Сергей Базанов

БИТКОИН для всех

Сергей Базанов

Биткоин для всех. Популярно о первой распределенной одноранговой денежной системе

«Издательские решения»

Базанов С.

Биткоин для всех. Популярно о первой распределенной одноранговой денежной системе / С. Базанов — «Издательские решения»,

ISBN 978-5-44-936582-8

Что такое Биткоин (Bitcoin)? Кто его создал, как он появился и чем отличается от привычных денежных систем, управляемых государством? Что такое блокчейн, одноранговые сети, майнинг и консенсус? Чем обеспечен биткоин и что влияет на его стоимость? Можно ли взломать Биткоин и каковы риски его использования?Ответы на эти и многие другие вопросы вы найдете в этой книге.В приложении — полезные ресурсы и словарь основных терминов и понятий из мира криптовалют.Для массовой аудитории.

ISBN 978-5-44-936582-8

Содержание

Биткоин для всех
Популярно о первой распределенной одноранговой денежной системе

Сергей Базанов

Дизайнер обложки Сергей Базанов
Редактор Екатерина Скиба
Корректор Татьяна Базанова

ISBN 978-5-4493-6582-8
Создано в интеллектуальной издательской системе Ridero

Предисловие автора

История написания этой книги такова. Изучая тему Биткоина и все больше погружаясь в неё, я перечитал кучу материалов, в том числе и переводных. Это были либо тексты для профессионалов, написанные сухим академическим языком, либо популярные статьи для начинающих.

И если первые были написаны с использованием специальных терминов, требующие первоначальной подготовки в математике, криптографии, программировании, экономике и т.п., то вторые грешили вульгаризацией и упрощением, что приводило к искажению понимания блокчейна и Биткоина, а то и вовсе вводило в заблуждение. Особенно это касалось темы майнинга.

Поэтому у меня появилось желание попробовать самому просто и доступно, с использованием понятных аналогий, объяснить сложные вещи, связанные с блокчейном. Так родились аналогии с навесным замком с двумя ключами (см. глава о шифровании с открытым ключом) и отпечатками пальцев человека (глава о хэшировании), а также объяснение блокчейна через хэшчейн на понятном простом примере.

Свои тексты о Биткоине я публиковал в блоге **Bitcoin Review**.

Первоначально это были статьи, популярно разъясняющие базовые криптографические понятия, на которых основывается технология Биткоина:

1. Криптография с открытым ключом.
2. Хэширование.
3. Электронная цифровая подпись.

Далее – блок статей о самом Биткоине, в котором доступно объясняется работа блокчейна и его составляющих частей:

1. Кошельки и транзакции
2. Блокчейн
3. Блок
4. Майнинг

Кстати, по многочисленным отзывам, текст о майнинге (глава **«Майнинг»**) – это лучшее, из того, что вы читали о нем. Не верите? Прочтите и убедитесь!

К осени 2018 года в моем блоге набралось уже несколько десятков статей о Биткоине, включая лучшие переводные, которые просто и понятно объясняли все технологические и экономические аспекты первой криптовалюты.

К сожалению, в последнее время вокруг этой темы много хайпа, мифов и спекуляций, за которыми теряется истинное предназначение Биткоина – изменить парадигму мира финансов, устранить монополию государства на деньги и посредничество банков в платежах и расчетах.

Я считаю, что для успешного продвижения Биткоина в массы необходима популяризация этой технологии, чтобы как можно больше людей узнали истину об этой криптовалюте и вышли из плена заблуждений, навязанных некомпетентными СМИ.

В преддверии 10-летнего юбилея Биткоина я подумал, что было бы хорошо собрать свои лучшие авторские статьи в единую книгу под названием **«Биткоин для всех»**. Это название отражает две взаимосвязанных цели – дать доступную для понимания информацию о первой криптовалюте для массовой аудитории и вовлечь её в процесс пользования Биткоином.

В книге вы не найдете советов, как внезапно разбогатеть и заработать или намайнить 100500 тысяч биткоинов. Она о другом – о цели, миссии, технологиях и инфраструктуре Биткоина – величайшего изобретения, которое меняет и, в конце-концов, изменит мир к лучшему.

Сергей Базанов

Посвящается 10-летию Биткоина
и его создателю – гениальному и загадочному
Сатоши Накамото (Satoshi Nakamoto).

Первое знакомство с Биткоином

Что такое Биткоин? Краткое объяснение

Биткоин (Bitcoin) – это компьютерная цифровая сеть транзакций. Он не требует, чтобы любое отдельное лицо или организация (банк, например) утверждали каждую транзакцию. Вместо этого он поручает делать одобрение транзакций всем участникам сети.

Как это работает. Каждый раз, когда создается транзакция, т.е. когда с одной учётной записи (биткоин-адреса) отправляется некоторое количество биткоинов на другую учётную запись, это транслируется (направляется) на все компьютеры в сети, которые представляют собой распределенный между пользователями реестр. Эта транзакция затем объединяется с другими транзакциями, поступившими в сеть примерно в одно и то же время, для формирования **блока транзакций**. Любой компьютер в сети имеет возможность проверить все эти транзакции в блоке и решить некоторую компьютерную задачу.

Со временем, чем большее количество компьютеров в сети пытается одновременно решить эту задачу, она становится все сложнее и сложнее. Сложность решения этой задачи автоматически (программно) подбирается таковой, чтобы занять около 10 минут для её решения в сети компьютеров. Чем больше и мощнее сеть компьютеров, тем сложнее задача.

Тот компьютер в сети, который первым решит компьютерную задачу, получает право сформировать блок всех новых действительных транзакций и за это вознаграждается определенным количеством биткоинов, которые выпускает сама сеть. Затем этот блок транзакций добавляется в реестр всех блоков, которые были одобрены до него, и эта база данных, называемая **блокчейном**, отправляется на каждый компьютер в сети. Любой компьютер, подключенный к сети, имеет возможность отслеживать все транзакции, которые произошли до этого момента.

Блоки транзакций в блокчейне **криптографически связаны** между собой таким образом, что даже самое незначительное изменение информации в одном блоке приведет к изменению информации во всех последующих блоках вплоть до последнего. Поэтому практически невозможно незаметно изменить информацию о транзакциях, уже записанную в блокчейн.

Блокчейн или список всей истории блоков транзакций – вот, что делает Биткоин **безопасным**. Поскольку каждый компьютер в сети может знать историю транзакций, он может знать, сколько биткоинов имеет каждая учетная запись (биткоин-адрес), и, следовательно, может проверять транзакции и следить за тем, чтобы ни одна учетная запись не использовала больше биткоинов, чем она имеет, или обманывала сеть каким-либо другим способом. Кроме того, технология блокчейна не позволяет вносить изменения в уже записанные блоки транзакций. Тем самым, обеспечивается целостность и неизменность информации.

Биткоин «на пальцах»
Простое и доступное объяснение, зачем нужен Биткоин и как он работает

Информация для тех, кто только начинает знакомство с первой криптовалютой и хочет, чтобы ему просто и доступно для понимания, буквально «на пальцах» объяснили, что же такое этот биткоин и чем он отличается от обыкновенных денег.

Сначала небольшой экскурс в мир денег и их оборота.

У большинства людей деньги ассоциируются с выпускаемыми государством **банкнотами** – бумажными денежными купюрами или мелкими долями – металлическими **монетами**.

Это очень понятно для обывателя: **есть банкноты – есть деньги** и наоборот. При этом безналичные деньги, хранящиеся на вкладах или текущих счетах в банках с точки зрения того же обывателя – это те же банкноты, но только их хранит банк и может выдать по требованию вкладчика или клиента. Даже деньги на пластиковой банковской карте – это тоже в конечном счете банкноты, но они передаются каким-то электронным путем.

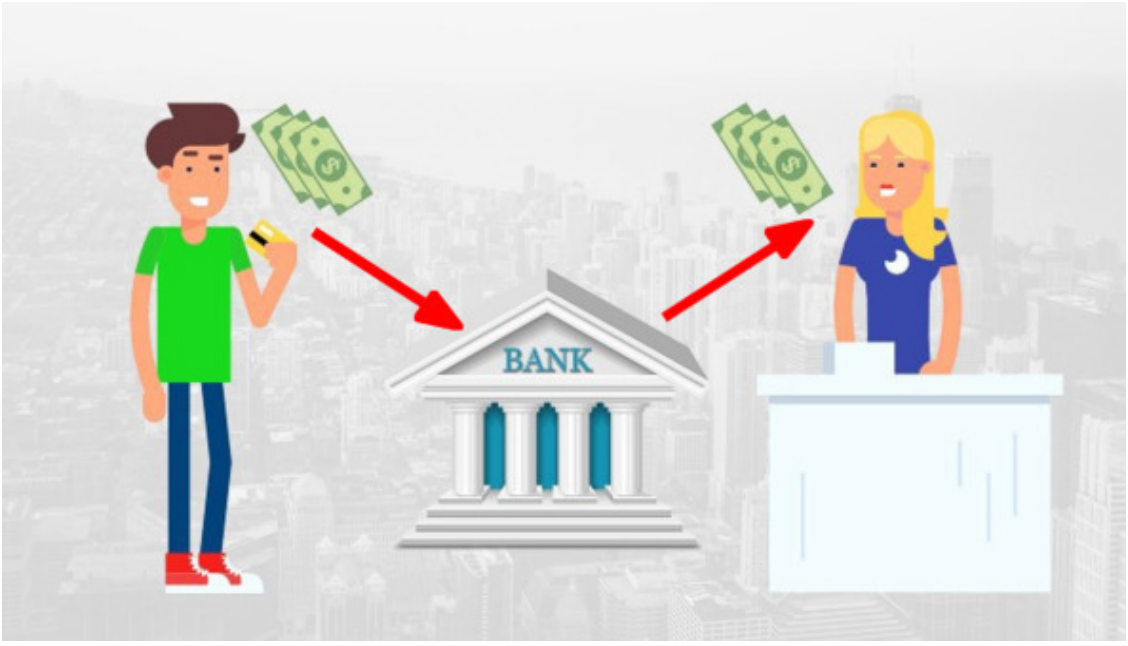
Но, банкноты и монеты – это лишь вещественное отражение такой сущности, как деньги. На самом деле, **деньги – это информация**. Информация о том, каким эквивалентом суммарной стоимости обладает субъект (индивидуум или организация).

Если у вас в кошельке имеется, к примеру, три банкноты по 100 денежных единиц (гривен, рублей или долларов), то это означает, что вы обладаете суммарным эквивалентом стоимости в 300 денежных единиц. На них вы можете приобрести товары и услуги, эквивалент стоимости (цена) которых менее или равна этим 300 денежным единицам.

При операции покупки/продажи происходит передача от покупателя к продавцу некоего **эквивалента стоимости** товара в денежном выражении. Эта операция называется **транзакцией**. При этом банковский счет или кошелек продавца пополняется, а покупателя уменьшается на сумму транзакции.

Если эта операция осуществляется наличными деньгами (банкнотами), то участие третьей стороны (помимо покупателя и продавца) не требуется. Покупатель просто передает продавцу из рук в руки некоторое количество банкнот. А взамен получает товар или услугу. Всё! Транзакция прошла и сделка совершена.

Если же покупка осуществляется дистанционно (на расстоянии) или посредством банковской карты, то в сделке принимает участие третья доверенная сторона – **банк**. При этом со счета покупателя в банке снимается некая сумма денег (эквивалент стоимости товара) и зачисляется на счет продавца. Это и есть транзакция, которую в данном случае проводит банк.



То же самое происходит, если вы переводите деньги другому лицу при помощи банковского перевода или с использованием платежной (кредитной или дебетовой) банковской карты. Как правило, банки берут за такие услуги **комиссионное вознаграждение**.

Любая денежная транзакция – это информация о том, кто и кому, когда и сколько передал денежных единиц. Банки ведут учет всех транзакций в больших бухгалтерских книгах, которые еще называются **регистрами** (***ledger***).

При этом после каждой транзакции **балансы** (суммы денежных средств на счетах) покупателя и продавца изменяются соответственно передаваемой сумме денег (эквивалента стоимости товара) с учетом комиссионных вознаграждений банка – у покупателя баланс уменьшается, а у продавца увеличивается.

Ведение учета транзакций и балансов клиентских счетов позволяет банкам избежать ситуации, которая получила название **«проблема двойных трат»** или **«двойного расходования»** – когда одни и те же деньги на банковском счете участвуют в нескольких транзакциях.

Подытожим вышесказанное. Любая денежно-финансовая система основывается на таких основных составляющих:

1. **Денежная масса** – количество учтённых денег, находящихся в обороте. Деньги выпускает государство в результате эмиссии, а попросту – печатает банкноты и чеканит монеты.

2. **Транзакции** – денежные переводы. Транзакции проводят доверенные финансовые учреждения – банки по распоряжению своих клиентов. Учет транзакций позволяет избежать «проблемы двойных трат».

3. **Владение деньгами**. Банки ведут учет балансов счетов своих клиентов. Распоряжаться деньгами на своих банковских счетах могут только сами клиенты, банки лишь выполняют их

распоряжения о переводе. При этом банки обязаны проверять личность владельца счета. Контроль за этим ведет государство в лице своих институтов и органов (центробанки).

Все эти составляющие **регулируются государством** при помощи законодательных актов.

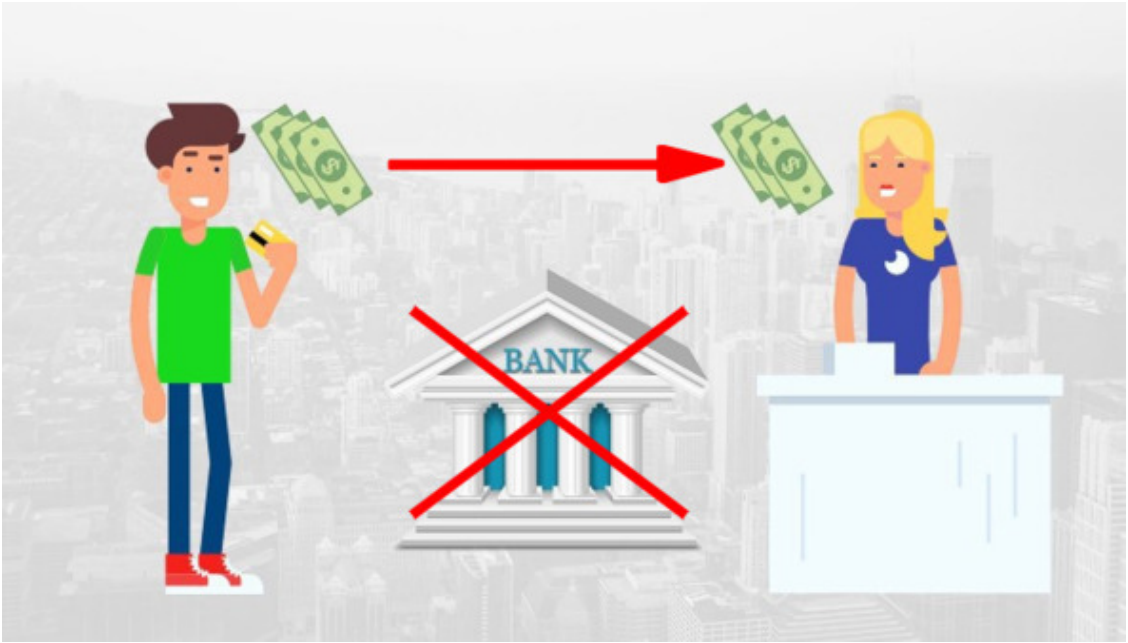
Длительное время люди пытались найти способ передачи денег на расстоянии без участия третьей доверенной стороны – банка. Ведь это было бы очень **удобно**, – как в наличных расчетах. И **дешево**, – не пришлось бы платить банку комиссионные вознаграждения. А также **надежно**, – не было бы риска потерять свои деньги, хранящиеся в банке, в случае его банкротства.

Было сделано много попыток создать т.н. **электронные деньги**, которые бы обходились без посредников, но все они были неудачными или несовершенными.

Но, наконец-то, **31 октября 2008 года** некий **Сатоши Накамото** опубликовал концепцию новой электронной денежной системы, названной им **«Биткоином»**, в которой операции (транзакции) производятся непосредственно между участниками без привлечения третьей доверенной стороны.

А **3 января 2009 года** эта система была запущена и начала работу. С тех пор наличные расчеты стали доступными всем в электронном виде.

По замыслу создателя, **Биткоин должен был стать альтернативой нынешней финансовой системе**, в которой господствуют банки, выступающие посредниками в денежных переводах и платежах между двумя субъектами.



В основе этой инновационной денежной системы была технология **публичного блокчейна**.

Что же это такое?

Собственно, сам **блокчейн – это база данных**, состоящая из последовательных блоков информации, которые связаны между собой таким образом, что изменив информацию в одном

блоке, она изменится во всех последующих. Попросту, блокчейн – это очень **защищенная база данных на основе криптографии**.

В блокчейн Биткоина записываются все транзакции. Таким образом, этот блокчейн представляет собой гигантскую **бухгалтерскую книгу – регистр**, наподобие тех, что ведут банки, для записи транзакций своих клиентов.

Условно можно представить, что каждый отдельный лист этой книги – это блок информации с записью транзакций. Примерно каждые 10 минут к этой книге добавляется новый лист (блок) с новыми транзакциями. При этом у каждого листа кроме транзакций есть служебная информация, в которой записана некая **«контрольная сумма»**, называемая **хэшем**, предыдущего листа (блока).

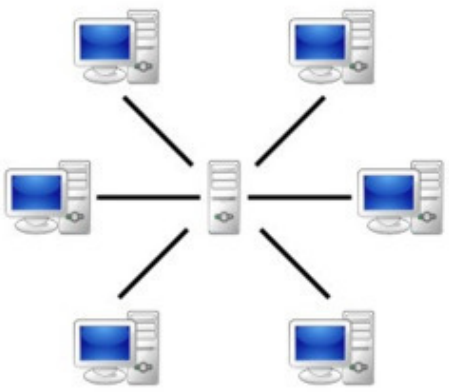
Если кто-либо попробует изменить хоть один символ в любом листе (блоке) этой книги, то «контрольная сумма» этого листа также изменится и не будет соответствовать той, которая записана в служебное поле на следующем листе, что повлечет изменение и его «контрольной суммы» и т. д. по всем последующим листам книги вплоть до последнего.

Таким образом обеспечивается защита информации в блокчейне от изменений. Записанную в блокчейн информацию **изменить невозможно** без нарушения целостности (связанности) блоков блокчейна. Это очень важный момент!

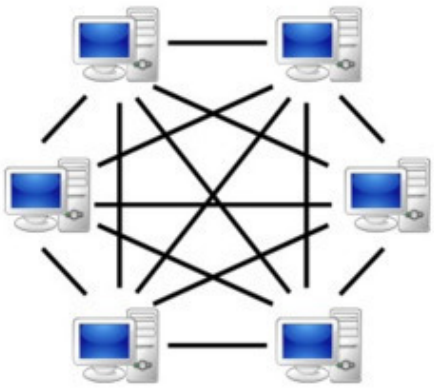
Но где хранится эта база данных – блокчейн? Как обеспечить её безопасное хранение?

Она хранится на множестве компьютеров, подключенных к сети Биткоина! Поэтому блокчейн Биткоина называется **публичным** – любой человек может подключиться к этой сети и скачать на свой компьютер блокчейн – полную бухгалтерскую книгу Биткоина.

Эта сеть является **распределенной** и **одноранговой** (peer-to-peer). Последнее означает, что в этой сети все узлы (компьютеры, серверы) равны и нет центральных управляющих серверов.



Серверная структура



Одноранговая (P2P) сеть

Таким образом, регистр Биткоина, он же блокчейн, одновременно хранится в одноранговой сети на тысячах компьютерах (серверах) во всем мире – от США до Японии и Австралии. Тысячи синхронизированных сетью одинаковых баз данных!

Этим обеспечивается его полная безопасность от внешнего воздействия. В отличие от банковских серверов, на которых хранятся транзакции клиентов банка, блокчейн Биткоина неуязвим, он не имеет единого центра управления и отказа.

Именно поэтому блокчейн еще называют **финансовым интернетом** – сетью, неуязвимой от внешних атак.

Как же работает эта сеть? Любой, кто хочет к ней подключиться, получает т.н. **биткоин-адрес** – это своеобразный аналог банковского счета. Одновременно с адресом клиент получает привязанный к этому адресу секретный **приватный ключ** – короткую последовательность символов, при помощи которой система идентифицирует владельца биткоин-адреса и позволяет ему совершать транзакции (денежные переводы). Подобрать к биткоин-адресу приватный ключ практически невозможно. Поэтому доступ к каждому биткоин-адресу защищен на уровне приватного ключа.

После получения биткоин-адреса его владелец может сообщить этот адрес любому пользователю сети Биткоин с тем, чтобы получить от него биткоин-перевод – платеж в **биткоинах – внутренней расчетной единице** (криптовалюте) сети Биткоин.

.

> **Примечание:** Здесь и далее используется слово **«биткоин»** (со строчной буквы) для обозначения внутренней расчетной единицы сети **«Биткоин»** (с прописной буквы).

Это аналогично тому, как клиент банка получает платеж на свой банковский счет, сообщив его номер другому клиенту банка.

Чтобы совершить перевод со своего биткоин-адреса на любой другой, владелец отправляет в сеть Биткоина **распоряжение** с указанием суммы перевода и биткоин-адреса получателя, подписанное с использованием своего приватного ключа.

Все поступившие в сеть Биткоина распоряжения о переводах программно проверяются серверами в сети, которые называются **«майнеры»**. В ходе проверки каждым майнером контролируется наличие достаточной для проведения перевода суммы денег на биткоин-адресе отправителя и формируется транзакция – запись о переводе.

Из множества транзакций формируется **блок** информации для добавления в блокчейн.

Но, поскольку майнеров много, кто из них будет записывать блок в блокчейн? Для этого Сатоши Накамото придумал хитроумный алгоритм – блок запишет тот майнер, который первым решит сложную криптографическую задачу, смысл которой состоит в поиске (методом подбора) некого числа, особым образом связанного с «контрольной суммой» сформированного майнером блока. Этот процесс называется **«майнинг»**.

Несмотря на то, что задача трудная, проверка правильности её решения выполняется быстро. Что и делают остальные майнеры после того, как ответ найден.

Поскольку майнеры несут затраты на оборудование и электроэнергию, протоколом (правилами) Биткоина предусмотрено вознаграждение в виде новых единиц (монет), поступающих в сеть в ходе **эмиссии**. Это вознаграждение получает только тот майнер, который записал блок в блокчейн, т.е. первым решил криптографическую задачу.

Майнинг – это необходимый и важный процесс в сети Биткоина, в результате которого решаются задачи:

1. Запись нового блока транзакций в блокчейн.

2. Выпуск новых монет биткоина (эмиссия).
3. Сетевое вознаграждение участникам сети (майнерам) за обработку транзакций и формирование нового блока.
4. Поверка транзакций и защита от «двойного расходования» – ситуации, при которой делается несколько транзакций, использующих одну и ту же исходную сумму.
5, Защита от т.н. **«атаки 51%»**, делающая экономически нецелесообразными попытки взлома и контроля денежной сети.

Последнее очень важно! Дело в том, что в Биткоине все решается **консенсусом** – принятием большинства узлов сети. Для того, чтобы злоумышленнику получить большинство (51%) мощности сети Биткоина, он должен затратить невероятно большие деньги – на момент написания этой книги (по состоянию на 14 октября 2018 года) это более **$9,3 млрд**[1]. И все это из-за высокой затратности майнинга.

Но как **расчетная единица** сети Биткоина, называемая также биткоин (со строчной буквы), имеющая биржевый тикер **BTC**, становится деньгами, средством, передающим стоимость?

Мы привыкли, что деньги выпускает государство. Именно ему принадлежит монополия на печать банкнот и чеканку монет. А по сути, **деньги – это товар**, только обладающий некоторыми уникальными свойствами:

– их **ограниченное количество** (эмиссия ограничена);
– их **трудно подделать** или воспроизвести;
– они **однородны и делимы**: первое означает, что денежные единицы не должны отличаться друг от друга, а второе – что деньги должны легко делиться, чтобы ими можно было заплатить любую сумму;
– они **хорошо сохраняются** (не портятся, не теряют вес и т.п.), т.е. остаются **неизменными**;
– они достаточно **компактны** (при высокой стоимости) и могут легко транспортироваться, т.е. **мобильны**;
– они имеют **внутреннюю стоимость** (полезность, значимость).

Биткоин обладает всеми вышеперечисленными свойствами:

– его **эмиссия ограничена** 21 миллионом единиц.
– его практически **невозможно подделать** (провести фальшивую транзакцию).
– он **делим до 100-миллионной части**, называемой **сатоши**. В отличие от доллара, который делится только до сотой части – цента, и других валют.
– он хранится в виде электронных записей на тысячах серверов по всему миру, т.е. **неизменен и фактически вечен**.
– может быть передан **на любое расстояние** с очень **высокой скоростью**.

[1] По данным сайта Gobitcoin.io

– обладает **высокой полезностью** – способностью быстро, надежно и относительно дешево передавать стоимость на большие расстояния без участия третьей доверенной стороны.

Кроме того, Биткоин:

– не связан с государствами и правительствами. Не несет рисков кризиса экономик и изменения законодательств.
– не имеет единого центра управления и регулирования, а также отказа.
– обеспечивает высокую защиту и анонимность

Мы видим, что биткоин, как валюта, обладает лучшими свойствами денег, чем все существующие фиатные валюты, выпускаемые государствами, а также золото и другие ценные металлы.

Именно поэтому он стал востребован и его рыночная цена стала расти.

Подводя итоги можно сказать, что Биткоин – это совокупность компонентов, которая включает:

– одноранговую компьютерную сеть, которую никто не может контролировать или отключить;

– распределенную бухгалтерскую книгу (distributed ledger) в виде защищенного **публичного блокчейна**, хранящегося на тысячах серверов в одноранговой сети;

– собственную расчетную единицу (криптовалюта ***биткоин***), выпуск (эмиссия) которой ограничен и контролируется программным протоколом.

– криптоэкономический дизайн механизмов[2] – сочетание криптографии и экономических стимулов.

Биткоин не контролируется и не может контролироваться ни отдельным лицом или группой лиц, ни корпорацией или компанией, ни правительством или центробанком.

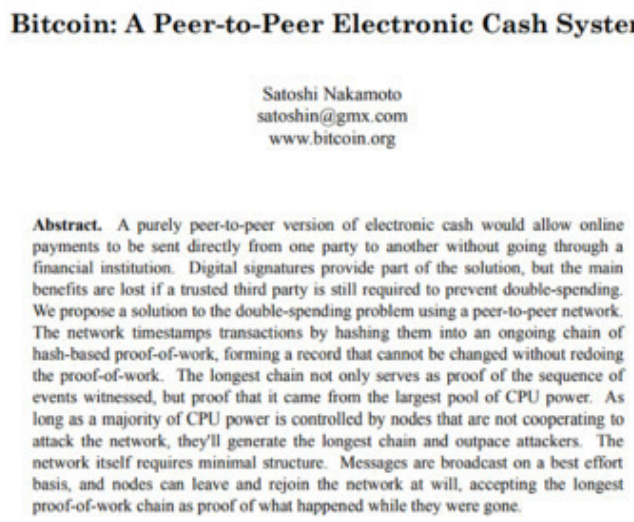
Биткоин – это альтернативная государственным денежная система.

Вы можете возразить, что биткоин ничем не обеспечен, а также спросить: **«Кем управляется Биткоин?»**. Ответы на возражения и вопросы читайте в разделе **«Биткоин: Мифы и предрассудки»**.

А пока я вам расскажу краткую историю возникновения Биткоина.

[2] **Дизайн механизмов** – в экономике – подход, создающий механизм взаимодействия, при котором действия отдельных экономических субъектов приводят к оптимальному решению для всей системы.

Genesis: Как появился Биткоин
Краткая история зарождения первой массовой криптовалюты



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Первая страница доклада Сатоши Накамото о Биткоине (фрагмент).

31 октября 2008 года несколько сотен энтузиастов и специалистов по криптографии, включенных в закрытый список e-mail рассылки (**The Cryptography Mailing list**[3]), получили письмо, подписанное неким **Сатоши Накамото** (***Satoshi Nakamoto***). В нём он сообщил, что работает над созданием новой электронной системы денежных расчетов, в которой операции производятся непосредственно между участниками без привлечения третьей доверенной стороны.

В письме содержалась ссылка на короткий текст (9 страниц) доклада под названием **Bitcoin: A Peer-to-Peer Electronic Cash System** («Биткоин: Одноранговая электронная денежная система»), в котором в строгом академическом стиле, кратко, но ясно, со схемами и формулами описывалась технология новой денежной системы, названная автором **Биткоином (*Bitcoin*)**.

До сих пор неизвестна личность человека (или группы людей?), который скрывается под псевдонимом **Сатоши Накамото**.

.

Японское имя Сатоси (именно так звучит по-японски ***Satoshi***) означает **«ясно мыслящий, мудрый, сообразительный»**. Слово ***naka*** переводится с японского как «в, внутри», а ***moto*** **–** «начало, основание, базис».

То есть Сатоси (Сатоши) Накамото можно перевести с японского как **«ясно мыслящий в основании (чего-то)»**, проникающий в суть вещей.

В то же время, имя Сатоси Накамото записывается по-японски тремя иероглифами – **###**

Здесь **#** – собственно имя Сатоси (Сатоши).

[3] В настоящее время рассылка хранится на сайте www.metzdowd.com

А **##** – переводится как «в книге».

Т. е. Сатоси (Сатоши) Накамото можно также перевести с японского как **«ясно мыслящий в книге»** (знаток, мудрец).

В одном из постов на форуме криптологов Сатоши Накамото сообщил, что начал работать над концепцией Биткоина в **2007 году**.

А 15 августа 2008 года Патентное бюро США зарегистрировало заявку на патент **20100042841 A1** под названием **Updating and Distributing Encryption Keys** (*Обновления и распространения ключей шифрования*), в которой описывается криптографический алгоритм, во многом схожий с принципами, на которых строится технология Bitcoin.

Примечательно, что в этой заявке используется редкая фраза ***«computationally impractical to reverse»***, которая встречается только в вышеуказанном докладе Сатоши Накамото.

Авторами заявки были **Нил Кинг** (*Neal King*), **Владимир Оксман** (*Vladimir Oksman*) и **Чарльз Брай** (*Charles Bry*). Они также являются авторами ещё нескольких патентов, связанных с криптографией и близких к технологии Bitcoin.

Однако, все трое опровергают свою причастность к созданию Bitcoin и связь с Сатоши Накамото.

Личность человека, создавшего Биткоин, пытались установить многие, но пока безрезультатно.

Например, 6 марта 2014 года американский журнал **Newsweek** опубликовал в качестве темы номера расследование американской журналистки **Лии Гудман** (*Leah McGrath Goodman*) под названием The face behind Bitcoin (*«Лицо Биткоина»*), в котором она утверждает, что этим человеком является **Дориан Прентис Сатоси Накамото** (*Dorian Prentice Satoshi Nakamoto*) – 64-летний американец японского происхождения.

Однако, сам Дориан буквально на следующий день после публикации выступил в прессе с опровержением своей причастности к Биткоину и его создателю.

Дориан Сатоши Накамото (Dorian Prentice Satoshi Nakamoto). Фото: AP.

Другой исследователь личности Накамото – **Скай Грей** (*Skye Grey*) в своей статье Occam's Razor: who is most likely to be Satoshi Nakamoto? (*«Бритва Оккама: кто более всего похож на Сатоши Накамото?»*) привел много улик, указывающих на то, что создателем Биткоина может быть **Ник Сабо** (*Nick Szabo*) – криптолог и ученый-правовед, известный своими исследованиями в области истории денег и умных контрактов. Кстати, первые идеи умных контрактов (*smart-contracts*) были предложены Сабо еще 1994 году.

С 1998 года Ник Сабо разрабатывает механизм, позволяющий децентрализовать цифровую валюту. А созданная им система **Bit Gold** является прямым предшественником архитектуры биткоина.

Но и Сабо открестился от участия в создании Биткоина.

Ник Сабо (Nick Szabo)

Поиски мифической личности – создателя первой массовой криптовалюты, – безусловно, будут продолжаться и далее. И не только потому, что всем интересно узнать истинное лицо создателя революционной технологии, которая изменяет мир.

По оценкам известного криптографа **Серхио Лернера** (*Sergio Demian Lerner*) – одного из соавторов технологии оптимизации майнинга **ASICboost**, количество биткоинов, которое лично намайнил Сатоши Накамото составляет порядка **1 млн монет**, что соответствует по текущему курсу (на момент написания этой книги) примерно **$6,5 млрд**.

По сути, каждый 17-й биткоин в сети Биткоина находится в руках у его создателя и при желании Сатоши может обрушить криптовалюту так же стремительно, как и вывел её на мировой рынок.

Доверие – краеугольный камень любой финансовой (денежной) системы, а таинственность настораживает, когда речь идет о деньгах.

Но, вернемся к истории…

18 августа 2008 года, через три дня после подачи вышеупомянутой патентной заявки, был зарегистрирован домен **bitcoin.org**.

Этот домен был зарегистрирован на сайте **anonymousspeech.com**, который позволяет пользователям анонимно регистрировать доменные имена.

Впоследствии Сатоши Накамото утверждал, что выкупил этот домен. Но не сообщил, у кого.

Через 9 дней после обнародования доклада Сатоши Накамото о Биткоине, **9 ноября 2008** года проект Bitcoin был зарегистрирован на ресурсе **SourceForge.net** – сайте, ориентированном на разработку и распространение программного обеспечения с открытым кодом (**Open Source Software**).

В своем докладе, который, кстати, был опубликован на вышеупомянутом домене bitcoin.org, Накамото предложил новую технологию децентрализованного оборота цифровой наличности, которая состояла из двух составляющих.

Одним из компонентов Биткоина стал разработанный его создателем инновационный **блокчейн** – распределенный реестр, состоящий из цепочки блоков финансовых транзакций, в которой каждый последующий блок был криптографически связан с предыдущим. Поэтому, любая правка уже внесенной информации о транзакциях была невозможна. Этим достигалась неизменность всех транзакций в реестре и его защищенность от попыток кражи или двойного использования денег.

Второй компонент представлял собой криптографический алгоритм **майнинга** («добычи») биткоинов, который определял механизм вознаграждения участников сети за то, чтобы они выделяли достаточно ресурсов (вычислительной мощности и электроэнергии) для поддержания работоспособности блокчейна.

Но, большинство получателей письма со ссылкой на доклад Накамото отнеслись к нему скептически, а некоторые подписчики рассылки подвергли критике новую технологию. Одни писали, что электроэнергия, необходимая для майнинга биткоина, обойдется дороже, чем будет стоимость новой криптовалюты. Другие указывали, что правительства ни одной из ведущих стран мира не позволят биткоину функционировать в крупных масштабах. Третьи вообще считали, что идея оборота денег без участия доверенного посредника (банков) утопична, поскольку ранее неоднократно делались попытки её реализации и все они были безуспешны.

Также негативную роль сыграло то, что никто из получателей письма не знал, кто такой Накамото. Тут следует заметить, что подписчиками закрытой e-mail рассылки, в которой был обнародован доклад Накамото, были членами сообщества шифропанков и криптологов. Они придавали большое значение анонимности, но друг друга более-менее знали.

В онлайновых сообществах, как и в реальном мире, репутация каждого участника зависит от степени его вовлеченности в общую деятельность. А до октября 2008 года никто ничего не слышал о Сатоши Накамото – он внезапно появился ниоткуда.

Криптографы и шифропанки повидали достаточно «великих проектов» от малограмотных новичков, так что их скептическая реакция была предсказуемой.

Понимая, что сетевую технологию, каковым является Биткоин, невозможно продвинуть без поддержки и участия сообщества, Накамото прибег к маркетинговому приему.

«Может, имеет смысл приобрести немного монет (биткоина) на случай, если проект будет успешным», – посоветовал он одному скептически настроенному оппоненту на форуме криптологов.

Эти слова оказались пророческими!

Как бы то ни было, но раскрутку Биткоина надо было с чего-то начинать и Накамото стал первым его пользователем.

3 января 2009 года Сатоши Накамото запустил написанную им же программу для майнинга биткоина.

Первый блок с 50 монетами биткоина был добыт в **18:15:05** по Гринвичу. На самом деле первый блок имел **№0** и получил название **Genesis** (зарождение, возникновение).

В параметр **coinbase**[4] блока **Genesis** Сатоши Накамото вместе с обычными данными записал загадочную фразу:

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

The Times от 3 января 2009: «Канцлер на грани второй помощи банкам»

Это заголовок статьи с первой страницы британской газеты **The Times** от **3 января 2009 года**.

Речь в ней идет о планируемой финансовой помощи британским банкам со стороны Казначейства Её Величества (*Her Majesty's Treasury*). **Канцлер** – это Канцлер казначейства Великобритании (*The Chancellor of the Exchequer*) – официальное наименование министерской должности в Кабинете министров Великобритании, ответственной за экономические и финансовые вопросы.

Что хотел этим сказать Сатоши Накамото? Об уязвимости банковской системы и её зависимости от государства? Или он просто хотел показать, что первый блок Биткоина записан в блокчейн не ранее этой даты? Скорее всего – и то, и другое.

[4] **Coinbase** – это содержимое Входа (Input) транзакции генерации. В то время, как обычные транзакции используют Входы для ссылки на свои родительские транзакции, транзакция генерации не имеет родителя.

THE TIMES

Max 5C, min -5C

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salman Rushdie I won't marry again

Pages 22, 23

Giant killing? Guide to the FA Cup third round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the hoof" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1969 levels

Business, page 47

Первая страница газеты The Times от 3 января 2009 года.

Целую неделю Накамото держал свой компьютер включенным и в одиночку майнил биткоины, паралельно отлаживая компьютерную программу.

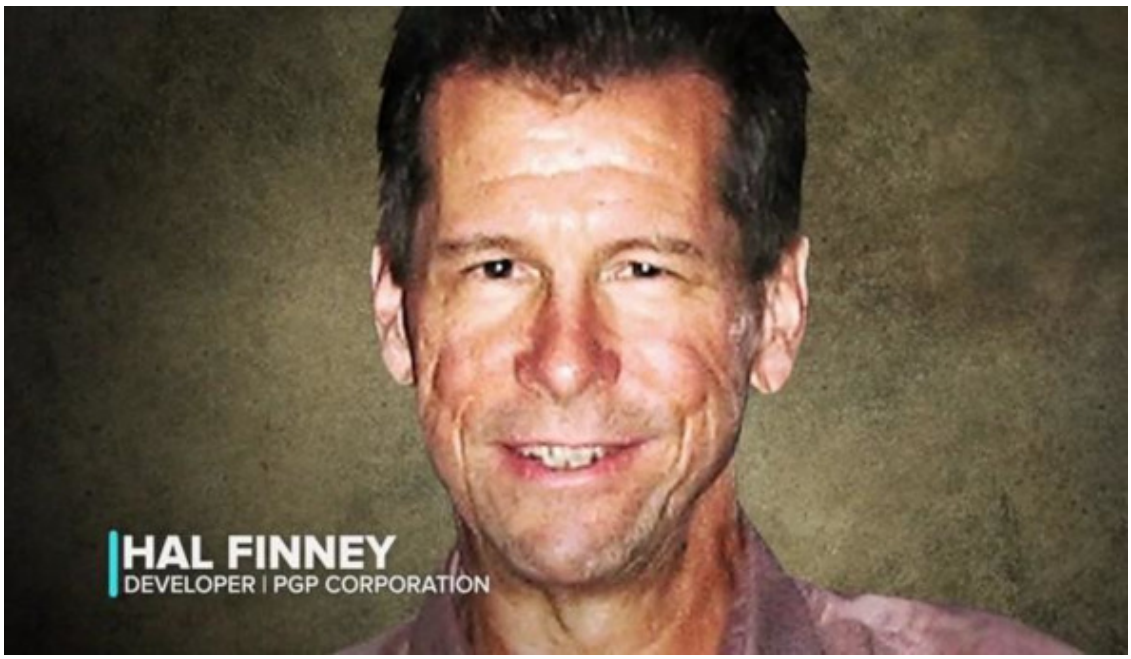
9 января 2009 года Накмото публикует на сайте **bitcoin.org** первый релиз своей программы-клиента[5] **Bitcoin Core** version 0.1, при помощи которой можно не только добывать

[5] **Программа-клиент** взаимодействует с сервером, используя протокол Биткоина. Все узлы в сети Биткоин одновременно являются серверами и клиентами. Они обмениваются информацией между собой, используя программу-клиент.

биткоины, но и осуществлять переводы между биткоин-адресами в сети (отправлять и получать монеты).

Мы никогда не узнаем, как бы в дальнейшем сложилась судьба детища Накамото, если бы не один человек, у которого 9-страничный доклад о Биткоине вызвал прилив энтузиазма.

Этим человеком был американский программист **Хэл Финни** (*Hal Finney*), известный также как **Гарольд Томас Финни II**.



Хэл Финни (Hal Finney)

На тот момент 33-летний Финни был ведущим разработчиком **PGP** (*Pretty Good Privacy* – «На редкость надежная приватность») – системы шифрования с открытым ключом для электронной почты, созданной легендарным криптологом **Филиппом Циммерманом** (*Philip R. Zimmermann*).

Финни также считают автором многих криптографических инноваций, включая анонимные почтовые серверы, позволяющие отправлять электронную почту без раскрытия личности отправителя.

Он также был известным участником движения **шифропанков** – сообщества людей, интересующихся криптографией и сохранением анонимности.

Шифропанки выступают против тотального вмешательства государства в лице его правительства и спецслужб в личную жизнь граждан. Они рассматривают криптографию, как инструмент защиты неприкосновенности личной жизни, а также передачи власти от бюрократизированных централизованных учреждений непосредственно гражданам.

Среди известных шифропанков были такие личности, как уже упоминавшийся выше **Филипп Циммерман**, а также основатель WikiLeaks[6] **Джулиан Ассанж** (*Julian Paul Assange*).

[6] **WikiLeaks** (от ***wiki*** – сокращенно от Wikipedia и ***leak*** – «утечка») – международная некоммерческая организация, которая публикует секретную, как правило государственную, информацию, взятую из анонимных источников или при утечке данной информации.

Хэл Финни давно интересовался криптографическими схемами платежей. Он был лично знаком с Ником Сабо и даже делал попытку создания собственной валюты, основанной на алгоритме доказательства проделанной работы, под названием **PoW**, изобретенного в 1997 году британским криптологом **Адамом Беком** (*Adam Back*).

Поэтому Финни нашел проект Накамото весьма интересным и даже написал ему электронное письмо по указанному в докладе адресу (**satoshin@gmx.com**). Так завязалась их переписка. И неудивительно, что Финни стал вторым (после Накамото) пользователем Биткоина.

В субботу, **10 января 2009 года**, в семье Финни был праздник – день рождения сына. Но Хэл с утра уединился в своем кабинете, запустил свой настольный IBM ThinkCentre и кликнул по ссылке на сайте bitcoin.org, которую он получил накануне от Накамото.

При первом запуске программа Накамото сгенерировала для Хэла биткоин-адрес и приватный ключ к нему. Но дальше она дала сбой. Проанализировав файлы журналов работы программы, Финни написал Накамото письмо, в котором указал, что произошло и как это исправить. В дальнейшем они постоянно обменивались электронными сообщениями, стремясь доработать протокол Биткоина и отладить его работоспособность.

Вечером того же дня, после нескольких неудачных попыток Хэлу Финни все же удалось вторым после Накамото сгенерировать блок данных и получить 50 монет на свой биткоин-адрес. Это был блок под номером 78. А в сети Биткоина появился узел (node) №2.

Ободренный этим успехом, Хэл написал поздравительное письмо Сатоши Накамото, текст которого также направил в группу подписчиков рассылки, где 31 октября 2008 года Накамото обнародовал свой проект новых цифровых денег.

> ***«Представьте, что Биткоин станет главной платежной системой в мире***, – писал Финни, – ***тогда его суммарная стоимость сравняется со всеми богатствами в мире»***.

По подсчетам Хэла, в этом случае стоимость одного биткоина будет около $10 млн.

> ***«Даже если вероятность этого события будет всего лишь 1 к 100 млн, стоит подумать!»***, – закончил свое послание известный криптолог.

12 января 2009 года Сатоши Накамото в качестве тестовой операции перевел на биткоин-адрес Хэла Финни 10 биткоинов. Это была **первая транзакция** между двумя адресами в сети Биткоина. Она была записана в блок **№170**.

Таким образом, Хэл Финни стал первым человеком в истории, который получил денежный перевод в биткоинах.

Первые недели после запуска Биткоина пользователи не спешили присоединяться к его сети. Поэтому Накамото, чтобы поддерживать сеть, использовал собственные компьютеры.

Он также всеми способами популяризировал Биткоин и старался оперативно отвечать всем на вопросы о своем проекте.

Хэл Финни также всячески поддерживал детище Накамото.

> ***«В пользу Биткоина говорит то, что он распределен и не имеет единой точки сбоя, он децентрализован и не принадлежит никакой компании»***, – отвечал Финни на вопрос одного из многочисленных скептиков.

Но со временем и Финни стал терять энтузиазм. Его стал раздражать шум постоянно работающего компьютера, на котором велся майнинг биткоинов. Потом он вовсе отключил функцию майнинга, опасаясь быстрого износа компьютера.

Впоследствии, когда у биткоина появилась реальная стоимость, Финни жалел об этом. В **марте 2013 года** стоимость «добытых» им ранее монет, а их оказалось около 1000, составила почти **$60 тыс**.

> ***«Я немного пожалел, что прекратил майнинг, тем не менее, мне невероятно повезло присутствовать при рождении биткоина»***, – писал в то время Финни.

К сожалению, окончательно Финни выбила неизлечимая болезнь. В августе 2009-го врачи поставили ему диагноз «боковой амиотрофический склероз» (БАС), также называемый болезнью Лу Герига, по имени известного бейсболиста, страдавшего ею.

В конце-концов, Хэл Финни покинул уже начавшее формироваться биткоин-сообщество.

А 28 августа 2014 года Хэл Финни умер. Но без него, возможно, Биткоин так бы и не состоялся.

Как бы то ни было, уход Хэла Финни из сети Биткоин не оказал негативного влияния на развитие криптовалюты, поскольку уже появились лица, заинтересованные в её продвижении и видевшие большие перспективы.

Одним из них был финский студент **Марти Малми** (*Martti Malmi*).

«Мне хотелось бы помочь с биткоином, если я могу быть чем-либо полезен», – написал он Накамото в начале мая 2009 года.

К тому времени уже зарождалось понимание, что предложенная Накамото альтернативная денежная система, основанная на надежном и стойком к внешним атакам алгоритме, заслуживает большего доверия, чем склонные к ошибкам и мошенничеству люди, управляющие крупными организациями, в сердце традиционной денежной системы.

Тут следует отметить, что всего лишь за полтора месяца до обнародования Накамото концепции электронной криптовалюты произошло важное событие на финансовом рынке США – банкротство инвестиционного банка **Lehman Brothers**, – одного из крупнейших в мире. Мировой финансовый кризис перешел в свою острую фазу.

На Уолл-стрит настроения были близки к паническим – ведущие американские финансисты готовились к полному параличу самой мощной финансовой системы в мире, доверие к банкам было подорвано. Некоторые опасались что завтра американские банки вообще не откроются.

Как уже отмечалось выше, доверие – краеугольный камень любой финансовой (денежной) системы.

В условиях продолжения финансового кризиса, появление Биткоина, как независимой от государств и правительств денежной системы, которая продемонстрировала свою работоспособность благодаря настойчивости Накамото и энтузиазму Финни, вызвало растущий интерес не только в среде программистов и криптологов.

Марти Малми (Martti Malmi)

Одним из новых евангелистов Биткоина и стал Марти Малми. В то время он был студентом Хельсинкского политеха и впервые узнал о Биткоине весной 2009 года.

Прежде чем написать письмо Накамото, Малми оставил несколько сообщений о Биткоине на сайте **anti-state.org**. В одном из них он писал:

> ***«Широкое распространение систем, подобных Биткоину, может подорвать способность государства эксплуатировать граждан»***.

Ранее Сатоши Накамото, Хэл Финни и другие касались только технической стороны работы системы. Но постепенно Накамото пришел к пониманию, что для продвижения своего проекта нужно уделять внимание идеологической мотивации.

> ***«Главный недостаток традиционных денег состоит в том, что они нуждаются в доверии, – мы должны верить в честность центробанков, но история полна примеров, когда банки подрывали это доверие, обесценивая фиатные деньги»***, – писал Сатоши.

В Марти Малми он увидел человека, который способен продвинуть идею децентрализованных цифровых денег в массы. Он предложил Марти попробовать себя в качестве копирайтера и писать статьи на официальный сайт Биткоина – **bitcoin.org**.

С этой задачей Малми прекрасно справился. Он подготовил вводную статью о Биткоине, в которой объяснял, что это такое и давал ответы на различные вопросы, типа: **«Безопасен ли Биткоин?»** или **«Почему следует использовать Биткоин?»**.

> ***«Защититесь от несправедливой монетарной политики центробанков-монополистов»,*** – писал он, отвечая на второй вопрос.

За несколько недель общения с Сатоши Накамото Марти коренным образом переделал весьма примитивный до этого сайт bitcoin.org.

Осенью 2009 года при непосредственном участии Малми был запущен **Биткоин-форум**, который привлек регулярных посетителей, ставших писать на нем свои сообщения.

Один из них, под ником **NewLibertyStandard**, высказал мысль, что неплохо бы создать биржу, на которой можно было бы продавать и покупать биткоины за фиатные деньги.

Марти Малми живо откликнулся на эту идею и отправил NewLibertyStandard 5050 биткоинов, за которые получил на свой счет в PayPal $5,02. Таким образом состоялась **первая сделка по обмену биткоинов**. Её курс был примерно 1000 биткоинов за 1 доллар.

Эта сделка породила дискуссии о том, как должен рассчитываться обменный курс биткоина к доллару. В результате, отправным пунктом для расчета курса послужила стоимость электроэнергии, потребляемой компьютером в процессе майнинга.

Вычислялся курс обмена по формуле: средняя электрическая мощность, потребляемая процессором в результате майнинга одного блока, умножалась на стоимость электроэнергии в США и делилась на число получаемых за блок биткоинов (в то время – 50 штук).

5 октября 2009 года на специально созданном для обмена сайте **New Liberty Standard**[7] был опубликован курс: **1309,03 биткоина за $1**.

Т.е. за 1 биткоин тогда давали около **0,08 цента**.

Однако, для Сатоши Накамото покупка за биткоины была важнее обмена его на фиатные валюты.

> ***«Было бы неплохо, если бы люди смогли начать использовать биткоин для чего-нибудь***, – писал Сатоши в письме Марти Малми в конце августа 2009 года. – ***Нам нужно найти какую-то сферу его применения»***.

Тем не менее, первая сделка по покупке за биткоины состоялась только в следующем, 2010 году.

Программист из Флориды **Ласло Ханеч** (*Laszlo Hanyecz*) ранее прославился тем, что первым написал программу, которая позволяла майнить биткоины при помощи графического процессора (GPU), что на порядок подняло вычислительную мощность майнинга.

В результате Ласло удалось намайнить 70 тысяч биткоинов, которые он решил потратить на что-то материальное и попросил на форуме доставить ему две пиццы, пообещав за них заплатить 10 тыс. биткоинов.

Не сразу нашлись желающие. Но все же, один человек из Калифорнии заказал за доллары пиццу из сети пиццерий **Papa John's** с тем, чтобы ее доставили Ласло.

22 мая 2010 года в дверь дома Ласло постучал курьер, который доставил ему пиццу, за которую Ханеч фактически заплатил **10 000 биткоинов** (по курсу на момент написания этой книги – **$65 млн**).

Ласло затем еще не раз заказывал пиццу, пока не закончились добытые майнингом монеты.

---

[7] К сожалению, сайт New Liberty Standard в настоящее время уже не работает, но первые курсы обмена до конца 2009 года можно посмотреть в архиве: **http://web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate**

После того, как Ласло опубликовал фотографии одного из своих заказов, Марти Малми написал: ***«Поздравляю, Ласло, это важный рубеж!»***.

Действительно, это была первая зафиксированная в истории сделка, в которой криптовалюта (биткоин) была обменена на товар.

Но вернемся в 2009 год…

Через неделю после обнародования первого обменного курса биткоина, 12 октября 2009 года, заработал чат-канал **#bitcoin-dev** в IRC[8], который в то время стал основным местом общения биткоин-сообщества.

Затем Малми взялся за программирование и изучив язык C++, на котором был написан код Биткоина, принял активное участие в его усовершенствовании.

Появившаяся **16 декабря 2009 года** новая версия **Bitcoin Core 0.2** была в значительной мере написана самим Малми. Так он стал, по сути, основным разработчиком кода Биткоина.

К концу 2009 года количество работающих майнинговых узлов в сети Биткоина стало таким, что пришлось впервые увеличить сложность решаемой криптографической задачи майнинга.

Это произошло **30 декабря 2009 года** при добавлении блока **№32256**. При этом сложность возросла с **1,0** до **1,18289953**.

Так состоялось рождение Биткоина, как распределенной и децентрализованной сети электронных денежных расчетов.

Хронология:

– 18 августа 2008 года – зарегистрирован домен **bitcoin.org**

– 31 октября 2008 года – Сатоши Накамото обнародовал доклад **Bitcoin: A Peer-to-Peer Electronic Cash System** («Биткоин: Одноранговая электронная денежная система»), в котором описывалась технология новой денежной системы.

– 9 ноября 2008 года – проект Bitcoin был зарегистрирован на сайте разработчиков **SourceForge.net**

– 3 января 2009 года – Сатоши Накамото сгенерировал первый блок Биткоина (**Genesis**) и получил на свой биткоин-адрес первые 50 монет. В первый блок был включен текст: **«The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.»**

– 9 января 2009 года – Сатоши Накамото опубликовал первый релиз программы **Bitcoin Core v.0.1.** в в списке рассылки **Cypherpunks**.

– 10 января 2009 года – в сети появился узел №2 Биткоина. Вторым пользователем Биткоина стал **Хэл Финни**. В этот же день он сгенерировал блок №78 и получил первые 50 монет на свой биткоин-адрес.

[8] **IRC** (*Internet Relay Chat*) – протокол прикладного уровня интернета для обмена сообщениями в режиме реального времени. Позволяет общаться через личные сообщения и обмениваться данными, в том числе файлами.

– 12 января 2009 года – первая в истории транзакция по переводу биткоина – Сатоши Накамото отправил на биткоин-адрес Хэла Финни 10 монет. Это зафиксировано в блоке **№170**.

– 5 октября 2009 года – на сайте **New Liberty Standard** опубликован первый обменный курс биткоина к доллару США.

– 12 октября 2009 года – заработал чат-канал **#bitcoin-dev** в IRC.

– 16 декабря 2009 года – вышла версия **Bitcoin Core 0.2.**

– 30 декабря 2009 года – впервые увеличена сложность майнинга.

Популярно об основах криптографии, используемой в протоколе Биткоина

В основе Биткоина лежит **криптография** – наука о методах обеспечения **конфиденциальности** (невозможности прочтения информации посторонним), **целостности данных** (невозможности незаметного изменения информации) и **аутентификации** (проверки подлинности авторства или иных свойств объекта).

Биткоин построен на трех основных криптографических технологиях – **хэшировании**, **асимметричной криптографии** и **электронной цифровой подписи (ЭЦП)**. Собственно, эти технологии лежат и в основе самой криптографии, позволяя обеспечивать конфиденциальность, целостность данных и аутентификацию.

Разумеется, для понимания работы Биткоина необходимо понимать, как же работают технологии, на которых он базируется. Я просто и наглядно расскажу об этом.

Хэширование: Просто и наглядно

Хэширование, или хэш-функция – одна из основных составляющих современной криптографии и протокола Биткоина.

Но, что это такое? Как наглядно представить сущность хэша?

Начнем с того, что хэширование – это особое преобразование любого массива информации, в результате которого получается его некое отображение, **образ** или **дайджест**, называемый **хэшем** (*hash*) – уникальная короткая символьная строка, которая присуща только этому массиву входящей информации.

Из этого следует, что для любого объема информации, будь-то одна буква или, например, роман Льва Толстого «Война и мир» (или даже всё Полное собрание сочинений этого автора) существует уникальный и неповторимый хэш – короткая символьная строка. Причем, если в той же «Войне и мире» изменить хотя бы один символ, добавить один лишь знак, – хэш изменится кардинально до неузнаваемости.

Как такое может быть? Целый многотомный роман и короткая строчка, которая отражает его!

В этом смысле хэш подобен **отпечатку пальца** человека или его **ДНК**[9]. Хотя последняя аналогия не полностью передает суть хэша[10].

[9] **ДНК** – Дезоксирибонуклеи́новая кислота́ – макромолекула, обеспечивающая хранение, передачу из поколения в поколение и реализацию генетической программы развития и функционирования живых организмов.

[10] Хэш-функция, в отличие от ДНК, необратима. Невозможно по хэшу восстановить исходный массив информации. В то же время, ДНК является носителем всей информации об организме.

Хэш подобен **отпечатку пальца** человека

Как известно, отпечаток пальца уникален и в природе не существует людей с одинаковыми отпечатками. Даже у близнецов отпечатки пальцев разные. Это же касается и структуры ДНК человека. Она уникальна! Нет людей с одинаковой структурой ДНК.

Но ведь ДНК, а тем более отпечаток пальцев – относительно короткие наборы информации. И, тем не менее, они являются неким кодом, присущим конкретному человеку. Можно считать, что это и есть «хэши» этого человека. С тем лишь отличием, что эти «хэши» не меняются с возрастом человека.

Итак, первое свойство хэша – его **уникальность**:

Каждому набору (массиву) информации присущ строго определенный, уникальный хэш.

Тем не менее, иногда встречаются т.н. **коллизии** – случаи, когда хеш-функция для разных входных блоков информации вычисляет одинаковые хэш-коды.

Математики-криптографы стараются создать такие хэш-функции, вероятность коллизий в которых стремилась бы к нулю.

Следует отметить, что функций, которые вычисляют хэш, существует множество. Но наиболее распространена (в частности, используется в протоколе блокчейна Биткоина) хэш-функция под названием **SHA-256** (от *Secure Hash Algorithm* – безопасный алгоритм хеширования). Эта хэш-функция формирует хэш в виде строки из **64 символов** (длина – **256 бит** или 32 байта).

Попробуем при помощи функции SHA-256 получить хэш для заголовка этой главы (**«Хэширование: Просто и наглядно»**).

Это будет:

ef3c82303f3896044125616982c715e7757d4cd1f84c…

Примечание: Здесь и далее с целью удобства представления на странице будем обрезать хэш до 44 символов, заканчивая троеточием.

А теперь изменим заголовок всего лишь на один символ – добавим знак восклицания в конце (**«Хэширование: Просто и наглядно!»**).

Получилось:

a6123e137d1d7f0aad800cdbc0918a65bb7a778a607c…

Как видите, изменение всего лишь на один знак исходного массива информации привело к кардинальному изменению его хэша!

И это второе важное свойство хэша:

– при самом незначительном изменении входной информации её **хэш меняется кардинально**.

Это свойство важно при использовании хэширования в цифровой подписи, так как позволяет удостовериться, что подписанная информация не была изменена во время её передачи по каналам связи.

Третье важное свойство хэша вытекает из того, что **хэш-функция необратима**. Другими словами:

> **– не существует обратной функции**, которая из хэша может восстановить исходный массив информации.

Из этого следует, что восстановить по хэшу соответствующий ему массив информации возможно только перебором всех возможных вариантов. Что практически невозможно, поскольку количество информации бесконечно!

Это свойство важно, поскольку делает взлом хэша (восстановление исходной информации по её хэшу) или невозможным, или весьма дорогостоящим занятием.

Еще одно важное свойство хэш-функций – это относительно высокая скорость работы.

Хэширование позволяет достаточно быстро вычислить искомый хэш из весьма большого массива входной информации.

Этим хэширование существенно отличается от **кодирования** (шифрования) и **декодирования** (дешифрования).

Хэширование или хэш-функция используется во многих алгоритмах и протоколах. В частности, в электронной цифровой подписи (ЭЦП) и **блокчейне**.

Шифрование с открытым ключом: Наглядная иллюстрация

Долгое время традиционная **криптография** использовала шифрование с тайным или **симметричным ключом** – один и тот же ключ использовался как для шифрования, так и для расшифровки (дешифрования) данных.

Наглядно это можно представить в виде **замка**, которым запирался сундук с тайным сообщением. Пара одинаковых ключей к этому замку была как у отправителя сообщения (**шифровальщика**), так и у получателя (**дешифровальщика**).

Разумеется, в действительности никто не отправлял сообщения в запертых сундуках. Тексты, которые надо было зашифровать, видоизменялись с использованием **тайного ключа** – последовательности символов, которая, смешиваясь с передаваемым сообщением особым образом (называемым **алгоритмом шифрования**), приводила к получению шифровки (**шифротекста**) – сообщения, которое невозможно было прочитать, не зная алгоритма и ключа.

Шифрование с симметричным ключом[11]

Но для наглядности процесса мы представим, что наше сообщение помещалось в некий прочный сундук и закрывалось надежным **навесным замком**, одинаковые ключи от которого были у обеих сторон – отправителя и получателя.

Вот этот ключ, которым запиралось (зашифровывалось) и открывалось (расшифровывалось) сообщение, назывался **тайным симметричным ключом**.

Проблема была в том, что при смене ключа (шифра) в целях безопасности, его необходимо было доставить получателю, который зачастую находился далеко и на враждебной территории. Передавать тайный ключ открытыми каналами связи было небезопасно.

Долгое время проблема безопасной передачи нового ключа (шифра) оставалась неразрешенной. Как правило, для этого использовали тайных курьеров, что не гарантировало на 100% того, что шифр (ключ) не попадет к нежелательным лицам, которые смогут им воспользоваться для дешифрования тайных сообщений.

[11] Рисунок из книги Филиппа Циммерманна «Введение в криптографию».

Проблема с ключами была решена только в 1975 году, когда **Уитфилд Диффи** (*Bailey Whitfield «Whit' Diffie*) и **Мартин Хеллман** (*Martin E. Hellman*) предложили концепцию шифрования с парой ключей: **открытым** (публичным – *public key*), который зашифровывает данные, и соответствующим ему **закрытым** (приватным – *private key*).

Эта система шифрования получила название **криптографии с открытым ключом** или **асимметричной криптографии**.

Работает эта система так:

1. Генерируется случайный **закрытый** (приватный) ключ (напомним, что ключ – это последовательность символов) и по определенному алгоритму подбирается к нему другой – **открытый** (публичный) ключ. При этом для любого закрытого ключа существует только один вариант открытого. Т.е. эти ключи (приватный и публичный) **всегда работают в паре** (связке).

2. Далее полученный открытый (публичный) ключ пересылается по любым открытым каналам связи отправителю тайного сообщения.

3. Получив открытый (публичный) ключ, отправитель при помощи него зашифровывает сообщение и отправляет его получателю, у которого есть соответствующий закрытый (приватный) ключ.

4. Получатель расшифровывает секретное сообщение, используя свой закрытый (приватный) ключ из пары с открытым (публичным), которым было зашифровано сообщение.

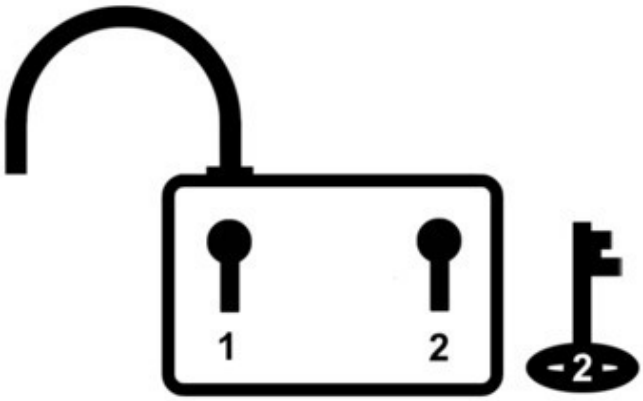
Следует отметить, что открытым (публичным) ключом **можно только зашифровать сообщение**, но расшифровать его уже этим ключом не получится. Для дешифрования нужен только закрытый (приватный) ключ из пары. Так работает алгоритм с асимметричным шифрованием.

Шифрование с асимметричным ключом

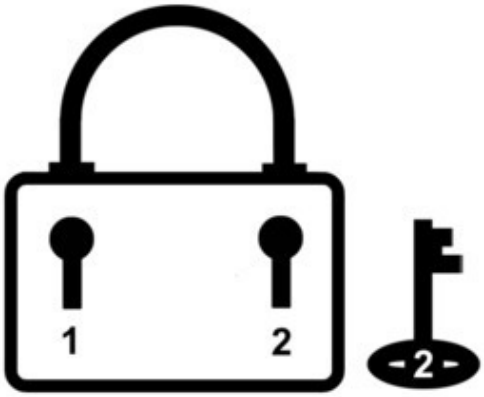
Но вернемся к нашему сундуку с сообщением. Как же теперь наглядно представить асимметричное шифрование? Как так можно – запирать одним ключом, а отпирать другим?

Представим себе **навесной замок с двумя замочными скважинами и двумя ключами** (см. рис. ниже) – левый ключ (1) через левую замочную скважину (1) может снимать фиксацию с левой половинки дуги замка, освобождая ее и открывая весь замок. Правый ключ (2) через правую замочную скважину (2) может фиксировать правую половинку дуги в замке, тем самым закрывая замок. Но после закрытия, этот ключ (2) не может уже освободить от фиксации правую часть дуги и тем самым открыть замок.

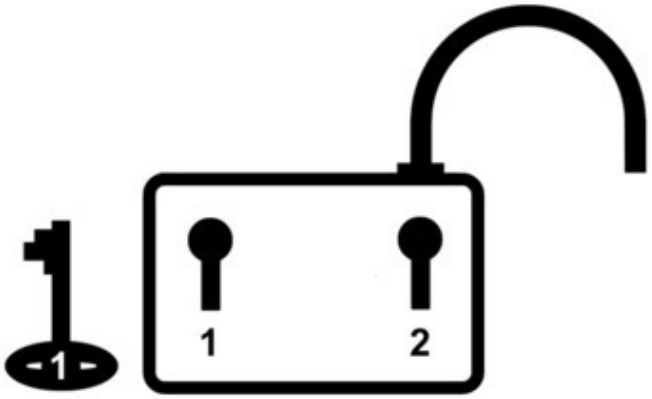
Первоначально замок с зафиксированной левой половинкой дуги (1) и расфиксированной правой (2), а также с ключом 2 (открытым) доставляется лицу, которое должно отправить тайное послание.



Получив замок и открытый ключ (2), отправитель навешивает его на сундук с тайным посланием и запирает его полученным ключом 2. Теперь сундук закрыт и даже отправитель не может его открыть, поскольку его ключ (2) может только зафиксировать правую часть дуги в замке, но не может освободить от фиксации.



Запертый замком сундук с тайным посланием отправляется получателю, у которого есть ключ (1), снимающий фиксацию левой половинки дуги и тем самым отпирающий замок. Но другие лица, даже если они будут иметь копию публичного ключа (2), открыть замок не смогут.



Получатель открывает замок ключом (1) и тайное послание прочитано!

Пользуясь терминологией асимметричной криптографии с открытым ключом, **ключ 1** – это закрытый (приватный) ключ, а **ключ 2** – это открытый (публичный) ключ.

В заключение отметим, что асимметричная криптография с открытым ключом получила широкое распространение не только в шифровании шпионских и дипломатических посланий. Асимметричную криптографию используют сайты с поддержкой протокола HTTPS[12], мессенджеры, Wi-Fi-роутеры, банковские системы и многое другое. На основе асимметричной криптографии базируется электронная подпись. Также на асимметричной криптографии построен алгоритм блокчейна, на котором, в свою очередь, построены все криптовалюты, включая Биткоин.

[12] **HTTPS** (*HyperText Transfer Protocol Secure*) – расширение веб-протокола HTTP для поддержки шифрования в целях повышения безопасности информации в WWW.

Электронная цифровая подпись: Просто и наглядно

Электронная цифровая подпись (ЭЦП) документа – это аналог обычной подписи, но возможности её гораздо шире.

Как работает ЭЦП? Как отправить по каналам связи (например, по электронной почте) заверенный и подписанный электронный документ? Попробуем разобраться…

С обычной бумажной почтой нет проблем – подписываете документ; заверяете его у нотариуса; отправляете заказным письмом. Всё! Ваш адресат, получив такое письмо, уверен, что документ подписан лично вами.

С электронной почтой (e-mail) так не получится. Конечно, можно отсканировать заверенный нотариусом документ и отправить его в виде файла, присоединенного к электронному письму. Но распечатка этого файла не будет легитимной.

Как же быть? На помощь приходит криптография!

Ранее в главе **«Шифрование с открытым ключом: Наглядная иллюстрация»** было рассказано об **асимметричном шифровании**, когда отправитель шифрует послание открытым (публичным) ключом, а получатель его расшифровывает соответствующим открытому закрытым (приватным) ключом.

У отправителя и получателя совершенно разные ключи, но они алгоритмически связаны – **открытым** (публичным) ключом можно только **зашифровать** (запереть) послание, а **закрытым** (приватным) – только **расшифровать** (отпереть).

Как это работает на примере с навесным замком с двумя замочными скважинами и двумя разными ключами было наглядно показано в вышеупомянутой главе.

А теперь представим ситуацию наоборот: отправитель зашифровывает (запирает) свое послание своим закрытым (приватным) ключом, а получатели могут расшифровать (отпереть) это послание соответствующим открытым (публичным) ключом, который они получили ранее от отправителя. Разумеется, эти ключи (приватный отправителя и публичный получателя) являются алгоритмически связанной парой – расшифровать послание можно только открытым ключом, который соответствует закрытому ключу отправителя.

Задача решена! Получатель по публичному ключу знает, что письмо отправлено конкретным отправителем, имеющим соответствующий приватный ключ.

Но в реальности нет необходимости зашифровывать само послание. Достаточно вычислить его **хэш-код** (см. главу **«Хэширование: Просто и наглядно»**), затем зашифровать этот хэш приватным ключом и присоединить к тексту сообщения. Вот этот зашифрованный хэш и есть **ЭЦП** – электронная цифровая подпись сообщения.

Получатель послания также вычисляет хэш-код сообщения и сравнивает его с расшифрованным публичным ключом ЭЦП. Если они совпадают, то всё нормально – письмо отправлено тем лицом, у которого есть соответствующий приватный ключ.

Но это еще не все! Использование хэширования послания позволяет также контролировать и его **целостность** – не были ли по пути к адресату в письмо внесены несанкционированные изменения?

Действительно, если расшифрованная ЭЦП не совпадает с хэшем текста послания, то из этого могут следовать две вещи:

1. Письмо подписал другой человек (публичный ключ не соответствует приватному).

2. В текст сообщения были внесены изменения после его отправки.

В любом случае, получатель не может считать принятое сообщение достоверным – оно **подделано**!

Остается вопрос: Как получатель сообщения узнает, каким публичным ключом надо расшифровывать ЭЦП? Ведь для каждого приватного ключа существует свой уникальный публичный ключ.

Для этого существуют т.н. **хранилища сертификатов ЭЦП**. Каждый отправитель документа подписанного ЭЦП должен получить в соответствующем органе специальный **электронный сертификат** вместе с приватным ключом, которым он будет зашифровывать хэши своих посланий. Этот сертификат – по сути электронный документ, содержащий открытый ключ и информацию о владельце ключа.

Орган, выдавший сертификат, является доверительной организацией, которая подтверждает, что соответствующий сертификат ЭЦП выдан конкретному установленному лицу.

Сертификат вместе с ЭЦП прикрепляется к отправляемому посланию и получатель по сертификату идентифицирует личность отправителя и получает публичный ключ, соответствующий приватному ключу отправителя.

Электронная цифровая подпись (ЭЦП) используются не только для отправки корреспонденции. При помощи ЭЦП заверяются документы (например, договоры), банковские операции и многое другое. Технология ЭЦП также используется в протоколах криптовалют, включая Биткоин.

Алгоритмы создания ЭЦП и её проверки.

Биткоин для «чайников» Краткий вводный курс в технологические основы Биткоина

Кошельки и транзакции

Как это ни странно звучит, но **«биткоин-кошельки»** не содержат биткоинов!

Да-да! Именно так! Собственно **биткоины**, как монеты или расчетные единицы, существуют только **в контексте протокола** блокчейна Биткоина, а именно в виде записей **транзакций** в распределенной базе данных, которую еще называют **ledger** – бухгалтерская книга или гроссбух. Это база данных – **блокчейн Биткоина** – содержит записи абсолютно всех транзакций за всю историю со всеми существующими на данный момент биткоинами (расчетными единицами).

Что же такое транзакция и как работают т.н. «биткоин-кошельки» (под этим термином будем подразумевать способ хранения приватных ключей к биткоин-адресам)? Попробуем разобраться…

Транзакция – это финансовая операция по передаче некоторого количества денег от отправителя к получателю. При этом и отправитель, и получатель должны иметь определенные адреса (метки), между которыми и происходит движение денег.

В этом смысле финансовая транзакция подобна почтовым отправлениям – отправитель со своего почтового адреса отправляет в конверте некую сумму денег на адрес получателя.

В банковских структурах финансовая транзакция называется **денежным переводом**. А адреса – **банковскими счетами**. Когда некое лицо хочет отправить определенную сумму денег другому лицу, оно обращается в банк с просьбой перевести эту сумму с его банковского счета на банковский счет получателя.

Представьте себе большую таблицу, в каждой строке которой содержатся следующие данные (поля):

– дата и время финансовой операции (перевода денег);
– биткоин-адрес кошелька отправителя;
– биткоин-адрес кошелька получателя;
– сумма перевода.

Это и есть запись финансовой транзакции.

В протоколе Биткоина банковский счет аналогичен т.н. **биткоин-адресу**, который еще называют **адресом кошелька**. Формально это некая уникальная буквенно-цифровая строка, например:

12ctspmoULfwmeva9aZCmLFMkEssZ5CM3x.

Это не просто набор символов, а последовательность, криптографически связанная с приватным ключом от этого адреса. Т.е. биткоин-адрес и приватный ключ к нему являются уникальной парой, подобной публичному и приватному ключу в асимметричном шифровании.

Владелец биткоин-адреса, используя приватный ключ, может отправлять переводы на другие биткоин-адреса. Эти переводы записываются в блокчейн Биткоина (гроссбух – ledger) в виде транзакций.

Отметим, что все транзакции в блокчейне хранятся в незашифрованном виде. Любой человек, используя блокчейн-браузер или Block explorer – специальный сайт, для просмотра содержимого блоков, может увидеть любую транзакцию, включенную в блокчейн, в понятном виде – когда, откуда и куда, какое количество биткоинов было переведено.

Поскольку в блокчейне хранятся абсолютно **все транзакции**, именно по ним можно не только отследить движение всех монет между биткоин-адресами, но и вычислить, сколько криптоденег находится в данный момент в любом кошельке по его адресу.

Как это происходит? Все транзакции в Биткоине используют **Входы** (Inputs) и **Выходы** (Outputs):

1. **Входы –** пополнения, когда данный адрес выступает в качестве **получателя** биткоинов.

2. **Выходы –** платежи, переводы и т.п., когда адрес выступает в качестве **отправителя**.

Посредством Входов и Выходов транзакции связаны друг с другом – каждый Вход ссылается на Выход предыдущей, родительской транзакции. Таким образом цепочки связанных транзакций отслеживают все денежные потоки между биткоин-адресами внутри блокчейна.

На Входы каждой транзакции поступают средства с Выходов каких-то предыдущих транзакций, тем самым пополняя биткоин-адрес получателя средств. Если Выход не связан с Входом последующей транзакции, он считается непотраченным. Подсчитав все непотраченные Выходы, можно узнать текущий баланс конкретного биткоин-адреса (кошелька).

Но как владельцы этих адресов (кошельков) управляют своими деньгами? Как они совершают платежи и переводы?

Вот для этого и нужны собственно **«биткоин-кошельки»**, в которых помимо уже упомянутого адреса хранятся **приватные ключи** (криптографически связанные с этим адресом), при помощи которых осуществляются транзакции-выходы.

Когда владелец соответствующего биткоин-адреса (кошелька) хочет перевести расчетные единицы (биткоины) на другой адрес, он дает соответствующее распоряжение в сеть Биткоина, подписанное электронно-цифровой подписью (ЭЦП), сформированной при помощи соответствующего приватного ключа от биткоин-адреса.

Собственно, эту операцию и совершают специальные компьютерные программы и приложения, называемые «биткоин-кошельками», такие как, например, **Electrum** или веб-приложение на сайте **Blockchain.info** и др. Они также подсчитывают баланс биткоин-адреса, отслеживая все непотраченные Выходы по данному адресу, и показывают все предыдущие транзакции по этому адресу.

Функции биткоин-кошелька может также выполнять и основной биткоин-клиент сети – программа **Bitcoin Core.**

Какие бывают биткоин-кошельки?

Прежде всего, отметим главное: **биткоин-кошельки хранят приватные ключи от ваших биткоин-адресов**. Это хранение может быть **«холодным»** или офлайн (без подключения к интернету) и **«горячим»** или онлайн (с подключением к интернету и сети Биткоин).

Поэтому условно все виды биткоин-кошельков можно разделить на две большие группы – «холодные» и «горячие»:

«Холодные» кошельки:

– **бумажные** – лист бумаги или другого материала (например, пластик) с нанесенным на него биткоин-адресом и приватным ключом. Может также дополняться соответствующими QR-кодами[13] для быстрого сканирования и добавления ключей в программу-клиент для совершения транзакций. Для надежности данные биткоин-адреса и приватного ключа к нему хранят отдельно друг от друга, снабдив их одинаковыми метками для сопоставления при пользовании.

– **аппаратные** – специальные компактные программно-аппаратные устройства, подключаемые к компьютеру через USB-разъем или другим способом. Внешне похожие на флешку. Позволяют надежно (в зашифрованном виде) хранить приватные ключи и осуществлять при помощи их биткоин-транзакции. В принципе, хранить ключи можно на любом внешнем носителе информации (флеш-карта, HD-диск и т.п.), но в этом случае безопасность гораздо ниже.

Образец «холодного» бумажного кошелька.

Преимущества бумажного кошелька заключается в том, что приватные ключи в нем сберегаются офлайн, поэтому не подвержены кибератакам или сбоям оборудования.

Однако, в последнее время бумажные кошельки стали применяться гораздо реже, поскольку их вытеснил более удобный способ хранения – **SEED-ключи** (см. ниже).

«Холодные» кошельки, как правило, используются для надежного и длительного хранения большого количества биткоинов. Разумеется, в данном случае подразумевается не соб-

[13] **QR-код** – матричный графический код, используемый для быстрого распознавания информации фото- и видеоустройствами.

ственно хранение биткоинов в кошельках, а хранение доступа к соответствующим биткоин-адресам, на балансе которых находятся биткоины. Фактически, как было отмечено выше, в «холодных» кошельках хранятся приватные ключи от этих биткоин-адресов.

«Горячие» кошельки:

– приложения для компьютеров (десктопов и ноутбуков) – специальные компьютерные программы-клиенты для работы с биткоин-адресами и осуществления транзакций. Позволяют также отслеживать историю транзакций и вести учет. Пример – Electrum, Bitcoin Core, Jaxx, Xapo и т. п.

– мобильные приложения – аналогичные программы для смартфонов. Могут дублировать соответствующие приложения для компьютеров.

– он-лайн (веб-сервисы) – веб-сайты, предоставляющие услуги онлайн доступа к биткоин-адресам и проведения транзакций. Например, упоминаемый выше Blockchain.info или Coinbase.com.

Безопасность «горячих» кошельков обеспечивается внутренним программным шифрованием биткоин-адресов и использованием пользовательских паролей и двухфакторной авторизации.

Большинство «горячих» кошельков поддерживают технологию т. н. **SEED-ключа**. Собственно, SEED – это набор случайных английских слов. Как правило их 12, но бывает и 18 или 24. Выглядит это так:

tango ten bravo game press go extra wink regular apple mimic anchor

Эта бессмысленная цепочка слов позволяет генерировать практически неограниченное количество биткоин-адресов, связанных с SEED. А программа биткоин-кошелька предоставляет доступ пользователю по конкретной последовательности SEED.

Зная свой SEED-ключ пользователь может воспользоваться любым программным кошельком, который поддерживает технологию SEED.

Краткие итоги:

– В биткоин-кошельках не хранятся собственно биткоины (расчетные единицы).

– Все биткоины существуют в контексте транзакций – записей их движения от одного биткоин-адреса к другому. Эти записи хранятся в блокчейне.

– Баланс конкретного кошелька определяется путем расчета всех непотраченных Выходов биткоин-адреса этого кошелька.

– Биткоин-адрес (кошелька) криптографически связан с приватным ключом, при помощи которого осуществляются выходные транзакции с этим адресом.

– Биткоин-кошельки для конкретного адреса хранят его приватный ключ.

– Биткоин-кошельки позволяют удобно управлять (просматривать баланс и транзакции), а также совершать переводы и платежи (выходные транзакции) с конкретного адреса.

– Биткоин-кошельки бывают «горячими» и «холодными».

– SEED-ключ позволяет получить доступ к множеству связанных с ним биткоин-адресов при помощи любого программного биткоин-кошелька, поддерживающего технологию SEED.

Блокчейн

Википедия определяет блокчейн, как **цепочку блоков транзакций**.

Само слово **«блокчейн»** (*blockchain*) в переводе с английского означает цепочку блоков (от *block* – блок и *chain* – цепочка). Но это определение не передает всю суть этой новой технологии, на которой построена криптовалюта Биткоин.

Так что же на самом деле такое блокчейн? И в чем его преимущества перед другими способами организации и хранения данных?

Начнем с того, что блокчейн – это **распределенная база данных**, полные копии которой находятся на множестве серверов (компьютеров), объединенных в **одноранговую сеть**.

Из этого следует, что **блокчейн не может существовать только на одном компьютере** (сервере).

Одноранговая сеть, называемая еще сетью **peer-to-peer** (P2P), означает, что все компьютеры, объединенные в неё, имеют одинаковые права и нет главного (центрального управляющего) сервера.

Из этого следует, что **блокчейн является децентрализованной системой** хранения данных.

Как я раньше уже писал в главе **«Кошельки и транзакции»**, в блокчейне Биткоина, называемом еще **ledger** (бухгалтерская книга) хранятся данные о всех прошедших на данный момент **транзакциях**, осуществленных с расчетными единицами Биткоина.

Технология блокчейна, как организации данных, обеспечивает **безопасное и целостное хранение информации**. Т.е. любые изменения уже записанных в блокчейн транзакций невозможны – нельзя ни удалить, ни откорректировать их.

И это очень важный момент! Поскольку мы имеем дело с финансовыми операциями, которыми являются транзакции. Но при этом нет единого доверенного центра (например, банка), который бы следил за сохранностью и неизменностью этих транзакций.

Как же это организовано в блокчейне? Давайте разберёмся…

Для этого нужно вспомнить, что такое хэш-код и хэширование. В главе **«Хэширование: Просто и наглядно»** я пояснил, что хэш-код или попросту **хэш** (*hash*) любого массива информации подобен **отпечатку пальца** человека – он представляет собой уникальную короткую символьную строку, которая присуща только этому массиву входящей информации. Точно так же, как отпечаток пальца присущ только одному человеку и нет людей с одинаковыми отпечатками, хэш присущ только одному набору входных данных.

И это свойство хэша – **каждому набору (массиву) информации присущ строго определенный, уникальный хэш**, – используется в блокчейне для контроля сохранности (неизменности) записанных транзакций.

Чтобы понять, как это реализовано в блокчейне, построим упрощенную схему данных, которую назовем **хэшчейном** (*hash-chain*) – цепочкой хэшей.

Представим, что данные в наш хэшчейн записываются построчно. Возьмем слово **Start** (просто так, чтобы с чего-то начать). Вычислим его хэш-код при помощи SHA-256 hash калькулятора.

Это будет:

e4bb9f1ece9af9264a3b9e3913bbdb2cf497457167b1…

Запишем это в первую строку в наш хэшчейн. Далее вычислим хэш-код этой строки. Получим:

1f26aab02f7e645b95b4973a0202b42f4059941cf470…

Запишем это второй строкой. Далее будем повторять операции, получая каждую последующую строку, как хэш от предыдущей:

e4bb9f1ece9af9264a3b9e3913bbdb2cf497457167b1…
1f26aab02f7e645b95b4973a0202b42f4059941cf470…
0b706bab77aab5157143417e5b05a7899c88beef136c…
805c72c5f0b8450ab6a0f9bbf1f65cc262d2cdab98fc…

И т. д. до бесконечности.

Это и будет наш хэшчейн – цепочка связанных хэшей, которую мы начали с хэш-кода слова Start, а каждая последующая строка – это хэш-код предыдущей.

Как несложно понять, при попытке злоумышленника изменить хотя бы один символ в этом массиве, все последующие хэши изменятся, поскольку ещё одно из свойств хэша – **при самом незначительном изменении входной информации её хэш меняется кардинально.**

Например, если мы во второй строке изменим первый символ (1) на 2, то наш хэшчейн с третьей строки станет совсем другим:

e4bb9f1ece9af9264a3b9e3913bbdb2cf497457167b1…
2f26aab02f7e645b95b4973a0202b42f4059941cf470…
495d58b76f9b95b0cd9a884b202ec7857ff5d53d199e…
05790b4b4ced45d6d6b5d9d39cc04ac1661187c125f7…

Разумеется, наш пример с хэшчейном бессмысленный с точки зрения содержания данных. Но он позволяет понять суть технологии.

Пойдем дальше. Представим теперь, что мы записываем данные в нашу базу в виде блоков, состоящих из двух строк:

– Заголовок (**Hash**)
– Строка осмысленных полезных данных (**Payload**).

При этом заголовок формируется, как хэш-код, получаемый из заголовка и данных предыдущего блока. Для первого блока заголовком будет пустая строка.

Для примера, в качестве данных возьмем первые 4 строки поэмы А.С.Пушкина **«Евгений Онегин»:**

Мой дядя самых честных правил,

Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог.

Будем записывать по одной строке в каждый блок. Всего у нас будет 4 блока:

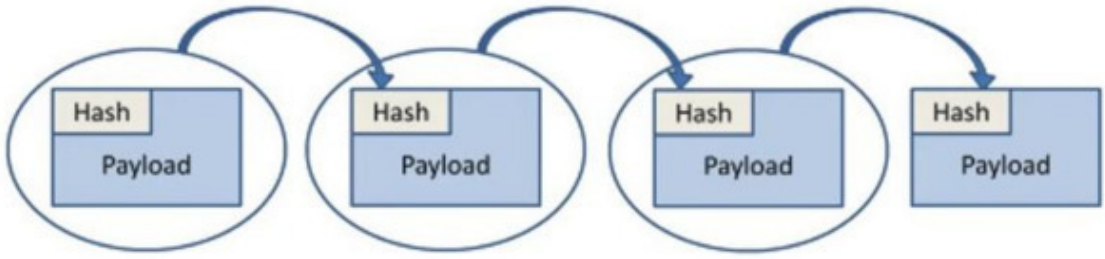
(нет заголовка)
Мой дядя самых честных правил

c55c1d6a76b4d5e2f67b5167fd6f8ded02bf94b4a552…
Когда не в шутку занемог,

fe11dbc29864cd135eb2a7ab20f7c6012f606615d3cc…
Он уважать себя заставил

b5fa6355fe7c54bc8a25c3711fd09c82bcb682b4a880…
И лучше выдумать не мог.

Здесь заголовки (первый строки) блоков, начиная со второго – это по сути, хэш-коды предыдущих блоков.



Теперь представим, что некий злоумышленник (шутник) решил изменить вторую строку на **«Когда он в шутку занемог,»**, заменив частицу **«не»** на местоимение **«он»**.

Получается:

(нет заголовка)
Мой дядя самых честных правил

c55c1d6a76b4d5e2f67b5167fd6f8ded02bf94b4a552…
Когда он в шутку занемог,

eb45a8d41c1903a7256fb2a0828136c2abf00a44fe89…
Он уважать себя заставил

6b0e9b6b534dbaea67f455be675906a9f816aa939363…
И лучше выдумать не мог.

Как видим, даже незначительное изменение текста второй строки полностью изменило заголовки всех последующих строк, вплоть до последней. Это изменение будет сразу автоматически замечено, поскольку копии блокчейна хранятся на множестве компьютеров в сети.

Именно по такому принципу работает блокчейн. Вся информация в него записывается поблочно и блоки связаны между собой через заголовки (хэши).

Разумеется, организация данных в блокчейне Биткоина гораздо сложнее, чем в показанном выше примере. Но суть остается та же – **между блоками устанавливается связь** посредством записи в заголовок текущего блока хэша предыдущего, а полезными данными (*Payload*) являются записи осуществленных транзакций.

Но кто и как записывает новые данные в блокчейн? Процесс такой записи в Биткоине называется **майнингом** и об этом я расскажу в главе **«Майнинг»** раздела **«Биткоин для чайников»**.

Подведем итоги:

Собственно **блокчейн** (*blockchain* – цепочка блоков) – это распределённая база данных, представляющая собой непрерывную последовательную цепочку связанных между собой блоков, содержащих информацию.

Технология Блокчейн Биткоина, называемая также технологией распределенного реестра учета (*Distributed Ledger Technology* или *DLT*) – это комбинация компонентов, включающих в себя:

– **одноранговые сети** peer-to-peer (P2P),
– **распределенное хранение данных**,
– **криптографию** (хэширование и шифрование с открытым ключом).
– **механизм консенсуса**.

Таким образом, технология блокчейна является надежным способом организации и долговременного хранения данных (информации), основанным на криптографической защите и децентрализации.

Кроме того, она позволяет достичь **консенсуса** между всеми участниками при условиях, что они друг другу не доверяют.

Блок

Базовой составляющей блокчейна является **блок** – единичная порция связанных в цепочку данных (информации).

Как мы уже знаем, **блокчейн Биткоина** – это некий бухгалтерский реестр или книга (ledger), в которой записаны абсолютно все транзакции, совершенные с монетами биткоина.

И если блокчейн – это бухгалтерская книга, то отдельные страницы этой книги – это и есть **блоки** блокчейна, в которых записываются финансовые транзакции, связанные между собой посредством хэшей так, что в заголовке каждого последующего блока хранится хэш-код предыдущего.

В этой громадной бухгалтерской книге невозможно ни удалить страницу (блок), ни изменить её содержание, поскольку сразу же изменится содержание заголовков всех последующих страниц (блоков) и программное обеспечение любого участника распределенной сети Биткоина, у которого хранится копия этой книги-блокчейна, сразу же заметит попытку подмены. Собственно, сама сеть Биткоина это заметит автоматически и отвергнет попытки внести все изменения в блокчейн.

.

> **Примечание**: На самом деле речь идет не о всей сети Биткоина, а о большинстве узлов (нод) этой сети. Подробнее см. в главе **«Захват управления блокчейном („атака 51%“)»**.

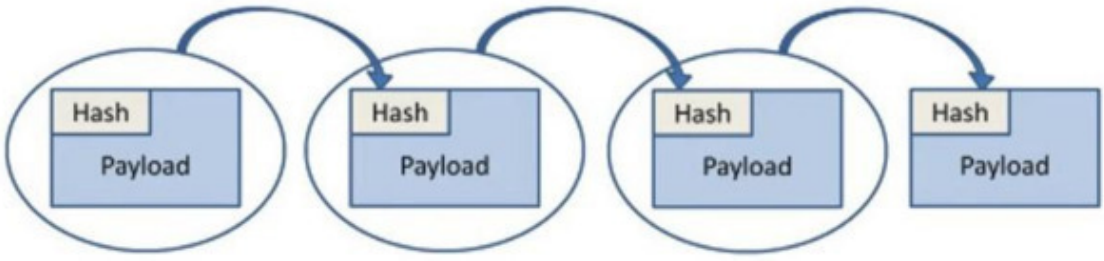
Таким образом, все **блоки, записанные в блокчейн, изменить уже невозможно**! Вообще, любое редактирование записанной в блокчейн информации (транзакций) запрещено. Можно только дописывать новые блоки.

Это важное свойство блокчейна, как распределенного реестра финансовых транзакций. Как невозможно исправить записи или удалить пронумерованные страницы в прошитой и скрепленной печатью бухгалтерской книге, так и невозможно это сделать в блокчейне.

При этом блокчейн гораздо надежней любой бухгалтерской книги или любого банковского реестра операций, поскольку копии блокчейна хранятся на множестве компьютеров (серверов) в распределенной одноранговой сети.

А теперь вернемся к блокам блокчейна Биткоина.

Каждый блок состоит из заголовка (**Head**), в котором хранится служебная информация, и полезной информации (**Payload**) – собственно записи транзакций.



Блоки в блокчейне и их связь между собой

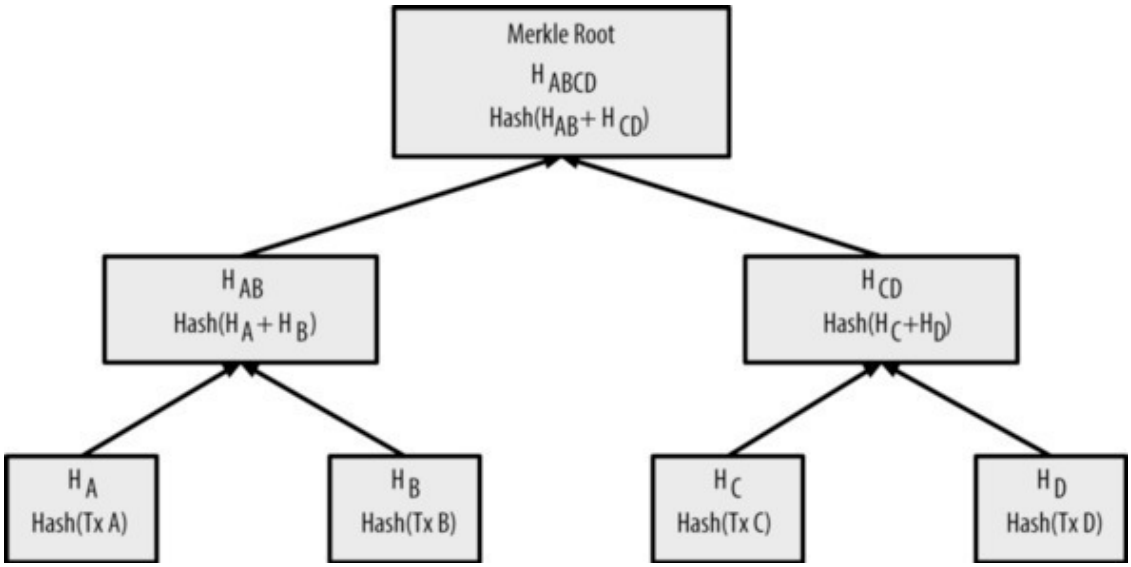
В заголовке блока содержится следующая информация:

– версия блока;
– дата и время создания блока;
– хэш-код заголовка блока;
– хэш-код предыдущего блока;
– хэш-код всех транзакций в блоке;
– специальные параметры **nonce** и **bits**, которые записываются при майнинге (подробнее об этом я расскажу в главе **«Майнинг»**).

Для понимания нам важны хэши в заголовке.

Сам **хэш-код заголовка блока** – это и есть то, что связывает предыдущий блок с последующим в цепочке блокчейна. Он записывается как хэш-код предыдущего блока в заголовок последующего.

Также в заголовке хранится хэш-код транзакций текущего блока. Он подсчитывается с использованием алгоритма, известного, как **дерево Мёркла** (*Merkle tree*) или бинарное дерево хэшей.



Дерево Мёркла

Работает это так:

1. Сначала считаются хэши всех транзакций в блоке (нижний уровень на схеме).

2. Потом считаются хэши от суммы хэшей пар транзакций.

3. Далее считаются хэши от суммы получившихся пар хэшей и далее по такой же схеме, пока не получится один единственный хэш-код – он и будет **хэшем транзакций в блоке**.

Тут следует учесть, что поскольку дерево бинарное (подсчет идет парами), то на каждом шаге должно быть четное число элементов. Поэтому если, на каком-то этапе получается нечетное количество хэшей, то последний просто дублируется для получения пары.

Именно заголовки позволяют отслеживать целостность содержимого самих блоков.

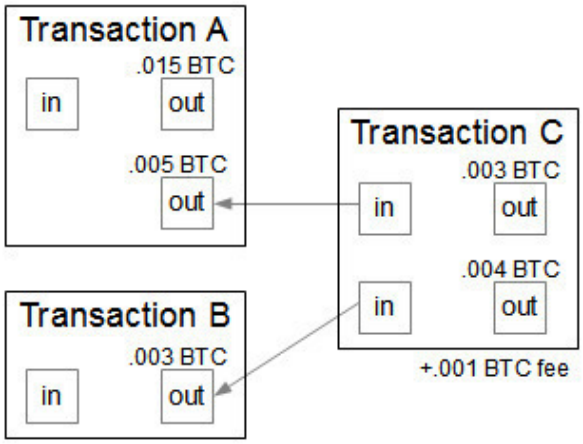
Теперь перейдем к собственно содержимому (**Payload**) блока. Как уже говорилось ранее, в блокчейн Биткоина записываются транзакции. Собственно, в общем виде, сама транзакция имеет вид:

С **<адрес 1>** отправить **<N>** биткоинов на **<адрес 2>**

В действительности транзакция, записанная в блок блокчейна, сложнее, поскольку протокол Биткоина оперирует такими понятиями, как **Входы** (*Inputs* или *In*) и **Выходы** (*Outputs* или *Out*).

Входы (In) – это поступление на биткоин-адрес, а **Выходы** (Out) – это суммы, которые переводятся на другие биткоин-адреса.

Поэтому в Биткоине новая транзакция через Входы (один или несколько) ссылается на Выходы (один или несколько) предыдущих транзакций и формирует Выходы (также один или несколько) для использования в последующих транзакциях. Если после пополнения биткоин-адреса переводов с него не было, Выход транзакции считается непотраченным (т. н. **UTXO –** unspent transaction output).



Новая транзакция C ссылается на две входящие транзакции – **A** и **B**. В результате на входе у транзакции получается **0.008 BTC** (0.005+0.003), которые потом разделяются на два выхода – на первый адрес отправляется **0.003 BTC**, а на второй **0.004 BTC**. Остаток (**0.001 BTC**) – комиссия майнеру.

Собственно структура записи транзакций в блокчейне Биткоина содержит:

– количество используемых Входов;
– хэш-код и индекс каждого Входа, а также служебную информацию;
– количество используемых Выходов;
– суммы Выходов, а также служебную информацию;
– метку времени транзакции.

Эта, на первый взгляд, сложная конструкция, на самом деле, показывает реальное движение денег между биткоин-адресами и дает возможность достаточно быстро подсчитать баланс любого биткоин-адреса на основании непотраченных Выходов (UTXO) транзакций с ним.

Возможность указать сразу несколько Выходов в транзакции – это очень важная вещь, потому что транзакцию (точнее – ее Выход) можно использовать как Вход только один раз и только целиком.

Например, если имеется входящая транзакция (Вход) на 1 биткоин (BTC), а нужно перевести куда-то 0,8 BTC, то создается транзакция с одним Входом и двумя Выходами: на 0,8 BTC – собственно перевод и на 0,2 BTC – возврат на биткоин-адрес отправителя.

Еще важный момент – это т.н. **комиссия за транзакцию** (*transaction fee*), которую получают майнеры – люди, компьютерное оборудование которых записывает новые блоки транзакций в блокчейн.

В транзакции, как правило, сумма Выходов меньше суммы Входов, а получившаяся разница отправляется на адрес майнера, записавшего блок с этой транзакцией в блокчейн. Это и есть его вознаграждение (помимо платы за создание нового блока или собственно майнинг).

Майнинг

«Майнинг» – второе слово после **«блокчейна»**, с которым у многих ассоциируется Биткоин.

Однако, не все знают истинную сущность этого понятия, а также его предназначения в **протоколе** (программных правилах) криптовалюты.

Для большинства майнинг – это какой-то фантастически непонятный процесс, в ходе которого при помощи компьютерного оборудования (видеокарт и ASIC-процессоров [14]) идет добыча электронных денег – монет биткоина.

Действительно, слово «майнинг» (**mining**) в переводе с английского означает добычу полезных ископаемых. А майнеры (**miners**) – это шахтеры.

Но, чтобы понять истинное предназначение и роль майнинга в процессе функционирования криптовалют и блокчейна, надо погрузиться не в горнодобывающую, а в финансовую сферу.

Вернемся к денежным переводам (транзакциям), которые составляют главную задачу и цель существования сети Биткоина.

Собственно, процесс **денежных переводов** в типичной финансовой среде описывается серией из четырех последовательных шагов:

1. **Submission** – отправитель посылает в систему платежное сообщение (поручение) о переводе некоторой суммы денег получателю;

2. **Validation** – сообщение проходит процедуру проверки отправителя и целостности сообщения;

3. **Conditionality** – проверяется наличие достаточного баланса для перевода на счету отправителя;

4. **Settlement** – проведение транзакции, перевод денежных средств на счет получателя.

В современной экономике эти процессы обычно поддерживаются **финансовыми посредниками**, такими как **банки**.

Отправитель (клиент банка) посылает платежное сообщение или поручение (**submission**) в платежную систему банка. Это сообщение должно пройти процедуру подтверждения (идентификации) клиента и целостности сообщения (**validation**). После успешной валидации сообщения банковская система проверяет необходимые условия для платежа (**conditionality**), а именно – достаточность средств на балансе клиента или наличие кредита. Если все проверки пройдены, банк окончательно (безусловно и безотзывно) проводит платеж (**settlement**) – пополнение счета получателя и уменьшение баланса счета отправителя.

[14] **ASIC** (application-specific integrated circuit – «интегральная схема специального назначения») – процессор, специализированный для решения конкретной задачи, например майнинга криптовалют.

Как видим, с одной стороны эта система **централизована –** основную роль в проведении платежей выполняет **финансовый посредник –** банк. С другой стороны, эта система построена **на доверии** к посреднику, поскольку клиенты доверяют банку проводить финансовые операции со своими деньгами.

Криптовалюты, в частности Биткоин, являются полностью **децентрализованными системами**, в которых вопросы доверия решаются **криптографическими методами**.

Поэтому процесс денежных переводов в них происходит несколько по-другому, а именно:

– Submission – отправитель перевода при помощи программного приложения «биткоин-кошелек» направляет в сеть Биткоина сообщение, в котором указываются **биткоин-адреса** отправителя и получателя, а также **сумма перевода** и сумма комиссии за перевод (опционально). Это сообщение автоматически подписывается электронной цифровой подписью (**ЭЦП**) отправителя, которая формируется при помощи закрытого (приватного) ключа отправителя и криптографически связана с его биткоин-адресом. Подробнее см. главу **«Электронная цифровая подпись: Просто и наглядно»**.

– Validation – это сообщение проходит проверку в сети по ЭЦП. Тем самым, происходит идентификация отправителя. Для проверки используется биткоин-адрес, поскольку он связан с приватным ключом отправителя, при помощи которого он подписал сообщение. На самом деле, личность отправителя не имеет значения, она остается анонимной. Под идентификацией отправителя понимается соответствие биткоин-адреса отправителя и сообщения (платежного поручения) криптографической подписи (ЭЦП). Тем самым подтверждается, что указанная сумма денег (монет биткоина) должна быть отправлена с конкретного биткоин-адреса.

– Conditionality – проверяется наличие достаточного баланса для перевода на счету отправителя. Для этого, согласно протоколу Биткоина, происходит подсчет всех **непотраченных Выходов** (т. н. UTXO – unspent transaction output) этого адреса. Подробнее см. главу **«Блок»**.

– Если все проверки прошли, сформированная транзакция ждет **добавления в блок и записи в блокчейн**.

И вот тут, собственно, и начинается процесс, который получил название **«майнинг»**. Что же это такое?

Казалось бы все просто – если платежное сообщение (поручение) прошло все проверки, то его можно записывать в реестр (бухгалтерскую книгу), каковым является блокчейн.

Но, во-первых, мы знаем, что данные (транзакции) в блокчейн записываются в виде **блоков** (транзакций). Следовательно, надо предварительно **сформировать блок**.

Во-вторых, как мы знаем, сеть Биткоина является **одноранговой** и **децентрализованной**, т.е. состоящей из многих разбросанных по всему миру постоянно работающих компьютеров (серверов), называемых **узлами** (*node*).

Следовательно, обработка поступивших в сеть платежных поручений о переводе биткоинов, может вестись **одновременно на многих узлах**. Каждый узел формировал бы и записывал свои блоки.

При этом могла возникнуть ситуация называемая **«проблемой двойных трат»**, когда некий недобросовестный пользователь Биткоин-сети решил отправить со своего биткоин-адреса, баланс которого, например составляет 1 BTC, одновременно два платежа по 1 BTC на два разных биткоин-адреса.

Эти платежи могли одновременно попасть на обработку в разные узлы и быть записаны в разные блоки. Но, как мы знаем, записанный в блокчейн блок исправлять уже нельзя.

В общем, ситуация, при которой все узлы сети Биткоина могут одновременно записывать блоки в блокчейн, привела бы к хаосу. Следовательно, необходимо делегировать право записи в блокчейн сформированного блока какому-то одному узлу.

Но какой именно узел будет это делать? Ведь сеть Биткоина одноранговая и все узлы имеют равные права. Как достичь **консенсуса** между равными узлами?

Автор Биткоина, некий Сатоши Накамото, предложил в протоколе использовать для определения такого узла известный ранее алгоритм, который получил название **Proof of Work (PoW)** – доказательство сделанной работы.

Записать новый блок в блокчейн могут только те узлы, которые **раньше других** выполнят **вычислительную работу** по решению некоторой **криптографической задачи** большой сложности.

При этом, все другие узлы могут быстро проверить правильность решения этой задачи, а также подтвердить, что все транзакции в сформированном блоке валидны.

Такой криптографической задачей в протоколе Биткоина является **задача по подбору параметра**, называемого **nonce**, который, будучи добавлен к заголовку сформированного блока, изменял бы его (блока) **хэш-код** так, чтобы он начинался с заданного количества **нулевых битов** (bits), что равносильно получению хэша, **менее или равного** заданному большому числу (Difficulty Target или попросту Target).

Другими словами, надо добавить такую короткую строку данных (**nonce**) в сформированный блок, чтобы получившийся хэш-код блока начинался с определенного количества нулей (точнее – нулевых битов).

Такую задачу можно решить **только методом подбора,** т.е. перебором большого количества разных параметров (nonce). Что очень трудоемко и требует больших вычислительных мощностей.

С другой стороны, проверка правильности решения этой криптографической задачи очень проста – надо при помощи хэш-функции **SHA-256** вычислить хэш-код сформированного блока, в заголовок которого добавлен найденный параметр **nonce**.

Поясню на простом примере, как это происходит. Для этого возьмем уже известный нам пример с четверостишьем А.С.Пушкина:

(нет заголовка)

Мой дядя самых честных правил

c55c1d6a76b4d5e2f67b5167fd6f8ded02bf94b4a552…
Когда не в шутку занемог,

fe11dbc29864cd135eb2a7ab20f7c6012f606615d3cc…
Он уважать себя заставил

b5fa6355fe7c54bc8a25c3711fd09c82bcb682b4a880…
И лучше выдумать не мог.

Как видим, в нашем примере все хэши в заголовках всех четырех блоков начинаются не с нулей. Добавим в заголовок блока параметр **nonce** и поставим задачу подобрать его таким, чтобы хэш-код предыдущего блока начинался с четырех нулей (*подчеркнуто*). Получится:

(нет хэша)
23106
Мой дядя самых честных правил

*0000*7cee3bff26415365c1453fe6758ad888edad3877…
27980
Когда не в шутку занемог,

*0000*83c4f4acb2239e607921f653e9320e050f71b955…
17007
Он уважать себя заставил

50405
*0000*b0f1e6d8b09e8bf005c7023a3696343fcff267cc…
И лучше выдумать не мог.

Здесь в каждом блоке:

– первая строка – хэш предыдущего блока;
– вторая строка – найденный параметр **nonce**;
– третья строка – строчка четверостишья – полезный контент.

Хэш строки первого блока «**Мой дядя самых честных правил,**» равен:

c55c1d6a76b4d5e2f67b5167fd6f8ded02bf94b4a552…

А если мы добавим параметр **23106** к этой строке и получим «**23106Мой дядя самых честных правил,**», то найденный хэш-код будет начинаться с 4-х нулей:

*00007*cee3bff26415365c1453fe6758ad888edad3877…

Аналогично и со всеми последующими блоками. Для них были также подобраны параметры таким образом, чтобы хэш-код блока начинался с 4-х нулей.

Все эти параметры были найдены методом перебора, на что ушло значительное вычислительное время компьютера. Причем, усложнение задания путем увеличения количества начальных нулей хэша блока приведет к увеличению компьютерного времени или потребует увеличения компьютерной мощности.

А проверка найденного параметра – дело простое. Для этого надо лишь вычислить хэш-код полученных данных блока с учетом этого добавленного параметра.

Эта идея и лежит в основе **Доказательства сделанной работы** (Proof of Work).

Тот майнер (узел), который первым найдет параметр **nonce** для своего созданного блока, и получает право записать этот блок в блокчейн. Иногда бывают случаи, когда несколько майнеров почти одновременно решают задачу по подбору параметра nonce. В этом случае все они получат право на запись своего блока в блокчейн и цепочка блоков разветвляется. Это состояние блокчейна получило название **форк** (от английского ***fork*** – *вилка*). Далее каждая ветвь прирастает своими новыми блоками, но побеждает та, где цепочка блоков будет длиннее. Все остальные ветви признаются невалидными и отсекаются от блокчейна. (Подробнее об этом читайте в главе **«Понимание механизма консенсуса»**).

Таким образом достигается **консенсус между узлами** в сети Биткоина.

Весь этот процесс по «цифроперемалыванию» – подставил новый параметр nonce, вычислил хэш, проверил результат и т. д. до получения нужного хэша с нулями в его начале – и есть пресловутый «майнинг»!

Следует добавить, что сложность решаемой криптографической задачи может изменяться (увеличиваться) в зависимости от суммарной мощности компьютеров, занятых майнингом. С ростом этой мощности количество нулевых битов в искомом хэше растет таким образом, чтобы максимальное время поиска результата (nonce) было **не более 10 минут**. Это автоматическое изменение сложности зашито программно в протоколе Биткоина и выполняется через каждые записанные **2016 блоков**, т.е. примерно один раз в две недели.

К слову сказать, растущая вычислительная мощность сети майнеров, а также связанная с ней сложность криптографической задачи и, как следствие, рост затрат на «добычу» биткоинов приводит к тому, что майнеры объединяются в т.н. **пулы**, чтобы повысить вероятность решения задачи и получения вознаграждения за блок. При успехе «добытые биткоины», включая и комиссионное вознаграждение, делятся пропорционально вычислительной мощности каждого участника пула.

Важный момент! Затраты майнеров на вычислительные ресурсы (стоимость оборудования и электроэнергии) являются надежной защитой от т.н. **«атаки 51%»** – состояния, когда более половины вычислительной мощности сети Биткоина контролируется одним майнером или группой майнеров. Теоретически, этот объём вычислительной мощности дает власть над сетью. Это означает, что каждая клиентская программа в сети верит в подтвержденный блок транзакций атакующей стороны, что позволяет атакующим осуществить контроль над сетью, включая следующие полномочия:

– создавать транзакции, конфликтующие с чужими;
– останавливать подтверждение чьей-либо транзакции;
– тратить одни и те же монеты несколько раз;

– мешать другим майнерам находить действительные блоки.

Затратность майнинга компенсируется высокой надежностью от попыток взлома денежной сети и осуществления над ней контроля, делая экономически нецелесообразной т.н. «атаку 51%».

Но вернемся к собственно майнингу… А где же добытые «шахтерами» (майнерами) деньги (биткоины)?

Разумеется, любая работа должна поощряться. Тем же протоколом Биткоина предусмотрено вознаграждение майнерам (в виде новых монет биткоина) за записанный ими в блокчейн блок транзакций.

Собственно, новые монеты могут попасть в сеть Биткоина только в результате майнинга. Тем самым осуществляется **эмиссия биткоина**.

Первоначально (в 2009 году) за каждый новый блок (т.е. каждые 10 минут) майнеры, которые добавили его в блокчейн, получали **50 монет BTC**. Но, опять же, протоколом Биткоина установлено, что через каждые 210 000 блоков (примерно 4 года) вознаграждение за новый блок уменьшается в 2 раза. Поэтому сейчас (2018 год) майнеры получают за добавленный блок 12,5 BTC. А суммарное количество биткоинов (эмиссия) не может превышать **21 млн монет**. Почему это так, читайте в главе **«Почему количество биткоинов ограничено»**.

Помимо платы за блок майнеры, добавившие блок в блокчейн Биткоина, получают **комиссионное вознаграждение** (*transaction fee*) с транзакций. При этом майнеры стараются наполнить блок в первую очередь транзакциями, в которых указана максимальная комиссия. Поэтому, если отправитель указал небольшую комиссию, его платежное поручение откладывается в исполнении. В результате некоторые платежи могут идти часами, а то и сутками.

Подведем итоги:

Майнинг – это необходимый и важный процесс в сети Биткоина, в результате которого решаются следующие задачи:

– **Запись нового блока** транзакций в блокчейн.

– **Выпуск новых монет** биткоина (эмиссия).

– **Сетевое вознаграждение** участникам сети (майнерам) за обработку транзакций и формирование нового блока.

– **Защита от т.н. «атаки 51%»**, делающая экономически нецелесообразными попытки взлома и контроля денежной сети.

– **Поддержание большого количество копий блокчейна в сети**. Это происходит из-за того, что майнерам необходимо иметь полную актуальную (последнюю) версию блокчейна для контроля (валидации) новых транзакций.

Почему количество биткоинов ограничено

Общеизвестно, что количество биткоинов не может быть более **21 миллиона монет**. Но не все знают, почему это именно так. Почему нельзя выпустить (намайнить) больше?

Дело в том, что «добыча» новых монет четко прописана в **протоколе биткоина** и зашита в его программный код. Согласно протоколу, вознаграждение майнерам «выплачивается» за каждый новый присоединенный к блокчейну (распределенной базе данных Биткоина) блок данных транзакций. Первоначально за каждый новый блок майнеры получали 50 BTC (биткоинов).

Но тем же протоколом предусмотрено, что через каждые записанные в блокчейн Биткоина **210 000 блоков** данных транзакций вознаграждение майнерам **уменьшается ровно в 2 раза**. А это означает, что если за первые записанные в блокчейн 210 тыс. блоков количество монет биткоина увеличилось на 10,5 млн (210 тыс. х 50), то за вторые 210 тыс. блоков – уже в два раза меньше, т.е. 5 млн 250 тыс. (210 тыс. х 25) и т. д.

Математически все это выражается последовательностью чисел, в которой каждый последующий член в два раза меньше предыдущего:

$$\mathbf{N + N/2 + N/4 + N/8 + N/16 + \ldots + N/2^k}$$

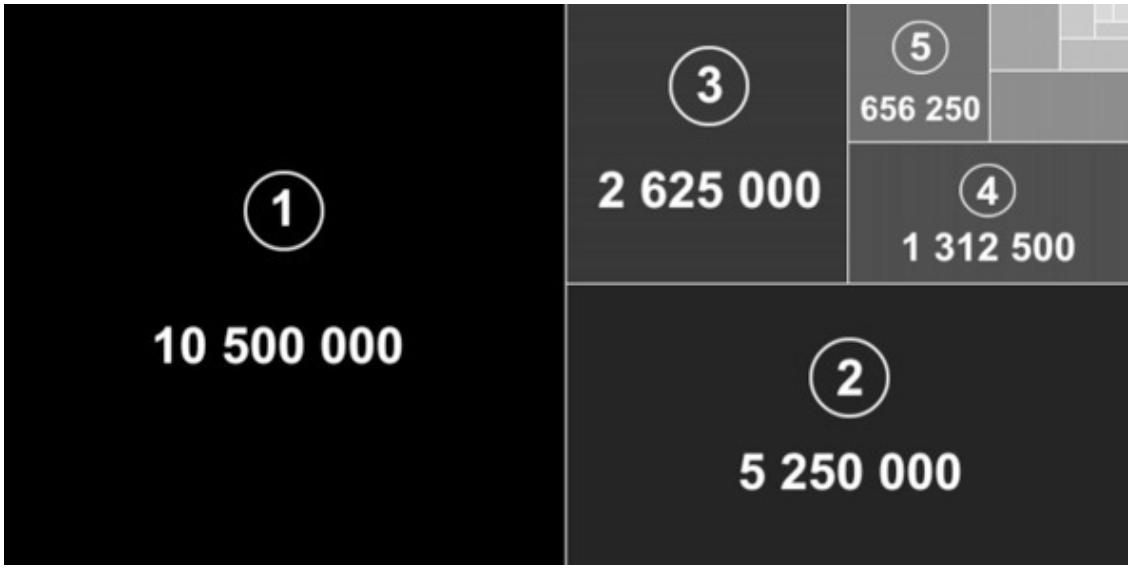
Здесь $\mathbf{2^k}$ – это 2 в степени k, где **k** – это номер члена в ряде, начиная с 0.

Такая последовательность называется сходящимся рядом, сумма членов которого стремится к **2N**.

В случае с биткоином **N = 210 000 x 50 = 10 500 000**, т.е. равно количеству биткоинов, «добытых» при записи первых 210 тыс. блоков данных в блокчейн (базу данных транзакций)

Таким образом, максимальное количество «добытых» биткоинов будет стремиться к **21 млн** (2 х 10,5 млн). В реальности это число будет несколько меньше – **20 999 999,9769**. Это связано с дробностью деления и ограничением кол-ва долей биткоина 8-м знаком после запятой.

Наглядно это можно представить следующей картинкой:



Здесь количество «добытых» биткоинов представлено в виде геометрических фигур – квадратов и прямоугольников. Причем, каждая последующая фигура по площади ровно в два раза меньше предыдущей.

Квадрат №1 имеет условную площадь **10,5 млн единиц**, что соответствует количеству биткоинов, «добытых» за запись первых 210 тыс. блоков данных транзакций.

Прямоугольник №2 – это половина первого квадрата и площадь его равна **5,25 млн единиц** (кол-во биткоинов, «добытых» за запись вторых 210 тыс. блоков данных транзакций.

Квадрат №3 – половина прямоугольника №2 и площадь его соответственно равна **2,625 млн единиц**. И т. д.

Очевидно, что при делении пополам все фигуры помещаются в условный квадрат в правой части картинки, который идентичен левому квадрату (№1). Следовательно общая суммарная площадь будет равна двум большим квадратам №1 или **21 млн единиц площади**.

Когда будет «добыт» последний биткоин

Теперь интересно разобраться, а сколько времени потребуется на «добычу» всех биткоинов?

В том же протоколе биткоина и его программном коде заложено, что каждый новый блок транзакций записывается в блокчейн примерно каждые 10 минут.

Таким образом в час будет записано примерно 6 блоков, а в сутки – 144. Это значит, что для записи 210 тыс. блоков понадобится **1 458, (3) дней** или примерно **3,99 года**.

Следовательно, примерно каждые 4 года количество «добытых» биткоинов будет уменьшаться в 2 раза. Т.е. у биткоина существует некий 4-летний цикл «добычи».

За первые 4 года было «добыто» 10,5 млн биткоинов, за вторые 4 года – еще 5,25 млн. Итого за первые 8 лет было «добыто» 15 млн 750 тыс. биткоинов. А на момент написания этой книги «добыто» **16 365 612 биткоинов**.

Но нас интересует, а **когда же будет «добыт» последний биткоин?**

Для этого пойдем с конца. Поскольку минимальное вознаграждение за записанный блок не может быть менее **1 сатоши** (0,00000001 BTC), то в последний период будет «добыто» не менее 210 000 сатоши или 0,00210000 BTC.

Осталось вычислить, через сколько 4-летних циклов кол-во биткоинов будет таким, как в первом цикле – 10,5 млн. Очевидно, что кол-во этих 4-летних циклов будет равно степени k числа 2 в выражении **0,00210000 x 2^k** (2^k – это 2 в степени k) при котором оно будет более 10,5 млн.

$$\mathbf{0{,}00210000 \times 2^k > 10\,500\,000}$$

Здесь $\mathbf{2^k}$ – это 2 в степени k.

Осталось вычислить число k – кол-во 4-летних циклов биткоина.

Это **33 (тридцать три)** 4-летних цикла или **132 года**. Следовательно. последний сатоши будет «добыт» в 2140 году.

Действительно, последний блок данных транзакций, который создаст монеты, будет блок **№6 929 999**. Он будет создан примерно в **2140 году**.

При этом за первые 7 (семь) 4-летних циклов (28 лет) или к 2036 году будет «добыто» более 99,2% всех биткоинов, поскольку на оставшиеся циклы приходится только 1/128 от общего кол-ва биткоинов. Следовательно, **менее 1% биткоинов будет «добываться» еще более 100 лет**!

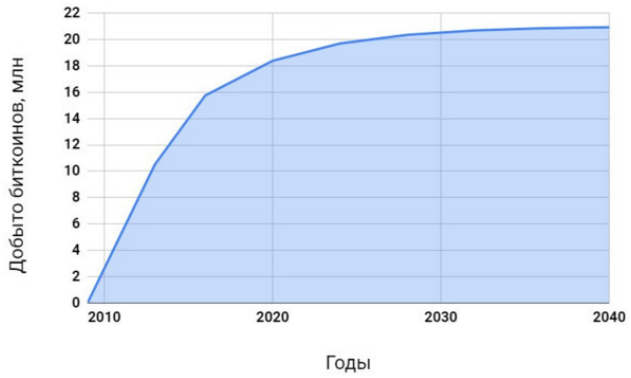


График «добычи» биткоинов до 2040 года

Следует отметить, что в реальности кол-во биткоинов в обращении будет несколько меньше из-за того, что кто-то в силу ряда причин потеряет доступ к своим кошелькам и все хранящиеся там монеты будут безвозвратно утрачены.

Понимание Биткоина

В основе Биткоина лежат три основных технологических компонента:
– Собственно блокчейн (база данных).
– Одноранговые (пиринговые – P2P) сети.
– Механизм консенсуса (майнинг – PoW).

Биткоин не сможет существовать, если какой-либо из этих компонентов отсутствует. Поэтому для понимания Биткоина важно понимание каждого составляющего его компонента.

Понимание собственно блокчейна

Попросту говоря, **блокчейн – это всего лишь способ структурирования данных**. Вот и всё! Это регистр, гроссбух (ledger): файл, который отслеживает записи бухгалтерского учета.

Как уже было сказано выше, этот файл сравним с книгой, которая никогда не заканчивается.

Как и страницы книги, блоки блокчейна заполняются информацией. Все блоки помимо номеров имеют метку времени, которая выполняет особую функцию. Новый блок всегда добавляется после блока с самой последней меткой времени. Таким образом формируется цепочка.

Блокчейны используют криптографию, чтобы отследить изменение информации в любом блоке (странице этой бесконечной книги). Это свойство делает блокчейн хорошей структурой данных, чтобы отслеживать сохранность записи чего-либо ценного и важного.

Как мы уже знаем, в блокчейне Биткоина блоки содержат информацию о транзакциях. В каждом блоке указано, какое количество биткоинов передается с какого адреса и на какой.

Поскольку блокчейн Биткоина использовался для отслеживания движения всех биткоинов с момента их создания, всегда можно проверить и точно знать, кому и сколько принадлежит биткоинов. Текущее состояние блокчейна Биткоина показывает **«кто чем владеет»**. Но также всегда можно отследить, как биткоины попали на тот или иной адрес.

Транзакция происходит только после её включения в блок и добавления блока в цепочку. Следовательно, когда блок добавляется в цепочку, биткоины перемещаются с адреса на адрес и состояние блокчейна обновляется.

Это означает, что любой может проверить, действительно ли кто-то совершил транзакцию на его адрес или нет, просто проверив текущее состояние блокчейна. Разумеется, чтобы это сделать, блокчейн должен быть общедоступным. Здесь на помощь приходят **одноранговые сети**.

Понимание одноранговых (P2P) сетей

Если бы блокчейн хранился только на одном компьютере (сервере) и вдруг оказалось бы, что он отключенный, то это было бы очень неприятно, если не сказать больше. На самом деле, текущее состояние блокчейна загружается, синхронизируется и предоставляется многими компьютерами во всем мире.

Эти компьютеры называются **«узлами»** или **«нодами»** (*nodes*), и они работают совместно в одноранговой *(peer-to-peer – P2P*) сети, чтобы гарантировать, что блокчейн является безопасным и актуальным. Каждый из этих узлов хранит полную, обновленную (актуальную) версию блокчейна. Каждый раз, когда добавляется новый блок, все узлы обновляют свой блокчейн. Использование одноранговой сети имеет определенные **преимущества**:

– Всегда можно проверить состояние блокчейна, используя программу-проводник – т. н. **Блокчейн-эксплорер** (*Blockchain explorer*) или **Блок-эксплорер** (*Block explorer*).

– Не надо полагаться только на одну сторону, чтобы знать истинное состояние блокчейна.

– Не надо полагаться на безопасность одного сервера, чтобы знать, что блокчейн защищен.

– Потенциальному злоумышленнику придется одновременно взломать тысячи узлов, а не один сервер.
– Всегда есть уверенность, что блокчейн никогда не исчезнет, потому что для этого придется отключить или уничтожить все узлы, которых тысячи по всему миру.

Это все очень важно, но вышеизложенное не означает, что блокчейн только из-за этого оказывается достаточно надежным, чтобы использоваться для хранения транзакций.

Например, как узнать, что все транзакции в блокчейне верны? Как узнать, что в блоках нет недействительных транзакций? И если есть разные версии блокчейна, откуда мы узнаем, которые из них являются истинными?

Все эти опасения весьма изобретательно решаются **консенсусным механизмом**, использование которого стало возможным, в первую очередь, благодаря одноранговой сети.

Понимание механизма консенсуса

Одноранговые сети и блокчейн (база данных) существовали и до Биткоина.

Однако, до появления Биткоина считалось невозможным достичь консенсуса между узлами в одноранговой сети (т.н. **проблема Византийских генералов**) для создания децентрализованной цифровой денежной системы.

> **«Задача о византийских генералах»** формулируется так. Несколько генералов, каждый во главе своего легиона, осадили город. Каждый из них знает, что половины всех их войск достаточно, чтобы взять город при одновременной атаке – но, если атака не будет одновременной, то сил не хватит, они потерпят поражение. Связываться друг с другом генералы могут только через гонцов, возможности проверить подлинность доставленных депеш нет, и есть основания подозревать, что некоторые из генералов – изменники, которые будут отправлять остальным ложные сведения. Какова должна быть стратегия переговоров генералов о едином времени штурма города, если нет ни взаимного доверия, ни единого верховного командования, а вероятность попыток помешать штурму ложными сообщениями велика?

В 2009 году гениальный Сатоши Накамото, загадочный и анонимный основатель Биткоина, объединил блокчейн с **механизмом достижения консенсуса**, основанным на криптографии.

Консенсусный механизм Биткоина – это то место, где происходит настоящая магия: он позволяет узлам в одноранговой сети работать вместе, **не зная друг о друге и не доверяя друг другу**.

Механизм консенсуса – это просто набор правил, который согласовывается узлами в сети, запуская программное обеспечение сети. Эти правила обеспечивают, чтобы сеть работала по назначению и оставалась синхронизированной.

Консенсусный протокол устанавливает такие правила:

– каким образом блоки должны быть добавлены в блокчейн,
– когда блоки считаются действительными,
– как разрешаются конфликты.

Добавление блоков в блокчейн

Механизм консенсуса, который используется в Биткоине, называется **Доказательством выполненной работы** (PoW).

Первое правило **PoW** состоит в том, что новый блок должен быть добавлен в блокчейн в среднем **каждые десять минут**.

Процесс добавления нового блока, как мы уже знаем, называется **«майнинг»**. Узлы, которые пытаются добавить блок в цепочку (называемые «майнерами»), используют вычислительную мощь своих компьютеров, чтобы попытаться решить некую криптографическую «головоломку». Правила утверждают, что только когда эта головоломка решена, блок может быть добавлен в блокчейн. Подробнее об этом читайте в главе **«Технологические основы майнинга»**.

Майнер, который решает задачу и «майнит» (добывает) новый блок, чтобы добавить его в блокчейн, вознаграждается сетью. Ему предоставляется некое предопределенное количество новых монет (биткоинов) вместе с комиссионной платой за все транзакции, содержащиеся в этом новом блоке.

Впоследствии все остальные майнеры начинают «добывать» следующий блок.

Проверка блоков

Когда какой-то майнер решит криптографическую головоломку и сформирует новый блок, все узлы в сети проверят, действителен ли блок (правильность транзакций), и добавят его в свою копию блокчейна. Сначала узлам необходимо достичь консенсуса относительно действительности. Только тогда сеть синхронизируется и блокчейн обновится.

Узлы будут добавлять новый созданный блок в цепочку, только если он будет следовать правилам, изложенным в протоколе консенсусного механизма. Программное обеспечение протокола проверяет, действителен ли блок или нет. Недействительный блок будет просто отклонен.

Естественно, что блок будет являться действительным, если действительными будут все транзакции, содержащиеся в нем. Например, в протоколе Биткоина говорится, что никто не может отправлять биткоины, которые он не получил первоначально от кого-то другого или в качестве вознаграждения за майнинг блока.

Другими словами, программное обеспечение узлов проверяет все транзакции в новом блоке, имеются ли у отправителей достаточное количество биткоинов для совершения своих транзакций. Для этого узлы проверяют состояние сети Биткоина.

При этом становится невозможной ситуация т.н. «двойной траты», поскольку узлы просто отклонят попытку двойного использования биткоинов.

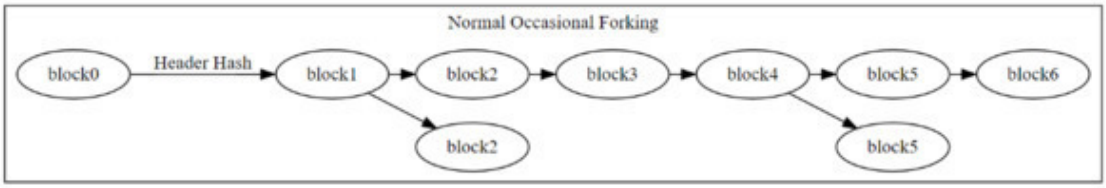
Правила также определяют, что транзакция действительна только в том случае, если она **подписана с цифровой подписью** владельца биткоин-адреса, с которого осуществляется перевод. Только лицо, которое контролирует кошелек или адрес, с которого отправляется биткоин, может подписать транзакцию. Поэтому только владелец этого адреса может потратить свои биткоины.

Как разрешаются конфликты

Может случиться так, что два майнера одновременно добавляют действительные блоки в блокчейн. Представьте, что часть узлов приняла один действительный блок, а другая часть приняла другой действительный блок. И внезапно возникли два разных состояния блокчейна в одно и то же время!

Это называется непреднамеренным **«форком»** (*fork* – «вилка»): блокчейн разветвляется на две разные цепи. Как определить, какая из двух разветвленных цепей блокчейна является «истинной»?

Консенсусный протокол решает эту проблему с помощью простого правила: **выигрывают самые длинные цепочки**.



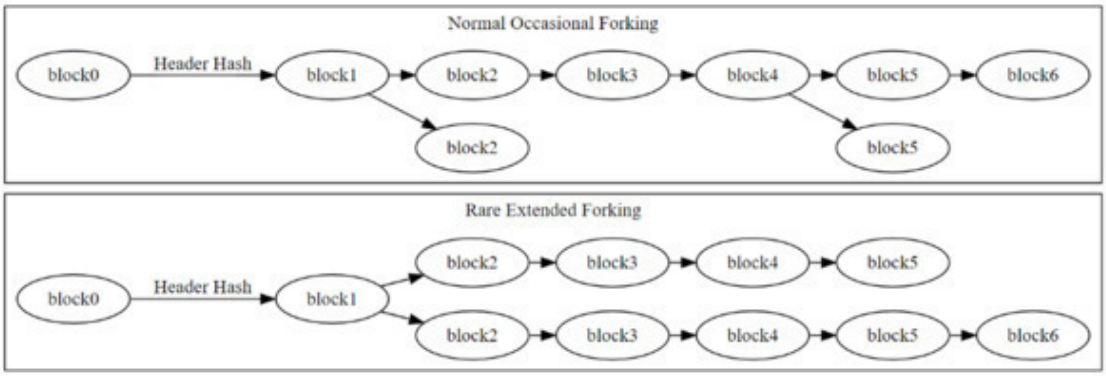
Когда случается непреднамеренный форк (разветвление), некоторые майнеры начнут добывать новые блоки в одной цепочке, а другие начнут добычу в другой цепочке. Неизбежно одна из этих цепочек будет иметь больше майнеров, чем другая, и соответственно в неё будут быстрее добавляться новые блоки. Остальные майнеры перейдут к более длинной цепи, и другая ответвленная цепь отомрет, ее рост прекратится. При этом основной цепочке не будет нанесен ущерб.

Почему есть уверенность, что это всегда произойдет?

Потому что **майнеры – это экономические субъекты, которые действуют в личных интересах**. Майнер не заинтересован в добыче на разветвленной цепи, зная, что она отомрет. Все транзакции (истинные транзакции) в разветвленной цепи никогда не происходили в основной цепочке, а это означает, что майнеры, которые добывали блоки на разветвленной цепи, не будут вознаграждены за свою работу. Издержки майнинга блоков, которые не будут включены в основную цепочку, просто слишком высоки. И майнерам невыгодно продолжать майнинг на альтернативной ветке.

В редких случаях может произойти, что разветвленная цепь обладает значительным количеством ресурсов для добычи. В этом случае может потребоваться некоторое время, прежде чем станет ясно, какая из ответвления цепей является основной цепью. Практика подсказывает, что разумно ждать **6 новых блоков**, чтобы действительно подтвердить транзакцию.

Правило, согласно которому побеждает самая длинная цепь, в сочетании с тем фактом, что требуется огромная вычислительная мощность для добавления блоков в цепочку, делает блокчейн **невероятно безопасным**.



Практически единственный способ атаковать сеть Биткоина – это вернуться к какому-либо блоку в блокчейне, и начать формировать с него новую цепочку блоков. Однако, для этого злоумышленнику придется переделать всю работу, проделанную майнерами с этого блока, и догнать основную цепь. Без большей вычислительной мощности, чем вся объединенная сеть майнеров, это просто невозможно. Проще говоря, электричество и процессоры, необходимые для такой операции, будут очень дорогостоящими.

Биткоин – первый продукт криптоэкономики
Термин «криптоэкономика» вызывает много путаницы, и люди часто не понимают, что это означает.

Само слово **Криптоэкономика** (*Cryptoeconomics*) может вводить в заблуждение, так как предполагает наличие некой параллельной крипто-версии всей экономики. Но это не так!

Криптоэкономика – это не применение макро- и микроэкономической теории для криптовалютных рынков или ICO. Это также не разновидность экономики, а скорее **область прикладной криптографии**, которая учитывает экономические стимулы и экономическую теорию.

Криптовалюты, основанные на публичном блокчейне (биткоин, лайткоин, ethereum и пр.) являются продуктами криптоэкономики. Да и сама технология блокчейна – также лишь один из продуктов этой новой практической науки.

Криптоэкономика базируется и существует в децентрализованных одноранговых (P2P) системах, которые не дают контроля над собой какой-либо третьей стороне.

Можно предположить, что в этих системах всегда будут злоумышленники, которые хотят нарушить работу системы.

Криптоэкономические подходы **сочетают криптографию и экономику** для создания надежных децентрализованных одноранговых сетей, которые развиваются, несмотря на то, что противники и злоумышленники пытаются разрушить сеть.

Криптография, лежащая в основе этих систем, делает безопасной работу одноранговых сетей, а **экономика** – стимулирует всех участников вносить свой вклад в сеть, чтобы она процветала с течением времени.

Сатоши Накамото (*Satoshi Nakamoto*) породил криптоэкономику, когда он создал Биткоин в 2009 году. Как и Галилео Галилей, который известен как отец-основатель физики, Сатоши навсегда будет известен как основатель криптоэкономики.

Биткоин – это первый продукт криптоэкономики. Его инновация заключается в том, что она позволяет многим субъектам, которые не знают и не доверяют друг другу, надежно достигать консенсуса относительно состояния блокчейна (регистра транзакций) биткоинов. Это достигается сочетанием экономических стимулов и основных криптографических инструментов.

Децентрализованные одноранговые (P2P) системы, основанные на криптографии, были известны до появления Биткоина. Но в этих децентрализованных системах не было экономического стимула, который бы позволил им развиваться и процветать со временем.

Сатоши добавил экономический стимул к одноранговым системам, когда создал Биткоин в 2009 году.

До появления Биткоина считалось невозможным достичь **консенсуса между узлами** в одноранговой сети (т.н. проблема Византийских генералов) для создания децентрализованной цифровой денежной системы.

Proof of Work (доказательство сделанной работы) является решением **задачи о Византийских генералах**.

Вот как сам Сатоши Накамото описывает это решение (*Cryptography Mailing List 13 ноября 2009*):

> Несколько византийских генералов, каждый из которых имеет компьютер, хотят атаковать королевский wi-fi грубо подбирая пароль, состоящий из некоторого количества символов.
>
> У них ограничено время, чтобы взломать сеть и стереть логи, иначе они попадут в беду.
>
> У них имеется достаточная суммарная компьютерная мощность, чтобы успеть взломать пароль, если большинство из них атакует одновременно.
>
> Время начала атаки не имеет значения, главное, чтобы все согласились атаковать одновременно.
>
> Было решено, что любой из генералов может объявить время начала атаки. Проблема в том, что сигнал в сети передается не мгновенно для всех, и если два генерала одновременно объявляют разное время начала атаки, то некоторые могут услышать время одного генерала, а другие – второго.
>
> Генералы используют доказательство работы (Proof-of-Work) для решения проблемы. Каждый генерал, как только получает любое первое время атаки, запускает свой компьютер для решения чрезвычайно сложной задачи, которая включает это время атаки в своем хэше. Решение этой задачи, которое называется доказательство работы (Proof-of-Work) настолько сложно, что, ожидается, займет 10 минут времени.
>
> Все генералы решают задачу, прежде чем один из них найдет решение. Как только один из генералов находит решение, он передает его в сеть, и все генералы изменяют их текущую расчетную работу, чтобы включить это доказательство работы в хеши, над которым они работают. Если кто-то работал над другим временем атаки, они переключаются на это, потому что его цепочка доказательств работы теперь длиннее.
>
> Через два часа единое время атаки должно быть хэшировано цепочкой из 12 доказательств работы. Каждый генерал, просто проверяя сложность цепи доказательств работы, может оценить, сколько параллельной мощности центрального процессора (ЦП) в час было затрачено на него, и убедиться, что большая часть компьютеров создала такое множество доказательств, работая в отведенное время. Все генералы это видят, потому что доказательство работы является доказательством того, что они работали над этим. Если мощность ЦП, присутствующая в цепочке доказательств работы, достаточна для взлома пароля, они могут безопасно атаковать в согласованное время.

Сочетание криптографии и экономических стимулов привело к созданию надежной, растущей платежной децентрализованной одноранговой сети **Биткоин**, капитализация которой сегодня (по состоянию на октябрь 2018) составляет более **$100 млрд** и в которой ежедневно совершаются транзакции на сумму в несколько сотен миллионов долларов.

Биткоин основан на экономических стимулах и затратах. Экономические стимулы используются для привлечения майнеров для поддержки сети. Майнеры вкладывают свои

средства и несут затраты на электричество для производства новых блоков транзакций в сети, за что они вознаграждаются некоторым количеством биткоинов, поступающих в сеть в виде эмиссии, а также в виде комиссионных от добавляемых транзакций.

Экономические затраты майнеров являются частью модели безопасности биткоина. Самый очевидный способ атаковать блокчейн Биткоина – получить контроль над большей мощностью (хэшрейтом) сети – так называемая **«атака 51%»**, которая позволила бы злоумышленнику контролировать все последующие транзакции (цензурируя и не пропуская неугодные).

Но вычислительная мощность майнинга стоит денег, потраченных на оборудование и электроэнергию. Протокол Биткоина **преднамеренно делает майнинг затратным**, а это означает, что получение контроля над большинством вычислительной мощности в сети чрезвычайно дорого для того, чтобы получить прибыль от «атаки 51%». Так, по состоянию на 14 октября 2018 года стоимость «атаки 51%» на Биткоин составляла бы около **$9,3 млрд** на аппаратные средства и еще более **$6,4 млн** ежедневно на электроэнергию[15].

Кроме того, «атака 51%» привела бы к падению рыночной стоимости биткоина и, тем самым, еще больше снизила бы свою экономическую целесообразность.

Без этих тщательно откалиброванных экономических стимулов биткоин не работал бы и не развивался. Если бы майнинг не был связан с высокими затратами, было бы легко начать «атаку 51%». А если не было бы вознаграждения за майнинг, то не было бы и майнеров, которые покупают оборудование и оплачивают электроэнергию, чтобы внести свой вклад в сеть и получить за это вознаграждение.

Биткоин также использует криптографические протоколы, которые дают базовые инструменты, необходимые для создания надежных и безопасных систем. Криптография с использованием открытого и закрытого ключей используется для обеспечения безопасности пользователей и исключительного их контроля над своими биткоинами. А хэш-функции используются для «связывания» каждого блока в блокчейн Биткоина, проверки порядка событий, целостности и неизменности предыдущих данных.

Без жестких криптографических протоколов, таких как хэширующие функции или криптография с открытым и закрытым ключами, не было бы безопасной расчетной денежной единицы, с помощью которой можно было бы вознаграждать майнеров. Без тщательно откалиброванного набора стимулов для поощрения майнеров эта расчетная единица (биткоин, BTC) не имела бы рыночной стоимости, поскольку не было бы уверенности в том, что система может сохраниться в будущем.

Таким образом, криптоэкономика требует мыслить о проблемах информационной безопасности и надежности в экономическом плане. Она фокусируется на проектировании и создании распределенных децентрализованных систем, работа которых поддерживается экономическими стимулами, которые в свою очередь основываются на криптографии.

По сути, **криптоэкономика – это междисциплинарный подход,** слияние криптографических протоколов и экономических стимулов.

---

[15] По данным сайта **GoBitcoin.io**

Биткоин: Мифы и предрассудки
Основные возражения скептиков криптовалют

Рассказывают, что когда запускали первый паровоз в Америке, одна дамочка бегала по перрону и все время причитала: **«Не поедет! Не поедет!»**. Когда же локомотив двинулся и начал набирать ход, она закричала: **«Не остановится!»**.

Эта байка вкратце описывает, как человечество принимает инновации, – через незнание и непонимание, недоверие, страх, возражение, борьбу и даже запрет, – к тотальному распространению новых и вытеснению старых технологий.

Каждая прорывная технология привлекает своих ненавистников и скептиков. Некоторые из них просто не понимают, другие не хотят понять, а третьи отказываются понимать в своих корыстных интересах.

«Лошадь будет всегда, а автомобиль – это лишь причудливая новинка» – так в 1903 году президент одного банка ответил адвокату Генри Форда[16] на предложение инвестировать в автомобильную компанию.

Спустя 80 лет американский физик, инженер и изобретатель **Марти Купер** (*Marty Cooper*) предсказал: **«Сотовые телефоны никогда не заменят местные проводные системы»**.

И вот, через 30 лет появились новые «эксперты» и «аналитики», которые хоронят новейшую технологию под названием «Биткоин».

Только в 2018 году по мнению не менее двадцати аналитиков, журналистов и других «экспертов» Биткоин либо обречен, либо умирает, либо уже мертв. Он провалился, говорят они, и у него нет будущего.

До этого Биткоин уже хоронили сотни раз.

– ***«Итак, это конец биткоина»*** – **Forbes** в 2011 году.

– ***«Биткоин умирает. Ну и ладно»*** – австралийский сайт **Gizmodo** в 2013 году.

– ***«Волатильность Биткоина и необратимость транзакций отправят его на свалку истории»*** – журнал **Wired** в 2013 году.

– ***«Биткоин – всего лишь шутка»*** – **Business Insider** в 2013 году.

– ***«Биткоин не является ни надежным средством сбережения, ни полезной расчетной единицей»*** – **Reuters** в 2014 году.

[16] **Генри Форд** (*Henry Ford*) – американский промышленник, владелец заводов по производству автомобилей, изобретатель, автор 161 патента США.

> ***– «Биткоин – это не валюта. Это финансовая пирамида для переброски денег от одного либертарианца к другому»*** **– Washington Post** в 2014 году.
>
> ***– «Биткоин достиг максимума, и вряд ли снова начнет расти… По сути это не что иное, как сложная финансовая пирамида»*** **– Forbes** в 2015 году.
>
> ***– «Курс валюты*** *(биткоина – прим С.Б.)* ***замер на несколько месяцев (за исключением кратковременного роста и спада в начале ноября под влиянием криптовалютного бума в Китае), а главное, весь мир потерял к ней былой интерес»*** **– Guardian** в 2015 году.
>
> ***– «Покойся с миром, биткоин. Время двигаться дальше»*** **– Washington** Post в 2016 году.
>
> ***– «Думаю, можно смело сказать, что биткоин мертв. У него нет поддержки, никто им не пользуется. Кажется, эксперимент с биткоином завершен»*** – эстонский предприниматель, гендиректор **TransferWise** Таавет Хинрикус в 2016 году.
>
> ***– «Биткоин – это мошенничество. Это хуже, чем тюльпанная лихорадка»*** – генеральный директор (CEO) **JPMorgan** Chase Джейми Даймон (*Jamie Dimon*) в 2017 году.

Тем не менее, Биткоин спокойно, методично и последовательно собирает, компилирует и проверяет транзакции в своем распределенном реестре (блокчейне), практически без остановок создавая новые блоки каждые десять минут или около того. Он имеет время безотказной работы свыше 99,99% с момента его создания – 3 января 2009 года, если быть точным.

Биткоин был задуман его автором, неким Сатоши Накамото, как **способ удаленной передачи стоимости** (ценности) от одного субъекта к другому **без участия третьей доверенной стороны** – банка или иного финансового учреждения. Для этого был использован инновационный **криптоэкономический дизайн механизмов** – сочетание криптографии с экономическими стимулами.

Первоначально это эпохальное изобретение было скептически встречено даже в узкой среде криптографов и криптоанархистов. Читайте об этом в главе **«Genesis: Как появился Биткоин»**.

Но постепенно появились энтузиасты, которые увидели в этой технологии колоссальный потенциал. Именно их вера и убежденность двигали Биткоин в первые месяцы и годы его существования – сеть развивалась и росла, совершенствовался программный код, появились первые обменные площадки и криптовалютные биржи, а также другие криптовалюты.

Впервые массово заговорили о Биткоине почти через 5 лет после его появления – **в конце 2013 года**. Тогда курс первой криптовалюты внезапно взлетел и преодолел отметку в **$1000**. Это было невероятно! О Биткоине писали и говорили практически все ведущие СМИ в мире.

Это было первое массовое признание Биткоина, но одновременно с ним пришло непонимание, недоверие и скепсис. Люди не могли понять, как «нечто, появившееся ниоткуда», может иметь такую высокую стоимость и даже выполнять функции денег?

С тех пор мало что изменилось – курс биткоина стремительно растет и в 2017 году преодолел **$10 000**, а количество его скептиков не уменьшается.

«Кто стоит за Биткоином?» – спрашивают одни. **«Чем он обеспечен?»** – задают вопрос другие. **«Это очередная финансовая пирамида и пузырь, который скоро лопнет!»** – утверждают третьи…

Я считаю, что эти возражения являются ключевыми препятствиями в массовом продвижении и принятии Биткоина человечеством. Поэтому рассмотрим наиболее распространенные возражения и мифы, бытующие вокруг Биткоина:

– Биткоин – валюта криминального мира.
– Биткоин ничем не обеспечен.
– Биткоин – это пирамида.
– Биткоин – это спекулятивный пузырь.
– Биткоины незаконны, потому что они не признаны государством.
– Биткоины – это средство ухода от налогов.

Миф 1: Биткоин – валюта криминального мира

За этим утверждением стоит тот факт, что все транзакции в Биткоине анонимны. На самом деле они псевдонимны, но это не имеет особого значения. В массовое сознание продвигается тезис, что если человек скрывает источник своих доходов и свои финансовые операции, то он преступник.

> *«[Bitcoin] won't end well, it's a fraud… worse than tulip bulbs… [but] if you were a drug dealer, a murderer, stuff like that, you are better off doing it in bitcoin than U.S. dollars»*
>
> «[Биткоин] плохо кончит, это мошенничество… хуже, чем луковицы тюльпанов … [но], если бы вы были торговцем наркотиками, убийцей, подобные вещи вам лучше делать в биткоинах, чем в долларах США».

Эти слова принадлежат **Джими Даймону** (Jamie Dimon) – американскому миллионеру, председателю совета директоров и генеральному директору (CEO) крупнейшего финансового холдинга **JPMorgan Chase.**

Джими Даймон (Jamie Dimon)

Разумеется, криминальный мир использует Биткоин для проведения своих финансовых операций. Но криминалитет также пользуется долларами США, евро, японскими йенами и многими другими валютами мира.

Кстати, финансовая корпорация **JPMorgan Chase**, которой управляет Джими Даймон, сама была недавно **уличена в отмывании теневых денег.**

Тезис о криминальном происхождении Биткоина базируется на том, что люди не понимают, **«кто стоит за Биткоином?»**.

Это непонимание, в свою очередь, исходит из исторической практики человечества – все финансовые институты государства кем-то управляются – центробанками, резервными фондами и т. п. Эти структуры производят выпуск (эмиссию) денег и контролируют их обращение.

И, если за Биткоином не стоит государство в лице его институтов, то, наверное, им управляет криминальный мир. Такая логика!

В основе такого понимания лежит невежество и инертность мышления – людям трудно осознать и, тем более, принять, что финансовая структура может **не иметь единого центра управления**, а основываться на распределенной одноранговой (пиринговой) **сети**, в которой все узлы равны, и управляться **сетевым протоколом**, т.е. компьютерной программой, в которую заложены все правила. И никто, включая разработчиков, не может вмешаться и повлиять на эти правила без одобрения большинства сети.

Это **новая парадигма**! Она требует времени на осознание и принятие.

Миф 2: Биткоин ничем не обеспечен

Это один из главных тезисов противников криптовалют. Они считают, что деньги, которыми они пользуются в повседневности, чем-то обеспечены. Какой-то мифической товарной массой или золотом.

Но правда состоит в том, что выпускаемые государством **фиатные**, **фидуциарные деньги**, такие как американский доллар, евро, китайский юань, японская йена и другие, также ничем не обеспечены. Они используются как средство расчетов и платежей исключительно потому, что государство так установило своими законами, обязывающими все организации и учреждения принимать в качестве законного платежного средства национальную валюту.

Попробуйте пойти в супермаркет и расплатиться на кассе иностранной валютой. У вас её не примут! Даже ту, которая явно сильнее и стабильнее, чем национальная, например доллар США или евро.

Да и сам американский доллар лишился своего золотого обеспечения[17] еще в 1972 году и держится исключительно на силе экономики США. В то же время, любой экономический кризис толкает людей вложить свои фиатные деньги в что-то более значимое и стабильное – золото, землю, предметы искусства и антиквариат и т. п.

Фиатные деньги не имеют никакой внутренней стоимости и ценности, кроме насильного принуждения государства их использовать. По сути, это цветные листки бумаги и они практически ничем не отличаются по своему функционалу от ракушек и наконечников стрел, использовавшихся древними людьми для взаимного обмена товарами.

Само слово **«фиатные»** происходит от латинского ***fiat*** – декрет, указание, а **«фидуциарные»** – от латинского ***fiducia*** – доверие.

Обеспечение денег – это на самом деле **доверие к ним** со стороны продавцов и покупателей. Это доверие у фиатных денег обеспечивается силой закона и стабильностью экономик, а также доверием к государству в том, что оно выполнит взятые на себя обязательства, а также будет умеренно печатать новые деньги (делать эмиссию).

Но государство зачастую включает печатный станок, чтобы:

– решить бюджетные проблемы;
– обслуживать постоянно растущие долги девальвированной, более дешевой валютой;
– предоставить своим экспортерам конкурентное преимущество.

Тем самым запускается **инфляция** и даже **гиперинфляция**, покупательная способность населения падает. А **дефолты** (отказ от выплаты государственного долга) случаются даже в крупных экономиках.

[17] **Золотое обеспечение** или **золотой стандарт** – гарантия того, что каждая выпущенная денежная единица может по первому требованию обмениваться на соответствующее количество золота.

Банкнота в 100 триллионов (100 000 000 000 000) долларов Зимбабве.

Эмиссия в Биткоине, в отличие от государственных фиатных, фидуциарных денег, ограничена. А доверие к криптовалюте основывается на сетевом контроле и криптографическом протоколе.

Биткоин обладает не внутренней стоимостью, а **очень высокой полезностью** – способностью достаточно быстро, надежно и дешево передавать эквивалент стоимости на большие расстояния.

Поскольку, согласно **закону Меткалфа**, полезность сети растет пропорционально квадрату численности ее пользователей, то в такой же пропорции растет и полезность, а значит и ценность биткоина. Чем больше будет узлов и пользователей в сети Биткоина, тем сильнее и дороже будет её расчетная единица – биткоин (BTC).

Биткоин, как система, сеть, – это даже не деньги, а метод, средство, протокол, используемый для надежной передачи стоимости. Его можно использовать для покупок, платежей и других финансовых операций. Это новое средство обмена стоимостью в наступающей цифровой эре.

Миф 3: Биткоин – это пирамида

Очень распространенное утверждение скептиков криптовалют. У меня даже есть картинка для них:

Разумеется, это шутка! :)

Не вникая в суть, многие считают, что Биткоин – это очередная финансовая пирамида наподобие известных в 90-е годы прошлого столетия **МММ**[18], **«Русского Дома Селенга»**[19] или **«Хопер-Инвеста»**[20].

Однако, Биткоин принципиально отличается от того же МММ, а криптовалюты и финансовые пирамиды – это совершенно разные сущности. Общее между ними сейчас лишь одно – быстрый рост доходности и обогащение тех, кто раньше начал. На этом сходство заканчивается. Поясню почему…

Пирамида или «схема Понци» – это финансовая афера, в которой доходы первых участников (вкладчиков) обеспечиваются притоком денег последующих вкладчиков. Разумеется, при этом должна быть постоянная, растущая в геометрической прогрессии эмиссия активов пирамиды (акций, облигаций, купонов и т.п.), которые бы покупали новые участники в обмен на обещания получения дохода (дивидендов). Эти деньги как раз и идут на выплату «дивидендов» тем, кто стал вкладчиком ранее. **Пирамида существует до тех пор, пока есть приток новых вкладчиков**, которые обеспечивают доход предыдущим. Как правило,

[18] **«МММ»** – крупнейшая в истории России финансовая пирамида, организованная Сергеем Мавроди.

[19] **АОЗТ «Русский дом Селенга»** – финансовая компания в России, от деятельности которой пострадали миллионы людей. В последней своей стадии превратилась в финансовую пирамиду.

[20] **ТОО «Инвестиционная компания „Хопёр-Инвест“»** – российская компания, ставшая впоследствии финансовой пирамидой, от деятельности которой пострадали миллионы людей.

деньги, привлеченные финансовыми пирамидами, не направляются в качестве инвестиций в бизнес-проекты, а только распределяются между участниками. При этом львиную долю получают организаторы пирамид. **Классическая пирамида не создает полезного продукта или услуги.**

Биткоин (Bitcoin) – это построенная на одноранговой (без единого центра управления) компьютерной сети распределенная система учета финансовых операций (транзакций) – своего рода гигантская бухгалтерская книга (реестр, гроссбух – ledger), называемая еще блокчейном. Из этого следует, что Биткоин, как денежная система, **обладает полезными функциями** – проведение и учёт транзакций. В этой системе используется своя внутренняя расчетная денежная единица – собственно биткоин или BTC, которую создает сама система в ходе постоянной эмиссии – выпуска новых единиц. Эмиссия биткоинов ограничена и сокращается со временем (уменьшается вдвое примерно каждые 4 года). При этом, все новые биткоины, полученные в результате эмиссии, используются, как финансовый стимул (поощрение) для тех членов системы (майнеров), которые выполняют полезную работу – обеспечивают контроль и запись новых транзакций в блокчейн. Впоследствии майнеры могут передавать часть своих биткоинов любому участнику системы по взаимной договоренности – в качестве оплаты за услуги и товары, включая фиатные деньги. В результате биткоины перераспределяются в сети между многими участниками.

Для Биткоина, как инновационной денежной системы, **важно привлечение новых участников, но не их фиатных денег**. Новые участники, особенно те, которые поддерживают на своем компьютере полную актуальную версию блокчейна или занимаются майнингом, увеличивают ценность сети Биткоина в целом. А собственные деньги – биткоины – система генерирует сама в ходе эмиссии при майнинге.

Таким образом, **доходность в финансовых пирамидах обеспечивают исключительно деньги новых вкладчиков**. У Биткоина же вообще нет такого понятия, как вкладчики и дивиденды, а есть пользователи, которые совершают транзакции (денежные переводы) между адресами (счетами) друг друга и майнеры, которые обеспечивают работоспособность системы и получают за это вознаграждение от той же системы (программно, без участия третьих лиц). Рост или падение стоимости биткоина зависит исключительно от **рыночного механизма** – спроса и предложения на криптовалютных биржах. Поскольку последнее ограничено (максимум 21 млн. единиц, в реальности значительно меньше), а спрос постоянно растет, то это и обеспечивает рост рыночной стоимости биткоина. Это подобно росту стоимости акций успешных компаний, а биткоин – своего рода цифровой актив, растущий в цене.

И главное. Целью проекта Биткоин, каким видел его основатель Сатоши Накамото и его последователи, было не получение доходов на росте стоимости криптовалюты, а создание принципиально новой, децентрализованной и независимой от государства денежной системы на базе одноранговой распределенной компьютерной сети. Успех этого проекта будет толкать стоимость биткоина вверх, а неудача – приведет к падению.

Как видим, финансовые пирамиды и криптовалюты имеют принципиальные различия. Тем не менее, мошенники, используя ажиотаж вокруг криптовалют и невежество населения, могут организовывать финансовые пирамиды прикрываясь разговорами о криптовалютах, тем самым дискредитируя последние.

Пользователи биткоинов могут быть объектами для мошеннических или высокорисковых инвестиционных схем.

Инновации и новые технологии часто используются аферистами для совершения мошеннических инвестиционных схем. Мошенники могут привлекать инвесторов, рекламируя инвестиционные «возможности» биткоинов как способ войти в ультрасовременное пространство, обещая или гарантируя высокие инвестиционные доходы. Инвесторам трудно устоять перед такими инвестиционными площадками.

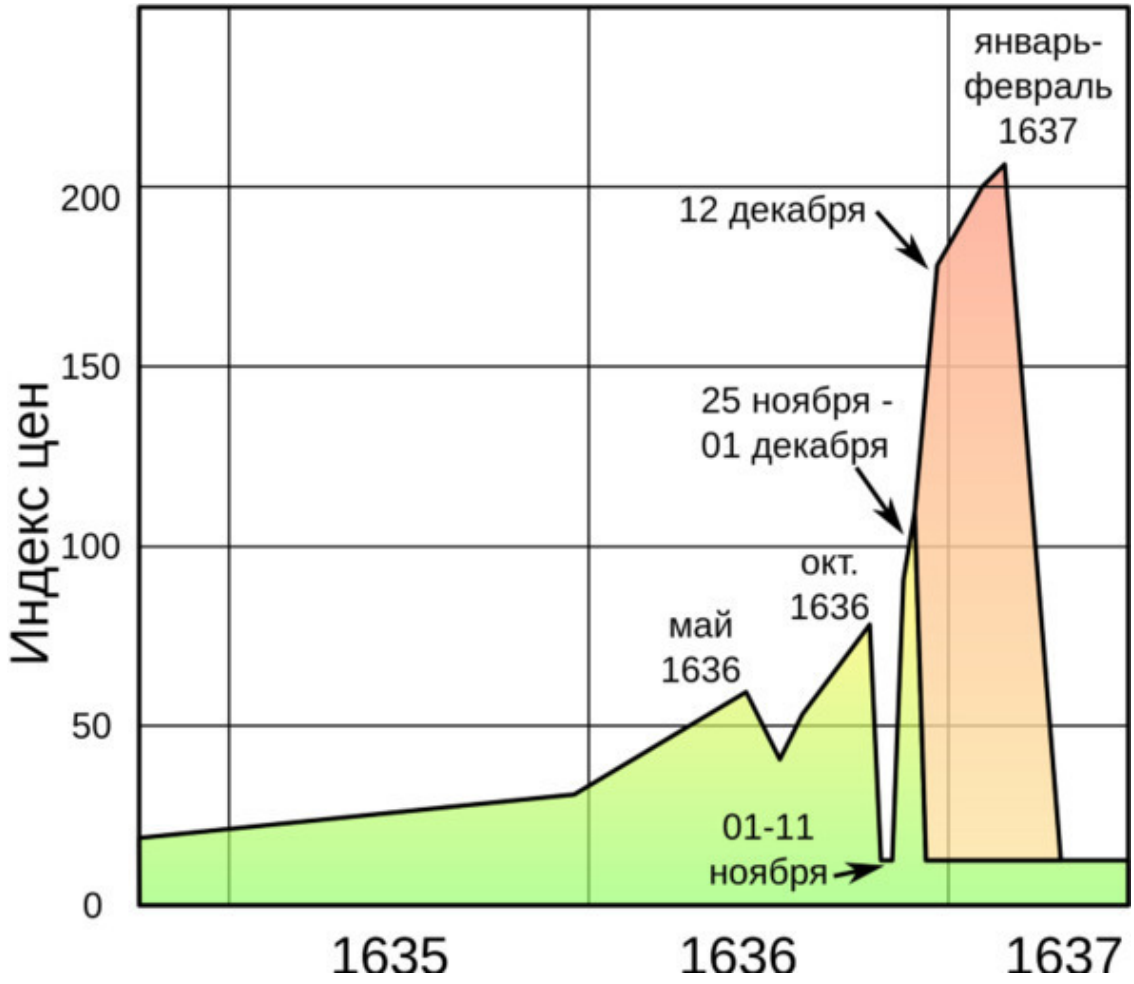
Биткоин в схеме Понци (Ponzi). В июле 2013 года SEC[21] обвинила частное лицо в предполагаемой схеме Ponzi, связанной с биткоинами (SEC v. Shavers). Обвиняемый рекламировал «инвестиционную возможность» биткоина на онлайн-форуме Биткоин, обещая инвесторам до 7% в неделю и что инвестированные средства будут использованы для деятельности Биткоина. Вместо этого обвиняемый якобы использовал биткоины, поступающие от новых инвесторов для оплаты уже существующим инвесторам и для личных расходов.

[21] **SEC** (The United States Securities and Exchange Commission, SEC) – Комиссия по ценным бумагам и биржам (США) – агентство правительства США. Является главным органом, осуществляющим функции надзора и регулирования американского рынка ценных бумаг.

Миф 4: Биткоин – это спекулятивный пузырь

Быстро растущая стоимость биткоина, – это динамика, которая возникает на любом «бычьем рынке», поскольку покупки порождают еще больше покупок и подгоняются страхом «упустить возможность».

Одним из наиболее популярных аналогов для растущей цены биткоинов является **«Тюльпаномания»**: спекулятивный финансовый пузырь, который произошел в Голландии в 1630-х годах.



«Финансовый пузырь» Тюльпаномании.

Биткоин очень часто сравнивается с Тюльпаноманией, но насколько справедливо это сравнение?

Спрос на красивые тюльпаны в 1630-х годах в Голландии породил рост цен на луковицы, из которых их выращивали. В свою очередь, рост цен на луковицы привел к тому, что очень много людей ринулись на этот рынок стремясь их купить, чтобы вырастив тюльпаны, затем продать еще дороже их луковицы. Тем самым, сначала на рынке росло количество покупателей луковиц, мечтавших быстро разбогатеть, и спрос превышал предложение, в результате цены быстро росли. Пузырь раздувался.

Но затем наступило насыщение, число продавцов выросло и предложение начало превышать спрос – рынок рухнул, а пузырь схлопнулся.

С Биткоином первичная ситуация похожа – рост цен на биткоины привлекает к нему новых пользователей, которые должны купить их у более ранних пользователей. А для этого они должны подключиться к сети Биткоина. Размер сети растет и, как мы отмечали ранее, согласно **закону Меткалфа**, растет её полезность, что еще больше толкает цену биткоина вверх. В то же время, эмиссия новых монет Биткоина не просто ограничена, она сокращается со временем. Насыщения рынка не происходит. Спрос на биткоины не удовлетворяется, а еще больше нарастает. Это также толкает цену вверх.

Создается парадоксальная ситуация – пузырь раздувается, но он не может лопнуть, поскольку спрос не падает ввиду отсутствия насыщения рынка. В результате краткосрочные периоды падения цены на биткоин (ввиду коррекции, негативных новостей и т. п. вторичных факторов) сменяются еще большим его ростом.

Резкий рост курсовой стоимости биткоина в декабре 2017 года и последовавшее за ним молниеносное падение на 60—70% заставило вновь заговорить о таком явлении, как экономический пузырь (также называемый «спекулятивным», «рыночным», «биржевым», «ценовым», «финансовым»).

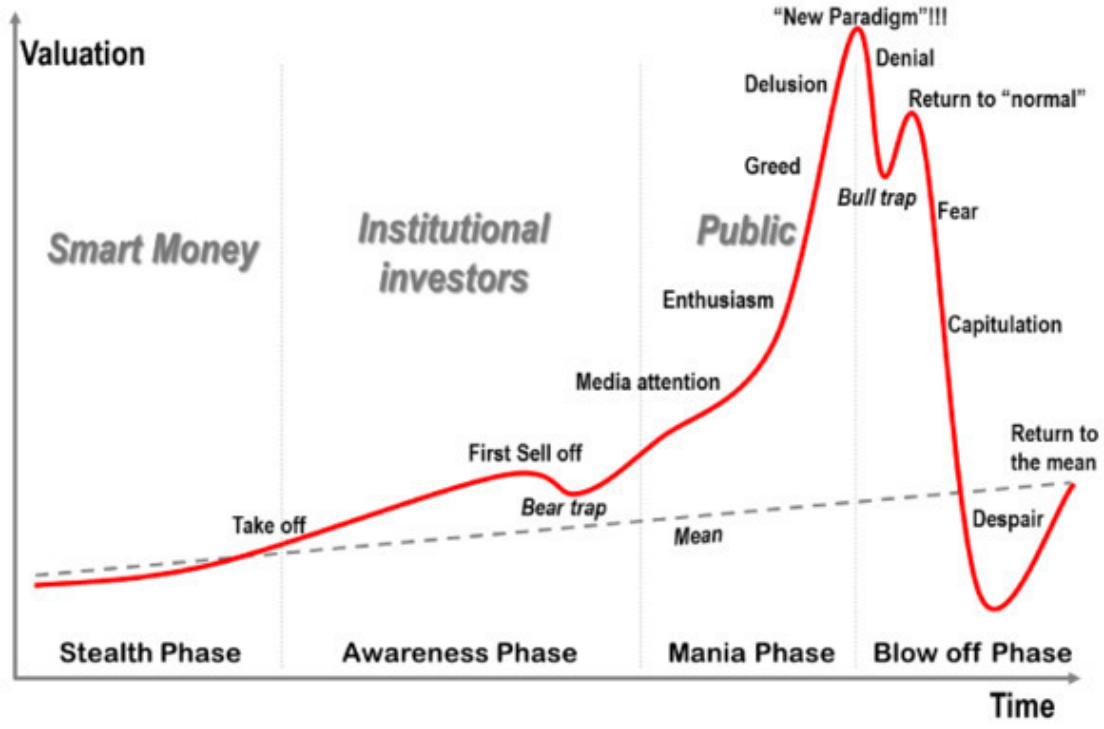


График типичного «рыночного пузыря»

График типичного «рыночного пузыря» представлен выше. Не вдаваясь в подробности, отметим четыре его основные фазы:

1. **Скрытая фаза** (Stealth Phase) – динамика рыночной цены (стоимости) актива отражает длительный умеренный рост.

2. **Фаза осведомленности** (Avareness Phase) – к активу проявляют интерес институциональные инвесторы. Наблюдается

повышенный рост рыночной цены. Для этой фазы характерен т.н. «медвежий капкан» (bear trap) – кратковременное падение рыночной стоимости актива из-за «медвежьего разворота», после которого наступает уже «бычий разворот» с нарастанием темпа роста рыночной цены.

3. **Маниакальная фаза** (Mania Phase) – повышенный рыночный рост и внимание СМИ к нему вовлекают в процесс широкие массы, желающие быстро разбогатеть на этом росте. Резко возрастает спрос на актив, который приводит к еще большему росту цены – в результате начинается лавинообразный эффект и рыночная стоимость актива взлетает.

4. **Фаза схлопывания пузыря** (Blow off Phase) – за быстрым ростом вдруг следует молниеносное падение. Но рынок еще сопротивляется и пытается восстановить цену, предшествующую падению. Однако, уже не все обладатели актива, особенно те, которые вступили в игру раньше, верят в восстановление и пытаются избавиться от него пока еще по достаточно высокой цене. После краткосрочного роста следует обвал, сопровождающийся, как правило, рыночной паникой и стоимость актива падает ниже уровня, предшествовавшего появлению «пузыря». В конце-концов, цена актива со временем уравновешивается на уровне тренда, который был в первой-второй фазе.

За всю историю Биткоина было несколько всплесков его рыночной стоимости, которые по своему характеру напоминают типичный **«рыночный пузырь»**. Но, их все отличает от классического графика «биржевого пузыря» то, что достигнув максимума на **маниакальной фазе**, биткоин никогда не падал ниже своего уровня в **скрытой фазе** и даже в **фазе осведомленности**. Другими словами, после схлопывания очередного «пузыря», биткоин никогда не падал ниже максимального уровня предыдущего «пузыря».

Рынок Биткоина будет насыщен и уравновесится, когда на него поступит очень значительная масса фиатных денег. Если биткоин, как резервный актив, займет место золота, то совокупная стоимость сети Биткоина (капитализация) может достигнуть размеров в **несколько триллионов долларов США**. Это означает, что текущая цена биткоина может вырасти еще на порядок и даже больше.

Миф 5: Биткоины незаконны, потому что они не признаны государством

С момента своего появления в январе 2009 года **Биткоин находится вне правового поля** большинства государств мира. Собственно, Биткоин, как децентрализованная денежная система, был задуман его создателем Сатоши Накамото, как способ уйти от монополии государства и банков в денежном обращении и предоставить обществу новый механизм обмена и передачи стоимости без участия третьей доверенной стороны.

Биткоину, равно как и публичному блокчейну, на котором он построен, не нужно государство и государственное регулирование. Это вполне самодостаточная система.

Само нахождение вне правового поля еще не означает незаконность. Есть многие сферы деятельности человеческой, которые не урегулированы действующими законодательствами. Во многих вопросах жизнедеятельности общество осуществляет саморегулирование на основе этики и морали, религиозных воззрений и норм, общепринятых понятий и правил или на основе целесообразности и рациональности.

Если действия индивидуума не наносят ущерба (материального или морального) другим людям и не противоречат общепринятым нормам морали и нравственности, то эти действия не могут запрещаться законом ибо в противном случае это будет нарушение базовых прав человека.

> *«При осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе».*
>
> п.2 ст.29 **«Всеобщей Декларации прав человека»**

Очевидно, что пользование системой Биткоин не является нарушением чьих-то прав и не противоречит моральным устоям общества.

Использование Биткоина для проведения транзакций также **не является предпринимательской деятельностью**, поскольку не подразумевает получения дохода.

Ведь, если вы совершаете денежный перевод в банке или на почте, вам не нужно получать разрешение на предпринимательскую деятельность или лицензию.

> **Примечание**: Не путайте трейдинг на криптовалютной бирже с пользованием системой Биткоин.

В этом смысле на Биткоин распространяется общедозволительный тип правового регулирования: **«разрешено всё то, что прямо не запрещено»**.

Кроме того, во многих странах до сих пор не определена правовая сущность биткоина (как внутренней расчетной единицы блокчейна). Что это? Валюта? Актив? Товар?

Проанализируем эту ситуацию на примере законодательства Украины. Учитывая действующие нормы (Гражданский кодекс Украины, закон Украины «О Национальном банке Украины», Декрет Кабинета министров Украины «О системе валютного регулирования и валютного контроля», закон Украины «О платежных системах и переводе средств в Украине», закон Украины «Об информации» и другие) понятие «криптовалюта» и регулирование операций с ней **не подпадают под режим регулирования** поскольку:

– криптовалюта не существует в форме банкнот, монет, записей на счетах в банках, поэтому она **не может быть признана деньгами** (денежными средствами, средствами, денежными знаками);

– криптовалюта не имеет привязки к денежной единице ни одного государства, поэтому она **не может быть признана валютой** или законным платежным средством иностранного государства и **не является валютной ценностью**;
– криптовалюта не выпускается банком и не является денежным обязательством определенного лица, поэтому она **не может быть признана электронными деньгами**;

– у криптовалюты отсутствуют признаки документа эмитента, а именно: нет установленной формы документа с соответствующими реквизитами, удостоверяющей денежное или другое имущественное право, нет определения взаимоотношений эмитента ценной бумаги (лица, выдавшего ценную бумагу) и лица, имеющего права на ценную бумагу, и не предусматривает выполнение обязательств по таким ценным бумагам, а также возможности передачи прав на ценную бумагу и прав по ценной бумаге другим лицам. А следовательно, **криптовалюта не может быть ценной бумагой**;

– у криптовалюты отсутствуют признаки документа в виде денежных знаков, отсутствует эмитент, а также отсутствует цель изготовления. Таким образом, **криптовалюта не может быть признана денежным суррогатом**.

Также криптовалюта **не обладает свойствами товара**. Собственно, биткоин существует только лишь в контексте записей транзакций с ним, а сам **не имеет ни материального, ни даже цифрового воплощения**.

«Добыча биткоина» майнерами – это всего лишь фигуральное выражение не имеющее ничего общего ни с добычей, ни с созданием товарного объекта.

Вывод: Биткоин и другие криптовалюты в настоящее время не попадают под правовое регулирование большинства государств, но это не означает, что они противозаконны.

Миф 6: Биткоины – это средство ухода от налогов

Очень распространенный тезис противников криптовалют. Но давайте рассмотрим, что за ним скрывается.

У любого налога есть база – **объект налогообложения** – реализация товаров (работ, услуг), имущество, прибыль, доход, расход и прочие обстоятельства, которые определены налоговым законодательством.

Поскольку, как я указал выше, правовая сущность биткоина во многих странах до сих пор не определена, все операции с ним **не регулируются налоговым законодательством и не попадают под налоговое регулирование** .

Многие считают, что владельцы биткоинов получают громадный необоснованный доход на росте курсовой стоимости криптовалюты и этот доход, якобы обязан подлежать налогообложению.

Но ведь курсовая разница иностранных валют не облагается налогом. Если вы, к примеру, купили американские доллары в 2008 году по 5 грн, а в 2017 продали по 25 грн, т.е. в 5 раз дороже, вы не обязаны платить налог с разницы между суммой покупки и суммой продаж.

В чем ситуация с биткоинами отличается от ситуации с американскими долларами? Вопрос риторический.

Можно ли взломать Биткоин? Возможные уязвимости и способы противостояния им

Так ли уж неуязвим Биткоин? Можно ли эту систему взломать? Ведь это означало бы, что надежность денежной системы и ваших денег в ней под угрозой.

Страх перед взломом Биткоина подогревается многочисленными сообщениями в СМИ о взломах криптовалютных бирж, начиная со знаменитого взлома биржи **Mt. Gox** в 2011 году, когда неизвестный злоумышленник (или злоумышленники) похитил биткоинов на сумму **$8,75 млн** (по курсу на тот момент).

Взломы криптовалютных бирж и компаний – не такое уж редкое событие. Вот, к примеру, список некоторых случаев:

– **июль 2014** – криптовалютная биржа ***Cryptsy*** (13 000 BTC и 300 000 LTC, что составляет примерно **$5,2 млн** по текущему курсу);

– **январь 2015** – популярная криптобиржа из Люксембурга ***Bitstamp*** (похищено около 19 000 BTC на сумму **$5 млн**);

– **апрель 2016** – ведущая платформа по торговле и обмену криптовалют ***ShapeShift*** (315 BTC, около **$130 тыс**.);

– **май 2016** – гонконгская криптовалютная биржа ***Gatecoin*** (суммарный ущерб составил 250 BTC (**$114 500**) и 185 000 ETH (**$1 850 000**), то есть суммарно около **$2 млн**);

– **август 2016** – ***Bitfinex***, одна из крупнейших криптовалютных бирж (119 756 BTC, что составило около **$70 млн**);

– **июль 2017** – ***Parity Wallet*** (хакеры взломали сервис онлайн кошельков и похитили 153 000 ETH – около **$32 млн**).;

– **январь 2018** – ***Coincheck***, одна из крупнейших криптовалютных бирж Японии, подверглась самой масштабной атаке на крипторынке. В результате взлома хакеры похитили 500 миллионов токенов NEM на сумму **$532 млн**, что стало крупнейшим ограблением в истории криптовалют;

– **февраль 2018** – взлом итальянской криптобиржи ***BitGrail***, в ходе которого было похищено 17 млн токенов Nano на сумму в более **$170 млн**.

И это далеко не все примеры.

Но взлом кода бирж еще не означает, что взломан сам Биткоин, как система. Это означает лишь то, что злоумышленники взломали стороннее хранилище приватных ключей, не более.

Например, причиной атаки на японскую криптобиржу **Coincheck** стала уязвимость в её работе, а именно то, что криптовалюты пользователей хранились на горячих кошельках, где активы всегда доступны онлайн.

Биткоин, как система, не несет и не может нести в принципе ответственности за ненадлежащее хранение приватных ключей от биткоин-адресов. Ответственность за это хранение возложена на самих владельцев адресов.

Поэтому взлом криптовалютных бирж, либо других сервисов, на которых временно хранятся приватные ключи пользователей, не является по сути взломом системы Биткоин.

> **Аналогия**: Если у вас супернадежный замок от входной двери вашей квартиры, а вор похитил из вашего кармана ключи, это не означает, что вор взломал сам замок.

За всю историю существования Биткоина (с 2009 года) не было ни одного серьезного инцидента, связанного с безопасностью и взломом, приведшего к фатальным последствиям.

Но, тем не менее, потенциальные угрозы существуют и мы сейчас их рассмотрим и выясним, насколько они реальны. Всего я выделяю три основных угрозы безопасности системы Биткоин:

– **Ошибка в коде системы**, приводящая к уязвимости.
– **Взлом приватных ключей**
– **Захват управления блокчейном** (т.н. «атака 51%»).

Ошибка в коде системы, приводящая к уязвимости

Биткоин – постоянно развивающаяся система и код её основного программного клиента **Bitcoin Core** неоднократно менялся и совершенствовался. Несмотря на то, что работу над этим кодом ведут независимые профессиональные программисты из разных уголков планеты, а окончательное решение по внесению изменений в код принимается после их всестороннего обсуждения, тем не менее существует потенциальная опасность возникновения непреднамеренных ошибок (багов) и уязвимостей. Этот риск мизерный, но он есть и его надо принимать во внимание. Тем более, что такое уже случалось в истории Биткоина.

15 августа 2010 года баг в программном коде стал причиной «грязной» транзакции в блоке **№74638** – более **184 млрд BTC** (точное значение – 184 467 440 737,09551616) были переданы в одном переводе. На два адреса было отправлено по **92,2 млрд BTC** на каждый и еще на один – дополнительно **0,01 BTC**, которых не существовало до транзакции. Это было возможно, потому что код, используемый для проверки транзакций, прежде чем включать их в блок, не учитывал настолько больших выходов, что они переполнялись при суммировании. Как известно, всего в системе может существовать **не более 21 млн BTC**.

Спустя час ошибка была обнаружена, код был исправлен в течение нескольких часов и в результате преднамеренного форка «чистый» блок **№74691** стал заменой для «грязного» в цепочке.

Это была единственная найденная и использованная существенная уязвимость за всю историю Биткоина.

Следует отметить, что подобного рода ошибки в блоках транзакций можно исправить только при помощи форка – создании более длинной цепи валидных блоков. При этом, разумеется, будут потеряны транзакции, попавшие в фейковую цепочку, но сохранены биткоины, бывшие на счетах клиентов до возникновения форка.

Взлом приватных ключей

Биткоин-адреса связаны с приватными ключами посредством криптографического алгоритма хэширования на основе функции **SHA-256**.

Хэш-функция SHA-256 является необратимой. Это означает, что невозможно вычислить приватный ключ по известному биткоин-адресу. Потребуется только перебор всех возможных вариантов, которых насчитывается 2 в 256—й степени или 10 в 77-й степени, т.е. единица с 77 нулями. Это настолько огромное число, что для него даже нет названия.

Перебрать все эти варианты в поисках соответствия адреса ключу за сколь-нибудь приемлемое время при существующем уровне развития компьютерной техники невозможно. Говорят, что если бы все компьютеры Земли одновременно решали эту задачу, то потребовалось время, сравнимое со временем существования нашей Вселенной.

Но компьютерная техника и технологии не стоят на месте, а стремительно развиваются. Не исключено, что хэш-функция SHA-256 будет когда-то взломана. Возможно, для этого будет использован разрабатывающийся сейчас **квантовый компьютер**. Однако, когда это случится, сколько для этого потребуется ресурсов, включая энергетические, пока предсказать сложно.

Более того, полноценный универсальный квантовый компьютер является пока гипотетическим устройством, а американский физик немецкого происхождения, бывший руководитель исследовательского подразделения IBM[22] **Рольф Ландауэр** (*Rolf Landauer*) и вовсе говорил, что:

> «…проекты квантовых вычислений, опираются на спекулятивную технологию. В своей нынешней форме она не принимает в расчет всевозможные источники шумов, ненадежностей и ошибок производства, так что работать, скорее всего, это не будет».

Поэтому, **взлом SHA-256 в настоящее время – это из области фантастики**.

[22] **IBM** (International Business Machines) – американская компания, один из крупнейших в мире производителей аппаратного и программного обеспечения, а также поставщик IT-сервисов и консалтинговых услуг.

Захват управления блокчейном («атака 51%»)

«Атака 51%» – это состояние, когда более половины вычислительной мощности сети Биткоина контролируется одним майнером или группой майнеров. Теоретически, этот объём вычислительной мощности дает власть над сетью. Это означает, что каждая клиентская программа в сети верит в подтвержденный блок транзакций атакующей стороны. Что позволяет атакующим осуществить контроль над сетью, включая следующие полномочия:

– создавать транзакции, конфликтующие с чужими;
– останавливать подтверждение чьей-либо транзакции;
– тратить одни и те же монеты несколько раз;
– мешать другим майнерам формировать действительные блоки.

Но высокая затратность майнинга вследствие применения **PoW** (доказательства выполненной работы) служит надежной защитой от попыток взлома денежной сети и осуществления над ней контроля, делая экономически нецелесообразной т.н. «атаку 51%».

В настоящее время (по состоянию на 14.10.2018) для проведения такой атаки необходимо приобрести оборудования на сумму более **$9,3 млрд** плюс нести затраты на электроэнергию в размере более **$6 млн в сутки**[23].

Теоретически это возможно, но практически трудно осуществимо.

Выводы:

В настоящее время система Биткоин имеет достаточно **надежную защиту от взлома и несанкционированных действий**. Эта защита обеспечена:

– надежным и открытым программным кодом, над которым трудятся профессиональные программисты со всего мира;

– надежным криптографическим алгоритмом хэш-функции SHA-256;

– надежной защитой от «атаки 51%», делающей её очень дорогостоящей.

[23] По данным сайта **GoBitcoin.io**

Биткоин: Предупреждение о рисках Основные опасности и угрозы, связанные с использованием децентрализованной электронной денежной системы Биткоин

Ранее в разделе **«Можно ли взломать Биткоин?»** я анализировал уязвимость Биткоина, как системы, но помимо уязвимости есть и другие опасности и угрозы, связанные с пользованием первой криптовалютой и несущие определенные риски для пользователя. Остановимся подробнее на этих рисках.

Все риски, связанные с электронной денежной системой Биткоин, можно условно разделить на две больших группы:

– Риски самой системы.

– Риски пользования системой

Начнем со второго, поскольку рядовой пользователь чаще с этим сталкивается.

Риски пользования системой

Как известно, Биткоин – полностью **децентрализованная система**, которая не имеет единого центра управления. **Вся ответственность** за безопасность доступа к биткоин-адресам, на которых хранятся собственно биткоины (криптовалюта) **лежит на пользователях**. Только они имеют (должны иметь) доступ к приватным ключам, связанным с соответствующими биткоин-адресами.

Поэтому безопасность использования Биткоина, как системы, – это **безопасность хранения и строго ограниченный доступ к приватным ключам**. Утрата приватных ключей в результате их потери или кражи ведет к потере управления биткоин-адресами и, как следствие, к потере криптовалюты, хранящейся на этих адресах. Желательно использовать биткоин-кошельки, поддерживающие технологию seed-ключа.

Подробнее об использовании биткоин-кошельков и их разновидностях читайте в главе **«Кошельки и транзакции»**.

Сама система Биткоин устойчива к взлому благодаря криптографическим алгоритмам защиты. Теоретически при нынешнем состоянии технологии эта система не может быть взломана в течение весьма длительного, практически неограниченного времени, и за период своего существования (с 2009 года) продемонстрировала свою защищенность и надежность.

Но различные сторонние онлайн-сервисы, обслуживающие эту систему, – обменные пункты, онлайн-кошельки, криптобиржи и т. п. – могут стать и неоднократно становились объектом хакерских атак в результате которых пользователи теряли свои средства.

Поэтому хранение криптовалюты на всевозможных онлайн-сервисах несет риски их утраты в случае взлома этих сервисов, а также недобросовестности их владельцев.

Другая опасность пользования системой Биткоин связана с тем, что **транзакции в ней отменить нельзя**. Нельзя также внести изменение в уже отправленное распоряжение о переводе. В случае ошибки можно лишь совершить возврат средств с биткоин-адреса, на который они были отправлены, и то по согласованию с владельцем этого адреса.

Это означает, что в случае неправильно указанного биткоин-адреса получателя переводимые средства попадут не туда и будет весьма проблематично, а чаще вообще невозможно их вернуть. Более того, при ошибке в адресе получателя эти средства могут быть безвозвратно потеряны в целом для системы, т.е. фактически изъяты из обращения.

Риски системы Биткоин

Опасностей и угроз, связанных с самой системой гораздо больше и их можно условно разделить на три группы:

– Технологические риски.
– Правовые и регуляторные риски.
– Социальные риски или риски принятия.

Технологические риски – это риски, связанные с самой технологией системы Биткоин. Они в свою очередь делятся на риски уязвимости и ошибок кода, взлома и несовершенства.

Серьезных уязвимостей, связанных с ошибками в коде, которые привели бы к неисправимым и катастрофическим последствиям, до настоящего времени не было обнаружено. Биткоин, как система, показал свою устойчивость на протяжении почти 10 лет своего существования. Следует отметить, что это постоянно развивающаяся платформа, которая может иметь технологические надстройки и расширения. Её создавали и продолжают совершенствовать одни из лучших программистов планеты. Программный код Биткоина открыт и это не только добавляет доверия к системе, но и позволяет любому человеку анализировать, искать ошибки и уязвимости и делать предложения по развитию.

Тем не менее, это не означает, что какие-то серьезные уязвимости и ошибки в коде, которые могут подорвать работоспособность системы, не могут быть уже обнаружены, а также преднамеренно или непреднамеренно внесены позднее. Это могут быть системные или программные ошибки, которые существенно подорвут веру в биткоин.

Также у Биткоина существуют **проблемы с масштабируемостью** (устойчивой работой при большом количестве транзакций в единицу времени). Но есть и пути их решения. То, каким образом это будет сделано, повлияет на дальнейшее развитие Биткоина, как системы.

Как уже отмечалось выше, **Биткоин – достаточно устойчивая к взлому и защищенная система**. Одна из возможных атак – подбор приватных ключей к биткоин-адресу – в настоящее время при текущем технологическом уровне развития человечества практически невозможна.

Для взлома алгоритма SHA-256, лежащего в основе создания биткоин-адресов и приватных ключей к ним, потребуется совершить 16 в 64-й степени итераций. Возможности современной вычислительной техники не позволяют выполнять вычисления такого объема в скольнибудь реальные сроки.

Однако, развитие техники не стоит на месте. Большие надежды в выполнении подобного рода операций возлагаются на т.н. **квантовые компьютеры** и **квантовые вычисления**. Однако, неизвестно, когда будет создан квантовый компьютер требуемой мощности и каковы будут энергетические затраты на подобные вычисления. Тем не менее, хотя бы теоретически, возможность взлома Биткоина в будущем существует. Вопрос лишь в том, насколько отдаленным будет это будущее? 10 лет, 10 столетий или 10 тысячелетий?

Другая известная атака на Биткоин – это т.н. **«атака 51%»**. Но это очень дорогое удовольствие, которое в коммерческом плане сейчас бессмысленно. В настоящее время (по состоянию на 14.10.2018) для проведения такой атаки необходимо приобрести оборудования

на сумму более **$9,3 млрд** плюс нести затраты на электроэнергию в размере более **$6 млн в сутки**[24].

Естественно, что сеть и рынок мгновенно отреагируют на эту атаку и курс биткоина обвалится, что делает подобное мероприятие, как отмечалось выше, абсолютно бессмысленным в коммерческом плане.

Но на такую атаку могут решиться **правительства и центробанки**, если увидят в Биткоине реальную угрозу существования денежным системам, которыми они управляют. В демократических странах Запада это вряд ли возможно, поскольку избиратели не простят таких действий своим властям и последние это прекрасно понимают, а в таких странах, как КНДР и Иран – вполне возможно.

Другого рода технологические угрозы Биткоину исходят от более совершенных в технологическом плане криптовалют, которые появляются и могут появиться в будущем. Но для успеха этих новых криптовалют мало иметь технологическое преимущество, необходимо создать сеть достаточных размеров, сообщество (пользователи, майнеры) и инфраструктуру (обменники, биржи, сервисы и т.п.), а также получить признание социума.

В любом случае, угроза Биткоину от новой, технологически более совершенной криптовалюты будет исходить постепенно, с нарастанием и сеть, а также пользователи сумеют вовремя на неё отреагировать.

Правовые и регуляторные риски для Биткоина исходят от действий государственных органов власти, которые будут стремиться установить правовой статус криптовалюты и правила её использования.

Государства мира впервые столкнулись с такой масштабной децентрализацией, как криптовалюты. Будучи по своей сути технологией передачи стоимости, которая не контролируется единым финансовым центром, криптовалюты, базирующиеся на публичном блокчейне, такие, как Биткоин, способны в долгосрочной перспективе заменить национальные деньги и привычное финансовое посредничество банков. Это создает угрозы государственной монополии на деньги и их обращение.

Поскольку Биткоин является полностью децентрализованной одноранговой системой, не имеющей единого центра управления и отказа, **у государств нет механизма воздействия на её работоспособность** (кроме «атаки 51%», о чем было сказано выше). Нельзя просто так взять и запретить криптовалюты! Для этого потребуется, как минимум, отключить повсеместно в мире интернет и (или) электричество.

Поэтому любые попытки со стороны государств регулировать собственно криптовалюты, их эмиссию и их транзакции обречены на провал.

Но государство может регулировать сферу, в которой криптовалюты соприкасаются с фиатными деньгами, а именно – криптовалютные биржи, обменные пункты, инвестиционные фонды и другие финансовые учреждения, оказывающие услуги на криптовалютном рынке. Государства также могут запретить предприятиям и организациям принимать биткоины в качестве оплаты за товары и услуги, а гражданам – расплачиваться биткоинами.

Некоторые государства, особенно авторитарные и тоталитарные, даже могут ввести уголовную ответственность за операции с криптовалютами и их майнинг.

Эти угрозы, исходящие от правительств, будут скорее всего локальны и распространятся на отдельные страны.

[24] По данным сайта **GoBitcoin.io**

Цивилизованный мир пойдет по другому пути – правительства и центробанки западных стран будут создавать свои, **альтернативные Биткоину, криптовалюты**. Поэтому Биткоин ждет скорее не запрет, а конкурентная борьба на денежных рынках.

Социальные риски или риски принятия исходят от населения. Это своего рода риски доверия – насколько массовым будет доверие общества к новому виду денег.

Эти риски в большей степени зависят от успехов и неудач самих криптовалют, а также от средств массовой информации, которые способны что-то скрыть, а что-то раздуть.

Процесс принятия и проникновения криптовалют будет непростым и длительным – бумажные фиатные деньги также не сразу вытеснили золотые и серебряные монеты. Но время здесь работает на Биткоин – приходит новое поколение, лояльное к новым технологиям, и уходит старое, привыкшее доверять государству и банкам.

Очевидно, что принятие населением криптовалют будет более быстрое в странах, где доверие к местной валюте падает, где высока инфляция, и правительства которых не справляются с финансовыми кризисами. Так, например, уже происходит в **Венесуэле** и **Зимбабве**.

Эти риски будут снижаться по мере роста общемирового признания и принятия Биткоина. Но они также связаны с технологическими и особенно правовыми рисками. Любая технологическая проблема Биткоина будет увеличивать и социальные риски, так же как и различные запреты и ограничения криптовалют, вводимые властями на законодательном уровне.

Я не затрагивал т.н. **инвестиционные риски** Биткоина, поскольку это другая тема. Безусловно, пользователи биткоинов могут быть объектами для мошеннических или высокорисковых инвестиционных схем. Но это применимо к любым активам, в том числе и фиатным деньгам. Это не проблемы Биткоина, как системы, это проблемы людей, которые доверяются различного рода мошенникам, играющим на алчности и создающим финансовые пирамиды с целью выманить деньги у доверчивого обывателя.

Я также не затрагивал риски, связанные с биржевыми играми (**трейдингом**) с биткоином. Это также другая тема, не имеющая прямого отношения к Биткоину, как системе. Эти риски мало отличаются от аналогичных рисков при трейдинге на фондовом рынке или на рынке FOREX.

Не были затронуты и риски, связанные с майнингом биткоина. Это отдельная тема…

Да и **«черные лебеди»**[25] появляются внезапно.
Помните об этом!

Биткоин, как система электронной денежной наличности, создавался, как альтернатива нынешней денежно-финансовой системе, которая монополизирована и контролируется государством.

За 10 лет своего существования эта первая (во всех смыслах) криптовалюта прошла большой путь – **от неизвестности, недоверия и непринятия до проникновения в умы и впечатляющего роста** капитализации, которая уже опережает объемы обращения многих национальных валют.

[25] **«Чёрный лебедь»** – теория, рассматривающая труднопрогнозируемые и редкие события, которые имеют значительные последствия. Названа по книге Нассима Талеба «Чёрный лебедь. Под знаком непредсказуемости», в которой он ввёл термин «события типа „чёрный лебедь“».

Способен ли Биткоин стать новым видом денег, а общество принять эту **новую денежную парадигму**, покажет время.

Три барьера на пути Биткоина
Биткоин в настоящее время имеет ряд препятствий, стоящих перед ним.

1. Масштабирование

В 2010 году создатель Биткоина Сатоши Накамото ввёл ограничение на размер блока транзакций в **1 мегабайт**. Это ограничение позволило улучшить совместимость узлов сети, а также снизить эффективность DDoS-атак[26], но привело к снижению максимальной пропускной способности сети до 3—7 транзакций в секунду. Если превысить эти пределы, то возникнет перегруженность сети, что приведёт к более высокой стоимости транзакций и потенциально более длительному времени проверки.

Предлагалось увеличить размер блока, что было реализовано в форках Биткоина **Bitcoin Unlimited** и более успешном **Bitcoin Cash (BCH)**. Но основная масса биткоин-сообщества не приняла этот подход к развитию Биткоина а, соответственно, и эти форки.

Для решения ряда проблем, в том числе и проблемы масштабирования, в конце 2015 года было предложено обновление **Segregated Witness** (SegWit). Суть его заключается в вынесении подписей транзакций в структуру вне основного блока, что значительно разгружает последний. SegWit был активирован **24 августа 2017 года.**

Новая технология в виде платежного протокола **Lightning Network**, который фактически является надстройкой над блокчейном, позволит значительно повысить масштабируемость Биткоина и сделать транзакции в сети практически мгновенными, вместо текущих 30—60 минут, чтобы получить 3—6 подтверждений блока. Сейчас (конец 2018 года) идет постепенное внедрение этой технологии.

Также ведутся разработки и других технологий, повышающих масштабирование Биткоина, таких, как **MAST**, **MimbleWimble** и др.

[26] **DDoS-атака** (*Distributed Denial of Service* — распределённая атака типа «отказ в обслуживании») – хакерская атака на вычислительную систему с целью довести её до отказа.

2. Пользовательский интерфейс

В настоящее время у вкладчиков банков есть несколько способов получить доступ к своим деньгам. Дебетовые карты, кредитные карты, банкоматы, онлайн-банкинг, наличные деньги (которые банки хотят ликвидировать), а также физические места для посещения и проведения банковских операций. Настройка банковского счета или перемещение денежных средств осуществляется с помощью пользовательских компьютерных интерфейсов, которые предлагают банки.

Люди привыкли к такому простому в пользовании банковскому интерфейсу. Биткоин никогда не будет принят массами, если не будет создан столь же простой и удобный в использовании интерфейс. Биткоин-банкоматы существуют, но не только это привлекает массового потребителя. Нужны очень простые и одновременно надежные пользовательские интерфейсы, позволяющие управлять биткоин-кошельками и транзакциями.

3. Одобрение властей и конфиденциальность

Различные правительства во всем мире имеют разные мнения относительно использования Биткоина. Более прогрессивные правительства рассматривают биткоин, как виртуальную валюту, которая облагается налогом на прибыль от прироста капитала, если торговля идет с прибылью, и облагается налогом с продаж, если она используется для покупки товаров и услуг.

Но для того, чтобы Биткоин и другие криптовалюты получили более широкое применение в качестве реальной валюты, должна быть публичная уверенность в том, что использование биткоинов при расчетах в магазине или в интернете не приведет к их аресту или другим неприятностям. Без этой гарантии широкое принятие криптовалют сильно затрудняется. Об этом говорилось в главе **«Риски системы Биткоин»**.

Альтернативой является более глубокая **конфиденциальность**. Биткоин анонимный, но не совсем. Его публичный реестр является неизменным и общедоступным. Если у вас есть кошелек (биткоин-адрес), который кто-то знает, то каждая транзакция, когда-либо сделанная с этим кошельком, прослеживается к любому другому кошельку, с которым вы совершали эту транзакцию.

Есть более новые и лучшие криптовалюты в плане анонимности и конфиденциальности, но это ничего не значит до тех пор, пока вы не сможете использовать их в качестве денег на белом рынке (любые товары и услуги, которые облагаются налогом). Т.е. необходимо **широкомасштабное принятие криптовалюты в качестве собственно валюты** (денег).

Биткоин – «финансовый интернет»

В мире до сих пор идут споры, чем же на самом деле является биткоин? Это валюта, товар, актив или средство сохранения стоимости? Может ли биткоин выступать в роли денег? Попробуем найти ответы на эти вопросы.

Деньги и Биткоин
Некоторые рассуждения о природе и эволюции денег

Денег в природе нет! Действительно, ни в животном, ни, тем более, растительном мире нет сущности, которую можно назвать деньгами. Во всяком случае, современной науке это неизвестно.

Деньги придумал человек. Они возникли в результате ***отношений*** между людьми.

И это действительно необычное и значимое изобретение, наряду с такими социальными изобретениями, как письменность, религия и государство.

Зачем же человеку понадобились деньги?

Деньги нужны для взаимного обмена товарами (торговли) и взаиморасчетов между людьми

Первоначально между людьми (племенами) существовал исключительно бартерный обмен:

> **Товар** (корова) – **Товар** (три мешка зерна)
> *Товар – это продукт или услуга (выполненная работа).*

Но потом человек придумал деньги и формула обмена изменилась (почти по Марксу):

> **Товар** (продажа) – **Деньги – Товар** (покупка)

Чтобы получить ***деньги***, надо что-то продать – или ***продукт*** (корову, мешок зерна, глиняный горшок, меч и т.п.), или ***услугу*** (выполненную работу). Получив деньги, на них можно что-то купить – другой продукт или другую услугу (работу).

Таким образом, из этого вытекают базовые функции (свойства) денег:

> **Деньги – это всеобщий эквивалент** (мера) **стоимости товаров** (продуктов и услуг) и **деньги – это средство обращения.** Они выступают как посредник в обмене (обращении) товарами.

Кстати, **деньги – это тоже товар.** Их можно продавать за другие деньги (золото за серебро, банкноты за золото, валютный обмен). Собственно, когда происходит продажа или покупка товара за деньги, то это есть ничто иное, как **обмен товарами**.

Но, поскольку деньги – это товар, то у него должно быть некое материальное воплощение.

Материальное воплощение товарных денег может быть различным – ракушки, наконечники стрел и т.п., золото и серебро, монеты. А следовательно: товарные деньги – это **способ сохранения стоимости.** Можно продать сначала один мешок зерна, получив за него деньги, затем (через время) – второй и третий, постепенно накапливая нужную сумму. И в итоге – купить корову.

Таким образом, деньги выполняют функцию **накопления богатства.** Это позволяет как бы переносить покупательную способность денег из настоящего в будущее. Если сейчас

вы не можете что-то купить, то накопив денег, вы купите это в будущем. Т.е. деньги способны сохранять свою покупательную способность во времени (с учетом инфляции /*см. ниже*/, разумеется).

Но можно договориться с продавцом коровы и купить её в долг, пообещав продавцу заплатить (внести платеж) позже, когда будут проданы мешки зерна.

Вследствии чего деньги также выступают как **средство платежа.** Т.е. не в момент совершения торговой сделки (покупки-продажи), а в другое время – ранее (предоплата) или позднее (кредит).

Но, чтобы ***товарные деньги*** стали деньгами, они должны иметь некоторые свойства, которые их выделяют среди других товаров.

Базовые свойства товарных денег:

– их ***ограниченное количество*** (добыча затруднена или эмиссия ограничена);

– их ***трудно подделать или воспроизвести***;

– они ***однородны*** и ***делимы*** (первое означает, что денежные единицы не должны отличаться друг от друга, а второе – что деньги должны легко делиться, чтобы ими можно было заплатить любую сумму);

– они ***хорошо сохраняются*** (не портятся, не теряют вес и т.п.), т.е. остаются ***неизменными***;

– они ***достаточно компактны*** (при высокой стоимости) и могут легко транспортироваться, т.е. ***мобильны***;

– они имеют ***внутреннюю стоимость*** (полезность, значимость).

Пример товарных денег – ***золото***. Запасы его ограничены, а добыча затруднена. Его трудно подделать. Оно не ржавеет и плохо подвергается воздействию агрессивной внешней среды, т.е. сохраняет свой вид и вес. Оно красиво (блестит) и может использоваться как украшение или как промышленный материал (имеет внутреннюю стоимость). Обладает высоким спросом на рынках, включая международные.

Поэтому золото, наряду с серебром, долгое время являлось основным материалом для изготовления товарных денег (монет).

Кстати, **монополию на изготовление денег присвоило себе государство** *(правители и правительства).* Сначала оно чеканило золотые и серебряные монеты, а затем стало печатать бумажные ***банкноты*** и делать монеты из дешевых материалов (медь и ее сплавы, сталь, алюминий), гарантируя их обмен на золотые монеты и товары по установленной стоимости (номиналу). Так, на замену товарным деньгам пришли т.н. ***фиатные деньги***.

Фиатные (фидуциарные) деньги – это бумажные деньги (банкноты) и монеты, которые выпускает государство. Их печатает (делает эмиссию) центробанк или монетный двор. При

этом установленная номинальная стоимость этих банкнот и монет не зависит от стоимости материала, из которых они сделаны.

Эти деньги не имеют т.н. внутренней стоимости (полезности) и обращаются исключительно основываясь на ***доверии*** к ним общества (продавцов и покупателей).

Доверие – краеугольный камень любой финансовой (денежной) системы

Доверие к фиатным деньгам в основном **обеспечивается законодательно** – закон обязывает все учреждения и организации принимать в качестве оплаты национальную валюту по её номиналу. Но у государства всегда есть соблазн напечатать больше денег, чтобы решить бюджетные проблемы.

Эмиссия – дополнительный выпуск денег государством, увеличение денежной массы. В результате часто происходит **инфляция**.

Инфляция – обесценивание денег, снижение их покупательной способности и, как следствие, возникновение недоверия к фиатным деньгам.

Но вернемся к **основным функциям денег**. Как мы выяснили ранее, они выступают как:

– ***мера стоимости***;
– ***средство обращения***;
– ***средство накопления;***
– ***средство платежа.***

Обмен (покупка-продажа) товарами и платежи – это **взаиморасчет** между сторонами (покупателем и продавцом, должником и кредитором). Деньги (как мера стоимости) – элемент этого взаиморасчета. Т.е. три из четырех основных функций денег сводятся к взаиморасчету.

Взаиморасчеты можно отражать **транзакциями** – записями, кто, сколько, кому заплатил. Собственно, банки и другие финансовые учреждения так и делают. Они ведут бухгалтерский реестр (***ledger***) всех транзакций своих клиентов и подсчитывают их платежный **баланс** (суммы денег на банковском счете), чтобы определять платежеспособность.

Банки пошли еще дальше и ввели т.н. ***безналичные расчеты*** – когда деньги списываются со счета покупателя или должника и зачисляются на счет продавца или кредитора. Наличные деньги в этой операции не участвуют. Разумеется, клиент банка может получить и наличные деньги (банкноты) в кассе банка или банкомате. Но для проведения безналичных платежей (включая и использование банковских пластиковых карт) достаточно иметь на своем счету (балансе) в банке необходимую сумму.

Банковские безналичные транзакции стали привычными. Осталось сделать следующий шаг – **полностью отказаться от наличных денег**. Для этого нужно обеспечить технологическую возможность повсеместного проведения безналичных транзакций.

В условиях централизованной банковской системы это будет означать, что люди в принципе не смогут обменяться деньгами и совершать сделки друг с другом без посредничества банков.

Наличные деньги не нужны, если есть всеобщая бухгалтерская книга (реестр), в которой отражены все транзакции и движение денег.

Но, как это сделать? Создать единый (на весь мир) банк, который будет вести все операции (транзакции) всех людей на Земле?

Или вовсе отказаться от банковских посредников и проводить взаиморасчеты (транзакции) напрямую? Но, кто тогда будет вести глобальный учет этих транзакций?

Собственно, эти мысли и вопросы привели к созданию первой в мире одноранговой (без посредников и единого центра) сетевой электронной денежной системы – Биткоина (*Bitcoin*).

Биткоин – это способ передачи стоимости от одного лица к другому без участия третьей стороны, посредника (банка). Он сам по себе не имеет денежного эквивалента стоимости; он обладает не внутренней стоимостью, а *очень высокой полезностью*. По сути – это ***инструмент*** *(метод, протокол)* ***для осуществления транзакций*** – передачи некоторой стоимости от одного субъекта к другому. Это своего рода ***финансовый интернет*** – сеть, которая обеспечивает совершение безналичных платежей и расчетов.

Биткоин, как система платежей, не привязан ни к одной денежной единице (валюте) мира. Он имеет собственную внутреннюю расчетную единицу, называемую ***биткоином (BTC)***. Это совершенно новый вид денег – ***криптовалюта***.

Биткоин, будучи децентрализованной системой, основанной на криптографии, **решает вопросы доверия** между участниками без привлечения третьей стороны. Как уже отмечалось выше, *доверие – краеугольный камень любой финансовой (денежной) системы*. В Биткоине вопрос доверия между субъектами решается математическими и ***криптоэкономическими методами***. Доверительный посредник (банк) становится ненужным в денежных отношениях. А, следовательно, сокращаются затраты на услуги этого посредника. Разумеется, полностью отказаться от комиссионных при проведении платежей в сети Биткоина невозможно, поскольку необходимо компенсировать затраты сети на майнинг (ведение реестра транзакций). Но суммы этих комиссионных значительно меньше, чем банковские услуги.

Собственно, биткоин, как денежная единица, **обладает всеми свойствами товарных денег:**

– ***ограниченное количество*** (эмиссия биткоина убывает со временем и ограничена 21 млн монет);

– ***чрезвычайно трудно подделать*** (биткоин защищен криптографическим протоколом);

– ***хранится вечно*** (фактически – это записи в распределенном реестре – базе данных на десятках тысяч компьютеров);
– они ***однородны*** и их можно ***дробить*** (делить) на очень мелкие единицы (до 0,00000001);
– ***внутренняя стоимость*** (полезность, значимость) биткоина обусловлена его уникальной способностью сохранения и передачи стоимости на расстояния без участия доверенного посредника, высокими затратами на т.н. *майнинг* – проведение транзакций и выпуск новых монет, а также его безопасностью и прозрачностью, что обеспечивается использованием технологии блокчейна, и отсутствием посредника при совершении сделок и платежей.

Биткоин также способен выполнять все **функции денег** – выступать как **средство платежа** и **обращения**, быть **мерой стоимости** (которую определяет рынок, а не центробанки) и способом **накопления богатства**. И, к тому же, не подвергаться инфляции. Кроме того, биткоин может вступать и в роли **мировых денег**, обеспечивая трансграничные платежи.

Подведем итоги:

Биткоин (Bitcoin) – это новая распределенная, децентрализованная, электронная денежная система, построенная на записи финансовых транзакций в реестр (единую бухгалтерскую книгу), называемый также блокчейном.

Её расчетная единица (биткоин) **обладает всеми свойствами денег и способна выполнять их функции.**

Кроме того, система Биткоин:

– имеет ограниченную эмиссию;
– обеспечивают гарантию владения и сохранности за счет криптографической защиты приватными ключами;
– не связана с государствами и правительствами;
– не имеет единого центра управления и регулирования;
– обеспечивает высокую защиту и конфиденциальность;
– способна достаточно быстро проводить транзакции независимо от их суммы;
– способна развиваться и совершенствоваться.

Разумеется, Биткоин – это пилотный проект и не лишен некоторых недостатков. В частности, высокой ***волатильности*** курса стоимости вследствие относительно небольшого объема сделок. Но это болезнь роста. Другие проблемы Биткоина, такие как ***масштабируемость*** и ***скорость транзакций***, являются вполне решаемыми технологически. К тому же, появление Биткоина спровоцировало лавинообразный рост других криптовалютных проектов.

Станет ли биткоин (или другая криптовалюта) настоящими деньгами – это дело будущего. И это – вопрос **доверия**. Но доверия уже в социальном смысле. Способен ли мировой социум **принять новую денежную парадигму**? Как некогда он принял фиатные деньги (банкноты), заменив ими золотые и серебряные монеты во взаиморасчетах.

Безусловно, появление Биткоина – это настоящая **революция** в области денег и финансовых систем. Мир денег уже не будет таким, каким мы его знали.

Что влияет на стоимость биткоина

В момент появления в начале 2009 года биткоин не имел никакой стоимости. К осени того же года за 1 биткоин давали 0,08 центов ($0,0008). Через 8 лет, к концу 2017 года, его курс перевалил за $10 000, достигнув почти $20 тысяч. А в 2018 году упал до $6500.

Поскольку биткоин, как децентрализованная криптовалюта, не подвержен регуляции со стороны государства, его курсовая стоимость по отношению к фиатным валютам (доллар, евро и пр.) сейчас в основном формируется в ходе торгов на криптовалютных биржах.

Биржевая цена формируется исходя из **баланса спроса и предложения**. Поэтому стоит проанализировать, что влияет на спрос на биткоин и как формируется предложение на него же.

1. **Ограниченное количество монет** (расчетных единиц). Дефицит порождает спрос, а следовательно, – цены на дефицитный товар растут. Как известно, максимальное количество биткоинов ограничено **21 млн монет** (почему это так, читайте в главе **«Почему количество биткоинов конечно»**). В настоящее время в обращении находятся чуть более 16 млн биткоинов. Ограничение на эмиссию биткоина вкупе с потерей монет при утрате доступа к кошелькам делают эту криптовалюту дефляционной. В перспективе именно ограниченная эмиссия биткоина будет толкать его рыночную цену вверх. В этом смысле биткоин подобен золоту – его так же трудно добывать и трудно подделывать.

2. **Торги альткоинов в паре с биткоином на криптовалютных биржах**. Эта особенность работы криптовалюных бирж приводит к тому, что при росте спроса на альткоины, одновременно растет спрос и на биткоин, поскольку для покупки альткоинов (будь то лайткоин, даш, монеро или любая другая криптовалюта) необходимо заплатить за них биткоинами. Что повышает спрос на последние и ведет к росту их курсовой стоимости.

3. **Рост сети биткоина**. Появляются новые пользователи (кошельки), новые ноды (узлы) и новые майнеры. Сам по себе рост сети уже ведет к увеличению её полезности (а значит и ценности), которая, согласно **закону Меткалфа**, пропорциональна квадрату численности пользователей. Кроме того, увеличение количества пользователей сети биткоина ведет к увеличению спроса на него.

4. **ICO (Initial Coin Offerings)** – способ привлечения первичного капитала с использованием криптовалюты. Этот новый инвестиционный инструмент не только стимулирует спрос на криптовалюты, включая и биткоин, но и привлекает к ним широкое внимание. Количество ICO и объемы привлекаемых ими финансовых ресурсов растут.

5. **Быстрый рост курсовой стоимости биткоина**. Рост активов всегда привлекает инвесторов. А быстрый рост – и подавно! За два года (2016—2018) биткоин вырос в рыночной цене в 10 раз. Это, с одной стороны, привлекает к нему растущий финансовый интерес, что ведет к росту спроса на криптовалюту, порождая эффект лавины. С другой стороны, биткоин попадает в ловушку **закона Грешема**, согласно которому **«худшие деньги вытесняют из обращения лучшие»** (другая формулировка: «дешёвые деньги вытесняют дорогие»). Владельцы биткоина неохотно с ним расстаются, поскольку эта криптовалюта становится хорошим **средством накопления богатства**. Последнее приводит к уменьшению предложения на рынке и, как следствие, – к росту цены. Как отмечалось выше, дефицитный товар стоит

дороже. Но у быстрого, лавинообразного роста есть и обратная сторона – после эйфории может так же быстро наступить и паника, которая обрушивает цены и рынок.

6. **Новостные индикаторы**. Это «палка о двух концах». Рынок быстро реагирует как на положительные новости о криптовалютах, так и на отрицательные. Разумеется, положительные события укрепляют бычий тренд и усиливают курсовой рост, а отрицательные – приводят к т.н. медвежьему развороту рынка – переходу от роста к падению котировок. Например, в январе 2017 года отрицательное решение Комиссии по ценным бумагам и биржам США (SEC) относительно ETF братьев Уинклвоссов (*Winklevoss Bitcoin Trust*) сломило бычий тренд биткоина и привело к падению его курса. Новостные индикаторы – самые непредсказуемые факторы, влияющие на рынок, включая и рынок криптовалют. Плохая новость может серьезно пошатнуть любую криптовалюту.

7. **Технологические прорывы и проблемы**. Отдельно выделим это потому, что среди прочих новостных индикаторов они занимают значимое место, поскольку имеют внутреннюю природу, а не внешнее влияние. Такие проблемы биткоина, как, например, масштабируемость, могут привести к утрате доверия к нему и, как следствие, – уходу рынка в другие криптовалюты и падение курсовой стоимости биткоина. С другой стороны, технологические решения, которые улучшают функциональные свойства биткоина и решают его проблемы, приводят к росту доверия к нему, росту его популярности и, в конечном счете, – росту его рыночной цены.

8. **Влияние государственных институтов**. Это внешний фактор, но игнорировать его не стоит! Современный финансовый мир в значительной мере зависит от государственного регулирования. Отношения государств к криптовалютам вообще и к биткоину, в частности, будут в ближайшее время влиять и на рынки этих криптовалют. Здесь есть как риски, так и возможности. Но практика показывает, что государственное вмешательство в бизнес чаще приводит к негативным последствиям для последнего.

9. **Теневой рынок**. Криминальные (наркотики, оружие, торговля органами, финансирование терроризма, уход от налогов и т.п.) и полукриминальные («серые» схемы, откаты и взятки и т.п.) сделки сейчас в большей мере осуществляются в более защищенных анонимных криптовалютах (даш, монеро, зеткоин и т.п.). Но, учитывая пункт 2, теневой рынок оказывает существенное влияние и на спрос на биткоины.

10. **Биржевые спекуляции**. Высокая волатильность курса биткоина привлекает большое количество биржевых спекулянтов, играющих как на повышение, так и на понижение курса, зарабатывая на этом. Спекулятивные ставки на биржах также влияют на изменение курса биткоина.

В заключение отметим, что биткоин, как новый привлекательный предмет инвестиций, несет и риски, которые надо учитывать при формировании инвестиционного портфеля. Подробнее об этом читайте в главе **«Биткоин: Предупреждение о рисках»**.

Из всех этих 10 пунктов стоит подробнее остановиться на пункте №3 – **Рост сети биткоина**.

Закон Меткалфа гласит, что полезность сети пропорциональна квадрату численности пользователей этой сети.

Ценность сети Биткоина устанавливается таким образом: **чем больше взаимодействий, тем больше ценности создается**. Чем больше и больше людей используют Биткоин, тем выше его ценность из-за сетевого эффекта. Этот акцент на биткоин, как технологию или социальную сеть, дает большую возможность для нелинейного роста.

В Биткоине проявляются **7 сетевых эффектов**:

1. **Спекуляция –** каждый спекулятивный доллар, торгующий биткоином, увеличивает стоимость.

2. **Принятие продавцами –** каждый новый продавец, который принимает биткоины, увеличивает стоимость сети.

3. **Принятие потребителями –** каждый раз, когда новый потребитель может купить что-то за биткоины, стоимость увеличивается.

4, **Безопасность / Стимулы –** поскольку спекуляция, а также принятие продавцами и потребителями повышают цену, стимулы майнеров растут.

5. **Осведомленность –** с ростом осведомленности населения о биткоине растет его стоимость.

6. **Финансирование –** при создании большего количества финансовых продуктов, таких как опционы на криптовалюту и страхование, в сеть добавляется больше стоимости.

7, **Принятие в качестве мировой резервной валюты –** это возможно в будущем, но по мере краха фиатных валют стоимость биткоина увеличивается. Мы уже видим это на событиях в Венесуэле и странах Африки.

Все эти «сетевые эффекты» работают совместно, создавая всё большую ценность для биткоина.

Биткоин в ловушке закона Грешема

Растущая курсовая стоимость биткоина с одной стороны способствует популяризации криптовалют, с другой – препятствует широкому использованию биткоина в расчетах и его обращению на рынках.

И причиной этому является ловушка **закона Грешема**.

Этот экономический закон, также известный как **«Закон Коперника – Грешема»**, гласит: **«Худшие деньги вытесняют из обращения лучшие»** (другая формулировка: «Дешёвые вытесняют дорогие деньги»).

Впервые этот закон сформулирован знаменитым польским астрономом, математиком и экономистом **Николаем Коперником** в трактате **«О чеканке монет»** в 1526 году.

В 1560 году английский финансист **Томас Грешем** разделил деньги на «хорошие» и «плохие» и окончательно дал формулировку закону, который стал носить его имя.

Под «хорошими» Грешем подразумевал деньги, «внутренняя стоимость» которых была выше, чем у «плохих» с аналогичным номиналом. Например, золотая монета – это «хорошие» деньги, в отличие от бумажной банкноты с тем же номиналом.

«Хорошие» деньги, как правило, меньше подвержены инфляции или даже растут в стоимости со временем.

Позже к закону Грешема появились дополнения:

> **«Деньги, искусственно переоценённые государством, вытесняют деньги, искусственно недооценённые им»**
>
> **«Деньги, с которых можно не платить налоги, вытесняют из обращения деньги, с которых налоги платить обязательно»** (авторство приписывается грузинскому экономисту Кахе Бендукидзе).

Все деньги выступают с одной стороны, как **средства обращения и платежа** (при покупках и оплатах долгов), с другой – **как средства накопления** (перенос ценности, покупательной способности на будущее).

Это – основные функции денег, наряду с мерой стоимости и мировыми деньгами.

Очевидно, что «хорошие деньги» более привлекательны, как средство накопления. Поэтому, их владельцы не спешат расставаться с такими деньгами и пускать их в оборот (делать покупки или осуществлять различные платежи). Владелец ценных монет (из драгметаллов или коллекционных) предпочтет оставить их у себя, а расчеты вести бумажными банкнотами или банковской картой.

Поскольку курсовая стоимость биткоина («внутренняя стоимость») быстро растет, то биткоин становится своего рода «цифровым золотом», которое скорее будет накапливаться владельцем, чем использоваться для платежей и покупок.

То же касается и недооценки государством биткоина – переоцененные центробанками фиатные деньги будут вытеснять из оборота криптовалюту.

Таким образом, **биткоин попадает в ловушку закона Грехема**, которая препятствует его распространению в расчетах и платежах на материальных рынках и рынках услуг.

Действительно, основная доля транзакций биткоина сейчас – это биржевые операции на криптовалютных биржах. Т.е. сделки, связанные с покупкой биткоинов за фиатные валюты, а также спекулятивный обмен биткоина на другие криптовалюты.

С другой стороны, сделки в биткоинах (как и прочих криптовалютах) сейчас практически не поддаются государственному регулированию, а, следовательно, не облагаются налогами. Поэтому, согласно вышеупомянутому дополнению Бендукидзе к закону Грешема, криптовалюты будут вытеснять из обращения фиатные валюты, которые полностью контролирует государство.

Таким образом, у криптовалют, до тех пор, пока их оборот каким-либо образом не станет контролировать государство, имеется возможность для широкого распространения на теневом рынке и в «серых» расчетах.

Биткоин HODL: Есть ли предел роста стоимости биткоина? Почему не стоит сейчас продавать биткоин и какой может стать его цена в будущем.

В мае 2010 года Ласло Ханеч (Laszlo Hanyecz) купил две пиццы общей стоимостью $30 за 10 000 биткоинов. Таким образом, на тот момент цена одного биткоина была **$0,003** или 3 десятых цента. Это была первая известная нам покупка материального товара за криптовалюту. Но сам Биткоин появился еще раньше, в начале 2009 года, и первое время практически вообще ничего не стоил.

В декабре 2017 года рыночная цена биткоина перевалила за **$15 000**. За 7,5 лет он вырос более чем в 5 000 000 (пять миллионов) раз!

Любопытно, как реагируют на это средства массовой информации. Когда происходит очередной головокружительный взлет цены биткоина, СМИ пишут о **«финансовом пузыре, который раздувается и вот-вот лопнет»**. Так было в декабре 2013, в мае, ноябре и декабре 2017 годов. Но стоит произойти коррекции цены, понижению её на 30—40%%, как пресса выходит с заголовками **«Курс биткоина резко обвалился!»**, **«Владельцы биткоинов потеряли миллионы долларов!»** и т. п.

Многие средства массовой информации и общество в целом склонны не замечать впечатляющего роста первой криптовалюты и больше сосредоточены на кратковременном снижении её цены.

У этого есть психологическое объяснение – люди хотят убедить себя, что были правы, не покупая биткоин ранее. **«Это пузырь (пирамида) и скоро лопнет (рухнет)»** – вот основной тезис большинства СМИ и людей, мало знакомых с сутью биткоина и криптовалют. Если вы не покупали биткоин, то чтение статей о 30—40% падении его цены заставляет вас чувствовать себя умнее.

Кроме того, у многих людей существует боязнь, что Биткоин могут взломать, и они потеряют все свои деньги, находящиеся на биткоин-адресах. Эти опасения постоянно подогревают СМИ рассказами о взломе криптобирж и «биткоин-банков». Но правда состоит в том, что сам Биткоин никогда не был взломан и практически это сделать невозможно – он защищен надежным криптографическим алгоритмом. Держать биткоины на счетах крипто-банков и криптобирж – небезопасно, а вот Биткоин является полностью безопасной системой.

Те же, кто имеют хорошие знания и понимание сути биткоина, наблюдая за невероятным ростом его стоимости, очень сожалеют, что не купили его тогда, в 2010—2016 годах.

Многие ранние приверженцы биткоина считают, что биткоин будет постоянно расти в цене и они не собираются тратить или продавать его. Они убеждены, что эра бумажных, фиатных денег заканчивается и вскоре доллары, евро, йены и др. обесценятся и станут бесполезными, как марки в Веймарской Республике Германии с 1918 по 1924 год.

Некоторые из них придерживаются т.н. философии **HODL** (*Hold On for Dear Life* – Держать так, как будто от этого зависит жизнь) – интернет-мема из мира биткоинов и крипто-

валют, который является преднамеренным орфографическим искажением слова **«hold»** (хранить, держать, сохранять) или его опечаткой. Оно вошло в обиход 8 декабря 2013 года, когда пользователь форума BitcoinTalk.org под ником GameKyuubi опубликовал пост под названием **I AM HODLING**. В понимании этих людей **HODL –** это держать и не продавать биткоин ни при каких обстоятельствах и скачках курса.

Эти люди считают, что доллар США очень похож на бумажные марки в Веймарской Германии. Обе валюты не поддерживаются золотом, серебром или чем-либо еще. Единственное различие заключается в скорости, с которой правительства делали эмиссию.

Немецкая веймарская бумажная марка (*Papiermark*) за шесть лет (с 1918 по 1923) потеряла более 99,99999999% своей стоимости, а доллар США с 1913 года потерял более 96% своей стоимости.

Если начнется массовое бегство из доллара в биткоин, то стоимость американской валюты начнет стремительно падать. Примерно так, как это было со стоимостью веймарских бумажных марок по отношению к золотой марке.

Одним из основных факторов роста стоимости биткоина является его **дефляционность –** всего за все время в оборот будет выпущено не более 21 миллиона единиц. В настоящее время (2018 год) их менее 17 миллионов. Для сравнения, сейчас в обороте находится более **1,5 триллионов американских долларов** и это количество продолжает расти, поскольку американское правительство продолжает печатать деньги. Т.е. если гипотетически допустить, что биткоин полностью вытеснит доллар США из оборота, то цена первой криптовалюты должна стать не менее **$70 000** (в текущей стоимости доллара, разумеется).

Объем мирового рынка золота превышает **$8,2 трлн**. И если биткоин сможет взять всего лишь 10—15% этого рынка, то его цена будет свыше **$50 тыс**., а если половину – то все **$200 тыс**.

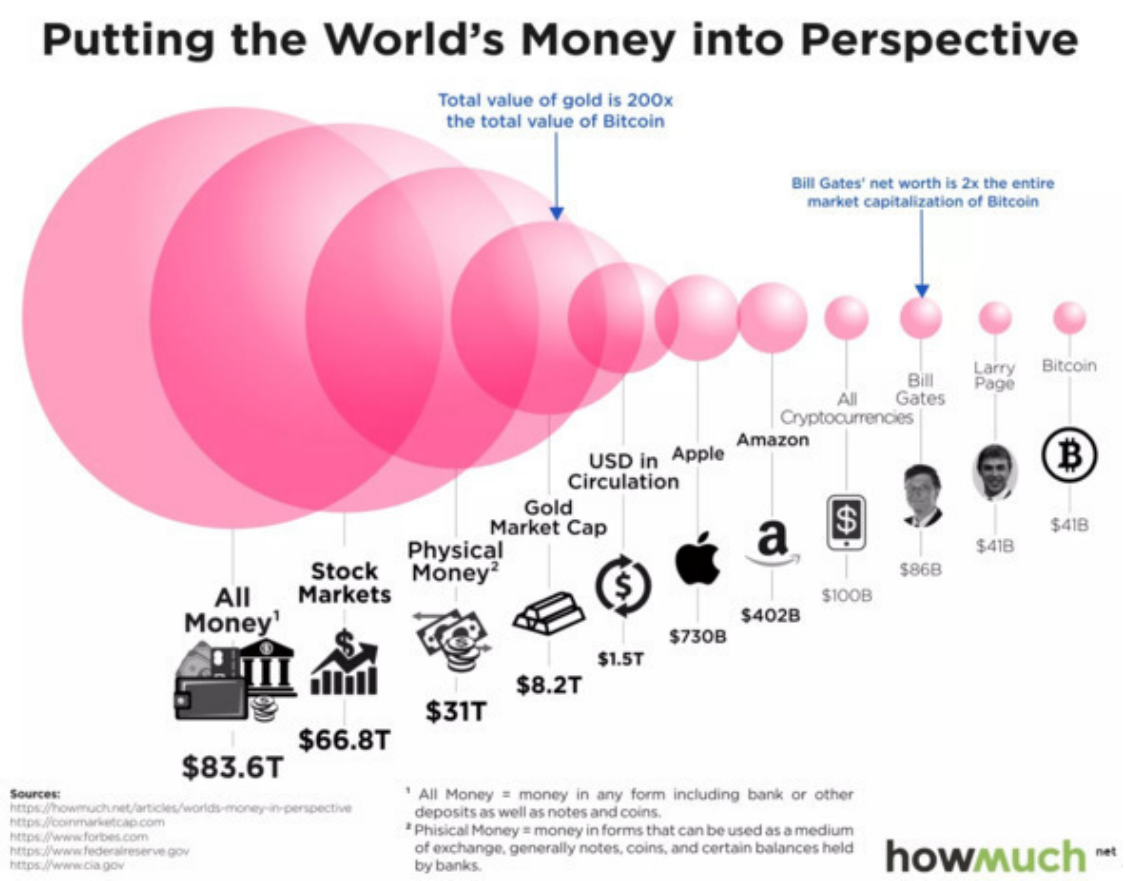
Объем мирового рынка всех фиатных денег оценивается более чем в **$31 триллион долларов**. И, опять же, если гипотетически биткоин когда-то вытеснит их, то его стоимость должна стать около **$1,5 млн**. Если же он займет только десятую часть этого рынка, то и тогда его стоимость дойдет до **$150 000**.

Никто не может точно предсказать, сколько будет стоить биткоин даже в недалеком будущем. Различные прогнозы максимальной стоимости разнятся в разы – от **$50 тыс**. до **$1 млн**. Примечательно, что каждый раз происходит их коррекция в большую сторону. Еще в начале 2017 года цена в **$10 тыс**. казалась чем-то далеким и маловероятным, но сейчас это уже пройденный этап.

Предсказание в Твиттере Джона Макафи (John McAfee), CEO MGT Capital Investments и создателя антивируса McAfee Security, – $1 млн к 2020 году.

«Когда я предсказал биткоин в $500 000 к концу 2020 года, то использовал модель, которая предсказала $5 000 долларов в конце 2017 года. [Однако,] BTC ускорился намного быстрее, чем мои предположения. Теперь я предсказываю, что биткоин составит $1 миллион к концу 2020 года».

***Джон Макафи** (John McAfee),*
CEO MGT Capital Investments
и создатель антивируса McAfee Security



Инфографика на картинке была сделана летом 2017 года и несколько устарела – капитализация биткоина уже превысила $100 млрд и по этому показателю обошла многие мировые валюты.

Но даже достигнув предела насыщения, биткоин будет продолжать расти в стоимости, поскольку его количество ограничено, а объем товарного рынка постоянно растет. Рост замедлится, но не прекратится. Собственно график роста стоимости биткоина будет представлять собой **S-образную кривую** и мы сейчас находимся в начале крутого восходящего участка этой кривой.

Если биткоин когда-то станет единой валютой всей Земли, то его стоимость в **$1 млн** не будет казаться такой уж большой. Население Земли сейчас превышает **7 млрд человек**. Если все биткоины распределить равномерно между всеми жителями нашей планеты, то каждому достанется менее **0,003 BTC**. При цене 1 биткоина **$1 млн** это всего лишь **$3 000**.

А обладателями 1 биткоина могут быть не более **21 млн человек** (на самом деле гораздо меньше). Это даже не «золотой миллиард»!

Когда появился интернет, многие в мире также скептически воспринимали его и не верили в потенциал. Сегодня интернет практически вытеснил бумажные почтовые письма и серьезно потеснил телефонию, особенно международную. Интернет практически убил бумажную ежедневную прессу и теснит телевидение. И это произошло за какие-то последние 10—20 лет.

Биткоину уже 10 лет и он может повторить успех интернета – вытеснить фиатные деньги и серьезно потеснить золото на финансовых рынках.

На наших глазах рождается **новая денежная парадигма**.

Новая денежная парадигма, или ради чего был создан Биткоин

К сожалению, не только общество, но и бизнес-круги, и деловая пресса еще не готовы принять Биткоин, как новую денежную парадигму, а рассматривают его исключительно как некий новый цифровой актив и средство инвестиций.

Но Биткоин это не только новый цифровой актив и/или объект инвестиций, **Биткоин – это средство и способ избавиться от государственной и банковской монополии на деньги и денежное обращение**.

И именно эту цель преследовал создатель Биткоина некий Сатоши Накамото – по его задумке **Биткоин должен был стать альтернативой нашей нынешней финансовой системе**.

До Биткоина процесс ведения бухгалтерского учета оставался практически неизменным с тех пор, как в XIV веке был придуман двойной учет транзакций. Этот метод бухгалтерского учета требовал от банков вести бухгалтерскую книгу с отображением проведенных операций дебета и кредита. Современная финансовая система – это просто сеть этих бухгалтерских книг, хранящихся на компьютерных серверах в каждом банке.

Биткоин изымает глобальную книгу транзакций из-под контроля банковской системы и размещает её на каждый компьютер, подключенный к сети Биткоин. Финансовые гиганты больше не контролируют систему. В Биткоине финансовая система находятся под контролем её пользователей. И это есть новая денежная парадигма!

Сосредотачиваясь на биткоине, как инвестиционном активе (средстве быстрого роста стоимости) многие упускают из виду его истинную ценность, благодаря которой растет его цена на биржах. Эта ценность – **уникальная способность сохранения и передачи стоимости на расстояния без участия доверенного посредника**.

В этом смысле Биткоин имеет преимущества как перед выпускаемыми государствами фиатными деньгами, так и перед золотом.

Биткоин существует вне государственных институтов и не нуждается в государственном регулировании. Это вполне самодостаточная система.

Единственный способ взять Биткоин под контроль государства – это осуществить т.н. «атаку 51%». Но в этом случае криптовалюта сразу же потеряет свою привлекательность и резко упадет в стоимости. Повторюсь, ценность Биткоина состоит в отсутствии цензуры и какого-либо стороннего контроля и управления, кроме сетевого, основанного на протоколе (жестко прописанных программных правилах). Именно это делает Биткоин **надежным, защищенным и неуязвимым**.

Биткоин также не нуждается в легализации. Само нахождение вне правового поля еще не означает незаконность. Об этом читайте в главе **«Миф 5: Биткоины незаконны, потому что они не признаны государством»**.

Безусловно, Биткоин, в силу своих особых свойств, указанных выше, является привлекательным объектом для инвестиций. Но не это является его основной функцией и миссией. **Биткоин пришел в этот мир, чтобы разрушить государственную монополию на деньги**

и их обращение. И создать новую денежную парадигму – отныне передача стоимости возможна без посредников, как в наличном расчете – из рук в руки. Без центробанков и других финансовых организаций. Без неконтролируемой денежной эмиссии и инфляций.

Попытки вмонтировать Биткоин (и другие криптовалюты) в существующую государственную денежную систему бессмысленны и непродуктивны. Бессмысленно государственное регулирование майнинга и криптовалютных транзакций. Да и у государств, к счастью, нет возможности это осуществить, кроме как применяя запретительные и карательные меры.

Еще 40 лет назад известный экономист и философ, лауреат Нобелевской премии **Фридрих фон Хайек** (*Friedrich August von Hayek*) задался вопросом, почему государственная монополия на денежную эмиссию рассматривается как неизбежная. В своей работе **«Частные деньги»** он предложил денационализировать деньги, поскольку, по его мнению, государственная монополия в области эмиссии вредна для общества.

Только свободный обмен и беспрепятственное хождение различных валют! Пусть в конкурентной борьбе победит сильнейшая!

Манифест Блокчейна

Основатель **AngelList** – сайта для стартаперов и инвесторов, – **Naval Ravikant** написал **твитсторм** (серию постов в Твиттере), который можно назвать **Манифестом Блокчейна**:

– Блокчейны заменят существующую рыночную инфраструктуру.

– Люди являются сетевыми существами. Это первый биологический вид, который сумел посредством сети преодолеть генетические границы и таким образом захватить весь мир.

– Сети позволяют нам сотрудничать, иначе мы бы всё делали самостоятельно. И в сетях распространяются плоды нашего сотрудничества.

– Множество пересекающихся сетей образуют основу и организовывают наше общество. Физические, цифровые и психические связи соединяют всех нас.

– Деньги – это сеть. Религия – это сеть. Корпорация – это сеть. Дороги – сети. Электричество – это сеть.

– Сети должны быть организованы в соответствии с правилами. Для контроля и выполнения этих правил необходимы администраторы. Против мошенников.

– Сети обладают «сетевым эффектом». Добавление нового участника увеличивает ценность сети для всех существующих участников.

– Таким образом, сетевые эффекты приводят к тому, что победитель получает всё.

– Ведущая сеть стремится стать единственной сетью.

– И управители этих сетей становятся самыми влиятельными людьми в обществе.

– Некоторые сети управляются царями и священниками, которые решают, что есть деньги и права, священные и светские. Это закрытые правила, основанные на силе.

– Много сетей находятся в ведении корпораций. Социальная сеть. Поисковая сеть. Телефонные и кабельные сети. Они закрыты, но изначально меритократичны.

– Некоторые сети управляются элитами. Университетские сети. Медицинские сети. Банковские сети. Отчасти открытые и отчасти меритократические.

– Немного сетей управляются толпой. Демократии. Интернет. Общины. Они открыты, но не меритократичны. И очень неэффективны.

– Диктаторские режимы более эффективны в войне, чем демократические. Интернет и общины перегружены злоупотреблениями и спамом.

– В 20-м веке был создан новый вид сети – рыночные сети. Открытые и меритократические.

– Преимущество на рынке определяется затратами ресурсов. Ресурс – это деньги, в виде замороженного и готового к торговле времени.

– Рыночные сети – это титаны: кредитные рынки, фондовые рынки, сырьевые рынки, финансовые рынки. Они сильнее государств.

– Рыночные сети работают только там, где есть заинтересованность в деньгах. В противном случае они просто сети толпы. Применения ограничены.

– Так было до настоящего времени.

– Блокчейн – это новое изобретение, которое позволяет объединиться достойным участникам в открытую сеть, чтобы управлять без администраторов и без денег.

– Это основанные на заслугах, защищенные от взлома, открытые и избирательные системы.

– Достойные участники – это те, кто работает над развитием сети.

– Так же как общество дает нам деньги за то, что оно хочет, так и блокчейн дает монеты за то, что мы даем сети то, что хочет она.

– Важно отметить, что блокчейны платят своими же деньгами (монетами), а не общераспространенными (долларами) на финансовых рынках деньгами.

– Блокчейны платят монетами, но монеты – это просто следствие проделанной работы. И разные блокчейны требуют разной работы.

– Биткоин платит за обеспечение сохранности (защищенности) бухгалтерского реестра. Эфириум оплачивает выполнение и проверку расчетов.

– Блокчейн сочетает открытость демократии и интернета с меритократией рынков.

– Для блокчейна заслуга (ценность) может означать безопасность, вычисление, предсказание, внимание, пропускную способность, мощность, хранение, распространение, содержание…

– Блокчейн переносит рыночную модель в те места, где она не могла быть раньше.

– Блокчейны, открытые и основанные на рынках, могут заменить сети, которыми раньше управляли короли, корпорации, аристократии и толпы.

– Блокчейн не имеет смысла без своих монет (криптовалюты) также, как бессмыслен рынок без денег.

– Бессмысленен блокчейн, управляемый государством, корпорацией, элитой или толпой.

– Блокчейн дает нам новые способы управления сетями. В банковской деятельности. В избирательных системах и голосовании. Для поиска. В социальных медиа. Для телефонии и энергосистем.

– Сети управляются не царями, жрецами, элитами, корпорациями и толпой. Сети управляются теми, кто приносит пользу сети.

– Сети, основанные на блокчейне, заменят существующие сетевые рынки. Сначала медленно, а затем внезапно. Сначала в одном месте, затем везде.

– В конечном счете, государство – это просто сеть (сетей).

Спасибо, Сатоши Накамото. И всем гигантам, на плечах которых стоял Сатоши.

Оригинальный текст

– Blockchains will replace networks with markets.

– Humans are the networked species. The first species to network across genetic boundaries and thus seize the world.

– Networks allow us to cooperate when we would otherwise go it alone. And networks allocate the fruits of our cooperation.

– Overlapping networks create and organize our society. Physical, digital, and mental roads connecting us all.

– Money is a network. Religion is a network. A corporation is a network. Roads are a network. Electricity is a network…

– Networks must be organized according to rules. They require Rulers to enforce these rules. Against cheaters.

– Networks have «network effects.» Adding a new participant increases the value of the network for all existing participants.

– Network effects thus create a winner-take-all dynamic. The leading network tends towards becoming the only network.

– And the Rulers of these networks become the most powerful people in society.

– Some are run by kings and priests who choose what is money and law, sacred and profane. Rule is closed to outsiders and based on power.

– Many are run by corporations. The social network. The search network. The phone or cable network. Closed but initially meritocratic.

– Some are run by elites. The university network. The medical network. The banking network. Somewhat open and somewhat meritocratic.

– A few are run by the mob. Democracy. The Internet. The commons. Open, but not meritocratic. And very inefficient.

– Dictatorships are more efficient in war than democracies. The Internet and physical commons are overloaded with abuse and spam.

– The 20th century created a new kind of network – market networks. Open AND meritocratic.

– Merit in markets is determined by a commitment of resources. The resource is money, a form of frozen and trade-able time.

– The market networks are titans. The credit markets. The stock markets. The commodities markets. The money markets. They break nations.

– Market networks work where there is a commitment of money. Otherwise they are just mob networks. The applications are limited.

– Until now.

– Blockchains are a new invention that allows meritorious participants in an open network to govern without a ruler and without money.

– They are merit-based, tamper-proof, open, voting systems.

– The meritorious are those who work to advance the network.

– As society gives you money for giving society what it wants, blockchains give you coins for giving the network what it wants.

– It's important to note that blockchains pay in their own coin, not the common (dollar) money of financial markets.

– Blockchains pay in coin, but the coin just tracks the work done. And different blockchains demand different work.

– Bitcoin pays for securing the ledger. Etherium pays for (executing and verifying) computation.

– Blockchains combine the openness of democracy and the Internet with the merit of markets.

– To a blockchain, merit can mean security, computation, prediction, attention, bandwidth, power, storage, distribution, content…

– Blockchains port the market model into places where it couldn't go before.

– Blockchains' open and merit based markets can replace networks previously run by kings, corporations, aristocracies, and mobs.

– It's nonsensical to have a blockchain without a coin just like it's nonsensical to have a market without money.

– It's nonsensical to have a blockchain controlled by a sovereign, a corporation, an elite, or a mob.

– Blockchains give us new ways to govern networks. For banking. For voting. For search. For social media. For phone and energy grids.

– Networks governed without kings, priests, elites, corporations and mobs. Networks governed by anyone with merit to the network.

– Blockchain-based market networks will replace existing networks. Slowly, then suddenly. In one thing, then in many things.

– Ultimately, the nation-state is just a network (of networks).
Thank you, Satoshi Nakamoto. And to all the shoulders that Satoshi stands upon.

Заключение

Биткоин – это первая в мире работоспособная система цифровой пиринговой наличности или децентрализованная электронная денежная система. Она была анонсирована **31 октября 2008 года** неизвестным автором (или группой авторов), скрывающимся под псевдонимом **Сатоши Накамото** (*Satoshi Nakamoto*), в докладе под названием **Bitcoin: A Peer-to-Peer Electronic Cash System**.

3 января 2009 года Биткоин был запущен в эксплуатацию и с тех пор непрерывно работает. В основе его надежной и безотказной работы лежит инновационная **технология блокчейна**, называемая также технологией распределенного реестра учета (*Distributed Ledger Technology* или ***DLT***).

Биткоин был задуман, как **платежная система, основанная на криптографии, а не на доверии**, и которая позволила бы любым двум участникам осуществить перевод средств напрямую, без участия посредника, анонимно и без цензуры.

По замыслу его неизвестного создателя, **Биткоин должен стать альтернативой нынешней финансовой системе**, в которой государство и центробанки контролируют выпуск (эмиссию) и оборот денег, а коммерческие и государственные банки выступают посредниками в денежных операциях.

Биткоин – это деньги без правительства. Его транзакции не требуют специального разрешения должностных лиц. Ни одно правительство не может контролировать работу этой электронной денежной системы. Она никому не принадлежит, а пользоваться ею может каждый. Для этого не нужны ни документы (паспорт и т.п.), ни прописка (регистрация), ни справки и нотариальные доверенности. Поистине, **Биткоин – для всех**!

Само существование Биткоина это предупреждение правительствам, что деньги – последний объект, который они контролировали, – уже не являются их монополией. По словам математика и философа **Нассима Талеба** (*Nassim Nicholas Taleb*), **биткоин – это первая органическая валюта**.

Без криптовалюты не было бы стимула для людей тратить деньги на компьютеры, необходимые для запуска программного обеспечения Биткоин. Блокчейн без биткоина воспроизводит ту же самую финансовую систему, которая уже существует. Именно криптовалюта биткоин создает стимул для людей запустить новую финансовую систему, которая находится вне традиционной.

Криптовалюта плюс блокчейн создают самостоятельную финансовую систему, которая никогда не существовала в современных финансах. Криптовалюта плюс блокчейн создает конкурента современной финансовой системе, который имеет потенциал для перераспределения богатства, используя силу по настоящему свободных рынков.

У Биткоина уже 10 лет безупречного послужного списка, этого достаточно для того, чтобы признать его право на существование.

Разумеется, путь его будет непростым, будут взлёты и падения. Он может даже потерпеть неудачу, но тогда процесс можно будет легко запустить заново, поскольку теперь известно, как это работает.

По мере того, как Биткоин и Блокчейн продвигаются вперед, индустрия тоже не отстает. Тысячи разработчиков, предпринимателей, инвесторов и пользователей строят его, пока вы

читаете эти строки. Сделки, хэшрейт, стоимость, пользователи, кошельки, биржи – по всем этим направлениям разработка программного обеспечения Bitcoin продолжает ускоряться. **Lightning Networ**k, **Segwit**, **MAST**, **Schnorr**, **TumbleBit**, **MimbleWimble** и другие технологии разрабатываются лучшими инженерами в мире, чтобы сделать сеть Биткоина масштабируемой для глобальной торговли.

Блокчейн Биткоина не волнуют разговоры о его якобы смерти. У него нет тумблера, который можно выключить. У него нет чувств. Но каждые десять минут он делает шаг вперед. Каждые десять минут он увеличивает свою ценность и силу своей сети. Ни один человек или учреждение не может это остановить. Каждые десять минут он продвигается вперед. Каждые десять минут выполняется проверка транзакций и обновление реестра. Он делает то, что должен делать, ни больше ни меньше.

Блокчейн не волнует цена биткоина или то, что СМИ говорят об этом, – он просто работает и каждые десять минут продолжает создавать новый блок транзакций. Пока это не прекратится, он жив. Он просто продолжает двигаться вперед, по одному блоку – шаг за шагом.

Не беспокойтесь о текущей цене биткоина, это не имеет значения, в конце концов. Ничто не может разрушить эту технологию!

Приложения

Биткоин: Полезные ресурсы Справки, информация, инструменты, статистика – все о Биткоине в WWW

Подборка веб-ресурсов, полезных для знакомства, изучения, аналитики, статистики и многого другого, необходимого для работы с системой Биткоин (Bitcoin).

Bitcoin.org

Это, пожалуй, самый главный сайт, с которого надо начинать знакомство с Биткоином. Примечателен он еще и тем, что здесь находится знаменитый доклад Сатоши Накамото под названием **Bitcoin: A Peer-to-Peer Electronic Cash System** («Биткоин: Одноранговая электронная денежная система»), называемый еще **Bitcoin White Paper**, который он обнародовал 31 октября 2008 года.

На этом сайте имеется краткая инструкция **«Новичку о Биткоине»**. А также ссылки на скачивание валидных **программ-кошельков** Биткоина для всех видов устройств и операционных систем.

На отдельной странице находится релиз последней версии **Bitcoin Core** – официальной программы-клиента Биткоина, поддерживающего полную ноду – последнюю актуальную версию блокчейна.

Первую версию этой программы-клиента написал сам Сатоши Накамото. Поэтому она известна также под названием **Satoshi client**.

Bitcoin Core также можно загрузить на официальном сайте – **BitcoinCore.org**

А репозитарий с файлами исходного кода находится здесь: **github.com/bitcoin/bitcoin**

Также на сайте Bitcoin.org новички и не только найдут справочный раздел **F.A.Q**. – **«ЧАсто задаваемые ВОпросы»** – ответы на повторяющиеся вопросы и мифы о Биткоине и много другой полезной и справочной информации.

BitcoinWiki.org

Википедия о Биткоине. Сборник энциклопедических статей по различным аспектам Биткоина и криптовалют. К сожалению, в последнее время редко обновляется.

Из интересного здесь:

– Что такое Биткоин?
– Кто создал Биткоин?
– История Биткоина.

– Экономика Биткоина.
– Частые вопросы по Bitcoin (FAQ).

Также на этом сайте можно найти много информации о технологических подробностях Биткоина, майнинге, безопасности, узнать, как покупать и принимать платежи, а также хранить биткоины.

Bits.Media

Еще один справочно-информационный сайт о Биткоине на русском языке.

Здесь можно узнать:

– Что такое Биткоин?
– Как получить биткоины.
– Мифы о Биткоине.
– Часто задаваемые вопросы о Bitcoin. Еще один FAQ по Биткоину.
– Новости криптовалют
– Календарь мероприятий криптовалютной отрасли и блокчейна.

Также есть рекомендации по безопасности, майнингу и биржевой торговле (трейдингу) криптовалютами со списком бирж.

На сайте работает форум. Кстати о форуме…

BitcoinTalk.org

Самый крупный международный форум о Биткоине и криптовалютах. Существует с 2009 года. Имеется русскоязычный раздел.

Этот форум примечателен еще и тем, что на нем общался **Сатоши Накамото**, **Хэл Финни** и другие известные криптологи, стоявшие у истоков криптовалют.

Blockchain.info

Самая популярная веб-версия биткоин-кошелька. Поддерживает также кошельки **Bitcoin Cash** и **Etherium**.

Но этот сайт также содержит массу справочной и статистической информации о сети Биткоин. Здесь вы узнаете:

– рыночную цену биткоина в долларах США на ведущих биржах и график изменения цены;
– количество транзакций за последние 24 часа и график изменения количества транзакций в сутки;
– средний размер блока за последние 24 часа и график изменения размера блока;

– совокупный размер транзакций, ожидающих подтверждения, и график изменения размера транзакций.

Также получите статистику биткоина в диаграммах:

– динамику добычи биткоинов;
– изменение рыночной капитализации Биткоина;
– динамику изменения объема торгов на ведущих биржах.

Кроме того, получите подробную информацию о блоке Биткоина:

– общий размер всех заголовков блоков и транзакций;
– среднее количество транзакций на блок;
– среднее время подтверждения транзакций и др.

Также здесь много статистики майнинга биткоина:

– изменение хэшрейта сети майнинга;
– статистика по майнинговым пулам;
– изменение сложности майнинга;
– изменение доходности майнинга;
– суммарная стоимость транзакций;
– изменение доли дохода майнеров от суммы транзакций;
– изменение средней стоимости транзакций (доход майнеров / кол-во транзакций).

Дополнительно можно получить статистику по активности сети Биткоин:

– общее количество уникальных адресов, используемых в блокчейне;
– общее количество транзакций;
– предполагаемый суточный объем транзакций в USD;
– количество созданных блокчейн-кошельков;
– интерактивная карта последних неподтвержденных транзакций;
– последние крупнейшие транзакции;
– самые активные биткоин-адреса;
– отклоненные транзакции;
– странные транзакции.
– И много другой информации.

Также имеется **Центр поддержки пользователей**, где можно получить ответ на любой интересующий вас вопрос по использованию биткоин-кошелька.

CoinDesk.com

На этом сайте кроме всего прочего содержится **полная история курса биткоина** по отношению к доллару США.

GoBitcoin.io

Справочно-информационный сайт о Биткоине (на английском языке).

Содержит несколько полезных инструментариев:

– Генератор QR-кода для биткоин-адреса. Опционально можно задать и сумму транзакции, ожидаемой к переводу на этот адрес.
– Стоимость «атаки 51%». Показывает текущую стоимость атаки на сеть Биткоина, известную как «атака 51%».
– Волатильность курса биткоина (в USD). Волатильность является мерой изменения цены финансового инструмента с течением времени. Это позволяет понять, насколько меняются цены биткоина со временем и сравнить его с другими валютами.
– Некоторые другие инструменты (виджеты, транзакции в реальном времени и пр.)

CoinMap.org

Интерактивная карта, показывающая расположение компаний и организаций, работающих с биткоином во всем мире.

Spendabit.co

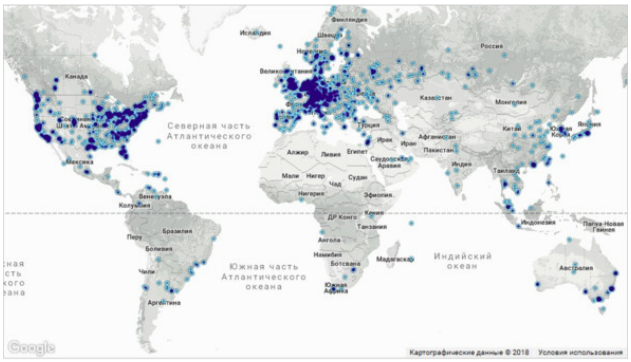
Поисковая система для товаров, которые вы можете купить с помощью биткоинов.

Coin. Dance

Сайт **глобальной статистики по сети Биткоин**. Включает не только технологическую и финансовую статистику, а также демографическую и поисковую. В частности, имеется отдельная статистика по нодам – полным узлам Биткоина.

BitNodes.earn.com

Полная статистика по нодам Биткоина, включая интерактивную карту нод и данные по странам. Например, на момент написания этой книги (по состоянию на 14 октября 2018) было зарегистрировано 10 069 работающих нод Биткоина.



Распределение полных нод Биткоина

BitcoinClock.com

Часы, ведущие обратный отсчет до изменения вознаграждения за блок (эмиссии биткоина).

При запуске Биткоина в январе 2009 года майнер, сформировавший и добавивший блок в блокчейн, получал вознаграждение в размере 50 биткоинов. Однако, согласно протоколу Биткоина, через каждые 210 000 блоков это вознаграждение уменьшается вдвое. За прошедшее время уже произошло два уменьшения и в настоящее время (8 ноября 2017) награда за блок составляет 12,5 биткоинов.

Согласно текущему показанию часов, следующее уменьшение вознаграждения до 6,25 биткоина за блок произойдет 12 июня 2020 года.

Другой вариант подобных часов находится на сайте **www.BitcoinBlockalf.com**. Там же есть и другая текущая статистика сети Биткоин: общее количество выпущенных биткоинов, количество оставшихся биткоинов, общая капитализация Биткоина в USD, сложность майнинга и пр.

Статистика Биткоина

Еще несколько веб-ресурсов по статистике Биткоина:

– BitcoinTicker.co
– BitInfoCharts.com
– TradeBlock.com/bitcoin/

BitAddress.org

JavaScript-генератор Биткоин-кошельков с приватными ключами на стороне клиента с открытым исходным кодом. Работает при отключенном интернете. Позволяет случайным образом сформировать новый биткоин-адрес и приватный ключ к нему. В результате можно получить биткоин-кошелек на бумажном носителе. Есть различные варианты генерации биткоин-адресов, включая адреса на основе паролей и пр.

Блок-эксплореры

Блок-эксплореры позволяют получить информацию о блоке и транзакции непосредственно из блокчейна. Список некоторых:

– BlockExplorer.com
– BTC.com
– ChainRadar.com

Медиа-ресурсы

Самые популярные информационно-новостные русскоязычные сайты, пишущие на тему Биткоина и криптовалют:

– BitNovosti.com – ведущий русскоязычный информационный сайт, освещающий блокчейн-технологии, криптовалюты и смежные темы. Имеет очень популярный YouTube-канал.

– ForkLog.com – культовый интернет-журнал о криптовалютах. Отслеживает актуальные новости, освещает события биткоин-индустрии, пишет о конференциях и других мероприятиях, а также делает интервью с главными представителями криптосообщества.

– Bitcoin Review (medium.com/bitcoin-review) **–** самый лучший блог о Биткоине.

Биткоин: Единицы измерения

Все деньги имеют помимо основных единиц дробные. Как правило, это сотые части базовой денежной единицы.

Базовая обменная единица криптовалюты Биткоин (Bitcoin) так и называется **биткоин** (bitcoin), но пишется со строчной буквы.

Для обозначения используется сокращение **BTC** и специальный символ (буква **B** с вертикальными черточками а-ля **$**). Этот символ был специально добавлен в **Unicode** версии 10.0 (**U +20BF**), а также в **HTML** (Ƀ). Также в качестве символа биткоина использовался тайский бат (**฿**) – номер в Unicode **U+0E3F** и HTML-код **&#3647**;

Дробные части биткоина:

Самая малая и часто используемая доля биткоина – это **сатоши** (*satoshi*) – 1/100 000 000 (0,000 000 01 BTC) – названа в честь **Satoshi Nakamoto** – псевдонима изобретателя биткоина.

На данный момент ведется множество дискуссий о названиях других долей биткоина. Основные кандидаты:

1/100 (0,01 BTC) = 1 cBTC = 1 **цento-биткоин** или **сантибиткоин** (также известный, как битцент);

1/1 000 (0,001 BTC) = 1 mBTC = 1 м**илли-биткоин** (также называется мбит (произносится **«эмбит»**) или **миллибит**);

1/1 000 000 (0,000 001 BTC) = 1 μBTC = 1 **микро-биткоин** (также называется **юбит** или **микробит**).

Криптовалюты: Термины и сокращения

Краткий словарь терминов и сокращений, используемых в криптоиндустрии и технологии блокчейна

Активно развивающаяся в последние годы криптоиндустрия породила ряд новых терминов и понятий. Для того, чтобы рядовому пользователю ориентироваться в них, предлагаю краткий словарь.

Он состоит из нескольких разделов:

– Словарь основных терминов.
– Англоязычные аббревиатуры и сокращения.
– Криптожаргон и сленг криптобирж.
– Список основных криптовалют.
– Термины, используемые в прохождении транзакций.

Словарь основных терминов

Автономные агенты (*Autonomous Agent*) – программные сущности (приложения и модули), которые могут принимать решения без необходимости участия и одобрения человека. Умный контракт (smart contract) – это своего рода автономный агент, базирующийся на блокчейне.

Адрес (*Address*) – биткоин-адрес используется для транзакций (отправки и получения биткоинов). Он состоит из буквенно-цифровых символов, но также может быть представлен в виде сканируемого QR-кода. Биткоин-адрес также является публичным ключом, используемым держателями биткоинов для цифровой подписи транзакций.

Адрес тщеславия (*Vanity Address*) – биткоин-адрес, содержащий определенный элемент, например, имя.

Альткоин (*Altcoin*) – общее название для всех криптовалют, предлагаемых в качестве альтернативы биткоину. В их числе – лайткойн (Litecoin), неймкойн (Namecoin), новакойн (Novacoin) и пр.

Атака 51% (*51% attack*) – состояние, когда более половины вычислительной мощности сети криптовалюты контролируется одним майнером или группой майнеров. Теоретически, этот объём вычислительной мощности дает власть над сетью. Это означает, что каждая клиентская программа в сети верит в подтвержденный блок транзакций атакующей стороны. Это дает им контроль над сетью, включая следующие полномочия:

– создавать транзакции, конфликтующие с чужими;
– останавливать подтверждение чьей-либо транзакции;
– тратить одни и те же монеты несколько раз;
– мешать другим майнерам создавать действительные блоки.

Биткоин (*Bitcoin*) – одноранговая цифровая денежная система, построенная на криптографических алгоритмах. Расчетная единица в этой системе называется биткоин (**bitcoin**), – пишется со строчной буквы в отличие от названия денежной системы, которое пишется с прописной буквы. Биржевый тикер биткоина – **BTC**. Биткоин – первая массовая криптовалюта.

Блок (*block*) – список проверенных транзакций, который добавляется к блокчейну в результате майнинга. Является базовым элементом структуры блокчейна. Состоит из двух частей – заголовка (Head) и полезной нагрузки (Payload) – собственно записи транзакций.

Блокчейн (*block chain* – цепочка блоков) – распределенный реестр, состоящий из цепочки блоков финансовых транзакций, в которой каждый последующий блок криптографически связан с предыдущим. См. также **DLT** (технология блокчейна).

Волатильность (*Volatility*) – изменение движений цен с течением времени на торгуемые финансовые активы (включая криптовалюты).

Двойная трата или **двойное расходование** (*Double spending*) – попытка потратить деньги дважды. Это происходит, когда кто-то выполняет финансовую транзакцию, а затем совершает вторую сделку с теми же самыми деньгами.

Кошелек (*wallet*) – программное приложение, позволяющее производить транзакцию с заданного адреса и просматривать его баланс.

Ключи (*keys*) – строка символов (битовая строка), используемая криптографическим алгоритмом при шифровании и дешифровании сообщений, постановке и проверке цифровой подписи, а также идентификации. Ключи бывают симметричные (один и тот же ключ используется для шифрования и дешифрования) и асимметричные (публичный и приватный).

Криптовалюта (*Cryptocurrency*) – распределенная и децентрализованная система безопасного обмена и передачи цифровых денежных знаков, основанная на средствах криптографии.

Криптография (от др.-греч. κρυπτός – скрытый и γράφω – пишу) – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации) и аутентификации (проверки подлинности авторства или иных свойств объекта).

Майнинг (*mining*) – необходимый и важный процесс в сети Биткоина и других криптовалют, в результате которого в блокчейн добавляется новый блок транзакций и происходит эмиссия монет.

Мастерноды (*Masternodes*) – специальные узлы (серверы) сети, обеспечивающие работу механизма перемешивания транзакций для увеличения степени анонимности.

Нода (*node*) – узел (сервер) сети Bitcoin – компьютер, на котором хранится полная актуальная версия блокчейна.

Нокоинер – см. Nocoiner.

Облачный майнинг (*cloud mining*) – веб-сервисы, продающие мощности для майнинга криптовалют. Само оборудование находится на площадке продавца и обслуживается его силами. Покупатель оплачивает заказанную вычислительную мощность и получает доход от майнинга.

Обфускация (запутывание, сбивание с толку) – технология, позволяющая увеличить степень анонимности криптовалютных транзакций.

Премайнинг (*Pre-mining*) – «добыча» криптомонет создателем криптовалюты до того, как официально объявлено о её появлении. Позволяет осуществить эмиссию криптовалюты до её выхода на рынок. Зачастую используется в мошеннических криптовалютах, но не все премайнинговые монеты являются мошенническими.

Приватный (закрытый) ключ (*private key*) – кодовая строка, при помощи которой осуществляется доступ к кошельку или биткоин-адресу. Необходима для осуществления транзакций.

Публичный (открытый) ключ (*public key*) – парная соответствующему приватному ключу кодовая строка, к которой имеется открытый доступ. Используется наряду с секретным приватным ключом для отправки транзакций. Публичный ключ соответствует биткоин-адресу.

Пул (*Pool*) или **Майнинг-пул** (*mining pool*) – сообщество майнеров, которые коллективно добывают блок, а затем делят полученное вознаграждение. Майнинг-пулы – способ увеличить доходность при росте сложности майнинга.

Сатоши Накамото (*Satoshi Nakamoto*) – анонимный создатель (или группа создателей) одноранговой электронной денежной системы **Биткоин** (Bitcoin).

Токен (*token* – жетон, талон) – единица учета цифрового актива. Представляют собой запись в блокчейне. Выпускается с целью привлечения инвестиций в криптовалютный проект и дает его владельцу определенные права и привилегии. Токены условно делятся на ***security*** («инвестиционные») и ***utility*** («полезные»).

Security-токены дают их владельцу право на реализацию его инвестиционных интересов, как то право собственности на долю в компании, капитале или прибыли и т. п.

Utility-токены дают их владельцу право на получение товаров, услуг и сервисов криптовалютных проектов.

Тест Хоуи (***Howey test***) позволяет отделить security-токены от utility.

Токены зачастую выпускаются в ходе ICO и STO, а затем торгуются на криптовалютных биржах наравне с криптовалютами.

Транзакция (*transaction*) – перевод денег между двумя адресами.

Умные контракты (*Smart Contract*) – алгоритм, предназначенный для заключения и поддержания коммерческих контрактов, используя технологию блокчейн. Предметом умных контрактов являются цифровые активы, которые автоматически распределяются между сторонами, подписавшими контракт, согласно формуле, основанной на показателях, значения которых неизвестны на момент подписания контракта.

Форк (*Fork* – вилка) – создание альтернативной успешной версии цепочки блоков. Это может происходить умышленно, когда группа майнеров получает слишком много контроля над сетью (см. атаку 51%), случайно (одновременная запись новых блоков разными майнерами или из-за ошибки в системе), или целенаправленно, когда команда разработчиков решает представить новые функции в новой версии клиентской программы.

Форк успешен, если он становится самой длинной версией цепочки блоков с точки зрения сложности. В этом случае альтернативная ветка блокчейна отвергается и становится невалидной.

Также форком называют изменение программного протокола криптовалюты, которое создает две отдельные версии блокчейна с общей историей.

Часто форком называют новую криптовалюту, которая построена на протоколе существующей. Например, лайткоин (LTC) является форком биткоина (BTC).

Холодное хранение или **оффлайн хранение** – в широком смысле – хранение криптовалюты без доступа к интернету. На самом деле – хранение приватных ключей или **seed** на устройствах, не имеющих доступа к интернету. Например, распечатанными на бумаге. Осуществляется в целях безопасности.

Цветные монеты (*Colored coins*) – надстройка над протоколом биткоина, которая позволяет пользователям биткоинов наделять их дополнительными свойствами, задаваемыми самим пользователем, позволяя маркировать биткоины как «акции» или даже «реальные активы». Это позволяет использовать биткоины как токены («жетоны») для любой другой собственности.

Цифровая подпись (ЭЦП – электронная цифровая подпись) – код, который генерирует алгоритм шифрования с открытым ключом, прикрепляемый к транзакции для проверки неизменности её содержимого и идентификации отправителя. Используется для подтверждения транзакции владельцем биткоин-кошелька отправителя.

Англоязычные термины и сокращения

Airdrop – бесплатные криптомонеты, которые раздают в качестве рекламы, чтобы донести информацию о токене до потенциальных инвесторов и энтузиастов криптовалют.

ASIC (*Application-Specific Integrated Circuit*) – интегральная схема специального назначения или асик, – процессор для работы с хэшами, используемый в майнинге криптовалют.

ATH (*All Time High*) – наибольшее значение за всё время. Максимальный курс криптовалюты.

BIP (*Bitcoin Improvement Proposal*) – **Проект развития Биткоина**, – документ, в котором описывается технический дизайн, новые возможности, новые процессы или программная среда, меняющие протокол Биткоина.

Bitcoin Investment Trust (*Биткоиновый инвестиционный фонд*) – частный фонд, который совершает инвестиции исключительно в биткоины и использует хранение биткоинов от имени и по поручению своих вкладчиков. Предоставляет финансовые услуги для людей, желающих инвестировать в биткоины, без необходимости самому покупать и безопасно хранить криптовалюту.

Bitcoins per Block или **Block Reward** (*биткоинов за блок*) – вознаграждение, выплачиваемое майнеру за успешное решение криптографической задачи и присоединение блока к блокчейну.

BPI (*Bitcoin Price Index*) – индекс цены биткоина, – разработанный биржей **Coindesk**, представляет среднюю цену биткоина на крупнейших мировых биржах.

Coinprizm – приложение (кошелек) и одноименная сеть для цифрового подтверждения прав собственности на произвольные объекты и работы с цветными монетами (Colored coins).

CryptoNote – протокол, обеспечивающий обфускацию (запутывание) транзакций с целью увеличения степени анонимности.

DA или **Dapp** (*Decentralized Application*) – децентрализованное приложение – программа с открытым исходным кодом, которая работает автономно и хранит свои данные в цепочке блоков.

DAO (*Decentralized Autonomous Organization*) – децентрализованная автономная организация (ДАО).

Difficulty (*сложность*) – параметр, характеризующий сложность майнинга, т.е. сложность решения криптографической задачи.

DGW (*Dark Gravity Wave*) – алгоритм подстройки сложности майнинга.

DLT (*Distributed Ledger Technology*) – Технология распределенного реестра учета (например, блокчейн Биткоина) – комбинация компонентов, включающих в себя сети peer-to-peer

(P2P), распределенное хранение данных и криптографию. Существуют такие основные виды DLT: **публичные** или **открытые** (*Public*), **частные** или **закрытые** (*Private*), **неограниченные** (*Permissionless*), **эксклюзивные** или **ограниченные** (*Permissioned*).

DPoS (*Delegated proof-of-stake*) – алгоритм достижения консенсуса в децентрализованой среде, альтернативный консенсусам **PoW** и **PoS**. Был разработан в 2014 году в рамках проекта Graphene и впервые был задействован в проекте **Bitshares**, позже в проекте **Steemit**.

EEA (*Enterprise Ethereum Alliance*) – некоммерческий альянс финансовых и технологических компаний и фондов, целью которого является продвижение и поддержка технологий и стандартов, основанных на Эфириуме, а также согласование референсной архитектуры **EntEth 1.0**.

Членами EEA являются ряд крупных банков, в числе которых **JP Morgan**, **Santander**, **UBS** и **BNY Mellon**, а также IT-компании **Microsoft**, **Intel** и другие.

ECDSA (*Elliptic Curve Digital Signature Algorithm*) – алгоритм с открытым ключом для создания цифровой подписи. Используется для подтверждения транзакций в протоколе Bitcoin.

Equihash – алгоритм хэширования, применяемый в **Proof-of-Work** некоторых криптовалют (ZCash, Bitcoin Gold и др.). Представляет собой довольно сложную функцию хэширования и требует много оперативной памяти для выполнения. Оптимизирован для майнинга при помощи графических карт, т. н. GPU-майнинга.

ETF (*Exchange Traded Fund*) – биржевый инвестиционный фонд. Фонд, паи (акции) которого обращаются на бирже.

EVM (*Ethereum Virtual Machine*) – виртуальная машина Эфириума.

FOMO (*Fear of missing out*) – синдром упущенной выгоды, навязчивая боязнь упустить выгоды от роста цены криптовалют.

Hashrate (хэшрейт или вычислительная мощность) – вычислительная производительность компьютерного оборудования для майнинга криптовалют. Измеряется в хэшах (hash) в секунду.

HODL (*Hold On for Dear Life* – Держать так, как будто от этого зависит жизнь) – интернет-мем из мира биткоинов и криптовалют, который является преднамеренным орфографическим искажением слова **«hold»** (хранить, держать, сохранять) или его опечаткой.

Слово вошло в обиход 8 декабря 2013 года, когда пользователь форума **BitcoinTalk.org** под ником **GameKyuubi** опубликовал пост под названием **I AM HODLING**. В этой заметке он признает, что находится под влиянием алкоголя, и объясняет причину поведения BTC на медвежьем рынке.

Howey test (*тест Хоуи*) – критерии, используемые для определения инвестиционного контракта и ценных бумаг. Включает в себя четыре признака:

– Инвестирование денег.
– Общее предприятие.

– Ожидание прибыли.
– Усилия промоутера или третьих лиц.

Другими словами, согласно тесту Хоуи, инвестиционный контракт – это инвестирование денег в ожидании прибыли от общего предприятия, в зависимости исключительно от усилий промоутера или третьей стороны.

ICO (*Initial Coin Offering* – первоначальное предложение монет) – аббревиатура по аналогии с **IPO** (*Initial Public Offering* – первая публичная продажа акций компании) – это способ привлечения первичного капитала с использованием криптовалюты. Инвесторам, пропорционально их вкладу, предлагаются ***токены***.

ISO (*Initial Scam Offering* – первичное предложение аферы) – игра слов, аллюзия на ICO, с намёком, что большинство (если не все) из них являются пустышками. Придумал фразу предприниматель и разработчик Ethereum **Жюльен Бутелу** (*Julien Bouteloup*), чтобы предупредить людей об афере на рынке криптовалют.

InstantSend – сервис для мгновенных транзакций.

Lightning Network (LN) – технологическое решение по масштабированию биткоина и других криптовалют (Lightcoin etc.). Предложено компанией **Blockstream**. Представляет собой надстройку над протоколом биткоина, которая позволяет проводить транзакции без предварительной записи в блокчейн. Функционирует в виде двунаправленных платежных каналов.

MAST (*Merkelized Abstract Syntax Trees* – меркелизованные абстрактные синтаксические деревья) – технология расширения Биткоина, которая позволяет повысить гибкость смарт-контрактов, улучшить масштабируемость и увеличить приватность. Объединяет потенциал **P2SH** с возможностями **деревьев Меркла**. Находится в стадии разработки.

MimbleWimble – предложение по масштабированию Биткоина, направленное на повышение приватности, масштабируемости и взаимозаменяемости. Название взято из книги Джоан Коллинз (*Joan Collins*) «Гарри Поттер и дары смерти», где «Mimblewimble» – это заклятие косноязычия, которое связывает язык жертвы, не позволяя сказать ни слова.

Nocoiner (*нокоинер*) – человек, у которого нет биткоинов. Нокоинеры (как правило, социалисты, юристы или экономисты MBA) – это люди, которые упустили возможность купить биткоин по низкой цене, потому что считали, что это мошенничество, и сейчас жалеют, что упустили возможность. Нокоинер скрывает свое сожаление, постоянно заявляя, что биткоин рухнет, что это мошенничество, это пирамида или пузырь. Худшие нокоинеры – это академики и финансисты («золотые жуки»). Они полагают, что мир должен им всё, чего они хотят, потому что они являются частью элиты.

Nonce («*нонс*») – числовой параметр, искомый в ходе майнинга (алгоритме PoW) и записываемый в заголовок блока. Собственно, целью майнинга, как соревновательного процесса за право добавить блок транзакций в блокчейн, и есть подбор такого Nonce, чтобы искомый хэш блока (Block Hash) был меньше некоторого заданного числа Target, что равнозначно получению хэша блока, начинающегося с определенного числа нулевых битов.

P2P (*Peer to Peer*) – одноранговая компьютерная сеть, в которой все участники (узлы) равноправны и могут взаимодействовать друг с другом, являясь клиентом и сервером одновременно.

P2SH (*Pay to Script Hash*) – технология мультиподписи, снижающая нагрузку на инфраструктуру Биткоина с точки зрения хранения данных.

PoI (*Proof-of-Importance*) – альтернативный **PoW** алгоритм достижения консенсуса при записи блока в блокчейн, при котором определение пользователя, который будет записывать следующий блок, происходит с учетом вклада каждого участника процесса в развитие и продвижение криптовалюты.

PoS (*Proof-of-Stake* – подтверждение доли владения) – альтернативный PoW алгоритм достижения консенсуса при записи блока в блокчейн, при котором вероятность записи нового блока в блокчейн и получение соответствующего вознаграждения пропорциональна доле владения пользователя в системе:

– отдельно взятый держатель валюты, имеющий долю ***P*** от общего числа монет в обороте, создает новый блок с вероятностью ***P***.

PoW (*Proof-of-Work* – доказательство выполненной работы) – алгоритм, при помощи которого сеть майнинга биткоина приходит к консенсусу, определяя какой из майнинговых узлов запишет сформированный блок в блокчейн.

Суть PoW сводится к двум основным пунктам:

– Необходимости выполнения определенной достаточно сложной и длительной вычислительной задачи.
– Возможности быстро и легко проверить результат.

PPS (*Pay per Share*) – метод оплаты (награды) за майнинг в пуле. Оплата за каждый найденный шейр (шару).

PPLNS (*Pay Per Last N Shares*) – метод оплаты (награды) за майнинг в пуле. Оплата за последние N шейров (шар).

PROP (*Proportional*) – метод оплаты (награды) за майнинг в пуле. Награда рассчитывается пропорционально доле отправленных майнером шейров (шар) при нахождении блока пулом.

RBF (*Replace-By-Fee*) – в Биткоине замена существующей транзакции новой транзакцией с повышением комиссии. Эта функция предоставляет возможность увеличивать размер комиссии для ускорения процесса подтверждения существующей транзакции в блокчейне.

RBF описан в **BIP-0125**. С помощью Replace-By-Fee пользователи могут заменить собственную транзакцию на более новую транзакцию с уже включенной увеличенной комиссией.

Schnorr – Схема Шнорра – одна из наиболее эффективных и теоретически обоснованных криптографических схем аутентификации.

Scrypt – криптографический алгоритм хэширования, разработанный для валюты лайткоин (LTC). По сравнению с функцией SHA-256 вычисления происходят быстрее и требуют меньшей вычислительной мощности.

SEC (*The United States Securities and Exchange Commission*) – Комиссия по ценным бумагам и биржам США – агентство правительства США, осуществляющее функции надзора и регулирования американского рынка ценных бумаг.

Seed (*семя, источник)* – кодовая фраза (последовательность слов), при помощи которой пользователь получает доступ к приватному ключу (private key) от кошелька или биткоин-адреса.

SegWit (*Segregated Witness* – «отделенный свидетель») – софтфорк, предложенный командой разработчиков Bitcoin Core, целью которого является оптимизация размера блока.

SHA-256 – криптографическая функция хэширования, лежащая в основе протокола доказательства выполнения работы Bitcoin, а также некоторых других криптовалют.

Share (*шейр* или *шара*) – часть задачи по поиску крипторешения, которую выдаёт майнинг-пул клиентам-майнерам.

Smart Contract – См. **Умные контракты**.

Solidity – язык программирования на платформе Ethereum для разработки умных контрактов.

SPV (*Simplified Payment Verification*) – упрощенная верификация платежей – особенность протокола Bitcoin, которая позволяет нодам заверять транзакцию без загрузки полной цепочки блоков. Вместо этого для верификации транзакции достаточно загрузки заголовков (Head) блоков, в которых содержатся хэши.

State channels (Каналы состояния) – технология, позволяющая проводить обмен информацией (транзакциями) между узлами в сети без предварительной записи в блокчейн. Идея каналов состояния заключается в перемещении многих промежуточных процессов вне блокчейна, сохранив при этом характерную надежность блокчейна.

STO (*Security Token Offering*) – способ инвестирования криптовалютных проектов и привлечения первичного капитала с использованием криптовалюты. В отличие от ICO, при STO оперируют только с security-токенами или токенизированными ценными бумагами с целью получить дивиденды, долю в собственности или право голоса. STO всегда подпадает под регулирование SEC.

Target или **Difficulty Target** (*целевая сложност*ь) – максимальное число, которое не должен превышать хэш блока (Block Hash). Фактически определяет количество нулевых битов в начале вычисляемого при майнинге хэш-кода блока.

Testnet – тестовая цепочка блоков транзакций. Используется разработчиками, чтобы не тратить деньги в основной цепочке.

TGE (*Token Generating Event*) – в общем случае синоним ICO, а если точнее, то одной из стадий ICO, а именно – выпуск и распределение токенов (**Token sale**).

TumbleBit – совместимая с Биткоином система конфиденциальности, обеспечивающая закрытые, недоверительные и масштабируемые платежи. При помощи TumbleBit, любой его пользователь сможет совершать быстрые анонимные платежи вне блокчейна, при помощи недоверительного посредника под названием Tumbler (тумблер).

UTXO (*unspent transaction output*) – непотраченный Выход транзакции – неделимые куски биткоинов, привязанные к конкретному владельцу, записанные в blockchain, и признанные валютой во всей сети.

В Bitcoin не существует понятия счетов или балансов; есть только непотраченные Выходы транзакций (UTXO).

Wire transfer (*Безналичный или банковский перевод*) – перевод денег от одного человека другому в электронном виде. Обычно используется для отправки и получения традиционной валюты в обменниках криптовалют.

X11 – система алгоритмов хеширования, использующая цепочку из 11 хеш-функций. Используется для доказательства выполнения работы при майнинге криптовалюты **DASH**.

Zero Knowledge Proof – Доказательство с нулевым разглашением – интерактивный криптографический протокол, позволяющий одной из взаимодействующих сторон («The verifier» – Проверяющей) убедиться в достоверности какого-либо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны («The prover» – Доказывающей).

Криптожаргон и сленг криптобирж

Бигблокеры (*Big Blockers*) – сторонники увеличения лимита размера блоков Биткоина свыше 1 Мб, как способа масштабирования. Чаще всего бигблокерами называют представителей **Bitcoin Unlimted** и сторонников **Bitcoin Cash**.

Биток – Биткоин.

Бросок кобры – резкое кратковременное изменение (повышение или понижение) курса криптовалюты.

Быки – биржевые игроки, играющие только на повышениях цен.

Дамп (*dump* – сброс, демпинг) – намеренная продажа криптоактивов в больших количествах с целью искусственного понижения их курсовой стоимости в краткосрочной перспективе.

Качели – краткосрочные скачки курса в малом ценовом диапазоне.

Кит (*Whale*) – крупный криптотрейдер или группа трейдеров, которые в состоянии повлиять на рыночную ситуацию.

Кран (*faucet*) – сайт, который предоставляет возможность зарабатывать небольшое количество криптовалюты за просмотр рекламы или выполнение несложных заданий.

Крипта – обобщенное название всех криптовалют.

Лонг (Long – длинные позиции) – биржевая операция, целью которой является игра на повышение и стремление впоследствии продать криптоактивы дороже.

Манихолд (*money hold*) – задержка на возможность использования, ввода или вывода денежных средств на бирже.

Медведи – биржевые игроки, играющие только на понижении цен.

Рект (*Rekt* – от *Wrecked* – крах, провал) – потеря денег в результате очень невыгодной сделки.

Сопля – резкое снижение курса за короткий отрезок времени.

Туземун (*to the Moon*) – буквально «полет на Луну» – стремительный рост курсовой стоимости криптовалют.

Памп (*pump* – насос, накачивание) – намеренная покупка криптоактивов с целью искусственного повышения их курса в краткосрочной перспективе.

Пендинг (*pending*) – незавершенная транзакция (транзакция, находящаяся в ожидании завершения).

Полынь (поло) – сленговое название популярной криптобиржи **Poloniex.com**.

Ферма – оборудование для майнинга криптовалют.

Фиат – т.н. фиатные деньги – деньги, выпускаемые государством.

Флэт (*flat* – горизонтальный) – боковое движение цены, когда цена ни растет, ни падает, а движется в границах плоского канала.

Фоло (*FOLO – Fear of losing out*) – синдром упущенной выгоды. Поспешные и непродуманные действия трейдеров на бирже в опасении проиграть или не получить доход. Как правило, подталкивают к совершению невыгодных сделок.

Халвинг (от англ. *halving* – уполовинивание, уменьшение в два раза) – искусственное сокращение вдвое эмиссии монет биткоина, заложенное в его протокол. Происходит через каждые добавленные 210 000 блоков (примерно раз в 4 года).

Хеджирование (от англ. *hedge* – страховка, гарантия) – страхование рисков от колебаний цены актива на рынке путём открытие сделок противоположной позиции на другом рынке. Неблагоприятное изменение цены хеджируемого актива компенсируется прибылью, получаемой по другому инструменту. По виду используемого инструмента различают три вида хеджирования: ***фьючерсное, форвардное и опционное***.

Ходлинг (от *HODL*) – удержание и накопление определенной криптовалюты (как правило, биткоина). Стратегия, основанная на вере, что курс криптовалюты будет постоянно расти.

Хомяки – начинающие биржевые игроки (новички), подверженные массовой панике.

Шиткоин (*Shitcoin*) – буквально *дерьмокоин.* Шиткоинами называют не имеющие реальной ценности криптомонеты, которые предлагают мошенники.

Шорт (Short – короткие позиции) – биржевая операция, целью которой является игра на понижение стоимости криптоактивов. Если трейдер уверен в падении цен, он берет криптоактивы взаймы у Брокера, продает их по текущей цене и старается позже откупить (закрыть короткую позицию) по более низкой цене.

Прохождение транзакций (термины)

Unconfirmed input – неподтверждённые входящие биткоины в транзакции;

Unconfirmed output – неподтверждённые потраченные биткоины в транзакции;

Unconfirmed parent – транзакция использует «неподтверждённые» монеты в качестве новых input;

Unconfirmed RBF – неподтверждённая транзакция, которую пометили как транзакцию с «заменяемой комиссией»;

RBF («*double spend!*») – деньги были отправлены с низкой комиссией, и отправитель через некоторое время создал новую транзакцию и отправил те же монеты на те же адреса, но хэш транзакции уже другой (первоначальная транзакция исчезнет из блокчейна);

1 confirmation – транзакция включена в блок, ей более или менее можно доверять.

Майнинг: Термины и параметры

Майнинг – это необходимый и важный процесс в сети Биткоина, в результате которого в блокчейн добавляется новый блок транзакций и происходит эмиссия монет биткоина.

В результате майнинга решаются **2 основные задачи**:

1. Определяется узел сети Биткоина (*node*), который получает право записи очередного блока в блокчейн. Этим достигается консенсус в одноранговой сети.

2. Производится эмиссия (дополнительный выпуск) монет биткоина, которые в качестве вознаграждения (стимула) получает майнер, записавший новый блок.

Первая задача решается при помощи алгоритма, который получил название **Proof-of-Work (PoW)** – доказательство выполненной работы.

С него и начнем…

PoW (*Proof-of-Work*) – доказательство выполненной работы – алгоритм, при помощи которого сеть майнинга биткоина приходит к **консенсусу**, определяя какой из майнинговых узлов запишет сформированный блок в блокчейн.

Суть PoW сводится к двум основным пунктам:

1. Необходимости выполнения определенной достаточно сложной и длительной вычислительной задачи. В сети Биткоина это подбор хэш-кода, отвечающего заданным критериям.
2. Возможности быстро и легко проверить результат.

PoW используется в протоколах Биткоина и многих других криптовалют.

Bitcoins per Block или Block Reward (*биткоинов за блок*) – вознаграждение, выплачиваемое майнеру за успешное решение криптографической задачи и присоединение блока к блокчейну. Для Биткоина изначально это количество составляло **50 BTC**, однако каждые **210 000 блоков** (примерно каждые 4 года) это количество уменьшается в два раза. Об этом подробнее читайте в главе **«Почему количество биткоинов ограничено»**.

На момент написания этой книги (2018 год) вознаграждение составляет **12,5 BTC за блок**. Следующее уполовинивание до **6,25 BTC за блок** ожидается в **2020 году**.

Основные параметры майнинга

В ходе майнинга в заголовок блока записывается ряд параметров:

Nonce – числовой параметр, искомый в ходе майнинга (алгоритме PoW) и записываемый в заголовок блока. Собственно, целью майнинга, как соревновательного процесса за право

добавить блок транзакций в блокчейн, и есть подбор такого Nonce, чтобы искомый хэш блока (**Block Hash**) был меньше некоторого заданного числа **Target**, что равнозначно получению хэша блока, начинающегося с определенного числа нулевых битов.

Difficulty Target, также называемая **difficulty bits** или **bits** – целевая сложность – максимальное число, которое не должен превышать искомый при майнинге хэш блока (**Block Hash**). Фактически определяет количество нулевых битов в начале искомого хэша. Часто сокращенно называется **Target**.

Собственно **Target** – это само число, а **bits** – особый формат записи Target в заголовок блока. В bits записывается сразу два числа: первый байт – **экспонента** (exponent), оставшиеся три байта – **мантисса** (mantissa). Для того, чтобы получить Target из bits, нужно воспользоваться следующей формулой:

$$\textbf{Target} = \textbf{mantissa} * 2^{(8 * (\textbf{exponent} - 3))}$$

Bitcoin Difficulty, или **Difficulty bits**, или просто **Difficulty** – параметр, характеризующий сложность майнинга, т.е. сложность решения криптографической задачи.

Этот параметр представляет из себя отношение

Max_Target / Current_Target,

где **Max_Targe**t – максимально возможный **Target**, а именно **0x00000000FFFF0000000000000000000000000000000000000000000000000000** (**0x1d00ffff** в формате bits). Это значение Target использовалось при запуске Биткоина в январе 2009 года;

а **Current_Target** – это текущее значение **Target**. Например, для блока **№475468**, добавленного в момент написания этой главы книги (12 июля 2017), значение Target было равно **0x18018d30** в формате **bits**, а значение **Difficulty** равно **708659466230,332**.

Именно bits, как правило, указывается во всех **Block explorer**.

Между **Difficulty** и **Target** существует обратная связь – чем выше сложность (Difficulty), тем меньше Target (больше количество нулевых битов в искомом хэше).

На самом деле, сначала вычисляется **Bitcoin Difficulty** (сложность майнинга), а затем из неё выводится текущий **Target**.

Первоначальная сложность (Difficulty) при запуске Биткоина в январе 2009 года была равна 1 (единице). Но в связи с увеличением суммарной компьютерной мощности майнинга, необходимо увеличивать и сложность, чтобы нахождение **Nonce** и запись нового блока происходило примерно каждые 10 минут.

Пересчет (коррекция) сложности происходит через каждые **2 016 блоков**. Это по времени соответствует примерно **20 160 минут** или **две недели**.

На самом деле, поскольку вычислительная мощность возрастает, время, затраченное на майнинг последних 2 016 блоков (*Actual Time of Last 2016 Blocks*), получается несколько меньше, чем 20 160 минут.

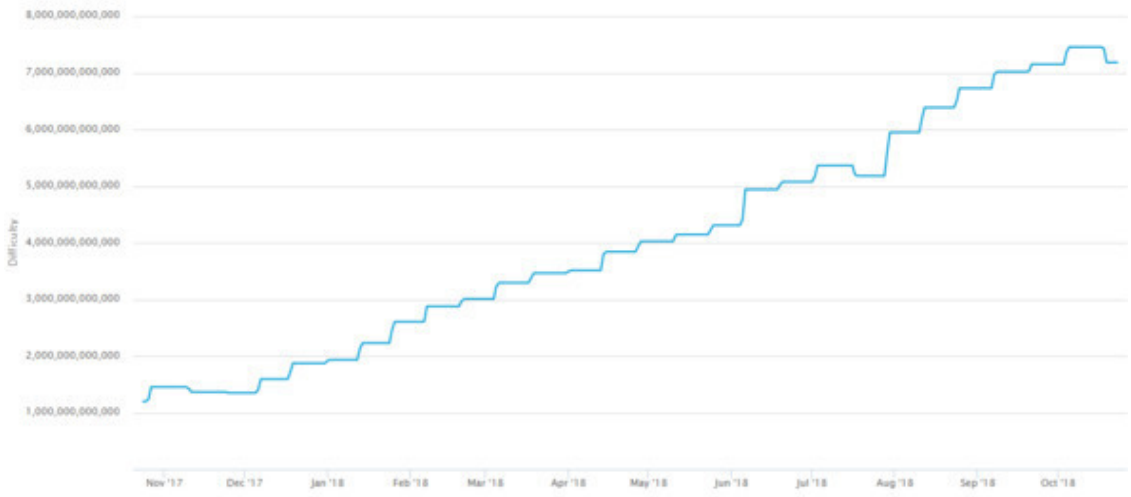
Отношение необходимого времени (20 160 минут) к реально затраченному на майнинг – это и есть поправочный коэффициент, который изменяет сложность майнинга. Таким образом, новое значение сложности (New Difficulty) рассчитывается по формуле:

New Difficulty = Old Difficulty * (20 160 minutes / Actual Time of Last 2016 Blocks)

Далее из New Difficulty рассчитывается новое значение Difficulty Target по формуле:

Difficulty Target = Max_Target / New Difficulty

где Max_Target = 0x1d00ffff (в формате bits)



Изменение сложности майнинга биткоина

Merkle Root – хэш-код транзакций текущего блока, рассчитанный с использованием алгоритма, известного, как **дерево Мёркла** *(Merkle tree*) или бинарное дерево хэшей. Подробнее об этом читайте в главе **«Блок»**.

Height – номер блока в блокчейне.

Timestamp – временная метка записи блока (дата и время). Записывается в формате UNIX-время (секунды от эпохи UNIX).

Number Of Transactions – число транзакций, записанных в блок.

Previous Block – предыдущий блок.

Подведем краткие итоги…

В процессе майнинга решается криптографическая задача по подбору некоторого параметра **Nonce**, который, будучи записанным в заголовок блока, приводит к тому, что получившийся хэш-код блока (**Block Hash**) удовлетворяет заданному условию, а именно – меньше или равен числу **Target**, которое записывается в формате **bits**.

В свою очередь, число **Target** связано со сложностью майнинга (**Bitcoin Difficulty** или попросту **Difficulty**), которая пересчитывается через каждые **2 016 блоков** (примерно 2 недели) и зависит от суммарного времени майнинга этих блоков – чем быстрее происходит майнинг (за счет увеличения вычислительной мощности), тем более высокая сложность (Difficulty) устанавливается и тем меньше число Target.

Следующие понятия используются в расчетах эффективности майнинга:

Hashrate (*хэшрейт* или *вычислительная мощность*) – вычислительная производительность компьютерного оборудования для майнинга криптовалют. Измеряется в хэшах (hash) в секунду.

Основные используемые единицы:

kH/s (килохэш/сек) – 1 тысяча хэш/сек или 1 000 хэш/сек.
MH/s (мегахэш/сек) – 1 миллион хэш/сек или 1 000 000 хэш/сек.
GH/s (гигахэш/сек) – 1 миллиард хэш/сек или 1 000 000 000 хэш/сек.
TH/s (терахэш/сек) – 1 триллион хэш/сек или 1 000 000 000 000 хэш/сек.
PH/s (петахэш/сек) – 1 квадриллион хэш/сек или 1 000 000 000 000 000 хэш/сек.
EH/s (эксахэш/сек) – 1 квинтиллион хэш/с или 1 000 000 000 000 000 000 хэш/сек.

По состоянию на конец октября 2018 хэшрейт Биткойна установился на уровне в **55 EH/s**, это на 550% больше, чем в 2017 году.

Изменение суммарного хэшрейта майнинга биткоина

Electricity Rate (*стоимость электроэнергии*) – обычно измеряется в стоимости 1 kW/h ($ за кВт/час).

Power consumption (*энергопотребление*) – Электрическая мощность, потребляемая оборудованием майнинга. Обычно измеряется в ваттах.

Pool fees (*комиссия пула*) – прибыль пула майнеров распределяется между всеми участниками с учетом того, какой объем вычислений произвел каждый майнер (то есть, исходя из хэшрейтов участников).

Time Frame (*временные рамки*) – количество времени, потраченного на майнинг. При расчете эффективности (доходности) добычи, необходимо определить временные рамки майнинга. От этого зависит не только количество потенциально добытых биткоинов, но и энергозатраты.

Profitability decline per year (*снижение рентабельности в течение года*) – на снижение рентабельности, а значит и доходности, влияет увеличение сложности майнинга (см. график выше), а также курсовые колебания криптовалют.

Используемая литература

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto

2. «Введение в криптографию», Филипп Циммерман.

3. «Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок», Майкл Кейси, Пол Винья.

4. «Цифровое золото», Натаниэл Поппер.

5. «Биткоин – деньги для всех», Адам Теппер.

6. Mastering Bitcoin, Andreas M. Antonopoulos.

7. Cryptocurrency / Mercatus Center, George Mason University.

8. Bitcoin in a nutshell, Melvin Draupnir.

9. Bitcoin, Foreword to the book by Saifedean Ammous, Nassim Nicholas Taleb.

10. Blockchain: Simple Explanation, Oleg Mazonka.

11. Distributed ledger technology in payments, clearing, and settlement, David Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird.

11. What kind of evolutions or upgrades does Bitcoin and other cryptocurrencies require to solve its current drawbacks?, Frederick Briggs.

12. Making Sense of Cryptoeconomics, Josh Stark.

13. The Quick, 3-Step Guide to Blockchain Technology, Thijs Maas.

14. Bitcoin Is Dead? The Blockchain Didn’t Get The Memo, Miguel Cuneta.