заработать. Почему же курс криптовалют так волатилен? Причин может быть несколько. На курс большинства монет влияет текущая стоимость биткоина и ее изменение. Новости, например, о запрете ICO в Китае, могут резко обрушить курс биткоина и следом всех остальных валют, особенно олицетворяющих платформы по запуску ICO. Новость о введении фьючерсов на биткоин в США подтолкнула его курс вверх. Но ведь и в мире фиатных валют и активов каждый день публикуются новости, почему они не оказывают такого влияния? Дело в том, что курсы криптовалют – это по большей части результат притяжения или неприятия сообществом актива, именно участники криптоэкономики наделяют тот или иной актив ценностью. В обычном мире стоимость акций или товаров – это совокупность оценочных категорий, и она привязана к чему-то более реальному, чем интерес публики. Валюты на FOREX также поддерживаются эмитировавшими их государствами и их экономиками. У большинства криптовалют нет централизованной поддержки, именно поэтому их курс может изменяться столь существенно. Ранее я писал, что у добычи биткоина есть некая себестоимость, слагаемая из затрат на добычу одной монеты. В основном это электроэнергия и ускоренная амортизация оборудования. По подсчетам экспертов, средняя себестоимость добычи одной монеты биткоина может составлять около 4500 долларов США на середину октября 2018 года, соответственно, ниже этой планки он может падать лишь кратковременно. Опять же, существует масса кошельков, на которых монеты добыты при себестоимости 1000 долларов и ниже, значит, реальную среднюю себестоимость всех добытых монет просто невозможно посчитать. Это означает лишь одно – биткоину точно есть куда падать. Но почему в декабре 2017 года цена биткоина превышала 20 000 долларов? Возможно, причиной был общий позитивный настрой, масса хороших новостей разного плана, успешные сборы многих ICO и волна интереса широких масс к технологии блокчейн и биткоину в частности.

Как бы то ни было, изменить ситуацию пока невозможно, и лишь достаточно отдаленное будущее может внести коррективы в колебания курсов криптовалют. А пока волатильность лишь помогает некоторым удачливым трейдерам, даже непрофессиональным, зарабатывать на разнице курсов. Особенно поспособствовало этому появление площадки BitMEX, которая позволила торговать криптовалютами с плечом 1:100, тогда как ранее максимальное плечо 1:5 предлагала биржа Kraken, а другие – не более x2-x3. С таким большим плечом, просчитав или просто угадав движение курса, можно заработать в сотни раз больше имеющегося на бирже депозита. С другой стороны, риск потерь также велик, и именно это отталкивает крупные финансовые институты и так называемых институциональных инвесторов, привыкших более детально просчитывать риски.

Резкие искусственно созданные скачки волатильности называют «пампами» и «дампами». На цивилизованных рынках такая практика относится к манипуляциям и, естественно, наказуема. В криптовалютах же ничего не мешает определенным кругам – нечистым на руку биржам, трейдерам и организованным сообществам – претворять данную схему в жизнь. Пампы (от англ. *pump* – надувать или накачивать) и дампы (от англ. *dump* – сброс) – это спекулятивная схема, при которой организуется рост цены какой-то монеты – накачивание, затем происходит вовлечение в покупки рядовых инвесторов, а потом следует продажа собственных монет организаторов по максимальной цене – сброс. На сленге можно услышать выражение «стрижка хомячков», как раз характеризующее финальную стадию процесса. Упрощенно вся схема выглядит так: выбирается монета для пампа, удовлетворяющая ряду критериев, таких как листинг на нескольких биржах и достаточное количество монет в свободном обороте. Предварительно закупается нужный объем монет без огласки, небольшими суммами. Далее организаторы пампа подстраиваются под имеющийся информационный повод или создают свои новости для организации первой волны – публичной скупки монет с целью повысить ее курс. Далее идет работа по привлечению к покупкам рядовых инвесторов, которые начинают подключаться к процессу, создавая вторую волну пампа. А когда с помощью рядовых инвесторов курс достигает требуемых значений, происходит неминуемый дамп, третья волна – сброс всех монет организаторами «на хаях» – высоких значениях курса (от англ. *high* – высокий). Дамп неминуемо приводит к падению цены монеты до первоначальных значений или даже ниже, чем до начала первой волны. Если монета представляет интерес для долгосрочных инвестиций, организаторы могут на теперь уже низком курсе откупить какой-то объем монет назад – на будущее. Либо же просто остаться в прибыли, номинированной в биткоин или иную более-менее стабильную монету. Существует ряд информационных каналов, где по заявлению организаторов публикуется закрытая информация о готовящихся пампах. Также каналы публикуют торговые сигналы, могут выбрасывать подобную информацию. Однако следует помнить, что задачей организаторов является собственное обогащение, поэтому может оказаться, что вас пытаются привлечь в качестве тех самых хомячков для последующей стрижки. Я очень скептически отношусь к возможности заработка на информации о пампах, хотя в принципе это возможно. Так можно ли вообще заработать на биржевой торговле криптовалютами? Несомненно, да.

## Можно ли заработать на бирже криптовалют?

Биржевой трейдинг сегодня – один из популярнейших способов заработка на теме криптовалют. Биржевая торговля является самым развитым элементом криптовалютной экономики. Самый простой вариант заработка для новичков – это покупка недооцененного молодого актива, с прицелом продать его через несколько месяцев или даже лет. Для этого можно обойтись и без биржи – например, купить интересующую монету на ICO или поучаствовать в прямой сделке. На бирже же можно задействовать простейший инструментарий – приобрести актив по сегодняшней цене и выставить ордер на продажу по цене в несколько раз выше. Если когда-то цена достигнет искомого значения ордер сработает и вы получите свою прибыль. Также можно заработать и на падении, открывая короткие позиции. Стратегий заработка на криптовалютных биржах достаточно много: есть агрессивные и высокорисковые, есть консервативные и менее рискованные. По общему мнению активных участников биржевой торговли, доход на депозит в размере 10 % в месяц – легко достижимая величина. Для меня биржевая торговля – процесс не очень знакомый во всех деталях, я не могу выступить профессиональным консультантом и тем более взять в управление чужие средства для торговли.

Но есть в данном секторе профессионалы, готовые за вознаграждение управлять вашими средствами и извлекать прибыль. Возможны и убытки, если доверенный трейдер выберет неправильную стратегию торговли. При этом, торгуя самостоятельно, не имея практического опыта и профессиональных знаний, этот риск может быть во много раз выше. Общаясь в профильных чатах, я часто вижу отчеты разных пользователей об их успешных сделках, порой фигурирующие суммы вполне достаточны, чтобы сравниться с хорошей зарплатой в российской глубинке, иногда переваливают за цифры с шестью нулями. Что точно можно сказать, криптовалютный рынок – это рынок возможностей.

Еще одним вполне понятным способом заработка на торговле криптовалютой является покупка доли в бирже. Только за 2018 год я был свидетелем более пяти ICO, призванных собрать средства на открытие очередной биржи. Токены популярных бирж, появившихся в 2017 году, продемонстрировали очень хорошую доходность. Многие площадки предлагают выплату доходов от деятельности биржи для держателей токенов либо существенные скидки на биржевые комиссии, в зависимости от количества токенов во владении.

Ряд бирж, например Poloniex, предоставляет возможность пользователям кредитовать сделки других пользователей с помощью специального аккаунта. С баланса основного счета вы переводите свои средства на кредитный и отдаете их в долг на короткий срок. Процентную ставку формирует рынок. Чаще всего она низкая, но в период больших скачков курса ставка может достигать вполне ощутимой величины – до 1 % в день. Для точного расчета необходим длительный эксперимент, но мой короткий опыт работы с долговым аккаунтом на Poloniex в 2016 году показал, что от 0,5 до 1 % в месяц можно было получить, ничем не рискуя. Если ваши средства ждут лучших времен, например возможного роста в 2021 году, небольшая гарантированная доходность может быть весьма кстати. Биржа не даст заемщику спустить ваши деньги, в опасной ситуации его заявки будут принудительно закрыты, и ваши средства вернуться на кошелек. Но сегодня размер дневной ставки не превышает 0,01 % в день, или чуть более 3,5 % годовых, что может быть выгодным только для развитых стран с низким уровнем инфляции.

## Глава 7

# Собственная криптовалюта

### Как создать свою монету

Многих моих друзей интересует вопрос: можно ли создать собственную монету и выпустить ее на рынок? И если три года назад я бы назвал технический процесс сложным, то сегодня с уверенностью могу сказать – создать свою криптовалюту легко. На сегодняшний день самый простой способ – это создать токен, который был бы встроен внутрь инфраструктуры специализированной платформы, например, Ethereum и Waves. Вскоре к списку платформ для создания токенов могут добавиться возможности китайской NEO и спорной (по разным причинам) EOS. Если под созданием монеты понимать именно выпуск токена, то проще процесс выглядит на Waves: вам нужно лишь заполнить 4 поля с базовыми параметрами токена в официальной программе-кошельке Waves, оплатить комиссию в 1 waves и нажать кнопку «Выпустить». Все, ваш токен готов, и он сразу доступен для торгов на внутренней бирже Waves DEX. Им можно сразу начать торговать, если ваш потенциальный круг клиентов уже знаком с системой Waves и имеет монеты Bitcoin или Waves на счету кошелька. Биржа Waves DEX встроена в кошельки как для настольных компьютеров, так и приложений для мобильных устройств. Первый раз процесс может показаться немного сложным, потребуется какое-то время на знакомство с системой, установку кошельков, однако при определенном опыте он занимает не более 5 минут. Платформа Waves не имеет такого широкого распространения, как всем известный Ethereum, и выбор в пользу токенов Waves для создания собственной монеты или проведения ICO сделали лишь несколько процентов. Сегодня существует несколько площадок, готовых провести листинг токенов платформы Waves, но их перечень очень узок.

Наибольшую популярность для создания токенов получила платформа Ethereum, во многом благодаря широкому распространению самой монеты ETH среди майнеров и криптоэнтузиастов. Так же, как и в Waves, токен в Эфириуме – это цифровой актив, созданный внутри платформы, с тем лишь отличием, что процесс эмиссии токена более сложный, но при этом и более гибкий. До недавнего времени создание смарт-контракта токена требовало некоторой предварительной

подготовки и базовых навыков программирования, а теперь есть автоматические инструменты для создания контрактов «на лету», с возможностью выбора дополнительных параметров монеты. Если задача стоит сугубо экспериментальная, базовый код смарт-контракта токена вполне подойдет. Его необязательно публиковать в главной сети – Mainnet, для экспериментов существуют тестовые сети, как публично доступные, так и создаваемые пользователями свои локальные версии – Testnet. Если бы каждый разработчик для создания токена использовал отдельный код, можно было бы предположить сложности в интеграции разных токенов с разными сервисами, биржами, кошельками. Поэтому и появились стандарты, применяемые для создания токенов, называемые Ethereum Request for Comments – запрос на комментарии (в сообществе) Эфириум, или сокращенно ERC. Это своего рода предложения по улучшению системы, которым присваивается порядковый номер. Сегодня существуют два основных стандарта токенов – ERC20, подходящий для большинства решений, и ERC721 для невзаимозаменяемых токенов или NFT (от англ. *Non-Fungible Tokens*). ERC20 описывает все базовые потребности сторон, предъявляемые к токену, и постоянно дополняется новыми правилами и рекомендациями, что делает работу разработчиков новых монет более простой и понятной. Имеется и более продвинутая версия стандарта – ERC223, позволяющая возвращать токены со смарт-контракта, отправленные туда по ошибке, а также удешевляющая стоимость обработки запросов, которые осуществляет смарт-контракт. По сути, в ближайшее время стандарт ERC20 вберет в себя весь функционал ERC223. Второй популярный стандарт токенов появился в ключе необходимости создания уникальных цифровых активов, где все выпускаемые токены – разные и несовместимые с любыми другими токенами, они чаще всего представляют из себя некий предмет для коллекционирования. Этот стандарт под номером ERC721 также часто называют стандартом NFT. Ярчайший пример применения такого токена – игра «КриптоКотятка» или «CryptoKitties», наделавшая много шума в 2017 году и ставшая лидером по числу транзакций в сети Ethereum. Каждый котенок уникален, имеет собственные отличительные признаки, которые можно увидеть в официальном приложении. Чуть раньше появился подобный проект КриптоПанки, также предлагавший уникальные токены, которые были привязаны к пиксельным картинкам голов панков. В более практической плоскости стандарт ERC721 может быть использован для подтверждения права владения уникальными вещами ручной работы, коллекционными ценностями. Также реально использовать токен в качестве членства в закрытом клубе, проведения голосований, подтверждения прав владения активами. Токен NFT является неделимым, его нельзя разделить на части, как, например, любой ERC20 токен или монету эфира, биткойна, дэш и других представителей криптовалют. Кстати, число знаков после запятой может быть задано произвольно. Вам необязательно делить свой актив на миллион частиц, всегда можно ограничиться и двумя знаками после запятой, хотя признанным стандартом является наличие восьми знаков после запятой, как у биткойна. Стоимость внедрения смарт-контракта токена может составить от небольшой суммы в эфире, требуемой для исполнения контракта, до сотен ETH на привлечение команды, способной создать связку нескольких смарт-контрактов в единое целое, если такая необходимость продиктована целями и задачами проекта. На создании токенов я остановлюсь чуть подробнее в одном из следующих разделов.

Следующий вариант – это сделать форк монеты, то есть взять исходный открытый код проекта, который общедоступен на специализированных ресурсах, например на GitHub. Форк (от англ. *fork* – вилка) – это разветвление кода проекта. Фактически вы копируете проект и переделываете его под себя, устраняя недостатки или снабжая полезными нововведениями. Практически любой разбирающийся в программировании человек может «форкнуть» монету за один день, пользуясь доступными в Интернете пошаговыми текстовыми инструкциями и видеоруководствами. По сути, большинство имеющихся сегодня монет – это форки исходного кода биткойна, либо форки его форков, как бы странно это ни звучало. Кажущаяся простота этого процесса не означает, что после копирования кода не придется попотеть над базовыми настройками, установкой первых нод – узлов сети, тестированием кошелька, внедрением отличного от изначального алгоритма майнинга или форжинга, внедрением элементов безопасности и т. д. Сегодня существует масса предложений от команд разработчиков, предлагающих осуществить форк той или иной монеты за плату, чаще всего от 1 BTC и выше. За минимальную сумму вы получите и минимальный функционал. Существуют автоматические

сервисы наподобие [cryptonotestarter.org](http://cryptonotestarter.org) или [forknote.net](http://forknote.net) для простого форка монет, основанных на [Bytecoin](http://Bytecoin) и его самом известном последователе – [Monero](http://Monero).

Пойти самым сложным путем и сделать новую монету с уникальным блокчейн-решением, авторским кошельком и обновленным вариантом применяемого языка программирования – самый сложный и затратный путь. Такая задача под силу только большому коллективу разработчиков и при большой поддержке сообщества. Трудно оценить временные и финансовые затраты на внедрение подобного решения. А самое главное, спорным остается вопрос необходимости существования еще одной монеты. По мне игра стоит свеч, только если в команде есть талантливые люди, выдвигающие революционные идеи, и исполнители, готовые реализовать данные идеи в готовый продукт. Сегодняшний выбор монет настолько широк, что удивить рынок можно только чем-то из ряда вон выходящим, прорывным. В 2018 году есть как минимум две амбициозные заявки – это не раз упомянутые EOS Дэна Ларимера и TON Павла Дурова. Оба этих проекта привлекли миллиарды долларов на реализацию поставленных задач. Если с такими деньгами им это не удастся – криптовалюту ждет серьезное потрясение. При этом история криптовалют знает примеры появления нестандартных проектов и новых монет, которые не обладали подобным стартовым капиталом, при этом смогли сделать нечто из ряда вон выходящее, полезное сообществу и продвинутое в технологическом плане. Стержнем таких проектов стали либо новые усовершенствованные алгоритмы хеширования, либо расширенные возможности анонимной отправки и использования монет, либо решение вопросов пропускной способности сети, либо привязка монеты к инновационной бизнес-идее. Выбор в пользу создания собственной монеты, помимо реализации авторских амбиций, может быть продиктован и сугубо экономическими мотивами. При создании собственной монеты команда разработчиков имеет возможность создать большое количество монет для своих нужд при генерации 0-го блока (генезис-блока), а также поучаствовать в ее добыче на ранних стадиях, с низкой сложностью и высоким количественным вознаграждением. Максимальный контроль над блокчейн и его развитием – также весомый аргумент в пользу своего собственного решения.

В создании собственных монет под бизнес-проект есть один существенный нюанс: важно понять, действительно ли нужна собственная монета или токен для становления и развития этой идеи? Может оказаться так, что монета будет никому не нужна, а ее поддержка будет отнимать силы и средства. История криптовалют знает сотни подобных историй, а в ближайшем будущем тысячи проектов окажутся заброшены. Пока вы не научились создавать монеты, или токены, вам кажется, что главное для монетизации проекта – это именно некий цифровой актив на блокчейн, остальное уже не проблема. Да, создать монету просто, но нужно дополнить ее идейным содержанием, создать вокруг идеи сообщество последователей, привлечь к проекту инвесторов, а это уже не так легко. При этом зачастую проще привлечь инвесторов в проект стандартным путем, испытанным, понятным, законодательно оформленным. Распределение долей может произойти с помощью простой компании с ограниченной ответственностью, учет затрат и доходов может вестись с помощью стандартных бухгалтерских программ, а перечисления средств – через стандартную фиатную систему. Я лишь пытаюсь сказать, что манипулировать словом «блокчейн» и создавать какой-то блокчейн-актив без понимания его места в бизнесе, без наличия у монеты утилитарной ценности – не стоит. Если речь идет лишь о привлечении инвестиций – лучше ограничиться простым ERC20 токеном, с возможностью его обратного выкупа у инвесторов в будущем периоде и последовательного сжигания выкупленных токенов.

## Токен, монета и цифровой актив

Еще раз попробуем разобраться с этими тремя понятиями. По сути и тем, и другим, и третьим словом можно называть все, что относится к криптовалюте, особенно при пространственных разговорах. Однако это не совсем одно и то же. Для меня монета – это отдельная платформа, отдельный уникальный блокчейн. Биткойн – это монета, его форки – тоже монеты. Часто отличительной особенностью монеты является наличие у нее собственного алгоритма консенсуса – PoW, PoS, DAG и т. д., монеты можно добывать – майнить. Зачастую эмиссия монет бесконечна, хотя в большинстве случаев есть будущий лимит эмиссии, достигнуть которого можно за несколько лет, а то и десятков лет. Сложность добычи монеты напрямую влияет на ее стоимость.

Токен – это как бы «подмонета», которая находится внутри уже существующего блокчейна – Ethereum, Waves, BitShares, OMNI или NEO. Например, с помощью 1 монеты Waves можно создать один вид токена, но указать любое количество токенов в первоначальной эмиссии. То есть, 1 Waves может стать 1000 других единиц, а может превратиться и в 1 млн и более токенов. Токены майнить нельзя, а их число изначально ограничено определенным числом. Создатель сразу выпускает весь первичный объем токенов, в редких случаях возможен вариант дополнительной эмиссии, опять же, в виде объемной серии, так сказать. Стоимость токена чаще формируется за счет идейного содержания проекта.

Цифровой актив (с англ. *digital asset*) – это тот же токен, или монета, в общем понимании. Вся криптовалюта – это цифровые активы. В законопроекте «О цифровых финансовых активах» в РФ и монета, и токен относятся к цифровым финансовым активам, и критерием отнесения их к таковым является способ создания (с помощью криптографии) и внесение записи об этом в распределенный реестр (блокчейн). В разнообразных источниках цифровым активом принято считать любой объект в двоичном коде. Электронная книга, цифровая фотография, файл или программа могут с тем же успехом считаться цифровым активом. Поэтому российские законодатели попытались сузить спектр возможных толкований и ввели уточняющее слово «финансовый» в понятие цифрового актива.

Я бы считал идеальным цифровым активом токен, привязанный к реальному товарному или финансовому активу: золоту, нефти, квадратным метрам недвижимости, объему электроэнергии или попросту национальной валюте государства. Такие активы также называют стейблкоинами. Обычно их количество как-то привязано к количеству базового актива, и чаще всего предполагается регулярная дополнительная эмиссия таких токенов, или монет. Например, 1 токен проекта Digix DAO привязан к 1 грамму золота. Т. е. созданный на платформе Ethereum актив является цифровым золотом. Чаще активом выступает именно токен какой-то платформы, и гораздо реже для этого создается отдельная монета. У обеспеченного цифрового актива предполагается меньшая волатильность, однако проблемой является доказательство наличия требуемого обеспечения. Например, большие сомнения вызывало присутствие у токена Tether (USDT) резерва в виде американской валюты, равного объему выпущенных токенов. Большое количество цифровых активов создавалось на платформе BitShares, однако некоторая сложность в использовании площадки не дала проекту стать полноценным аналогом товарной или фондовой биржи в цифровом обличье. Возможно, скоро нас ждет появление отдельной биржи для цифровых активов – площадки, на которой будут торговаться только обеспеченные реальной стоимостью токены и монеты. Может ли это случиться в России? Возможно, только вышеуказанный законопроект предполагает такое же отношение к участникам рынка цифровых активов, как и к фондовым биржам и традиционным финансовым компаниям. Соответствовать правилам закона «Об организованных торгах» или ФЗ «О рынке ценных бумаг» смогут лишь единицы из компаний, пытающихся работать в криптоиндустрии. Если не будут введены отдельные правила – рынок цифровых активов так и останется в серой зоне. Я очень надеюсь, что итоговые правила будут несколько упрощены, что позволит добиться широкого применения возможностей новой цифровой экономики в нашем государстве, а деятельные личности смогут создавать любые виды собственных или корпоративных цифровых финансовых активов.

## Премайн и инстамайн

Премайн (от англ. *pre* – пред и *mine* – добывать) – это процесс пред-добычи монеты до ее официального появления, когда ее очень легко генерировать в большом количестве и без применения специализированного оборудования. Создатель Bitcoin, Сатоши Накамото, намайнил небольшое количество монет до того, как он представил свою систему широким кругам, и после анонса также смог долгое время генерировать блоки без особых усилий. Также он дал возможность майнить Bitcoin своим ранним последователям, чтобы совместно решить некоторые технические вопросы и протестировать систему. Таким образом, выходит, узкий круг людей оказывается в наиболее выгодных условиях, действуя без конкуренции. Сегодня считается, что более 30 000 первых блоков в блокчейне Биткоин являются именно премайном, но если быть скрупулезным – Сатоши добыл лишь 14 блоков в одиночку до официального старта проекта. При появлении лайткоина его создатель, Чарли Ли, официально заявил, что сгенерировал три блока с общей наградой в 150 LTC в качестве премайна. Сегодня многие проекты осуществляют премайн в

неприличных масштабах, что может негативно сказаться на будущем монеты и не вызывает одобрения у потенциальных майнеров и инвесторов. Премайн не предполагает увеличения суммы вознаграждения в первых блоках, он возможен только в период, когда единичные майнеры имеют доступ к генерации блоков.

Инстамайн (от англ. *instant* – мгновенный и *mine* – добыча) – это генерация большого количества монет в 0-ом блоке (генезис-блоке) или запрограммированная высокая награда в нескольких блоках после генезиса. Инстамайн – это тоже премайн, но в нулевом блоке он может произойти вообще без участия вычислительных мощностей, а количество блоков с непропорционально высокой наградой добывается буквально за несколько часов после старта самими разработчиками. Например, проект DeepOnion coin в 2017 году заявил о премаине 90 % в генезис-блоке, намереваясь раздать эти монеты сообществу, однако вернее было назвать такой процесс инстамайном. Инстамайн вызывает гораздо больше подозрений. Но кто проконтролирует честное распределение такого инстамайна? Также в несправедливом инстамаине обвиняли создателей дэш, когда за 48 часов от момента запуска сети около 2 млн монет было сгенерировано майнерами. А это, на минуточку, 10 % от общего объема выпуска монеты, рассчитанного на годы. Создатели объяснили проблему ошибкой в коде алгоритма пересчета сложности. Тем не менее факт остается фактом. Можно сказать, что все токены на площадках по их созданию появляются путем инстамайна – мгновенно.

Понятия премайна и инстамайна часто путают, называя все именно премайном. Считается, что премайн – более вредное явление. Но от премайна и инстамайна может быть польза. При экстренном переходе блокчейна на новую цепочку блоков, например при хард-форке, можно запрограммировать передачу балансов из старого блокчейна в новую цепочку. Также можно быстро провести первичную эмиссию для проведения ICO и продажи монет ранним инвесторам. При создании собственной монеты важно соблюсти баланс – слишком большой премайн, назначение которого туманно или прямо направлено на обогащение создателя, может отпугнуть сообщество. Признаком хорошего тона считаются заморозка большей части активов, полученных создателями монеты путем премайна или инстамайна, или внедрение публичного надзора за расходованием такого фонда.

## Эмиссия и инфляция

Объем эмиссии той или иной монеты может быть ограниченным или неограниченным, что зависит только от воли создателей криптовалюты. В Ethereum объем эмиссии неограниченный, а в Bitcoin эмиссия ограничена 21 миллионом монет. Монет с ограниченной эмиссией гораздо больше, чем тех, у которых эмиссия не ограничена. Связано это с тем, что многие разработчики слепо подражают идее Накамото, а также не имеют понятия о том, как можно управлять инфляцией в монетах с неограниченной эмиссией. Процесс эмиссии криптовалют происходит путем выброса на рынок новых монет, добытых майнерами. Награда за каждый новый найденный блок составляет определенную величину, например, 50 монет. Учитывая, что существует механизм роста сложности майнинга, который также усредняет время появления нового блока, за сутки может появиться лишь определенное количество блоков, а следовательно, будет эмитировано определенное количество новых монет. В начале майнинга биткоина награда за блок составляла 50 BTC и при среднем времени блока в 10 минут за сутки могло быть добыто 144 блока, что в итоге составляет 7200 биткоинов. Большая цифра, и, если бы так продолжалось всегда, потребовалось бы лишь 3000 дней или лет для того, чтобы все 21 млн биткоинов были добыты. Однако Сатоши заложил в код своего детища механизм уполовинивания награды, который срабатывает каждые 210 000 блоков, или примерно раз в 4 года. За первый цикл с наградой 50 BTC было добыто 10,5 млн биткоинов или половина планируемой эмиссии, за второй цикл с наградой 25 BTC уже 5,25 млн монет, или четверть эмиссии, а идущий сегодня третий цикл с наградой 12,5 BTC продлится до мая 2020 года и позволит майнерам добыть лишь 2,625 млн BTC. Данный процесс описывается определенной математической последовательностью, представляющей из себя сходящийся ряд. Подробные понятные объяснения легко найти в открытых источниках. Нам интересен лишь вывод из этой истории. Если производить математические расчеты дальше, то для добычи всех 21 млн биткоинов нам понадобится около 132 лет, что означает, что последний биткоин будет добыт приблизительно в 2150 году. Но здесь есть один маленький нюанс:



в последних блоках добываться будут уже сатоши – дробные единицы биткойна, т. к. награда за блок снизится до своего минимума. Очень интересно, какова будет стоимость 1 сатоши к тому моменту. Блоки же с наградой, близкой к 1 BTC, перестанут добываться уже после 2036 года, и к этому моменту будет добыто более 99 % всех возможных BTC. Соответственно, после 2040 года награда за блок опустится менее 0,5 BTC, и в оборот будет поступать ничтожное количество новых монет. Такая схема эмиссии призвана бороться с инфляцией биткойна, а также призвана увеличивать ценность монет во времени. Здесь еще раз стоит обратить внимание на важную функцию майнеров – они производят эмиссию денежных знаков в монетах, основанных на алгоритме PoW. И раз майнерам должно быть выгодно печатать деньги, цена монеты должна расти после уполовинивания награды. Такое явление было явно заметно в 2016 году, когда после майского снижения награды с 25 до 12,5 BTC за блок стоимость биткойна выросла с 400 до почти 800 долларов. Последовавшее за этим удорожание майнинга вызвало дальнейший рост цены монеты, т. к. себестоимость добычи одного BTC также резко возросла.

В монетах, применяющих иные способы достижения консенсуса – PoS или комбинированные виды, также применяется система снижения наград для борьбы с инфляцией и обесцениванием монет. При распределении награды за блок между майнерами и мастернодами или стейкхолдерами (держателями балансов с целью получения PoS-вознаграждения) может быть изначально смещен баланс в пользу майнеров, а в последующем – в пользу стейкхолдеров. Например, первые 100 000 блоков награда делится в пропорции 70 % майнерам, 20 % мастернодам и стейкхолдерам, 10 % отчисляется в фонд развития монеты. Со 100 001-го блока вознаграждение выравнивается и составляет 45 % на 45 % и все те же 10 % остаются разработчикам. При достижении блока 200 001 и реализации важных задач командой взнос в фонд может быть отменен, а награда составлять 30 % майнерам и 70 % мастернодам и стейкхолдерам. Делается это для того, чтобы изначально майнеры произвели достаточную эмиссию и из них или покупателей на свободном рынке начали формироваться инвесторы – держатели и владельцы мастернод. Чем больше монет заблокировано в мастернодах или кошельках стейкхолдеров, тем меньше шансов на резкий обвал курса монеты, связанный со сбросом монет. Например, в мастернодах Дэш заблокировано чуть менее 60 % текущего объема выпущенных монет, их количество составляет почти 5000, в каждом 1000 монет. Соответственно, всего около 5 млн дэш из общих 8,4 млн в обороте не участвуют в торгах, а выполняют роль монетных дворов, участвуя в эмиссии. Также мастерноды играют важную роль в подтверждении транзакций и поддержке безопасности сети. Множество появляющихся сегодня монет – форков дэш или PIVX – не могут похвастаться грамотным расчетом параметров эмиссии, что часто приводит к чрезмерной инфляции и последующему резкому обвалу курса монет. Задача разработчиков в этом случае – настроить эмиссию так, чтобы в первое время объем генерации монет мастернодами показывал высокий показатель ROI, зачастую превышающий тысячи процентов годовых. Беда лишь в том, что незадачливые инвесторы смотрят на показатель ROI в моменте относительно текущего курса монеты, используя ресурсы мониторинга, такие как [masternodes.online](http://masternodes.online) и подобные. Постоянное снижение курса монеты в долларах США или BTC относительно точки входа в корне меняют результат. Сервисы сообщают вам о высокой доходности именно в самой монете, а не каком-то более стабильном мериле стоимости. Например, монета проекта GIN демонстрирует доходность 95 % годовых и срок окупаемости вложений около 380 дней. Но если цена монеты упадет с 2 долларов до 1 доллара, показатели доходности на сайтах-кошельках могут даже вырасти, т. к. объем суточной эмиссии будет поделен между меньшим количеством мастернод в связи с тем, что многие их владельцы предпочтут продать свои монеты, не дожидаясь еще большего падения. Сервис проведет перерасчеты исходя из текущей цены монеты, и так каждый день. Если же смотреть относительно цены входа, то показатель доходности снизится примерно в 2 раза, а срок окупаемости вырастет вдвое. Даже если сервис демонстрирует вам доходность 500 % годовых, при падении цены в 5 раз это значение составит лишь 100 % в реальном выражении. Неконтролируемая эмиссия монет, большой премайн – настоящая беда подобных начинаний, а высокие показатели, не просчитывающие параметры окупаемости относительно цены входа в актив, – реальная ловушка для начинающих инвесторов.

При этом абсолютно во всех криптовалютах существует естественный процесс выбытия монет из оборота. Забытые пароли от кошельков, отправка монет на неправильный адрес, сбои в работе приложений и сервисов – все это может вести к безвозвратной потере некоторой части криптовалют. Для контролируемого управления инфляцией часто применяется «сжигание монет»

разработчиками – принудительная отправка некоторого их количества на несуществующий адрес. Часто комиссии с транзакций подлежат сжиганию, что призвано благотворно отразиться на цене монеты.

Вопрос управления эмиссией и инфляцией монеты – очень важный аспект, который нужно учесть при создании проекта именно отдельной монеты, что не требуется при выпуске токенов на созданных для этого платформах. Лишь при создании токена с возможностью дополнительной эмиссии следует подумать, как увеличение количества токенов в обороте повлияет на их стоимость и общую капитализацию криптоактива. Это уменьшает объем ликвидности и может способствовать снижению волатильности. Но не все в судьбе монеты зависит только от разработчиков. Комьюнити проекта – сообщество его приверженцев – также играет немаловажную роль как в становлении, так и в развитии монеты.

## **Сообщество монеты**

Сообщество – это один из ключевых факторов жизнеспособности монеты. Если представить фантастический сценарий, что появится какая-то крутая новая монета и большинство пользователей других монет переключатся на нее, то остальные криптовалюты превратятся в пыль, потому что никому не будут нужны. Момент пользы для определенного сообщества, ключевой группы людей важно учитывать при запуске нового проекта. Кто и зачем будет пользоваться моей монетой? Это один из первых вопросов, который должен прозвучать в голове создателя.

Комьюнити монеты – это не только люди, пришедшие в качестве ранних инвесторов. Это и основатели, и команда, и майнеры, и пользователи сервисов, которые может олицетворять монета или токен. Даже так называемые хейтеры – ненавистники, публикующие нелицеприятные сообщения в соцсетях или на форумах, – также являются частью сообщества.

Сообщество монеты может не только выполнять пассивную роль наблюдателей, но и помогать развивать проект делом. Одним из трендов 2018 года стало добавление в функционал монеты возможностей по проведению голосований по вопросам, явно влияющим на дальнейшую судьбу проекта. Конечно, сбор подобной обратной связи от пользователей возможен и с помощью сторонних сервисов – корпоративных сайтов и чатов, систем управления проектами и так далее, но именно внедрение инструментов общественного управления проектом в его код делают такой проект более децентрализованным и, значит, конкурентоспособным на фоне других.

Формирование сообщества задолго до запуска нового проекта может стать отличным поддерживающим фактором в период становления бизнеса. Многие команды разработчиков подключают профессиональных комьюнити-менеджеров к этому процессу. Оценка размера целевой аудитории, создание каналов первичной коммуникации с ней, разработка материалов для создания и поддержания интереса к этим каналам, учет количества активных и пассивных подписчиков, поддержка и ответы на запросы, прочие мероприятия – огромный объем ежедневной работы, который может оказаться не под силу никому из узкого круга основателей. Дальнейшее удержание сообщества в период отсутствия важных новостей, пока проект находится в долгой фазе становления и разработки, – также немаловажная задача. Если угаснет интерес целевой аудитории к вашей идее – монете или токену, эту идею олицетворяющему, придется несладко.

Также интересным является формат привлечения первичного интереса общественности через так называемые Эйдропы и Баунти. Airdrop – выброска, десантирование – термин, применявшийся для распространения рекламных или пропагандистских листовок с самолетов. Суть Airdrop в криптовалютах – это принудительная рассылка токенов по ненулевым кошелькам определенного блокчейна, чаще платформ, поддерживающих токены. Например, можно сделать снимок балансов всех кошельков Ethereum на определенную дату и всем кошелькам с ненулевым балансом произвести перечисление токенов. Количество токенов может быть пропорционально балансу кошелька Эфира, а может составлять равное количество монет для каждого из кошельков. Таким образом можно привлечь внимание большого числа активных пользователей к своей монете, а иные проекты именно так и распределяют большую часть эмиссии собственных токенов. Bounty-кампания – это программа вознаграждения ранних участников сообщества, взявших на себя какие-то функции по продвижению проекта. Например, может быть назначено вознаграждение за создание и просмотры ролика на YouTube-канале; оплачено размещение рекламного баннера в подписи на форуме bitcointalk; начислено чуть-чуть токенов за подписку на

Telegram-канал или Twitter, за репосты в Facebook и Instagram; за привлечение некоторого количества новых подписчиков в Discord и так далее. Мне лично импонирует формат создания первичного комьюнити на основе сервиса управления сообществами Discord. Широкий функционал, мультиплатформенность, наличие базовой целевой аудитории криптоэнтузиастов – повод включить Discord в необходимый инструментарий маркетологов. Процесс Эйрдропа можно сделать частью Баунти-кампании, если произвести сбор адресов для разброса токенов среди потенциальной аудитории. Для проведения подобных акций должен быть выделен определенный фонд, размер которого строго фиксирован и его целевое назначение отражено в первичной документации – белой бумаге и иных чувствительных документах.

Немаловажную роль в формировании сообществ играют лидеры общественного мнения – ЛОМЫ. Привлечение на свою сторону людей, обладающих влиянием на сотни и тысячи имеющихся у них сторонников, может сильно помочь начинающему проекту на всех стадиях его жизни, придав проекту вполне ощутимую ценность.

### **Способы придания ценности криптовалютам**

Основным способом придания первичной ценности криптовалютам является наполнение проекта неким идейным содержанием. Чем ближе идея к мыслям, посещающим большинство членов сообщества, тем проще она может быть монетизирована. Идея может состоять не только в создании чего-то нового и доселе не применявшегося, а в доработке существующих решений, комбинации нескольких идей в одну. Как я уже писал ранее, продукт Сатоши Накамото – это не что иное, как доосмысление ряда существующих технологий, комбинация некоторых из них в одном проекте, да и платформу Ethereum Виталик Бутерин создал не на пустом месте. В сети даже можно встретить обвинения Виталика в плагиате при написании им ряда статей для профильных криптовалютных изданий, что наталкивает на мысль о доработке чужих идей при выпуске собственного продукта. В дальнейшем развитии криптовалют также можно проследить подобный тренд. Некоторые монеты стали успешными благодаря улучшению кода биткоина, созданию надстроек над его блокчейном, внедрению сервисов, упрощающих применение или же, наоборот, призванных нарушить гегемонию биткоина.

Зачастую ценность проекта создается за счет футуристической идеи, которая пока не реализована, но теоретически возможна. Она может быть не связана напрямую с технологией создания и функционирования монеты, а отражать смелые мечты человечества о будущем – например, построить базу на Луне, заселить Марс. Если эта концепция близка большому числу людей, ее начнут обсуждать, выдвигать контраргументы, говорить слова поддержки. Кто-то начнет ее ругать, кто-то хвалить, но вокруг появится информационный ажиотаж. Подогревать интерес к проекту будет как раз то, что в его основу заложено что-то доселе невиданное, но теоретически реализуемое. Например, при проведении ICO российской монеты RMC.ONE помимо обещания производить «русские» майнеры для биткоина и отгружать их владельцам монет по себестоимости основатели пообещали создать уникальный чип Multiclet, который сможет превзойти мощность видеокарт при добыче некоторых монет, как Ethereum, Zcash или Monero, более чем в 35 раз. Никто не видел ни этот чип, ни его тесты – лишь теоретические расчеты, основанные на имеющихся старых российских разработках. Но тем не менее сама идея позволила людям верить, что компания сможет выпустить микросхему, создать на ее основе майнер и обогатить своих инвесторов. Образец чипа и майнера должен был быть готов летом 2018 года, однако позитивных новостей сообщество так и не услышало. Ко всему прочему, китайские разработчики ASIC смогли выпустить микросхемы для хеширования на алгоритмах Ethash, Equihash и Cryptonight, что сделало даже возможное позднее появление продукта от RMC гораздо менее востребованным. Если это была лишь маркетинговая уловка, скоро компанию ожидают полный крах и возможные коллективные иски от сообщества, т. к. именно обладание майнером Мультиклет было целью инвестирования в проект для многих инвесторов. Поэтому, насыщая проект футуристической идеей, важно четко представлять себе перспективу ее реализации в виде достаточного финансирования, а главное, возможности уложиться в поставленные сроки.

Как уже писалось выше, наличие большого и дружного сообщества во главе с влиятельными персонами как в криптовалютом мире, так и в области, на которую нацелен проект, – один из важных факторов поддержки стоимости криптовалюты. Монета, у которой нет комьюнити, не сможет пробиться на сколько-нибудь заметные места в сегодняшних рейтингах. Достаточно

посмотреть на аналитику социальной составляющей криптоактивов на ресурсе [coingecko.com](http://coingecko.com), чтобы оценить влияние данного фактора на стоимость. У биткойна почти миллион подписчиков на Reddit, 65,5 тыс. в Twitter, 40 тыс. лайков официальной страницы на Facebook. Количество подписчиков онлайн достигает 10 000. У валюты № 2 – эфириума – более 400 тыс. подписчиков в Reddit и Twitter, 130 тыс. лайков страницы на Facebook и 4500 активных пользователей онлайн. Ближе к концу первой сотни рейтинга находится достаточно старый проект MONA Coin, у которой всего 2,7 тыс. последователей в Reddit, 1,6 тыс. фолловеров в Twitter, в Facebook их страницу отметили как понравившуюся лишь чуть более 300 раз. Активных пользователей в сети меньше полутысячи. Стоимость монеты составляет 1 доллар и постоянно снижается. Вывод напрашивается сам собой: забота о сообществе очень важна.

Привязка монеты к реальному активу или внедрение ее как платежного средства в существующий бизнес-процесс – еще два важных способа сделать монету ценнее и дороже. Если создать монету или токен, привязанные к квадратным метрам недвижимости, цена не сможет упасть ниже определенного минимума, а рост стоимости квадратного метра будет провоцировать рост стоимости монеты, что вполне логично. Например, взглянем на теоретическую возможность приобрести условную долю в гостинице на побережье путем покупки токенов данного проекта. Если гостиница работает и получает прибыль – будет расти стоимость токена. Если можно оплатить услуги размещения и сопутствующие сервисы с помощью токена – он будет востребован не только у инвесторов, но и у рядовых постояльцев, что также не даст цене токена снижаться.

Но важно думать не только о придании ценности монете в некотором моменте времени, но и поддержке уровня на протяжении длительных промежутков. Особенно это важно после запуска проекта, в период ожидания сообществом реализации дорожной карты и прописанных в ней задач. Уже описанное выше нарушение проектом RMC сроков реализации идеи майнера Мультиклет негативно сказывается на цене. Поэтому задачей как разработчиков, так и лица, ответственного за связи с общественностью, является постоянное информирование о ходе протекающих процессов. Неведение кого угодно может заставить нервничать, а нарушение сроков – повлечь массовую распродажу токенов или монет. Правильный прогноз реализации дорожной карты, разбитой на важные этапы и подэтапы, дальнейший отчет о текущих и выполненных работах поддержат ценность проекта в глазах инвесторов и не дадут паническим настроениям негативно повлиять на цену.

## Создание токенов в блокчейне Ethereum

Хочется уделить чуть больше внимания процессу создания токенов, как наиболее легкому способу поставить свой проект на рельсы блокчейн-технологий. Существуют 18 платформ, на которых можно осуществить эмиссию собственного токена, но неоспоримым лидером является Ethereum. Для создания токенов нужен смарт-контракт, а порой и не один. Цепочка смарт-контрактов бывает нужна для того, чтобы провести различные стадии сборов – от предпродажи до основной стадии продаж, а возможно, и для обратного выкупа токенов. Но обычно требуется лишь один простой смарт-контракт. Напомню, что простейший смарт-контракт и инструкция по его развертыванию в сети есть в соответствующем разделе на сайте Фонда Эфириума – [ethereum.org/token](http://ethereum.org/token). Наличие опыта программирования приветствуется, но не является обязательным. Любой программист начального уровня, ознакомившись с языком программирования смарт-контрактов Солидिति по адресу [solidity.readthedocs.io](http://solidity.readthedocs.io), сможет писать ЛЮБЫЕ смарт-контракты за несколько минут. Профессиональный разработчик также может помочь решить одну большую проблему – проблему безопасности. Написав собственный код на основе проверенного контракта, он сможет избежать проблем с уязвимостями или лазейками, которые могут присутствовать в смарт-контрактах, взятых из открытых источников. Однако, если смарт-контракт сложный, а опыта у разработчика нет, желательно провести аудит смарт-контракта, дабы избежать серьезных проблем с работоспособностью и утраты собранных на ICO средств. Проект [ico.positive.com](http://ico.positive.com) может помочь в решении таких вопросов. И действительно, почему обязательно взваливать все вопросы на себя, когда есть профессионалы, готовые взять на себя ответственные и важные функции? Мое видение сегодня таково, что нужно использовать накопленный опыт других людей, особенно в таких инновационных областях, как блокчейн, и не стесняться пользоваться типовыми решениями. Если же бюджет мал, а желание сильно, можно

просто скопировать код проверенного контракта с ресурса etherscan.io, пройдя во вкладку tokens и выбрав один из последних контрактов ICO. Далее нужно нажать на адрес контракта вида 0x123456789...0 – и вы сможете увидеть его код в соответствующей вкладке. Изменив в нем ряд простых значений с помощью редактора и произведя компиляцию, можно развертывать контракт в сети с помощью дополнения к браузеру MetaMask или стандартного официального кошелька Ethereum. Но рекомендую начать с тестовой, например, Ropsten. Пошаговых инструкций по запуску смарт-контрактов хоть отбавляй. Смарт-контракты токенов это просто и быстро. А есть ли способ еще проще? Конечно, есть!

В сети есть бесплатные сайты, помогающие не только при создании кода смарт-контракта, как fondu.io или tokenfactory.surge.sh, но и в проведении маркетинговых мероприятий Airdrops и Bounty, как rocket.etherparty.com. Есть и платные продвинутое решения, как mywish.io, позволяющие заложить ряд важных параметров в смарт-контракт. Что ж, невеликая работа, но упрощает жизнь. Остается только научиться развертывать контракты в сети, хотя уже существует совмещенный инструментарий – создающий контракт и публикующий его за вас. Децентрализованное приложение – dApp – для создания токенов wizard.oracles.org позволяет не только создать и опубликовать контракт с разными параметрами, но и сгенерировать страницу инвестора для отслеживания статистики сборов, и все это абсолютно бесплатно. Что же могут предложить конкуренты?

### Создание токена на платформе Waves

Лидерство по скорости и простоте создания токена на сегодняшний день принадлежит платформе Waves. Единственное условие – у вас уже есть кошелек Waves и минимум 1 монета на нем. В кошельке есть вкладка «Выпуск токена». Вы заполняете 4 поля (как и в случае с простейшим токеном Эфира): выбираете название, даете краткое описание токена, вводите, сколько всего токенов создается, в выпадающем меню выбираете, перевыпускаемый ли токен, и задаете количество знаков после запятой от 0 до 8. После нажимаете «Выпустить» – все готово! Через некоторое время транзакция попадет в блокчейн Waves, и токен появится во вкладке «Портфель». Так можно создать десятки токенов, по текущей цене лишь немногим больше 2 долларов за каждый. Токены можно использовать для рекламы, в т. ч. выступать спонсором по оплате комиссий. Для получения опыта и достижения некоторых маркетинговых целей вполне интересно. Если же планировать продажу данного токена, необходимо рассчитывать на аудиторию, знакомую с Waves, или научить будущих инвесторов пользоваться кошельком платформы и находить торговую пару на внутренней бирже. Выход на другие биржи, кроме тех, где уже прошел листинг Waves, будет непростым. Тем не менее количество площадок, торгующих Waves, очень велико, и среди них есть очень достойные. Торговля токеном или переводы большому числу участников требуют наличия на балансе дополнительного запаса монет Waves для оплаты транзакций и биржевых ордеров. Создать свой токен на Waves очень просто, управлять им чуть сложнее. В истории площадки есть успешные примеры создания монеты на Waves. Ресурс coindata.vc располагает сведениями о 27 ликвидных токенах, созданных на данной платформе. Такое малое количество объясняется некоторой недоступностью информации о работе на площадке, простых примеров использования, дополнительных сервисов для потенциальных пользователей. Токен Waves сложно сделать массовым продуктом, сложно интегрировать в различные существующие решения для сбора статистики или отслеживания криптовалютных портфелей. И сложность эта именно из-за недостатка информации.

Возможно, я ошибаюсь, и ряд нововведений исправили ситуацию. Совсем недавно платформа Waves обновила свой сайт, сообщив о выходе в свет расширений для блокчейна Waves. Публике доступны тьюринг – полный язык программирования RIDE – и возможность создания смарт-контрактов и децентрализованных приложений. С вводом этих новшеств расширяются возможности по проведению ICO на Waves, приближаясь по функционалу к конкуренту – Ethereum. В силу того, что площадка с российскими корнями, очень хочется пожелать ей успеха и бурного развития, но сегодня создание токена на Waves не может конкурировать с ERC20 токенами Ethereum.

## Глава 8

# Футуристический взгляд на криптовалюты

## Ксеракомпьютеры планетарного масштаба

В этой главе я буду много фантазировать, предполагать, мечтать, а также рассматривать надежды криптоэнтузиастов на светлое будущее. Прошу считать мои пространные измышления лишь домыслами, робкой попыткой проникнуть сквозь пространственно-временную ткань хоть на четверть галактической секунды.

Сейчас централизованные суперкомпьютеры представляют собой построенный какой-либо компанией дата-центр с размещенным в нем специализированным серверным оборудованием различных типов, объединенным высокоскоростной сетью и управляемым специальным программным обеспечением. Я уже писал про суперкомпьютеры выше, и речь шла больше о централизованных решениях. Также я упоминал проекты децентрализованных туманных суперкомпьютеров, что несомненно является первым шагом к идее общепланетарного компьютера. Одним из первых суперкомпьютеров стал созданный в 1972 году легендарный Cray-1, мощность которого составляла 133 Mflops. Сегодня такую производительность продемонстрирует самая простейшая видеокарта из 90-х, а также любой встроенный видеоускоритель в современном смартфоне. При этом каждый смартфон обладает процессором, состоящим из нескольких ядер. Самый «многоядерный» суперкомпьютер – китайский Санвэй, занимающий вторую строчку в мировом рейтинге, – состоит из 10,6 млн ядер. Статистика утверждает, что сегодня в мире существует 5 млрд активных смартфонов и планшетов, у которых в среднем по 4 вычислительных ядра плюс графическое ядро, а также есть некоторый объем хранилища, обычно измеряемый десятками гигабайт. К 2020 году число смартфонов и планшетов может достигнуть 7 млрд. Итого 35 млрд процессорных ядер, добавить к ним 3 млрд персональных компьютеров и ноутбуков, в среднем по 3 ядра CPU и одному более-менее полноценному GPU в каждом. GPU содержит множество ядер, учитывающихся в тестах. Их называют просто – вычислительные единицы, или Compute Units (CU). В старых видеокартах их может быть 2–4, в современных – свыше 70. Учитывая то, что большинство домашних пользователей не экономят на графике, можно смело считать, что среднее количество ядер на каждый графический ускоритель будет не менее 20. В общем, очень округленно – только у населения в будущем году может быть до 100 млрд вычислительных ядер. Обратимся к параметрам нашего представителя топ-100 мировых суперкомпьютеров – Ломоносову. Он содержит 64 384 ядра и выдает 2474 Tflops. Пусть очень приблизительно мы получим синтетический показатель производительности около 0,04 Tflops на ядро. Будем прагматичны, наверняка домашние компьютеры и смартфоны не покажут более 0,01 Tflops на ядро. В мире 100 млрд ядер – итого 1 млрд Tflops = 1 млн Pflops = 1 тыс. Eflops = 1 Zflops. Один зетафлопс. Звучит странно. А что дальше? Если представить, что через 3–5 лет у землян будет уже 10 млрд восьмиядерных смартфонов со встроенным видеоускорителем, имеющим минимум 2 CU, только это даст 100 млрд вычислительных ядер. Плюс 5 млрд домашних ПК и ноутбуков также будут иметь по 8 ядер центрального процессора и 4 °CU в видеоускорителях – итого 240 млрд ядер... Более совершенные ядра станут показывать 0,03 Tflops производительности в тестах с плавающей запятой... Мы достигнем более 1 йотафлопс в расчетах. Останется лишь один рыбок до ксеракомпьютера в 1 ксерафлопс. И мы даже не учитываем миллионы слабых вычислительных устройств наподобие одноплатных компьютеров, роутеров, игровых приставок, телевизоров и иных устройств, способных объединяться в сеть проводным или беспроводным способом и имеющих микропроцессор, способный проводить вычисления. Десятки миллиардов многоядерных центральных процессоров, миллиарды графических ускорителей, миллиарды процессоров в бытовой технике – при наличии стандартной технологии и понятной мотивации такое объединение станет самой продуктивной вычислительной машиной в истории человечества.

Какой же еще может быть мотивация для включения личного компьютера или смартфона в общую сеть? Например, существуют такие проекты, как `folding@home`, `SETI@home` или `BOINC`, объединяющие домашние компьютеры в кластер, призванный решать общественные задачи в медицине и изучении космического пространства. Изначально волонтеры вознаграждались лишь некими баллами, не имевшими реальной стоимости, а сегодня существуют монеты `Foldingcoin`, `Cure coin`, которые выплачиваются за участие в медицинских программах, нацеленных на борьбу с раком, СПИДом, болезнью Альцгеймера и просто старением. При этом монеты имеют

определенную стоимость на криптовалютных биржах. Также создаются иные, более общие проекты, наподобие Gridcoin, для поддержки любых распределенных вычислений во благо человечества. Значит, помимо морального удовлетворения, чувства сопричастности и выполненной благотворительной миссии все-таки можно получать вполне реальную оплату своих трудов. Оговорюсь, не своих – работы своего вычислительного устройства, маленького нетребовательного работника, готового трудиться 24/7/365. Может ли заработок на таких монетах покрыть затраты на электроэнергию и амортизацию настольного компьютера или ноутбука, я сильно сомневаюсь. Но вот смартфон, лежащий на зарядке ночью, может потреблять ничтожное количество электроэнергии по дешевому ночному тарифу, а его амортизация и так заложена в личный бюджет. В таком случае объединение смартфонов для создания GRID – суперкомпьютеров (от англ. *grid* – решетка, сеть) – может открыть огромнейшие перспективы как для коммерческих, так и некоммерческих структур. Такой суперкомпьютер легко справится с массой задач по обеспечению необходимой мощностью всего киберпространства, во всяком случае, я бы попытался это проверить. Нельзя списывать со счетов разработки квантовых компьютеров, которые способны кардинально изменить наши представления о возможностях вычислений, но пока мы отталкиваемся от того, что есть в нашем распоряжении уже сейчас.

Планетарный суперкомпьютер может стать базой для искусственного интеллекта. Сейчас проблема его развития заключается в том, что на существующих вычислительных устройствах реализовать подобие человеческого мозга сложно, потому как наш мозг чаще оперирует аналоговыми сигналами, а не цифровыми. Конечно, есть специальные микросхемы, представляющие собой некоторое подобие человеческой нервной клетки, но их производство очень дорого, а массовое применение сомнительно. Однако огромный суперкомпьютер, который может предоставить условно неограниченное количество ресурсов для работы симулятора искусственного интеллекта и ресурс для его самостоятельного обучения, мог бы ответить на массу вопросов современных ученых, разгадать сотни научных загадок. Населенный искусственным интеллектом или даже цифровыми интеллектуальными сущностями, подчиненными смарт-законам и связанными смарт-контрактами, планетарный суперкомпьютер смог бы избавить человека от огромного количества рутинных процессов, высвободив для нас самый дорогой ресурс – время. Известно, что время, потраченное на самообразование и саморазвитие, приносит огромные плоды. Время, потраченное на творческую или духовную сферу, бесценно. И неважно, где в новой цифровой эпохе произойдут самореализация и полное раскрытие потенциала индивида – в виртуальном киберпространстве или привычном нам «реальном» вещественном мире. Важны достижение цели, воплощение идей, визуализация мыслей.

## Киберпространственные деньги

О чем же мечтает криптообщество? Многие хотят видеть в криптовалюте способ избавления от гегемонии государства в сфере контроля над финансами. Мы понимаем, что, пока в руках государства есть инструменты по печатанию денег, контролю за их курсом и переводами между счетами, распределением между бюджетными организациями, все являются заложниками решений государства по тем или иным вопросам монетарной политики и расходования бюджетных средств. При этом мы до конца не понимаем, какова точная стоимость той или иной государственной валюты, на чем основан ее текущий курс, чем реально обеспечены деньги – локально производимыми товарами, золотом, твердой иностранной валютой, зарубежными активами или просто словами? В случае с долларом США, которые печатает частное учреждение, не имеющее официального государственного статуса, его обеспечением являются лишь многочисленные долги. Контроль, в том числе силовой, над экономиками многих государств, а также широкое применение доллара в международных расчетах помогают национальной валюте США держаться на плаву. Военная и экономическая мощь государства также является определенной поддержкой. Но что произойдет с долларом США, если вдруг все население планеты откажется от него, попросту утратит веру в любое обеспечение валюты, кроме золотого стандарта? Хватит ли золотого запаса США и складов с американскими товарами, чтобы «выкупить» огромную массу наличных долларов у всего мира? Конечно, нет, да и никто не будет заниматься спасением обычной зеленой бумажки. Почему именно доллар США является мировой

валютой? Неужели нет более достойных кандидатов? К сожалению, пока нет. Ни европейские валюты, ни российский рубль, ни китайский юань не могут похвастаться идеальными параметрами, необходимыми мировой валюте. Все привыкли к наличному доллару, к американской межбанковской платежной системе SWIFT и процессинговым компаниям Visa и MasterCard. Доллар такой, потому что это доллар. Зачем вдаваться в подробности, копаться в деталях? Просто есть доллар и все. Так почему бы мировому сообществу не поверить во что-то другое, более совершенное, прозрачное, неподконтрольное сомнительным организациям, удобное в использовании и надежное в хранении? Что-то, что можно печатать самому, перевозить в любых количествах в любое место, передавать в любых объемах без каких-либо лишних вопросов, приватно хранить и тратить, в конце концов даже обеспечить реальными активами? Раз книга о криптовалютах, естественно, речь идет о них.

Что может помочь криптовалюте или отдельной монете завоевать мировое господство? Для начала общее приятие новой экономики. Должно пройти определенное время, возможно, сменится поколение жителей планеты, до сих пор не использующих смартфоны и компьютеры, появиться формация, у которой применение криптовалют войдет в привычку. Будут ли это люди поколения миллениалов или их дети из поколения Z, сказать сложно, но несомненно, факт постоянного вовлечения молодых людей от 1995 года рождения и младше в сетевую активность приводит к мысли, что им будет удобнее пользоваться деньгами, существующими в цифровом пространстве. Уже не кажутся нелепыми мечты утопистов и криптоанархистов о кибергосударствах, где естественные физические границы отсутствуют. Именно в таких виртуальных государствах электронные деньги и криптовалюты могут стать основой для будущего выхода из виртуального пространства в реальный мир – киберденьгами. Ведь то, что мы сегодня называем миром, с его странами и границами, правительствами и чиновниками, может напрочь отсутствовать в цифровом мире, где каждый может быть кем угодно и чем угодно, находясь где угодно и делая что угодно. Вопрос лишь в наличии морально-этического и духовного стержня, препятствующего неадекватному поведению в зоне виртуальной свободы. Киберпространство перестало быть просто игрушкой, о нем ведут беседы философы и социологи, в нем происходят встречи и свадьбы, ссоры и примирения, персонажи играют и работают, ведут бизнес. Практически любая экономическая активность в киберпространстве предполагает обмен ценностью, и трансформация этой ценности в реальный мир доступна только криптовалютам.

Криптовалюта децентрализована, а значит, трансгранична по своей сути, она не имеет центрального органа управления, а значит, управляется всеми. Ее можно использовать в любом уголке планеты, лишь при наличии смартфона и Интернета. Согласно отчету Global Digital 2018, проникновение Интернета в мир сегодня составляет более 50 %, из всех пользователей глобальной паутины 80 % проявляют активность в соцсетях. Мобильными телефонами владеют почти 70 % населения планеты, и те же 80 % из них используют смартфоны для выхода в Интернет. В развитых странах эти показатели намного выше и порой достигают значений 96 %. В общемировом масштабе пройден важный рубеж – абсолютное большинство населения имеет инструмент для выхода в глобальную сеть. А раз есть доступ в сеть – есть и возможность пользоваться цифровыми активами. Осталось только появиться унифицированному, легко признаваемому любым человеком цифровому финансовому активу. Сегодня на эту роль претендует биткоин, с потенциальным 1 млрд пользователей, судя по подпискам на ветку Bitcoin в Reddit. Хорошей попыткой может стать внедрение криптовалюты в социальные сети и мессенджеры. В конце концов, у каждого может быть привязанность к какой угодно цифровой валюте, лишь бы были быстрые и надежные инструменты ее конвертации в любую другую цифровую и физическую ценность. Недавно компании Visa и MasterCard объявили о скором запрете привязки криптовалютных кошельков к пластиковым картам, а это как раз был мостик для перехода ценности актива из цифрового пространства в физический мир. Для меня это не имеет значения, т. к. рынок р2р-платежей уже развился настолько, что криптовалюта может быть легко обменена на фиат без использования централизованных шлюзов или банков, осуществляющих конвертацию. Этот шаг только укрепит сообщество во мнении, что такие организации не нужны в космополитичном обществе, что централизованные посредники увидели угрозу своему господству и пытаются защититься. Слишком много их средств и сил вложено в инфраструктуру и технологию. Но технологии неизбежно устаревают, и прогресс не остановить, человечество живет в 3-м тысячелетии, в информационном обществе, где множество старых убеждений,



верований, привычек, способов межличностного культурного и финансового взаимодействия просто исчезнет. Так уже случалось в XX веке, когда правящие и финансовые круги противились распространению электричества и автомобильного транспорта, консервативные монополии защищались, саботируя внедрение новых промышленных технологий. Но такие меры могут быть лишь временным препятствием. Как только критическая масса людей в одном государстве или группе государств перешагнет определенный порог, запреты исчезнут сами собой. И тогда уже и правительства, и финансовые монополии вынуждены будут применять технологии блокчейн и криптовалюты, чтобы сохранить хоть часть своих функций. Уж лучше начать перестраиваться заранее, чтобы в один момент не потерять все и не бежать за уходящим поездом. Для такого объема вычислений, как трансформация миллионов одних цифровых активов в другие, и фиксации данных фактов понадобятся огромные вычислительные мощности и объемы хранилищ. Возможно, нас ждет появление очередной надстройки над Интернетом – глобальной туманной вычислительной машины и децентрализованного общемирового хранилища данных, прообраз которых я попытался представить в предыдущем разделе. А дальше только межпланетные и межгалактические деньги.

## Перераспределение мировых богатств

Киберпространственные или кросс-пространственные валюты – это хорошо, но наверняка многих читателей взволнует вопрос: а где же мои киберденьги, уже так много ресурсов распределено между достаточно небольшой группой людей? Опять возникает несправедливая ситуация, когда 10 % населения владеет 90 % всех мировых богатств. В «белой бумаге биткоина» Сатоши Накамото написал, что один процессор должен считаться одним голосом в ситуации, когда сеть раздвоилась и нужно проголосовать за ту или иную цепочку. Сегодня один ASIC-чип – это один процессор, следовательно, состоящее из 500 микросхем устройство будет иметь 500 голосов, тогда как домашний компьютер – лишь один. И в добыче биткоина такая диспропорция будет явно заметна, причем ASIC сможет работать в тысячи раз эффективнее домашнего компьютера. Налицо централизация эмиссии криптовалют, очень явно заметная в КНР, где компания-производитель ASIC Bitmine напрямую или косвенно владеет более 50 % генерирующих мощностей в алгоритме хеширования SHA-256. Напрашивается вывод, что должен существовать другой путь для справедливого распределения эмиссии криптовалюты, а также обязана появиться общественная криптовалюта, уравнивающая шансы всех жителей планеты на доступ к эмиссии. Благодаря самой технологии блокчейн вполне возможно осуществить справедливое и прозрачное распределение первичной эмиссии и сделать последующий выпуск монет более равномерным и децентрализованным.

Подобная попытка была предпринята в 2014 году в Исландии, где оборот криптовалют ограничен, но сегодня она является одной из столиц майнинга из-за холодного климата и дешевой геотермальной электроэнергии. Проект AuroraCoin условно распределил по 31,8 монеты каждому жителю страны, чьи данные имелись в базе данных национальных удостоверений личности на тот момент. Разработчики осуществили премайн в размере 50 % общей денежной массы в 21 млн монет и, поделив 10,5 млн полученных монет на 330 188 жителей, пришли к числу 31,8. Остался открытым вопрос, сколько жителей из 330 тыс. истребовали свои монеты и как можно было проверить, что потенциальный мошенник не получит монеты за кого-то другого? Применялся метод проверки по национальной базе биометрических паспортов, но итог оказался плачевным. Большинство монет не было истребовано, и, когда закончился период эйдропы, большой объем монет был сброшен на бирже, что снизило цену монеты в десятки раз. Сегодня монета торгуется очень вяло, и цена ее низка, несмотря на то, что разработчики заявили об уничтожении 80 % принадлежавших им монет. В общем, эксперимент можно считать неудавшимся.

Были ли еще подобные попытки – неизвестно. Одно можно сказать точно – при необходимости справедливо распределить эмиссию монеты необходимо создать новую монету с уникальным кодом и понятным языком программирования, с новым алгоритмом достижения консенсуса, с механизмами защиты от централизации эмиссии, с инструментами общественного управления и бюджетирования на основе смарт-контрактов и смарт-законов, со встроенными средствами анонимизации, реализовать алгоритм конвертации стоимости физических и цифровых активов в новую валюту, внедрить механизмы репутации на основе сетевой активности и времени

существования в сети, разработать оракулы для приема несовместимой с блокчейн информации, оградить среду от возможного негативного вмешательства квантовых компьютеров, подключить возможности искусственного интеллекта и машинного обучения, подключить функционал Интернета вещей, интегрировать социальные сети, создать специализированные боковые и частные цепочки блоков, и т. д. и т. п.

В случае если будет существовать криптовалюта, имеющая практически 100 %-ное распространение на планете, а ее капитализация достигнет уровня, равного объему всех мировых богатств, может быть поднят вопрос о глобальной токенизации всей экономики и перераспределении ее благ в сообществе. Перераспределение благ не значит отъем справедливо заработанных капиталов. Я лишь предполагаю, что в случае создания единого государства земли все принадлежащие государствам активы, как земли, недра, доли в предприятиях, интеллектуальная собственность и иные нематериальные активы, могли бы работать на благо активной части населения, прозрачно распределяясь с помощью инструментов цифровой экономики. Личный вклад каждого гражданина планеты во всеобщее процветание тоже должен быть адекватно оценен. Я не считаю коллективизацию и всеобщую уравниловку правильной идеей. И пусть не ругают меня капиталисты и власть имущие, такие идеи невозможно осуществить даже в отдаленном будущем. Возможно, тестовым плацдармом для эксперимента вполне могло бы стать карликовое островное государство. Маленькая территория, малочисленное население, минимум сфер экономической и социальной активности. Стоимость внедрения в такой среде могла бы быть вполне адекватной, но результат мог иметь мировое значение. Но даже этот сценарий фантастический, вряд ли государства так просто откажутся от своих рычагов управления, а круги, контролирующие финансовые потоки, поделятся доходами. Власть не позволит криптоанархии случиться, пока этого не захотят все люди, что допустимо только при смене одного или нескольких поколений и глубокой трансформации мировосприятия большинства из будущих граждан планеты. Возможно, начать нужно с одного человека, себя любимого?

### **Монета имени себя**

В будущем, как, впрочем, и сегодня, ничто не мешает каждому человеку иметь собственную монету и генерировать собственную ценность, подкрепляющую некий средневзвешенный курс этой монеты. Сегодня мериллом важности и ценности нашей сетевой социальной активности являются число подписчиков, сумма лайков, репутация на форуме, срок существования аккаунта, количество просмотров видео или фото. Общественное признание помогает нам чувствовать себя нужными, продолжать работать над собой, а некоторым и неплохо зарабатывать, продавая результат творчества, свои профессиональные услуги и продукты труда, а иной раз просто рекламируя чужие. Популярность в киберпространстве является одним из самых массовых стремлений поколения миллениалов и iПоколения – сегодняшних детей и подростков. Они тратят уйму времени, бродя по просторам Интернета и игровым виртуальным пространствам.

Представьте же себе, что вся полезная сетевая активность может быть оценена и монетизирована. И не с помощью мировых денег, а помощью собственных именных монет. Зачатки подобных процессов уже начались, и не вчера, а несколько лет назад. Например, сайт [tatianamogoz.com](http://tatianamogoz.com) принадлежит певице из США, выпустившей свою монету для поддержки личной творческой реализации еще в середине 2014 года. Артистка считает, что это была первая подобная монета. Среди заявленных способов применения банальное бахвальство, участие в домашних вечеринках криптоэнтузиастов и любителей музыки, приобретение именной продукции артистки – музыкальных альбомов и брендовой одежды. Именно последнее применение наиболее интересно. Продавая свою валюту TAT, Татьяна получила возможность работы на себя в любимом деле и, реализовав творческий продукт, наполнила свою монету некоторой ценностью. При том, что биржевой курс монеты неизвестен, он может быть рассчитан при заказе товара в личном магазине артистки на платформе [tokenMarkets](https://www.tokenmarkets.com/). Диск стоимостью 25\$ можно оплатить 250 TAT, значит, курс одной монеты равен 0,1 доллара США. При общем выпуске 100 тыс. монет творческая капитализация альбома певицы составляет 10 000 долларов, которые получены еще ДО выпуска альбома. Сборы велись в BTC и XCP, и, если певица сохранила хоть 1/10 часть из приблизительно 33 собранных биткоинов для себя, сегодня она владеет активом на 20 000 долларов при реализованном творческом проекте. К сожалению, невозможно установить точный

первичный курс продажи и сумму сборов, однако для понимания сути и этого достаточно. Известно, что часть сборов была потрачена на попытку создать платформу для финансирования талантов путем создания личных токенов для начинающих артистов.

Какими же будут именные монеты будущего? В их основу могут быть заложены ваш интеллект, уровень IQ, умения и таланты. Сегодня генетика, антропология и физиогномика предлагают возможность спрогнозировать области жизнедеятельности, к которым может быть наиболее склонен тот или иной человек. Но самое главное, современная жизнь позволяет нам заняться тем, к чему лежит внутренний мир человека. Когда вы в подростковом возрасте только начали понимать, что можете чего-то добиться, но получить необходимые знания и опыт, инструменты и материалы просто неоткуда, можно создать токен или монету, которая позволит инвесторам, финансовым ангелам, пользоваться вашими будущими свершениями в какой-то пропорции. Инвестиции в талантливого программиста могут дать возможность стать совладельцем IT-компании в будущем, спонсирование одаренного химика – привести к созданию лекарства, которое принесет огромную прибыль, финансирование спортсмена позволит получать часть гонораров от спортивных клубов и рекламодателей, при этом учет всех расходов и доходов человека будет вестись в блокчейн-бухгалтерии, прозрачной и понятной.

Личный токен пока может выглядеть фантастично, но существующие примеры говорят мне о больших перспективах подобных начинаний. Развитие и постепенное внедрение технологии смарт-контрактов сможет спонсорам отдельных личностей быть уверенными в том, что они получают часть успеха своего протеже либо в материальном виде, либо в виде его профессиональных услуг и времени, которое придется потратить на выплату долга инвестор-спонсору. Сегодняшний пример краудфандинга при финансировании глобальных проектов и смелых идей, которые реализуются большими командами, может быть перенесен на более приземленный уровень личного финансирования индивидуальных частных проектов длиной в несколько месяцев или в целую жизнь. Например, творения художников редко заслуживают признания при жизни. Меценатство, как процесс инвестиций в творческую натуру, взамен некоторой доли в его творениях – распространенная мировая практика уже сотни лет. Перевести этот процесс в киберпространство, на рельсы криптовалюты ничего не стоит. В подобных начинаниях остро стоит вопрос доверия, и здесь можно рассчитывать только на то, что большинство людей стремятся не к обману и разрушению, а больше к честному созиданию.

Даже я мог бы провести краудфандинговую кампанию для реализации идеи написания данной книги. Собрав пожертвования, я был бы уверен, что у меня заполнен холодильник, оплачены счета за квартиру и услуги по ее публикации, продвижению и рекламе. Будущий результат моей работы мог бы продаваться за мои же токены, а меценаты-спонсоры смогли бы также разместить рекламу на страницах книги либо получить от меня консультационные услуги для своего проекта за мою личную криптовалюту. Если бы моя работа стала коммерчески успешной, превратившись в бестселлер, то все, кто владел токенами имени меня, получили бы часть авторского гонорара и более существенных рекламных доходов. Фактически это было бы неофициальное акционерное общество в цифровом формате, где создателем и акционером может быть любой человек и все могут рассчитывать на свою часть прибыли. Но владение долями в проекте может предполагать и участие в его управлении, например в некоем совете меценатов, коллегии спонсоров и т. д. Почему бы и нет? В случае успеха первых творческих потуг дальнейшие темы для книг вполне могли бы выбираться голосованием моих инвесторов, а также одобрение расходов, выбор издательства, предложения рекламодателей и иные важные аспекты моей профессиональной деятельности.

## **Криптоанархия и киберутопия**

Есть мнение, что среди криптосообщества большинство людей – анархисты и их задача разрушить государства в том виде, в котором они существуют сегодня. Наверняка многим поклонникам криптовалют свойственны проявления анархических воззрений, что проявляется в устройстве криповалютных сообществ. Различные комьюнити криптовалют можно сравнить с системой независимых общин, а общее их объединение вокруг нескольких центров притяжения, таких как Bitcoin Foundation или Ethereum Foundation, с подобием федеративного устройства. Сравнение очень условно и, возможно, не совсем в точку. Анархических течений много, и основы учения некоторых из них прямо противоречат друг другу. Нам же интересно такое явление, как

криптоанархия, существующее чуть в стороне от радикальных видов анархии. Вылившись из среды шифропанков, криптоанархия перестала быть воззрением небольшой группы людей, а превратилась в целое философское течение, социальный феномен. Основным постулатом криптоанархиста является вера в то, что каждый индивид имеет право сохранять приватность личной жизни, личных коммуникаций, бизнес-активности, пока он этого хочет. В силу того, что по большей части речь идет о защите данных в информационном пространстве, криптоанархисты считают важным использование методов шифрования переписки и переговоров одним из важнейших аспектов сетевой активности, наравне с тайной финансовых операций. В целом можно сказать, что приверженцы такой философии не хотят ни отслеживания со стороны телекоммуникационных компаний, ни владельцев сайтов и разработчиков коммерческого программного обеспечения, ни банков и финансовых институтов, так как опосредованно такая информация может стать доступной спецслужбам. При этом криптоанархисты не затворники или параноики, не мошенники или хакеры, они ярые противники «полицейского государства» как проявления авторитаризма или тоталитаризма. В манифесте шифропанков явно разграничиваются понятия приватности и секретности, и уточняется, что шифропанк хочет сохранить право выбирать, когда и какую информацию о себе сделать публичной. Это можно назвать псевдоанонимностью, как в случае с применением биткоина. Пока вы намеренно или случайно не ассоциируете кошелек Биткоин с каким-то идентифицирующим вас информационным объектом, вы будете анонимны. Как только информация о вашем биткоин-кошельке станет публичной, ни о какой анонимности речи идти не может. До появления биткоина концепция криптоанархии была неполной, но с распространением криптовалют, причем полностью анонимных, достичь идеального образа жизни криптоанархиста стало гораздо проще. При этом в силу появления экономических причин для сохранения приватности идеи криптоанархизма стали переплетаться с либертарианством.

Сегодня в мире существует несколько действующих анархических и либертарианских общин, количество членов которых составляет сотни и даже тысячи человек. Самой интересной из этих утопий в контексте повествования является FSP (англ. *Free State Project*) – Проект Свободного Государства, расположившийся в штате Нью-Гемпшир, США. Интересной в том плане, что созданная в 2001 году коммуна признала биткоин официальной валютой, а сегодня активно поддерживает ETH и Zcash. Возможно, именно такая община станет прообразом будущей крупной криптоанархической утопии, т.к. остальные представители найденных мною примеров утопических общин больше зациклены на натуральном хозяйстве, единении с природой... В FSP существует явный акцент на активном использовании в жизни граждан информационных технологий и достижений цифровой экономики, что может стать существенным драйвером для роста численности общины и популярности подобного образа жизни в других штатах США.

Все вышесказанное о реальной жизни, а есть еще и виртуальное пространство. Речь не только о трехмерной виртуальной реальности, а обо всем цифровом пространстве за монитором компьютера или экраном смартфона. Уже не секрет, что огромная часть жителей планеты настолько поглощена виртуальным пространством, что это приводит к печальным последствиям. Однако это лишь крайние случаи, и наша эмпирическая реальность вполне способна свести с ума. Все началось еще в те времена, когда виртуальное пространство было текстовым. Веб 1.0 – я даже немного взгрустнул о тех временах... В сети существовал такой класс сообществ, как MUD – мультипользовательское подземелье, а, созданные с применением объектно-ориентированного программирования, они стали называться MOO. По сути это многопользовательская текстовая игра, сочетающая элементы квеста, ролевой игры с элементами сражений игроков, имеющая окно чата с возможностью общения или отправки команд серверу для выполнения игровых действий. Одной из старейших и популярнейших была LambdaMOO, в лучшие времена объединявшая до 10 000 пользователей. В игре имелся программируемый пользователем аватар, который мог взаимодействовать с другими персонажами и неживыми объектами в игре. Тысячи людей ежедневно заходили в виртуальный (текстовый!) особняк, чтобы поболтать и поиграть. Интерес широкой публики вызвал один случай, когда с помощью вредоносного кода один из пользователей завладел аватаром другой подписчицы и осуществил над ее аватаром акт виртуального текстового насилия. Случай получил огласку, и за ним закрепилось особое название – «Изнасилование в киберпространстве». Конечно, у владелицы персонажа и всех наблюдателей была возможность просто не смотреть на происходящее, однако как заявила жертва позже, она испытала

посттравматический синдром и была вся в слезах. Настолько сильно ассоциировала себя девушка со своим персонажем. Но важно и то, что было после. Сообщество объединилось против насильника, его аккаунт был уничтожен создателями (магами и вершителями судеб в игре), а также был поднят вопрос о создании неких законов поведения в виртуальном пространстве. Результатом стало внедрение разработчиками системы петиций и бюллетеней для постановки вопросов на голосование и организацию подсчета голосов. Налицо проявление первых форм общественного управления и некоторого типа права в цифровом мире. Сегодня развитие технологий настолько изменило компьютерные игры, что существуют огромные миры, двумерные и трехмерные, в которых количество подписчиков исчисляется десятками миллионов пользователей, а рекорды одновременного пребывания онлайн давно перевалили за 200 тыс. игроков. Дети и взрослые, мужчины и женщины проваливаются в виртуальную реальность, меняя возраст, пол, расу, ведут себя адекватно или демонстрируют девиантное поведение – в общем проводят время онлайн в свое удовольствие. Я знаю случай женитьбы парня и девушки, которые познакомились через онлайн-игру, при этом сначала поженив персонажей. Размыванию границ между эмоциями, испытываемыми оффлайн и онлайн, способствует и развитие трехмерной виртуальной реальности – VR-технологий. В криптовалютном сообществе заметным стало появление проекта Decentraland с токеном MANA, за который можно покупать виртуальное движимое и недвижимое имущество. Полностью трехмерный мир, создаваемый пользователями по собственному усмотрению. С возможностью выглядеть, как хочешь, делать, что хочешь, говорить, что хочешь. Следом пошли проекты виртуальных пространств с магазинами, ресторанами, аватарами известных личностей в качестве соседей по виртуальной квартире и возможных собеседников... Объединив все это, может нарисоваться картинка полностью виртуального государства – киберутопии. С бесконечной территорией, общественным управлением, с деньгами, которые можно использовать и в том, и в другом мире, неограниченными творческими возможностями, отсутствием психологического давления, с многими плюсами виртуальной свободы и без минусов реальной жизни. Возможно, такие миры станут настолько развитыми, что будут гораздо привлекательней скучному быту доинформационной эпохи. В них, несомненно, можно будет и зарабатывать себе на жизнь, например, помогая создавать виртуальные объекты для других – быть VR-архитектором, обменивать те или иные товары с выгодой, консультировать по каким-то вопросам, ведя незаконную деятельность (что представляется немного странным в выдуманном мире). Сращивание киберпространства с реальным миром уже началось и набирает обороты. Надеюсь, человечество сможет перенести в цифровую плоскость свою духовность, мораль и культурные традиции.

## **Честные выборы президента планеты**

Если предположить, что наступил утопический сценарий глобализации и все страны смогли объединиться в одно большое государство, то это могло бы породить массу сложностей, например при проведении избирательных кампаний. Однако если вести речь о государстве, внедрившем цифровые инновации и блокчейн-технологии, то все могло бы быть гораздо проще. Предполагается, что у каждого гражданина есть публичный электронный кошелек, в котором могут находиться как разменные, так и неделимые токены. Некий идентифицирующий токен – аналог гражданства, удостоверения личности – мог бы также создаваться в государственном блокчейн-реестре ЗАГС при рождении ребенка и обретать право голоса на выборах при достижении срока существования токена, равного 18 годам. При смерти владельца и наличии неопровержимого подтверждения этого факта токен аннулировался бы. В момент проведения выборов на кошелек всех граждан, достигших 18 лет и имеющих право голоса, автоматически перечислялся бы голосующий токен, имеющий минимальный функционал. Каждый кандидат в президенты мог бы создать простой, ограниченный временными рамками смарт-контракт голосования, привязанный к своему личному кошельку, предлагая всем избирателям переводить голосующие токены на его кошелек. Дальше все предельно просто. Специальная программа, аналог сегодняшних обозревателей блоков (англ. block explorer), мониторила бы один или несколько блокчейнов, собирая следующую информацию: общее количество выданных голосующих токенов, общее количество токенов, принявших участие в голосовании, и пропорции

распределения голосов между кандидатами. Если проголосовало более 50 % всех токенов – выборы признаны состоявшимися. Процент голосов, отданных за каждого кандидата, также прозрачен и доступен для всеобщего просмотра в открытых реестрах.

Если бы голосование проходило на блокчейне, такие махинации, как вбросы бюллетеней, карусели, подтасовка результатов, стали бы невозможными. Количество голосов было бы подсчитано программой честно и беспристрастно, любой гражданин мог бы убедиться в этом самостоятельно. Таким образом можно выбирать не только президента страны или планеты, но и главу крупной международной компании, многочисленные голосующие акционеры которой живут в разных уголках земного шара. Причем подобные структуры – ДАО – уже существуют. ДАО – это аббревиатура от английского словосочетания Decentralised Autonomous Organisation – децентрализованная автономная организация. И многие знают, что с этим названием связан один из крупнейших провалов ICO на платформе Ethereum. В будущем такие структуры вполне могут занять достойное место в цифровых экономиках кибергосударств. При этом модель ДАО может быть легко расширена до модели государства на блокчейне. Я уже упоминал об амбициях одной из команд блокчейн-энтузиастов реализовать сервис, названный eGaaS. Есть и конкурентные eGaaS проекты, наподобие neocarita.com и gprocivis.ch, первичной задачей которых является блокчейн-сервис цифровой идентификации граждан. Именно перевод основных государственных реестров на блокчейн позволит в дальнейшем реализовывать смарт-законы и смарт-контракты, упростив функции ЗАГСа, реестра недвижимости, базы данных юридических лиц и иных подобных государственных реестров. Взаимодействие между ними будет гораздо проще, нежели реализовано сегодня.

## Техногенная катастрофа

Все, о чем я писал раньше, все блага блокчейна, да и Интернета, как предшествующей прорывной технологии, станет бесполезным в случае техноапокалипсиса. Глобальные разрушения, вызванные деятельностью человека, сделают все виртуальные вещи неважными, и криптовалюта, как, естественно, и весь цифровой мир, перестанет существовать. В жестком апокалиптическом сценарии на первый план выйдут обычные бытовые нужды: крыша над головой, пропитание, защита от физических угроз. Вернется принцип натурального обмена ценностями через драгоценные металлы или прямым бартером. Конечно, с помощью источников резервного питания, солнечной и ветровой энергетики можно будет сохранить функционал связи, в том числе и Интернет. Понятно, что огромное количество узлов перестанет отвечать на запросы из-за отсутствия питания, но некоторые смогут поддерживать свое существование, а значит, будет теоретическая возможность обработки транзакций. Однако при упавшем до 0 хешрейте можно будет ожидать пересчета сложности до единицы и вскоре начать добывать PoW-монеты, как биткоин, одной видеокарты, как Сатоши Накамото в ранние денечки. Это лишит криптовалюту всякой ценности. Децентрализация уступит место централизации. Утопиям придет конец, на сцену выйдет бытовой прагматизм. Даже возможные малейшие предпосылки реализации такого развития событий заставят население резко пересмотреть свои привычки, изменить ближайшие планы и отказаться от цифровой реальности по щелчку пальцев. Подобная мрачная фантазия призвана задуматься о том, что в принципе придавать огромное значение виртуальным вещам можно лишь будучи уверенным в устойчивости реального мира. Будет чересчур бесшабашным перевести всю свою жизненную активность за пределы монитора и рассчитывать только на цифровую экономику в долгосрочном периоде. Жизнь настолько непредсказуема, что яркая картинка может смениться мрачной в один день. И техногенные катастрофы, и стихийные природные действия находятся в области возможных событий, как «черные лебеди» в философии Нассима Талеба. Быть готовым к вызовам эмпирической реальности не менее важно, чем следование трендам глобальной диджитализации.

## Послесловие

Вот и подошло к концу мое повествование. Надеюсь, читалось оно легко и интересно, стало полезным и новичкам в мире криптовалют, и матерым шифропанкам. Мне кажется, я сдержал слово и не лез в чересчур детальные подробности, привел множество примеров и провел достаточно аналогий, чтобы тема была раскрыта и вместе с общим ее пониманием у читателя вырисовалось собственное место в данной истории. По крайней мере, появилась база для

дальнейшего изучения и саморазвития или четкое понимание, что ни принципы криптоэкономики, ни технология блокчейн не представляют деятельного интереса для текущего жизненного этапа.

Работа над книгой застала меня в тяжелые времена для всей криптоиндустрии, что заставляло возвращаться к некоторым цифрам по несколько раз, пересчитывать курсы, менять расчетные значения. Наверняка 2018 год запомнится криптосообществу как один из ключевых моментов истории блокчейн-технологий и криптовалют, как провал многих начинаний, крах надежд, время массовых махинаций. Он же отложится в памяти рекордными сборами многообещающих ICO, пиковыми значениями курсов всех без исключения криптовалют в первые дни января, появлением массы прикладных инструментов, упрощающих вход для широких масс в мейнстрим.

Буду рад, если смог донести до читателей практические основы заработка на криптовалютном рынке и важность вопросов безопасности при обращении с криптоактивами. Мне будет очень приятно, если прочтение книги вдохновит кого-то на активные действия по запуску ICO, началу экспериментов с майнингом, выходу на рынок сопутствующих услуг или же, напротив, убедит занять пассивную выжидательную позицию.

Также я уверен, что завершение работы над книгой укрепит меня самого в правильности сделанного выбора – работать с блокчейн-технологиями и криптовалютами, поможет мне утвердиться с дальнейшими шагами в мире цифровой экономики, окажет содействие в привлечении сторонников в мои проекты и в сообщество криптоэнтузиастов в целом.

Хочется еще раз выразить признательность моему компаньону Роману за то, что дал возможность выделить время на работу с книгой, близким друзьям, кто поддерживал меня морально и помогал в личных делах, моим родным и особенно детям за то, что всегда вдохновляют меня идти вперед. Огромное спасибо Интернету и его ресурсам, которыми я активно пользовался для поиска новой или подтверждения имеющейся в голове информации, таким великолепным проектам, как Википедия, а также тематическим форумам и всем авторам, пишущим статьи, посты, ведущим видеоблоги и создающим сайты на тему криптовалют и блокчейн. Спасибо и Сатоши Накамото – без него совсем ничего бы не получилось. Но больше всего я благодарен тебе, дорогой читатель, если ты добрался до этих строк!

На этом я завершаю свое повествование.

*С наилучшими пожеланиями  
ваш Алекс Полански.*