

ТЕХНОЛОГИЯ БЛОКЧЕЙН И NFT

Базовый курс

Тимур Казанцев

16+

Тимур Казанцев

Технология Блокчейн и NFT. Базовый курс

http://www.litres.ru/pages/biblio_book/?art=66931378

SelfPub; 2022

Аннотация

Цифровой мир продолжает стремительно развиваться и уже ясно, что криптовалюты и технологии, основанные на блокчейне, прочно завоевали свое право на существование и используются не только отдельными лицами, но и крупными компаниями и даже правительствами отдельных стран. Все эти цифровые технологии уже меняют способы управления финансами, музыкой, медиа, интеллектуальной и прочей собственностью. С появлением «метавселенных» цифровой мир станет еще ближе к людям, и ожидается, что NFT займет в этом мире существенную роль. Так что же такое NFT, и почему о нем говорит каждый? Если у вас еще нет ответа на этот вопрос, то эта книга для вас. К концу этой книги вы узнаете, что такое NFT, почему все больше людей создают и продают их за крупные суммы. Вы также узнаете где можно покупать NFT, как их создавать самостоятельно, зарабатывать на них, и как они могут помочь вашему бренду. Кроме NFT, мы также узнаем что такое блокчейн и криптовалюта, потому что все эти термины тесно взаимосвязаны.

Содержание

Введение	4
О чем эта книга	6
Дисклеймер	7
Часть I. Основы блокчейн и криптоиндустрии	9
Что такое блокчейн?	9
Фиатные деньги vs Цифровая валюта vs Криптовалюта	12
Обзор глобального рынка криптовалют	17
Биткоин, эфир, стэйблкоины, альткойны	19
Биткоин	19
Эфир	22
Альткойны	25
Стейблкоины	27
Софт и Хард Форки	29
Что такое майнинг	32
Смарт-контракты	34
Публичные и приватные ключи, SEED фраза	38
Криптокошелек: холодное и горячее хранение	40
Конец ознакомительного фрагмента.	42

Тимур Казанцев

Технология Блокчейн

и NFT. Базовый курс

Введение

Вы все еще не можете понять, что такое NFT и почему о нем говорит каждый? Тогда эта книга для вас. К концу этой книги вы узнаете, что такое NFT, почему они настолько важны, что их сегодня обсуждают практически на каждом шагу, а все больше и больше знаменитостей и простых людей создают и продают их за сотни тысяч и миллионы долларов. Вы также узнаете, где их можно покупать и продавать, как их создавать, зарабатывать на них, какие технологии лежат в основе NFT, как они могут повлиять на вас лично, ваш бренд и ваш бизнес, и многое другое. Кроме самой технологии NFT, мы также узнаем что такое блокчейн и криптовалюта, потому что все эти термины тесно взаимосвязаны.

Цифровой мир продолжает развиваться семимильными шагами, уже ясно, что криптовалюты и технологии, основанные на блокчейне, прочно завоевали свое право на существование и используются не только отдельными предпринимателями, но и крупными корпорациями и да-

же правительствами многих стран. Все эти цифровые технологии могут изменить и уже меняют способ управления финансами, музыкой, медиа, интеллектуальной и прочей собственностью. С появлением метавселенных цифровой мир станет еще ближе к людям, и ожидается, что NFT займет в этом мире существенную роль.

О чем эта книга

Данная книга изначально была посвящена NFT. Но так как эта тема непосредственно связана с криптоиндустрией, то в первой части книги мы предоставим несколько лекций, где мы кратко разберем основы блокчейн и криптовалют для базового понимания. Те, кто уже знаком с этой тематикой, могут смело пропустить эту вводную часть про блокчейн и криптовалюты и переходить непосредственно к главам про NFT.

Во второй части, мы расскажем об основах NFT, технологии, лежащей в ее основе, истории возникновения, крупнейших сделках, компаниях и знаменитостях, которые занимаются NFT, а также коснемся рисков при инвестировании в эти токены.

И наконец, в третьей части книги мы покажем вам как и где можно купить NFT, а также как самостоятельно создать и начать продавать свои собственные невзаимозаменяемые токены, на каких маркетплейсах размещаться и много других практических советов.

Дисклеймер

1. Криптоиндустрия – быстроразвивающаяся, но в то же время достаточно волатильная отрасль, которая несет как много потенциального апсайда, так и множество рисков. Поэтому будьте предельно внимательны и осторожны, изучайте как можно больше информации, и используйте здравый смысл и техники риск- и мани-менеджмента при работе с криптоактивами.

2. Все названия криптовалют, маркетплейсов, компаний, NFT, криптокошельков, и пр. упомянуты исключительно в информационных целях. Никакое из упомянутых названий не может быть использовано в качестве инвестиционной, юридической, деловой рекомендации или призывом к действию.

3. Автор не является аффилированным лицом ни к какому из упомянутых в этой книге маркетплейсов или криптовалют или других компаний/активов в данной книге, и не призывает к покупке или продаже чего-либо.

4. Так как криптоиндустрия – относительно новая область, которая быстро развивается, законодательство в ее отношении еще до конца не установлено. В зависимости от страны и времени прочтения данной книги правовой статус криптовалют, NFT и других криптоактивов может отличаться. Поэтому уточняйте актуальность и законность работы с

криптоактивами, чтобы всегда оставаться в правовом поле.

5. Единственная цель данной книги – предоставить информацию о уже завоевавшей свое место в современном мире технологии блокчейн, а также о таком быстро развивающемся феномене как NFT, предоставить ее в максимально открытом, детальном и понятном формате.

Часть I. Основы блокчейн и криптоиндустрии

Что такое блокчейн?

И NFT, и криптовалюты создаются с помощью технологии **блокчейна**. Данная технология позволяет децентрализованно хранить и вносить записи о транзакциях. Все это делается с помощью криптографических методов защиты информации, которые позволяют исключить посредников. Ключевым понятием здесь является **децентрализация**. Децентрализация означает, что нет какого-либо одного центрального компьютера или сервера, где хранится вся информация. Наоборот, все данные хранятся одновременно на множествах устройствах в разных локациях. И поэтому, если вдруг произойдет взлом одного компьютера, то остальные компьютеры не потеряют всю информацию.

Транзакции, запись о которых вносится в блокчейн, могут включать в себя абсолютно разные данные: деньги (криптовалюты), медицинские записи, документы, контракты, итоги голосований, данные покупателей, удостоверения личности, и в целом все данные или активы, которые могут быть представлены в цифровом формате.

В зависимости от параметров сети транзакция подтверждается либо мгновенно, либо сначала она шифруется и помещается в очередь ожидающих подтверждения транзакций. Эти транзакции собираются в своеобразные **блоки**, которые проходят процедуру **валидации**, то есть подтверждения и проверки отсутствия спорных транзакций в прошлом. Эта проверка осуществляется **нодами** – то есть компьютерами и серверами в сети.

Каждому блоку присваивается **хэш** – то есть 256-битный номер, созданный с помощью алгоритма. В блоке присутствует заголовок, ссылка на предыдущий блок хэш и группу транзакций. Такая последовательность связанных блоков создает безопасную и взаимозависимую цепочку, которая и называется **блокчейном**. По сути, с английского «blockchain» так и переводится как «цепь блоков». Цепь блокчейна неразрывна, поскольку каждый блок содержит ссылку на предыдущий. Таким образом, всегда можно восстановить историю переходов того или иного актива от одного человека к другому и узнать его текущего владельца.

Блокчейн часто сравнивают с ожерельем из бусин. Каждая бусина – это блок с определенной информацией, и все они связаны с собой. Бусины невозможно изменить или удалить, но можно только добавить новые.

Блокчейн также называют **технологией распределенных реестров**, потому что записи о всех транзакциях (вся цепочка сделок и актуальный список владельцев) хранят-

ся одновременно на разных нодах (компьютерах), которые независимы друг от друга. Мы уже упоминали, что это еще называется децентрализацией – основным принципом блокчейна. И поэтому если один или несколько компьютеров дадут сбой, то информация не пропадет.



Блокчейн также не стоит путать с технологией облачного хранения данных. Потому что, в отличие от облачной базы данных, в блокчейне сохраняются не сами файлы и документы, а просто записи с доказанным подтверждением существования самой информации и история операции с ней.

Таким образом, по сути, блокчейн – это эффективная технология упорядочивания, шифрования, хранения и передачи данных.

Фиатные деньги vs Цифровая валюта vs Криптовалюта

Валюта, выпускаемая центробанками стран, называется **фиатной** валютой или фиатными деньгами. Это рубли, доллары, евро, йена и так далее. Они имеют бумажный аналог в виде банкнот, которые все мы держали в руках.

Раньше ценность и авторитет валюты ведущих государств обеспечивались наличием в государственной казне золота или серебра. То есть бумажные деньги были обеспечены золотом. И человек мог прийти и поменять банкноты на кусок золота или серебра соответствующей массы. Но это было раньше. Начиная с 1930-х годов страны начали постепенно отказываться от «золотого стандарта», потому что объемы выпускаемых товаров и услуг стали кратно превышать золото в государственных хранилищах. С тех пор валюты пустились в относительно свободное плавание, управляемое центральными банками этих стран.

На данный момент фиатные деньги всех стран обеспечены исключительно авторитетом и экономикой этих стран. Если авторитет страны падает, или экономика начинает ослабевать, то неизбежно ослабевает и национальная валюта этой страны. Например, страны, экономика которых очень сильно зависит от цены на нефть и газ, при падении этих цен, падает сильно и курс валюты этих стран.

Кроме этого, государства могут печатать абсолютно любое количество денег, и в подавляющем большинстве стран эти деньги с каждым годом обесцениваются ввиду инфляции.

Высокая инфляция обычно происходит ввиду неэффективной финансовой политики государства. Если посмотреть на историю, то от гиперинфляции в свое время страдали: Германия в 1920-е годы, когда инфляция составляла 25% в день, или около 1000% в месяц; Зимбабве с конца 1990-х годов и до 2009 года, когда в обороте начали появляться купюры достоинством 1 триллион зимбабвийских долларов, потому что инфляция достигала 231 млн %, а цены удваивались практически каждый день. В Венесуэле в 2018 году инфляция составила более 1 млн %, и страну в результате экономического кризиса покинуло более 3 млн человек.

Итак, мы поняли что такое фиатные деньги и в чем их недостатки. Давайте перейдем теперь к цифровым или виртуальным деньгам.

Под **цифровой валютой** можно понимать деньги, которые управляются виртуально с помощью электронных систем расчета. Например, Webmoney, у которых есть своя цифровая валюта: WMZ – это доллар, а WMR – рубли. Их стоимость привязана к фиатным валютам. Такие же электронные деньги внутри системы есть у крупнейших социальных сетей, внутри компьютерных игр и в других приложениях, которыми пользуются тысячи и миллионы пользовате-

лей. Но если мы покупаем такую цифровую валюту или заводим на такой счет деньги с наших банковских карт, то такая цифровая валюта начинает храниться на серверах этой организации, запустившей данную цифровую валюту. И теоретически, если какой-то злоумышленник взломает сервер этой компании или вашу учетную запись, или сама организация посчитает, что вы недобросовестный пользователь, то ваши цифровые деньги могут теоретически быть украдены или ваш аккаунт может быть заблокирован.

Криптовалюта – это вид цифровой валюты. Она не управляется государствами или банками или какой-то отдельной компанией/организацией. Если фиатные деньги хранятся в банках, а цифровые деньги на серверах организации, то вся информация о криптовалюте хранится в блокчейне, копии которого могут содержаться на тысячах компьютеров по всему миру. У криптовалюты нет физического эквивалента: банкнот или монет. Криптовалюты запрограммированы таким образом, чтобы никто не мог выпустить криптовалюту в обход самой системы.

Мы с вами уже говорили, что одна из основных проблем фиатных денег заключается в том, что им присуща инфляция, потому что они ничем не обеспечены, и правительства в лице центробанков могут проводить относительно неограниченную эмиссию своей валюты. То же самое, например, случилось при пандемии коронавируса, когда ФРС США влило в экономику более 2 трлн долларов, и правительства других

стран поступило схожим образом.

А теперь давайте посмотрим на криптовалюту, и в частности, на биткоин. Это первая криптовалюта, которая сейчас является и наиболее популярной и торгуемой. Так вот, биткоин похож на золото в том плане, что его количество ограничено. Криптовалюта – это, грубо говоря, программа, написанная человеком на компьютере. И создатель биткоина ограничил ее количество 21 миллионов штук. На конец 2021 года добыто около 19 миллионов биткоинов. После того как количество достигнет 21 миллиона, добыча прекратится. И поэтому у этой криптовалюты есть ценность, потому что она ограничена в количестве (в отличие от фиатных денег).

И так как все больше и больше людей видят ценность этой валюты и понимают, что она ограничена, все больше и больше людей хотят завладеть хотя бы одним биткоином или сатоши (одна стомиллионная биткоина). В результате этого растет спрос на эту криптовалюту, и как следствие – ее цена. С момента появления биткоина в 2009 году до конца 2021 года, биткоин вырос в цене с 0 долларов до 68 тысяч долларов (в самом начале биткоин обменивался бесплатно между первыми пользователями, в 2010 году он торговался в диапазоне от 0.0008 до 0.008 долларов).

Другим преимуществом криптовалют является то, что они регулируются не государством или банком, а строгими математическими алгоритмами. Представьте, что вы хотите перевести крупную (да даже необязательно крупную сумму

денег) своему родственнику или другу в другую страну. Банк обязательно возьмет комиссию с перевода, а может и вовсе заблокировать эту операцию, или может позвонить вам и начать уточнять с какой целью вы это делаете, или классифицировать этот перевод как подозрительный и заблокировать ваш счет полностью. А в случае с криптовалютами, такие посредники в виде правительств и банков отсутствуют, и в этом и заключается основная миссия криптовалют – создать деньги, которыми люди смогут расплачиваться друг с другом напрямую без посредников.

Обзор глобального рынка криптовалют

Как мы уже поняли, биткоин – действительно самая популярная, но не единственная криптовалюта. На конец 2021 года существует более 9000 криптовалют. Общая капитализация всего криптовалютного рынка составляет 2,6 триллиона долларов, что примерно сопоставимо с капитализацией компании Apple, или в 1,7 раз больше ВВП России.

Под капитализацией понимается сколько той или иной криптовалюты находится в обращении в пересчете на доллары. Например, если сейчас стоимость одного биткоина составляет 57 300 долларов, а всего в системе находится 18 900 000 биткоинов, то капитализация биткоина составляет 1 082 970 000 000 долларов, то есть больше одного триллиона. И если таким же образом перемножить стоимость всех криптовалют на их количество соответственно, то мы и получим общую капитализацию рынка криптовалют в мире в размере 2,6 триллионов долларов.

Кстати, всю статистику по криптовалютам, количество выпущенных монет, их стоимость, объемы торговли и другую информацию, касающуюся крипторынка, можно отслеживать на сайте www.coinmarketcap.com.

Рынок развивается очень волатильно, но все же растет достаточно быстро. Если в ноябре 2020 года капитализация

всех криптовалют составляла около 500 млрд долларов, то в ноябре 2021 года она приблизилась к 2,6 триллионам, то есть рынок вырос на 420%. Во многом, это произошло в результате нескольких факторов:

- масштабной эмиссии долларов, евро и других национальных валют для того, чтобы подстегнуть экономики стран после пандемии коронавируса, и как следствие, возникшей инфляции;

- бурному росту рынка NFT;

- все большему вовлечению институциональных инвесторов (крупных корпораций) в крипторынок, выходу криптобирж на фондовые рынки и так далее.

Биткоин, эфир, стэйблкоины, альткойны

Итак, давайте теперь поговорим о конкретных криптовалютах, и чем они отличаются.

Биткоин

Самой первой криптовалютой в современном понимании стал **биткоин**. Он был изобретен в 2008 году неким Сатоши Накомото, личность которого по-прежнему точно не установлена, возможно это псевдоним другого человека либо группы лиц. 31 октября 2008 года Сатоши опубликовал свою статью: «Bitcoin: A Peer-to-Peer Electronic Cash System» («Биткоин: Одноранговая Электронная Платежная Система»). В этой статье автор приводил подробное описание того как функционирует биткоин и принципы его работы. После публикации статьи работа над биткоином еще продолжалась некоторое время, а в январе 2009 года работа над протоколом была завершена и код программы-клиента стал общедоступным. Возможно, появление биткоина стало ответом на мировой финансовый кризис 2008 года, когда одни из крупнейших банков в мире потерпели крах, и многие люди потеряли работу и накопления.

Как бы то ни было, в самом начале своего существования

биткоин практически ничего не стоил. Никто и не знал как его оценивать. В первый год он торговался в диапазоне от 0,0008 до 0,008 долларов за один биткоин.

Самый известный случай использования биткоина в повседневной жизни, наверное, является случай с покупкой пиццы в 2010 году.

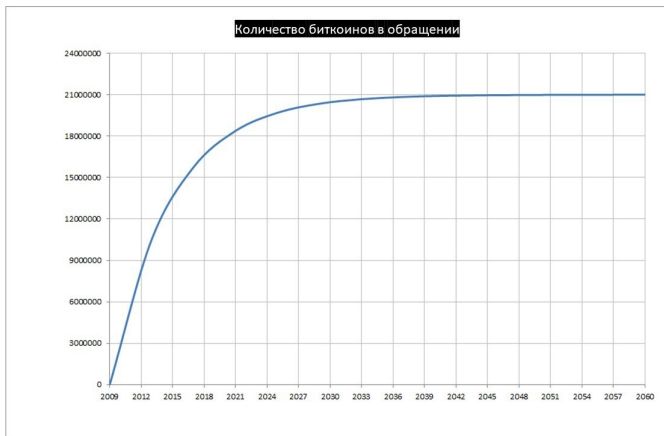
Программист из Флориды в США Ласло Ханэч потратил 10 000 биткоинов, чтобы получить 2 пиццы из местной пиццерии Папа Джонс. На тот момент эти 10 000 биткоинов стоили примерно 40 долларов, и Ласло на одном форуме пообещал перевести эти биткоины тому, кто купит ему 2 пиццы. Это случилось 22 мая 2010 года, и с тех пор этот день празднуется как День Биткоин Пиццы, потому что он неким образом коммерциализировал использование криптовалюты в реальном мире. И с учетом того, что на данный момент те 10 000 биткоинов составляют примерно 600 млн долларов, те 2 пиццы могут считаться самыми дорогими пиццами всех времен.

На декабрь 2021 года стоимость одного биткоина равняется 60 000 долларов. В июне 2021 года Эль Сальвадор стал первым государством, которое признало биткоин официальной валютой в стране. Сделано это было отчасти из-за того, что сальвадорцы, работающие за рубежом, тратят несколько сотен миллионов долларов в комиссиях банкам и традиционным платежным системам при переводе денег в свою страну.

Что касается технологии, то, как уже было сказано, биткоин работает на блокчейне, то есть записи о переводе монет, актуальных владельцах, количестве монет в обращении, и истории всех транзакций хранятся децентрализованно в сети, состоящей из нескольких тысяч узлов (узлов в сети).

Система запрограммирована таким образом, что количество биткоинов не может превысить 21 миллионов монет. С 2009 года и до конца 2021 года намайнено (сгенерировано) примерно около 19 миллионов монет. Часть монет утеряна навсегда, так как владельцы некоторых биткоин-кошельков попросту забыли свои пароли.

Блоки с транзакциями добавляются в блокчейн биткоина примерно каждые 10 минут. За добавление блока в сеть, майнеры получают вознаграждение в биткоинах. Каждые 4 года, количество генерируемых биткоинов при добавлении блоков, снижается на 50%. Таким образом, с каждым годом добыча биткоинов будет происходить сложнее, и их общее количество в сети также будет расти в более медленном темпе. Это как раз и ведет к тому, что их общее количество остается в определенном дефиците, что предотвращает инфляцию в отличие от фиатных денег, и поддерживает ценность криптовалюты. Если брать математически, то добыча биткоина выглядит как функция скорости суммарно добываемых монет от времени. И эта функция обратно пропорциональна, то есть скорость добычи со временем падает и стремится к нулю.



Биткоин – первая и, пожалуй, самая известная криптовалюта в мире. Мы говорили, что общая капитализация всего крипторынка составляет на декабрь 2021 года 2,6 триллиона долларов. Так вот, из них 1,08 триллиона (около 41,5%) – это капитализация биткоина. То есть биткоин по-прежнему самая популярная криптовалюта из всех существующих.

Эфир

Вторая по популярности криптовалюта – это **эфир (Ethereum – ETH)**. Она занимает примерно 22% от общего крипторынка с капитализацией 561 миллиард долларов.

И у биткоина и у эфира есть много схожих признаков: они

оба являются криптовалютами, которые торгуются на криптобиржах и могут храниться в криптокошельках. Оба токена децентрализованы, то есть они не выпускаются какой-то одной организацией или банком, и оба токена используют технологию распределенного реестра блокчейн. Однако, между биткоином и эфиром существуют также определенные различия.

Во-первых, сразу стоит отметить, что биткоином называют как платежную систему, так и саму криптовалюту. Так же и с эфиром, есть эфириум – как децентрализованная платформа, а есть эфир – сама криптовалюта.

Итак, а теперь по поводу различий между биткоином и эфириумом. Как уже сказали, если биткоин – это платежная система и криптовалюта, то эфир/эфириум – это криптовалюта и платформа для создания децентрализованных приложений на базе блокчейна, работающих на основе смарт-контрактов. По сути, эфир (или правильнее будет в данном случае «эфириум») – это децентрализованный компьютер или виртуальная машина, на которой можно создавать различные приложения.

Один из сооснователей эфириума – Виталик Бутерин опубликовал статью об эфириуме в 2013 году, а полноценная система была запущена в 2015 году с целью децентрализации всего в интернете. Благодаря смарт-контрактам, потенциал использования эфириума огромен, и появление NFT – один из таких примеров. Возможно, что основные направле-

ния использования эфириума еще и не созданы, так же как и социальные сети и Гугл не были изобретены сразу после появления интернета.

В то время как биткоин используется как средство обмена и хранения ценности, эфир используется для взаимодействия с приложениями внутри сети эфириум. Оплата за транзакции, создание смарт-контрактов и использование децентрализованных приложений, все это требует оплаты комиссий в эфире. И по мере того, ценность эфира начала расти вверх, он также начал использоваться как криптовалюта, имеющая свою ценность.

	Биткоин	Эфириум (Эфир)
Основатели	Сатоши Накамото	Виталик Бутерин, Михай Ализе, Энтони Ди Лорио, Чарльз Хоскинсон
Дата запуска	Январь 2009	Июль 2015
Назначение	Платежная система и криптовалюта, альтернатива традиционным фиатным валютам, средство обмена и хранения ценности	Платформа для работы программируемых смарт-контрактов и приложений с помощью криптовалюты Эфир
Время создания блока	В среднем 10 минут	В среднем 15 секунд
Скорость транзакций	7 транзакций в секунду	30 транзакций в секунду
Объем монет	Количество ограничено 21 млн биткоинов	Эмиссия не ограничена

Таким образом, создание биткоина и эфириума имело под собой различные цели. Если биткоин был создан как альтер-

натива национальным валютам, средство обмена и хранения ценности, то эфириум был создан как платформа для создания децентрализованных приложений и смарт-контрактов, которые бы работали с помощью собственной валюты – эфира (ETH).

Благодаря своей популярности и возможностям использования (децентрализованные финансы, искусство (NFT), игры и технологии), эфириум развивается огромными шагами. Только за 2021 год криптовалюта эфир (ETH) выросла на 510% по сравнению с биткоином (BTC), выросшим на 93%. В результате, если в январе 2020 года, капитализация эфира составляла 1/10 от капитализации биткоина, то в декабре 2021 года, она составляла уже 1/2.

Альткойны

Если вы будете иметь дело с криптоиндустрией, то часто будет встречаться такой термин как «альткойн». По сути, слово «альткойн» произошло от фразы «alternative coin» (альтернативная монета), и этим названием начали обозначать все криптовалюты, которые возникли после появления биткоина. Даже эфир, несмотря на то, что он является второй по популярности криптовалютой со своей отдельной экосистемой, он также рассматривается как альткойн.

Первые альткойны начали возникать в 2011 года, через 2

года после появления биткоина, и целью многих из них было прервать монополию биткоина, а также исправить его недостатки, среди которых можно выделить следующие:

- относительно низкая скорость транзакций,
- сложный и дорогой майнинг,
- высокая стоимость монеты,
- недостаточный функционал.

Несмотря на то, что некоторые альткоины в итоге смогли закрепиться на рынке и набрать достаточное количество пользователей, многие альткоины по-прежнему остаются не такими популярными. Зачастую зависимость многих альткоинов от биткоина выражается в корреляции их цен до 80%.

Для того, чтобы создать новый альткоин необходимо иметь хорошие знания в программировании. Каждая криптовалюта имеет в своей основе программный код, описывающий параметры и характеристики сети. Причем создать новую криптовалюту можно либо написав новый оригинальный код, либо модифицируя код уже существующей криптовалюты (добавив функционал и исправив возможные ошибки).

Чтобы о вновь созданной криптовалюте узнало как можно больше людей в первое время, создатели таких криптовалют часто практикуют бесплатную раздачу монет. В первое время они в любом случае стоят не так дорого. Такая практика носит название **AirDrop**. Бесплатные альткоины раздаются как награда за выполнение простых задач, таких как реги-

страция на сайте, комментарий или что-то еще.

На данный момент среди крупнейших альткойнов можно назвать: Cardano, Litecoin, Ripple, Enjin, Uniswap, Binance, Polkadot, и другие.

Несмотря на то, что каждая из криптовалют имеет свою специфику, все криптовалюты объединяет единая технология – блокчейн.

Стэйблкоины

С момента своего появления криптовалюты всегда отличались высокой волатильностью, то есть резкими колебаниями цены по отношению к фиатным деньгам. Это мешало использовать криптовалюты как полноценный источник инвестирования, а также как средство для оплаты товаров и услуг на повседневной основе из-за рисков для поставщиков и продавцов.

Чтобы решить эту проблему, были созданы стэйблкоины (stable coin), что в переводе означает «стабильные монеты». Такая криптовалюта привязана к запасам обычных фиатных валют, физических товаров (золота) или сырья (нефти), и как следствие, такие стейблкоины подвержены меньшим колебаниям цен, в отличие от курсов обычных криптовалют.

Первым таким стэйблкоином и на данный момент одним из самых популярных является Tether. В самом начале его создатели утверждали, что курс Tether привязан к доллару

США в отношении 1:1, однако с тех пор упоминалось, что резервы компании включают не только доллары, но и другие активы, дебиторскую задолженность по займам и пр. Читая статьи про Tether, неизбежно сталкиваешься с различными точками зрения – от всяческих тайн и манипуляций до восхищения монетой за ее стабильность и удобство. Как бы то ни было, на декабрь 2021 года монета по-прежнему популярна и занимает 4-е место по капитализации на всем криптовалютном рынке.

Среди других стэйблкоинов можно выделить USD Coin, Binance USD, CACHE Gold и другие.

Почему стэйблкоины пользуются спросом среди инвесторов? Потому что в отличие от других криптовалют, они относительно стабильны, и во времена медвежьего рынка (падения) они позволяют инвесторам обезопасить свои средства, действуя как временное убежище. Вместо того, чтобы выводить средства из криптовалюты в фиатные деньги во время падения крипторынка, можно вложить часть криптоденег в стэйблкоины, таким образом зафиксировав их стоимость в переводе на фиатные деньги.

Несмотря на свою стабильность, иногда бывает достаточно проблематично доказать инвесторам, что тот или иной стэйблкоин действительно обеспечен резервами, как заявляют об этом его создатели вначале, и поэтому при инвестировании в них в любом случае необходимо качественно изучать эти токены и понимать о возможном риске.

Софт и Хард Форки

Мы знаем, что криптовалюты основаны на блокчейне, который является децентрализованной технологией с открытым кодом, а это значит, что каждый может к ней подключиться. Технологии с открытым кодом полагаются на сообщества программистов, которые помогают поддерживать и развивать программный код этой технологии.

Форк случается, когда кто-то из этого сообщества решает внести изменения в протокол блокчейна, то есть в его набор правил. Когда происходит форк, цепочка блокчейна разделяется, производя вторую цепочку, которая имеет такую же историю, как и оригинал цепочки, но движется она уже в другом направлении.

Почему разработчики решают провести форк? Как правило, это происходит по следующим причинам:

- Добавить нового функционала;
- Решить проблемы безопасности;
- Решить разногласия среди разработчиков относительно будущего данной криптовалюты. Иногда в связи с этим создается абсолютно новая криптовалюта со своей экосистемой.

Существует два вида форка: мягкий (soft fork) и жесткий (hard fork).

При мягком форке происходит обновление кода блокчей-

на. Мягкие форки используются, чтобы привнести новые функции на уровне программирования. При мягком форке даже если часть нодов в сети не примет обновления, они все равно смогут взаимодействовать с нодами, которые будут пользоваться новыми правилами. Мягкий форк – это как обновление программного обеспечения на вашем компьютере или смартфоне. Привносятся определенные новые функции или ускоряются процессы, но даже если вы их не примете, вы все равно сможете работать с большинством программ и коммуницировать с другими устройствами.

Жесткие форки случаются, когда код изменяется так сильно, что новая версия больше не обратно совместима с прежними блоками. При этом сценарий блокчейн делится на две части, оригинальный блокчейн и новая версия, которая следует новому протоколу. При хардфорке узлы, не принявшие новые правила, не принимают информацию от узлов, которые их приняли. При хардфорке одна из ветвей может отмереть, либо обе ветви могут продолжить свое существование и будут действовать уже две новые криптовалюты. Например, криптомонеты Bitcoin Cash или Bitcoin Gold как раз появились при помощи жесткого форка из оригинального блокчейна биткойна. Другие примеры: Dogecoin (форк Litecoin), Expanse (форк Ethereum), Stellar (форк Ripple).

В 2016 году состоялся хардфорк сети Эфириум. Новая цепочка продолжила существование под прежним названием Ethereum (ETH), а оригинальная цепочка также сохрани-

лась и поддерживается уже под другим названием Ethereum Classic (ETC).

Что такое майнинг

Под «майнингом» (с англ. ‘mining’ – добыча) подразумевается добавление новых блоков с транзакциями в цепочку блокчейна. Транзакции в сетях блокчейн совершаются достаточно часто, и сами по себе они не добавятся в блок и не примкнут к главной цепочке. Этим и занимаются майнеры. Они берут транзакции, упаковывают их в блоки, и пытаются добавить новые блоки в цепочку. За это они получают вознаграждение от сети.

Почему «пытаются»? Потому что это не так легко. Чтобы добавить блок, необходимо решить сложную математическую задачу, генерируемую блокчейн сетью. Для этого необходимы мощные компьютеры. Компьютеры майнеров соревнуются друг с другом, они работают круглые сутки, чтобы решить такие сложные задачи. Вероятность того, что тот или иной майнер решит математическую задачу первым, присоединит блок и получит за это вознаграждение – как правило, зависит как раз от мощности его оборудования.

Если задача решена, то новый блок распределяется по сети и добавляется в основную цепь. Майнер, решивший задачу первым, получает вознаграждение, как правило, в виде криптовалюты данной сети.

Кроме подтверждения транзакций, майнеры также проверяют транзакции, зарегистрированные другими майнерами.

И также они хранят копии блокчейна, защищая информацию от потери или подделки.

Как правило (в сети биткоин, например), количество майнеров неограничено. И чем их больше в сети, тем лучше, потому что такая сеть становится более надежной.

При работе с криптовалютами, майнеры за свою работу получают награждение в виде криптовалюты: как комиссия от всех участников транзакций, записанных в блоке, а также вознаграждение от самой сети. Сеть генерирует и выпускает новые монеты, и общее количество монет увеличивается. Однако, как правило, в некоторых криптовалютах существует ограничение: когда общая сумма монет достигает определенного максимума, их выпуск прекращается. Дальше майнеры могут работать только за вознаграждение от участников. Например, сумма всех биткоинов, которые могут быть выпущены сетью изначально ограничена в 21 миллион биткоинов. На начало 2022 года было выпущено почти 19 миллионов единиц.

Так вот, мы уже говорили, что каждые 4 года, количество генерируемых биткоинов при добавлении блоков, снижается на 50%. Изначально, когда биткоин был только запущен, за добавление одного блока майнер получал 50 биткоинов, в 2012 году вознаграждение было сокращено вдвое до 25 биткоинов. В 2016, произошло очередное сокращение до 12.5. Следующее сокращение было в 2020 году – до 6.25 биткоинов за добавление одного блока.

Смарт-контракты

В технологии блокчейн присутствует возможность загрузить в него компьютерную программу, которая будет исполняться самостоятельно и автоматически. Такие программы называются смарт-контракты. Такие контракты вместе с результатами их работы хранятся в блокчейне и остаются там навсегда.

Само понятие «смарт-контракт» было введено в оборот еще в начале 1990-х годов программистом Ником Сабом. Он описал этот термин как компьютерный протокол, который самостоятельно совершает сделки с полным контролем над их выполнением. Сабо предполагал, что смарт-контракты будут намного лучше традиционных юридических контрактов, потому что будут обладать различными механизмами цифровой и криптографической защиты.

Настоящий же бум на смарт-контракты произошел в середине 2010-х годов с появлением и развитием сети Ethereum. Один из сооснователей Ethereum Виталик Бутерин понял, что технология блокчейна может использоваться намного шире, чем только для перевода и хранения криптовалют. Именно основываясь на этой предпосылке, и был создан Ethereum, который стал не просто еще одной криптовалютой и платежной системой, а полноценной децентрализованной блокчейн-платформой, на которой любой человек мог

бы программно реализовывать различные системы хранения и обработки информации. То есть был создан некий децентрализованный виртуальный компьютер, с помощью которого люди могли бы самостоятельно создавать децентрализованные приложения с помощью смарт-контрактов.

Именно на основе Ethereum были созданы такие проекты как:

- DeFi (децентрализованные финансы – аналоги традиционных финансовых инструментов, реализованных в децентрализованной архитектуре);

- утилитарные токены и блокчейны,

- NFT,

- биржи,

- социальные токены,

- криптоколлекционные игры,

- и другие проекты.

Ethereum, однако, не единственная платформа, на которой можно разрабатывать и внедрять смарт-контракты. Среди других платформ можно выделить HyperLedger Fabric, EOS, Stellar и другие.

Итак, в чем же преимущества смарт-контрактов. Во-первых, с помощью них можно проводить конфиденциальные транзакции без посредников, это более надежно и снижает транзакционные издержки, связанные с заключением договоров и оплат различных регистрационных взносов. Во-вторых, все транзакции сохраняются навсегда в блокчейне,

их можно легко отследить, невозможно обратить или подделать, потому что информация хранится одновременно на многих узлах в сети (=децентрализация).

В каких конкретных областях, сделках и примерах можно использовать смарт-контракты? Мы уже упоминали создание бирж, операции с криптовалютами, но применение смарт-контрактов можно распространить и на традиционные виды сделок и операций: регистрация автомобилей и объектов недвижимости, сделки с ними, и хранение данных об их владельцах; контроль продажи и учет товаров в магазинах; умное голосование, защиты товаров от двойных продаж, регулирование страховых случаев и многое другое.

Итак, как мы могли заметить, смарт контракты имеют перспективу стать одним из самых важных применений технологии блокчейн, потому что они могут применяться в огромном ряде различных отраслей и видов операций, а также могут привести даже к появлению новых бизнес-моделей.

Из недостатков можно выделить то, что большинство стран пока не признали смарт-контракты имеющими юридическую силу. На данный момент единственной страной, юридически закрепившей понятие «смарт-контракт» и порядок работы с ним стала Белоруссия, принявшая Декрет о развитии цифровой экономики в 2017 году, и последовавшие за ним постановления.

Кроме того, процесс создания самого смарт-контракта достаточно сложный, особенно в случаях, когда необходимо

учитывать много составляющих условий.

И в случае, если смарт-контракты все же начнут использоваться повсеместно, то это может привести к потере множества рабочих мест со стороны административного персонала регистрационных учреждений, банков и нотариусов.

Однако, эти недостатки не мешают развитию и применению смарт-контрактов в разных областях, и их область применения продолжает расширяться.

Публичные и приватные ключи, SEED фраза

Если вы решите купить криптовалюту, то для начала вам необходимо будет установить криптокошелек – то есть кошелек, где будет храниться ваша криптовалюта. Это можно сделать, зарегистрировав аккаунт на сайтах самих криптовалютных бирж, где проводятся операции купли-продажи криптовалют; либо можно установить отдельный криптокошелек. Существуют «горячие» и «холодные» кошельки, о них мы поговорим в следующей лекции, а пока познакомимся с такими терминами, как публичные и приватные ключи, а также SEED фраза.

Публичный ключ – это **адрес** вашего криптокошелька, чтобы люди знали куда переводить криптовалюту. Если вам кто-то хочет перевести криптовалюту, просто направьте этот публичный ключ этому человеку. Некоторые магазины вывешивают эти свои ключи через QR-коды, чтобы покупатель мог отсканировать его и сразу увидеть этот ключ.

Приватный ключ – это **пароль** от вашего кошелька. Его должны знать только вы, чтобы иметь возможность совершать операции с вашего кошелька, например, если вы хотите оплатить что-то или перевести кому-то криптовалюту.

SEED фраза – это набор из 12 слов, которые генерируются автоматически при создании вашего кошелька. Эти сло-

ва необходимо записать и хранить в отдельном месте. Они могут понадобиться, **если вы забудете свой приватный ключ**, то есть пароль от вашего кошелька.

Криптокошелек: холодное и горячее хранение

Криптовалюты и NFT могут стоять сегодня тысячи и сотни, и даже миллионы долларов, и хотя разрабатывается много технологий, чтобы обезопасить их от краж или потерь, такие случаи все же случаются.

Для начала попробуем понять как происходит кража криптовалюты с криптокошельков. Главное на что нацелены хакеры – это получить ваш приватный ключ (пароль от вашего кошелька).

В том что касается хранения криптовалют, существуют такие понятия как «горячее хранение» (hot storage) и «холодное хранение» (cold storage). Иногда их также называют «горячий» и «холодный кошелек».

Горячий кошелек – это кошелек с активным онлайн соединением. То есть если вы, например, храните криптовалюту на своем аккаунте на криптобирже, или установленном на своем компьютере кошельке, но ваш компьютер имеет подключение к интернету. Все что хранится в таком виде и подключено к интернету, может потенциально быть украдено хакерами, так же как хакеры могут взломать банковские системы или государственные базы данных. Далеко не факт, что такое произойдет именно с вашим криптокошельком, но такой риск имеется. С другой стороны, плюсы горячего ко-

шелька в том, что вы можете совершать операции с криптовалютами достаточно быстро.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.