Сергей Базанов

БИТКОИН для всех

Сергей Базанов

Биткоин для всех. Популярно о первой распределенной одноранговой денежной системе

http://www.litres.ru/pages/biblio_book/?art=39144096
ISBN 9785449365828

Аннотация

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.

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 мно-

го 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 становит-

ся 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 (бит-

коин-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 отра-

жение такой сущности, как деньги. На самом деле, **деньги – это информация**. Информация о том, каким эквивалентом суммарной стоимости обладает субъект (индивидуум или организация).

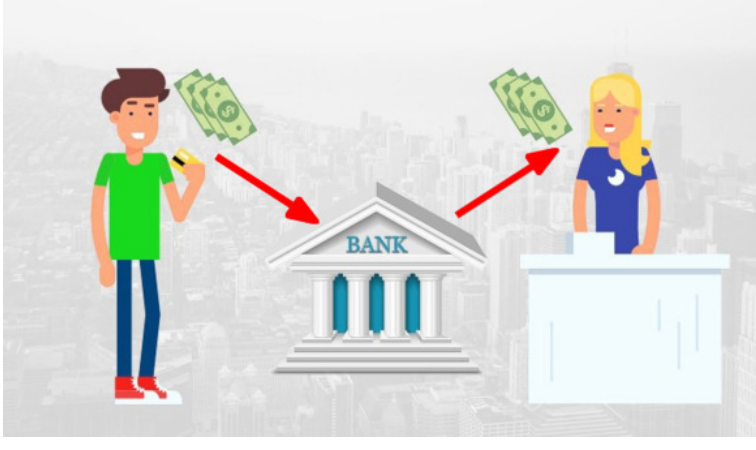
Если у вас в кошельке имеется, к примеру, три банкноты по 100 денежных единиц (гривен, рублей или долларов), то это означает, что вы обладаете суммарным эквивалентом стоимости в 300 денежных единиц. На них вы можете приобрести товары и услуги, эквивалент стоимости (цена) которых менее или равна этим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

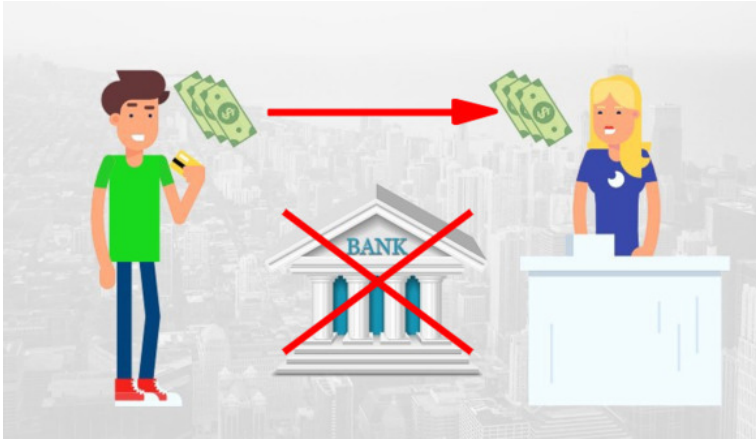
Было сделано много попыток создать т.н. **электронные деньги**, которые бы обходились без посредников, но все они были неудачными или несовершенными.

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 информа-

цию 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.

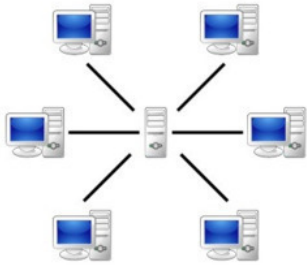
Таким образом обеспечивается защита информации в блокчейне от изменений. Записанную в блокчейн информацию **изменить невозможно** без нарушения целостности (связанности) блоков блокчейна. Это очень важный момент!

Но где хранится эта база данных – блокчейн? Как обеспе-

чить 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

[1] По данным сайта Gobitcoin.io

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**.
– 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] **–**

[2] **Дизайн механизмов** – в экономике – подход, создающий механизм взаимодействия, при котором действия отдельных экономических субъектов

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.

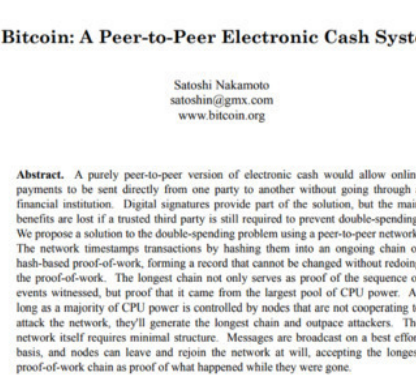
Биткоин – это альтернативная государственным денежная система.

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.

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,

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

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).

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 уста-

новить 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 об-

рушить 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**

Конец ознакомительного фрагмента.