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.

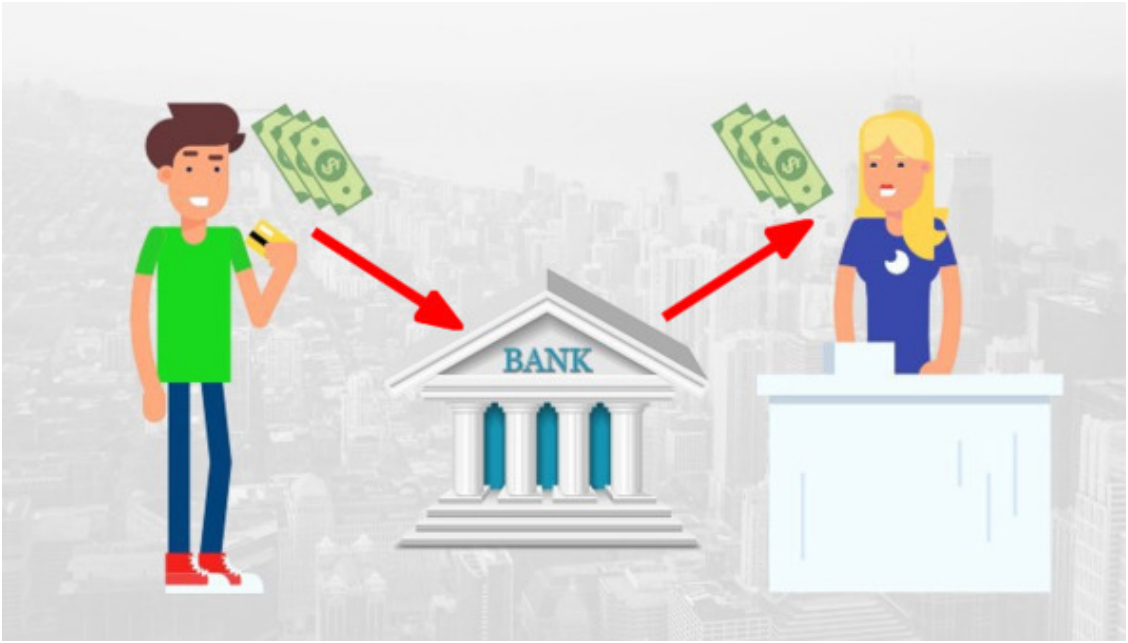
Но, банкноты и монеты – это лишь вещественное отражение такой сущности, как деньги. На самом деле, **деньги – это информация**. Информация о том, каким эквивалентом суммарной стоимости обладает субъект (индивидуум или организация).

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.

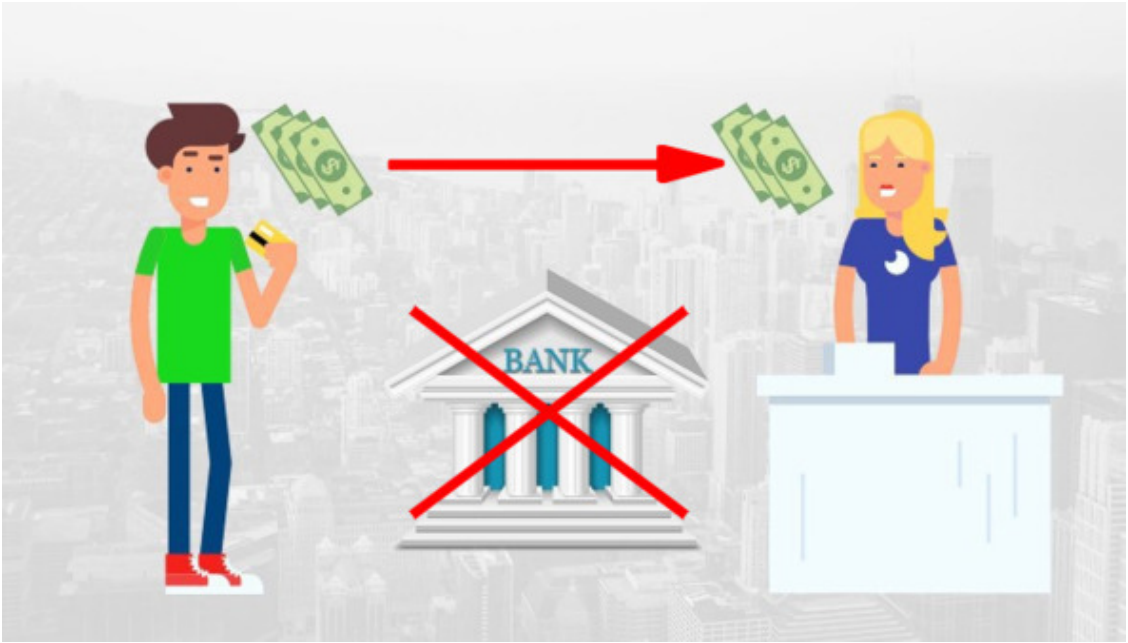
Длительное время люди пытались найти способ передачи денег на расстоянии без участия третьей доверенной стороны – банка. Ведь это было бы очень **удобно**, – как в наличных расчетах. И **дешево**, – не пришлось бы платить банку комиссионные вознаграждения. А также **надежно**, – не было бы риска потерять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

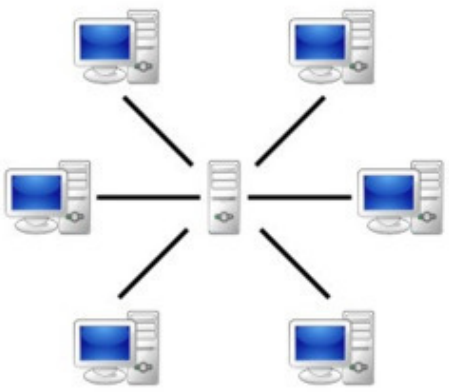
Если кто-либо попробует изменить хоть один символ в любом листе (блоке) этой книги, то «контрольная сумма» этого листа также изменится и не будет соответствовать той, которая записана в служебное поле на следующем листе, что повлечет изменение и его «контрольной суммы» и т. д. по всем последующим листам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

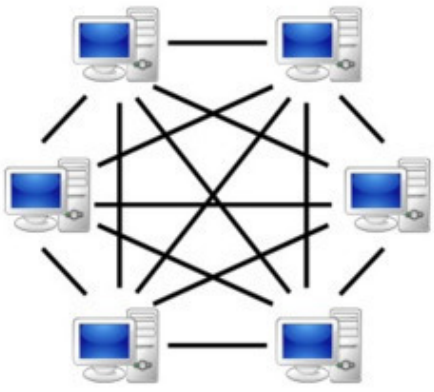
Но где хранится эта база данных – блокчейн? Как обеспечить её безопасное хранение?

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.

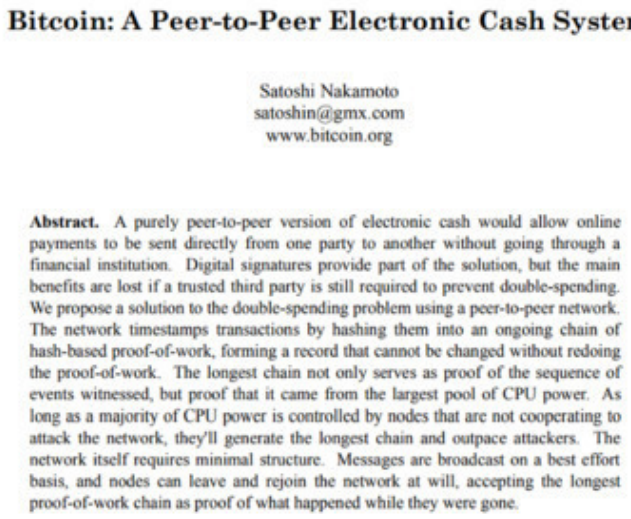
Биткоин – это альтернативная государственным денежная система.

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 1989 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.

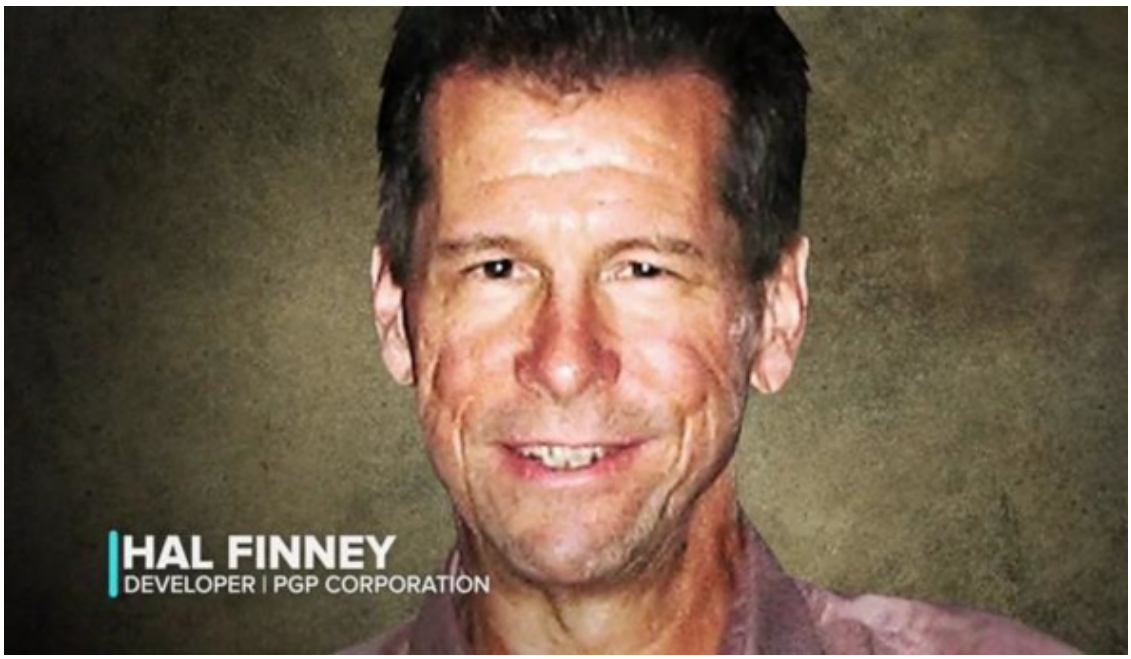
9 января 2009 года Накмото публикует на сайте **bitcoin.org** первый релиз своей программы-клиента[5] **Bitcoin Core** version 0.1, при помощи которой можно не только добывать

[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.

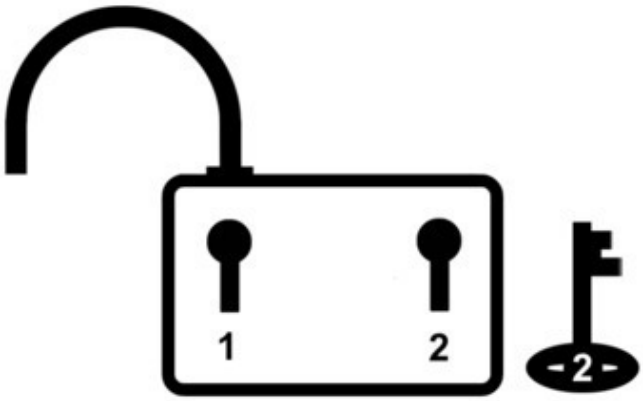
Следует отметить, что открытым (публичным) ключом **можно только зашифровать сообщение**, но расшифровать его уже этим ключом не получится. Для дешифрования нужен только закрытый (приватный) ключ из пары. Так работает алгоритм с асимметричным шифрованием.

Шифрование с асимметричным ключом

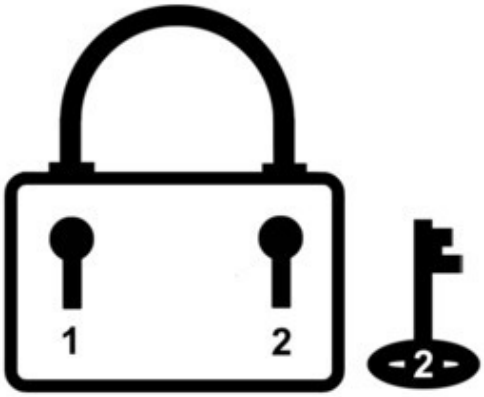
Но вернемся к нашему сундуку с сообщением. Как же теперь наглядно представить асимметричное шифрование? Как так можно – запирать одним ключом, а отпирать другим?

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.

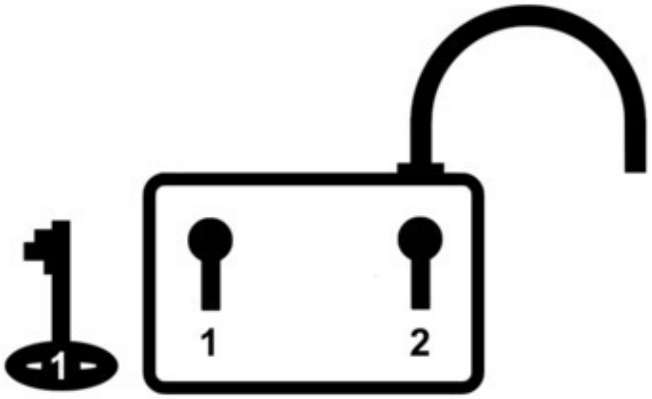
Первоначально замок с зафиксированной левой половинкой дуги (1) и расфиксированной правой (2), а также с ключом 2 (открытым) доставляется лицу, которое должно отправить тайное послание.



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.

Конец ознакомительного фрагмента.