

БИТКОИН ЗА



МИНУТ

Все, что вы всегда хотели знать о биткойне

Brought to you by **Relai**

ЧТО ТАКОЕ БИТКОЙН?

Очень успешная валюта биткоин попала в заголовки газет по всему миру и вызвала многочисленные дискуссии о деньгах, технологиях и инвестициях. Многие хотят извлечь выгоду из его успеха, другие относятся к нему равнодушно или даже скептически. Говорят о спекуляциях и пузырях, но также и об инновациях, денежной революции или даже об избавлении от нынешней денежной системы.

Несколько стран, включая Китай, видят в биткойне угрозу и объявили войну цифровой валюте. Правительства других стран, например, Сальвадора, ввели

биткоин в качестве официального платежного средства в надежде на восстановление экономики.

Но что такое биткойн? Это деньги? Цифровое золото? Мимолетное увлечение компьютерщиков и спекулянтов? Или что-то совсем другое?

Далее мы разберемся в этих вопросах и рассмотрим новую валюту более подробно, чтобы лучше понять, как она работает и какая философия лежит в основе Биткойна. Для этого важно начать с самого начала, то есть с истории возникновения Биткойна.

ИСТОРИЯ БИТКОЙНА

Биткойн зародился в начале девяностых годов. В 1992 году группа компьютерных ученых из Калифорнии создала список электронной почты, чтобы обмениваться с единомышленниками идеями о криптографии, математике, политике и философии. Они называли себя „Cypherpunks“ - игра слов от cyberpunk (человек в научно-фантастической литературе, который с подозрением относится к обществу - и по праву) и cipher (шифровать).

The Cypherpunks

Cypherpunks вскоре превратились в разношерстную команду. Несмотря на разное происхождение, их объединяло убеждение, что в

ближайшем будущем Интернет станет одной из самых спорных арен для человеческой свободы.

Чтобы защитить себя от угрозы контроля, слежки и цензуры в интернете и сохранить свободный и открытый интернет, шифропанки знали, как использовать мощное оружие: Криптография, т.е. шифрование информации.

В своем манифесте 1993 года они заявили: „Cypherpunks пишут компьютерный код. Мы знаем, что кто-то должен написать программное обеспечение для защиты конфиденциальности, и [...] мы его напишем“.

Но одной криптографии будет недостаточно для свободной

цифровой интернет-экономики. Потому что, и Cypherpunks были убеждены в этом, интернет не может быть по-настоящему свободным, если у него нет собственных денег. Деньги, независимые от государств, центральных банков и компаний, цифровые деньги, такие же справедливые и децентрализованные, как сам Интернет.

Денежные эксперименты

Однако создание независимых цифровых денег поставило перед шифровальщиками технические проблемы. Еще в 1990 году криптолог Дэвид Чаумс создал eCash, первую цифровую валюту, которая не была децентрализованной, но обеспечивала анонимность благодаря криптографии. Однако eCash не смогла в долгосрочной перспективе противостоять другим онлайн-платежным системам, поэтому через 8 лет компания была вынуждена подать заявление о банкротстве, и eCash исчезла.

Затем последовали другие попытки, среди которых выделялась компания E-Gold. E-Gold - это цифровая валюта, обеспеченная золотом, которая была открыта для всех. Основанная в эпоху доткомов в 1996 году, компания произвела фурор и в лучшие свои времена обрабатывала транзакции на сумму более двух миллиардов долларов США в год.

Но e-gold также контролировался центральным агентством и поэтому был уязвим. Вскоре последовали юридические проблемы, и правительство США возбудило судебное дело против E-Gold. В 2008 году суд США признал компанию E-Gold виновной в отмывании денег и нарушении Закона о переводе денег. Все активы были заморожены, и компания E-Gold была вынуждена прекратить свою деятельность.

В результате этих неудачных попыток шифровальщикам стали ясны два факта. Во-первых, и eCash, и e-gold были обеспечены залогом. Эти залогом оказались уязвимыми, поскольку они могут быть изъяты государствами. Поэтому цифровые деньги не должны иметь центральную точку атаки, такую как банковский счет, (юридическое) лицо или местоположение сервера. Во-вторых, правительства и регулирующие органы не заинтересованы в независимых от государства цифровых деньгах.

Поэтому основной вопрос, для которого до сих пор не было найдено решения, остался: как цифровые деньги могут работать без центральной стороны, которая ведет бухгалтерский учет и следит за тем, чтобы деньги не тратились дважды? Потому что если бы можно было решить проблему двойных расходов, не полагаясь

на центральную сторону, можно было бы создать цифровые деньги, которые являются родными для интернета.

Мистический акт творения

По этим причинам шифропанки начали обсуждать проекты цифровых денег без центральной партии и без обеспечения. Двумя наиболее важными концепциями были b-money (1998) и BitGold (2005). Эти теоретические проекты, которые так и не были реализованы на практике, по своей конструкции уже были очень похожи на Биткойн. Для шифрования была предусмотрена пара открытый/закрытый ключ, а для создания цифровых монет, как и в случае с биткоином, должно было быть предусмотрено доказательство выполнения работы. Изобретатель биткойна подтвердил, что ему известно о b-money и BitGold.

Однако, поскольку b-money и BitGold полагались на систему голосования для достижения консенсуса (согласования того, кому какие денежные единицы принадлежат в данный момент), они были уязвимы для злонамеренных хакерских атак, которые могли манипулировать выборами и тем самым искажать права собственности.

Для этой последней проблемы, которая все еще стояла на пути

создания новых интернет-денег, решение было представлено в пятницу, 31 октября 2008 года. В тот день по электронной почте шифровальщикам была разослана [„белая книга“ Биткойна](#), в которой Сатоши Накамото объясняет свою концепцию децентрализованной платежной сети. Два месяца спустя, 3 января 2009 года, сеть Bitcoin начала функционировать.

Реакция на новую сеть была сдержанной. Несколько энтузиастов начали тестировать сеть и сообщать об ошибках. Вначале, однако, в основном сам Сатоши Накамото поддерживал работу сети. Но постепенно новость о новых интернет-деньгах распространилась по компьютерным и техническим форумам, и интерес к сети вырос. Через год в сети Биткойн уже было несколько пользователей. Однако сам биткойн еще не имел никакой ценности.

Кто такой Сатоши Накамото?

Белая книга Биткойна, а также электронная переписка изобретателя Биткойна были подписаны именем Сатоши Накамото. Однако истинная личность изобретателя биткойна до сих пор неизвестна, поскольку это имя, по-видимому, является псевдонимом. Для того чтобы связаться с единомышленниками, а затем и с сообществом разработчиков Биткойна, Накамото



использовал как минимум три адреса электронной почты, которые он тщательно шифровал, чтобы невозможно было отследить истинную личность отправителя.

На роль Сатоши Накамото уже претендовали разные люди. Но до сих пор никто не смог доказать это. Потому что окончательное доказательство, а именно отправка биткойна с одного из адресов, который, скорее всего, принадлежит Сатоши, еще никем не было предоставлено.

Более того, группа тех, кто общался „лично“ с Сатоши Накамото через интернет, очень мала. Сатоши Накамото написал свое последнее сообщение сообществу Биткойн 12 декабря 2010 года, но это ни в коем случае не было прощальным посланием - Сатоши просто перестал писать после этого.

Однако его отзыв был предназначен только для широкой общественности. Накамото продолжал информировать небольшую группу основных программистов о дальнейших шагах по развитию сети Биткойн.

В апреле 2011 года он отправил последнее послание и этой группе. Так же таинственно, как Накамото появился на сцене, он снова исчез три года спустя.

Биткойн „День пиццы“

Так как же биткойн вообще обрел ценность? Вначале биткойн можно было добывать и пересылать, но цифровые единицы не имели никакой ценности. Кроме того, круг людей, которые знали биткойн, не говоря уже о том, что могли отправлять и получать его, был еще очень мал.

Все изменилось 22 мая 2010 года, когда на интернет-форуме „bitco-intalk.org“ появился необычный запрос. 28-летний Ласло Ханеч из Флориды предложил 10 000 биткойнов тому, кто закажет две пиццы к нему домой. Один калифорнийский студент воспользовался его предложением и получил две большие пиццы стоимостью 41 доллар, которые были доставлены ему на дом. В ответ Ханец отправил ему 10 000 биткойнов.

С того дня 22 мая ежегодно отмечается биткойнерами как „День пиццы“ биткойна. Этот день так популярен, потому что он иллюстрирует три вещи:

- С тех пор биткойны приобрели ценность

- Биткойны подходят в качестве средства обмена и платежа

- Биткойн как валюта является дезинфляционной.

Количество дополнительных биткойнов, введенных в обращение, неуклонно снижается, что может привести к росту стоимости.

Эти две пиццы вошли в историю как самые дорогие в мире. Если взять курс биткойна на конец 2021 года, то за них было заплачено невероятные 430 миллионов

швейцарских франков. Это большие деньги. Но получатель 10 000 биткойнов уже снова потратил их, по его собственной информации, на дорожное путешествие - по сегодняшнему курсу биткойнов, вероятно, самое дорогое дорожное путешествие в истории человечества.

Биткойн „День пиццы“ также впечатляюще иллюстрирует, почему „Hodln“ - производное от „держать“ - так популярен среди биткойнеров. Имеется в виду вечное хранение собственных биткойнов с целью никогда их не продавать. В конце концов, кто хочет тратить свои биткойны сегодня, когда в ближайшие несколько лет они могут стоить вдвое, втрое или даже в десять раз больше?

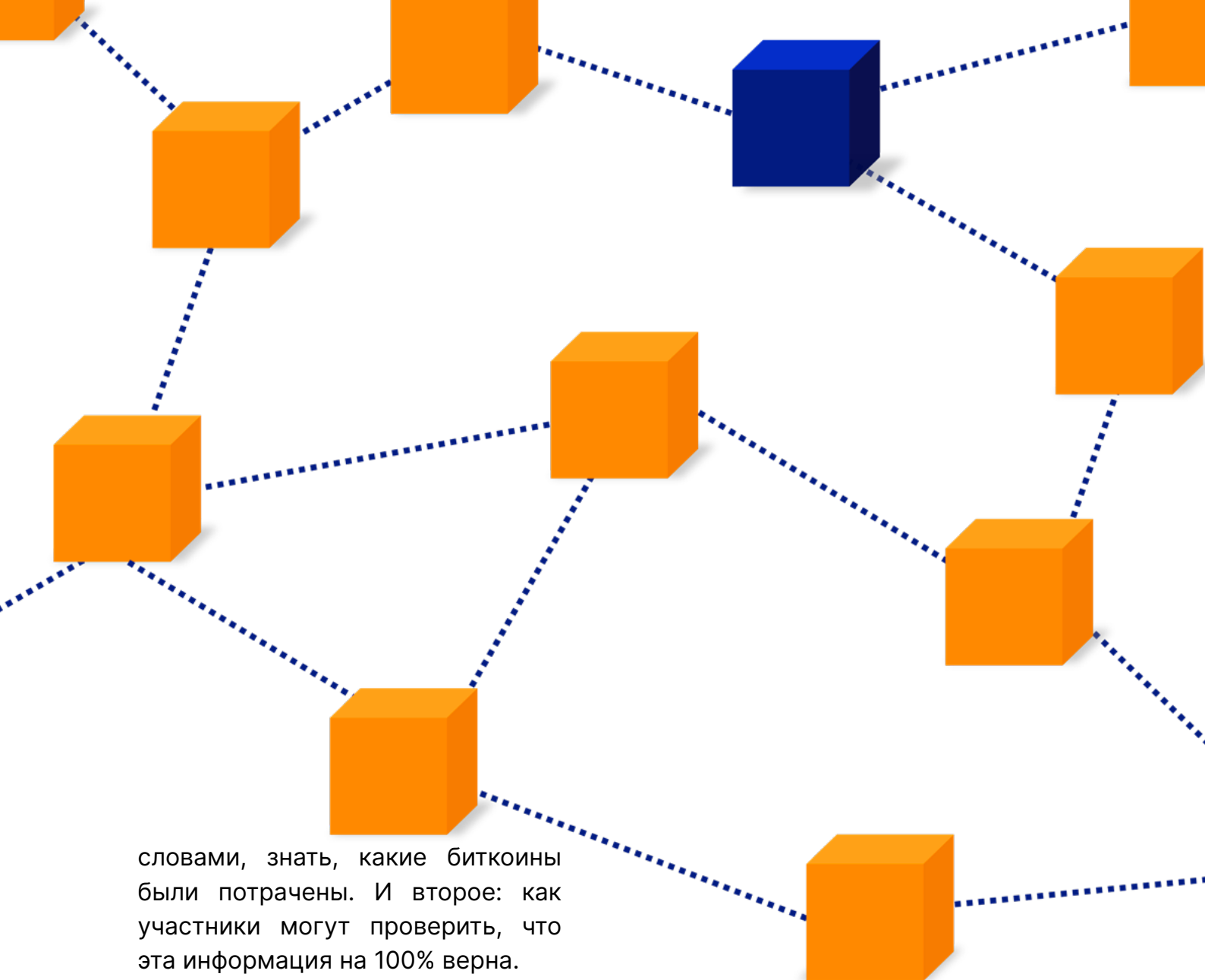
КАК РАБОТАЕТ БИТКОЙН?

Узнав об истории возникновения биткойна, мы теперь погрузимся в то, как работает эта цифровая валюта. Цель - понять, как работает сеть Биткойн, какие проблемы она решает и каковы практические преимущества.

Биткойн задуман как максимально децентрализованная сеть. Ни один из участников сети не должен принимать решения в одиночку - полномочия по принятию решений и надзору распределяются между всеми участниками. Это важно, потому что ни один человек, ни одно правительство или компания не могут изменить сеть самостоятельно, но изменения возможны только коллективно.

Биткойн работает таким образом, что каждый участник сети постоянно владеет идентичной копией текущей собственности - это означает, что все всегда знают, кто и когда владеет каким биткойном. Это означает, что никто не может утверждать, что владеет большим количеством биткоинов, чем у него есть, поскольку все остальные могут проверить это утверждение и признать его ложным.

До появления Биткойна этот тип децентрализованной сети столкнулся с двумя основными трудностями. Во-первых, как сделать так, чтобы все участники постоянно получали актуальную информацию о владении - другими



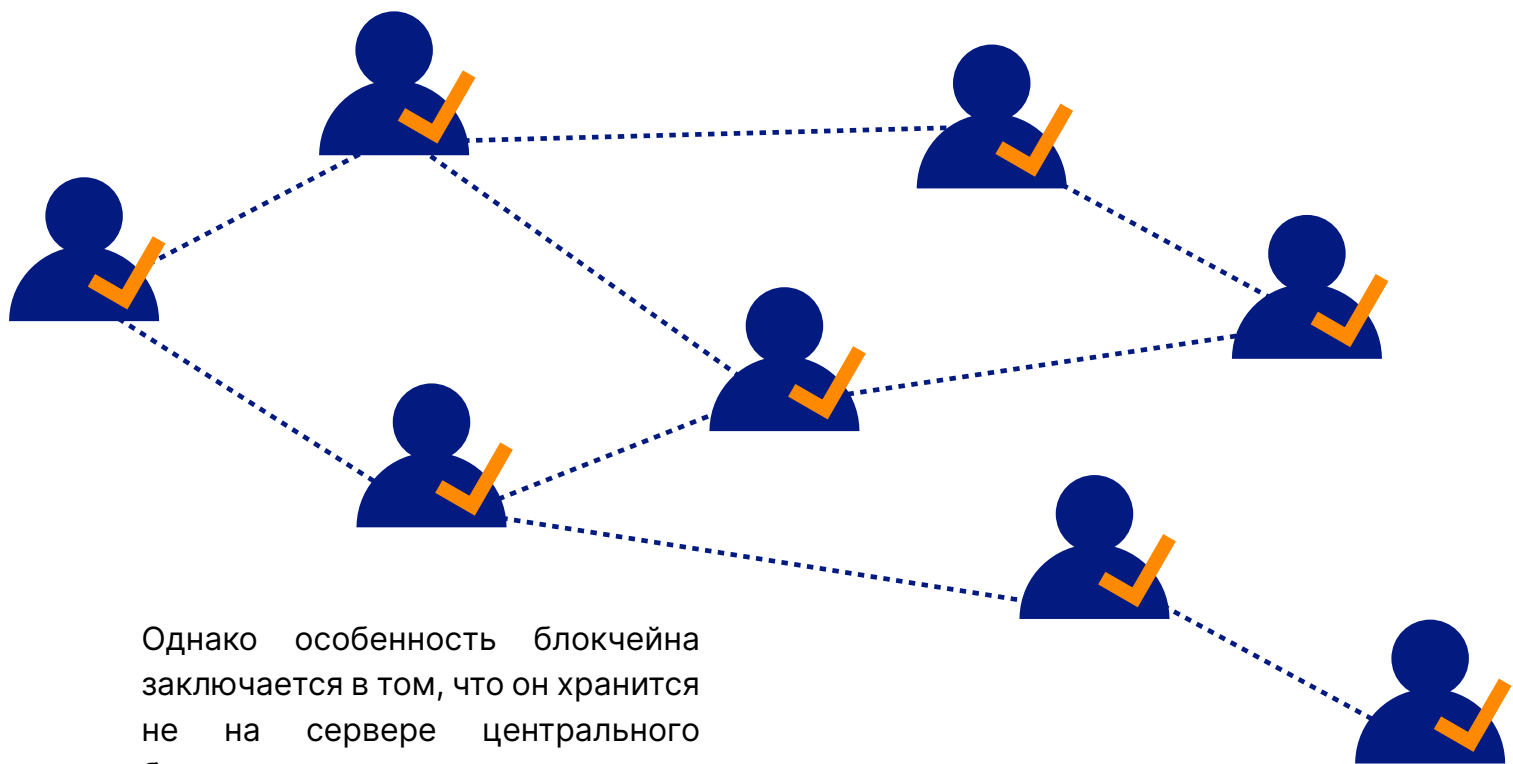
словами, знать, какие биткойны были потрачены. И второе: как участники могут проверить, что эта информация на 100% верна.

Блокчейн

Эти трудности были преодолены благодаря изобретению блокчейна. Блокчейн - это хронологическая последовательность информации. В случае биткойна все транзакции с момента создания биткойна хранятся в хронологическом порядке в отдельных блоках блокчейна биткойна. Каждый участник сети, желающий узнать, кому какой биткойн принадлежит, может проследить историю транзакций в блокчейне и таким образом точно определить, сколько

биткойнов кому принадлежит на данный момент. Если кто-то хочет отправить биткойн, каждый может проверить, действительно ли этот биткойн принадлежит данному человеку.

До сих пор в этом нет ничего особенного; банк делает точно так же. Если клиент хочет потратить франк, банк просматривает историю операций, чтобы узнать, принадлежит ли франк еще клиенту или он уже был потрачен.



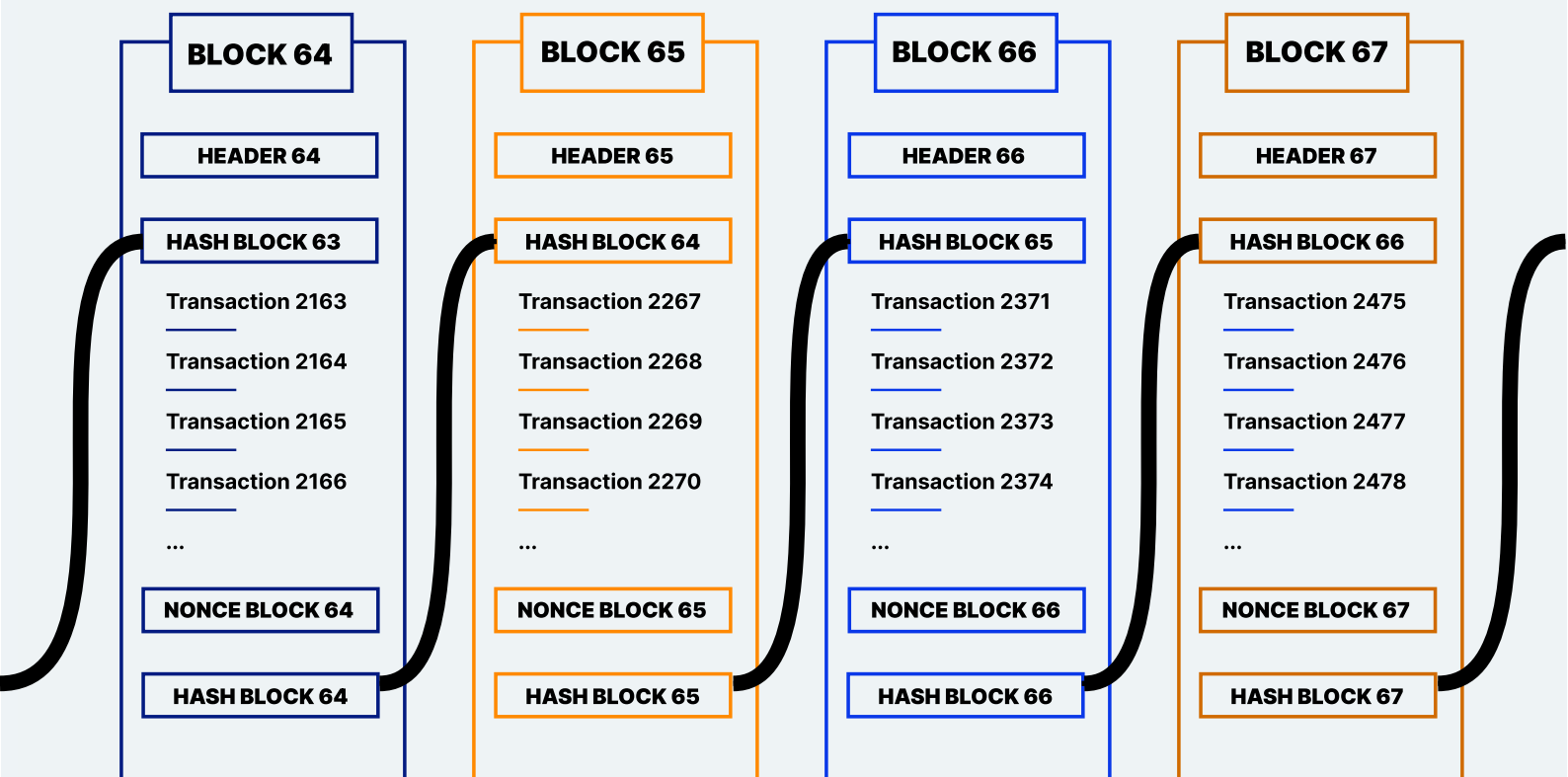
Однако особенность блокчейна заключается в том, что он хранится не на сервере центрального банка, а на соответствующих компьютерах участников сети (так называемых полных узлах) и, таким образом, существует в десятках тысяч копий по всему миру. Это также является причиной того, что Биткойн нельзя просто удалить - для этого пришлось бы удалить идентичную копию блокчейна со всех участвующих компьютеров по всему миру одновременно.

Суть теперь заключается в том, что каждый участник сети может с абсолютной уверенностью определить, что его копия блокчейна верна и что он не получает уведомлений о каких-либо ошибочных транзакциях. Поскольку в блокчейн постоянно добавляются новые блоки с новыми транзакциями, он постоянно растет и должен постоянно обновляться на всех компьютерах-участниках по всему миру. Эти вновь присоединенные блоки, в свою очередь, должны иметь возможность быть проверенными всеми.

Эта проверка осуществляется с помощью неизменных правил, которые определены в компьютерном коде сети. Они точно определяют, какие операции разрешены, а какие нет. Таким образом, каждый пользователь, загрузивший копию блокчейна, может проверить, соответствуют ли все транзакции правилам. Если транзакция нарушает правила, то есть является ложной или мошеннической, она отклоняется участниками сети (полными узлами) и не включается в историю транзакций.

Proof-of-Work (PoW) майнинг

Кроме того, в сети Биткойн существует механизм ограничения добавления новых блоков. Если бы новые транзакции и блоки могли добавляться в блокчейн кем угодно, сеть могла бы легко перегрузиться, так как блокчейн не сможет достаточно быстро



Заголовок, результат хэш-функции предыдущего блока, все транзакции текущего блока и nonce (случайное число) подставляются в математическую функцию. Нетс меняется до тех пор, пока результат хэш-функции не будет содержать достаточное количество предшествующих нулей. Этот процесс называется добычей полезных ископаемых.

обновлять себя до одного и того же состояния по всему миру.

Чтобы предотвратить это, Биткойн использует механизм доказательства выполнения работы. Для того чтобы кому-то было разрешено добавить новый блок в блокчейн, он должен предоставить доказательство своей работы. Подходящее сравнение - поиск иголок в стоге сена. Только тем, кто нашел иглу, разрешается добавлять новый блок в блокчейн, и они получают вознаграждение в виде новых единиц Биткойна и комиссии за транзакции, содержащиеся в блоке.

Математически это выполнение хэш-функции (хэш-алгоритм SHA-256). Хеш-номер предыдущего блока, транзакции текущего блока и случайное число (nonce) хешируются вместе. Уncia меняется до тех пор, пока хэш-функция не выдаст результат с минимальным количеством ведущих нулей. Например, блок #700000, созданный 11 сентября 2021 года, имел действительный хэш-номер: 0000000000000000000590fc0f3e-ba193a278534220b2b37e 9849e1a-770ca959.

Подведем итог: майнеры поддерживают работу сети Биткойн. Благодаря им

новые транзакции постоянно обрабатываются и добавляются в блокчейн. Полноправные узлы контролируют сеть и следят за тем, чтобы в блокчейн не попадали мошеннические транзакции.

21 миллион биткойнов

Хотя в блокчейн Биткойна постоянно добавляются новые блоки, а майнеры получают за эту работу вознаграждение в виде новых биткойнов, общее количество биткойнов ограничено 21 миллионом биткойнов. Никогда не будет больше 21 миллиона биткойнов. Но эти 21 миллион монет не были в обращении с самого начала. Скорее, они выпускаются кодом Биткойна в соответствии со строгим графиком эмиссии.

Когда биткойн был запущен, код выдавал майнерам 50 новых биткойнов примерно каждые 10 минут. Через четыре года после запуска количество биткойнов, выпускаемых за десять минут, сократилось вдвое. Этот процесс называется halving и описывает тот факт, что вознаграждение за блок для майнеров уменьшается наполовину каждые 4 года.

В настоящее время в обращении уже находится чуть менее 19 миллионов биткойнов. Оставшийся биткойн будет добываться до 2140 года. После этого майнеры будут получать компенсацию только за

счет комиссии за транзакции.

Абсолютно ограниченное количество единиц биткойна является одной из фундаментальных характеристик криптовалюты и делает биткойн крайне дефицитным товаром. Эта абсолютная цифровая нехватка является важной предпосылкой для его функционирования в качестве хранилища стоимости в течение длительных периодов времени, и именно поэтому биткойн часто называют цифровым золотом или золотом 2.0.

Результат: цифровая недвижимость

Если вы посмотрите на все особенности сети Bitcoin в совокупности, то поймете всю важность этого изобретения. Впервые в истории перед вами цифровой товар, который существует только в ограниченном количестве. Биткойн нельзя скопировать или продублировать.

Благодаря этой уникальности биткойн также часто называют цифровой недвижимостью. Ведь как каждый клочок земли на этой земле уникален и существует только один раз, так и каждая единица биткойна также уникальна и существует только один раз в цифровом пространстве.

Этими биткойн-единицами можно по-настоящему владеть. Только

тот, кто владеет соответствующим закрытым ключом, т.е. комбинацией цифр и букв, состоящей из 64 символов, может управлять связанным с ним Bitcoin. Это означает, что без этого закрытого ключа биткойн нельзя ни украсть, ни конфисковать, ни заблокировать. Это позволяет владельцу иметь абсолютный контроль над

собственными финансовыми ресурсами, независимо от того, является ли он миллионером, политическим беженцем или преследуемым кредитором. Таким образом, впервые с момента изобретения компьютера появилась возможность по-настоящему владеть цифровой собственностью.

ПОЧЕМУ ИМЕННО БИТКОИН?

Но почему столько шумихи вокруг биткойна? Возможность действительно владеть цифровой собственностью может стать революционной. Но зачем кому-то вообще владеть биткоином?

Лучшее из двух миров

В прошлые века в качестве платежных средств в основном использовались драгоценные металлы, а позднее наличные деньги в виде монет и банкнот. Преимущество этих платежных средств заключалось в том, что их можно было хранить и выпускать независимо от третьих лиц. Не зря в народе говорили: деньги - это напечатанная свобода. Недостатком драгоценных металлов, а также наличных денег является то, что их трудно использовать в новом, цифровом мире Интернета. В последнее время, с появлением интернет-

магазинов, кредитные карты стали использоваться широкими слоями населения.

Но теперь, когда люди все чаще используют цифровые деньги на банковских счетах и кредитных картах, риски контрагентов, которым они подвергаются, возрастают. Что делать, если финансовое учреждение объявит о своей неплатежеспособности и сбережения будут потеряны? Или если, как это случилось на Кипре в 2013 году, снятие наличных будет строго ограничено, платежи внутри страны и за рубежом будут заблокированы, и даже произойдет принудительная экспроприация сберегательных счетов? Или клиентам банка не разрешается отправлять деньги знакомому, потому что он живет на Кубе или в Иране?

С переходом на цифровые деньги, хранящиеся на банковских счетах, мы в конечном итоге перестаем контролировать свои собственные деньги. Однако до сих пор это обстоятельство было ценой, которую мы должны были заплатить за возможность участвовать в оцифрованной повседневной жизни.

Биткойн предлагает решение этой дилеммы. Будучи цифровыми деньгами, они идеально подходят для использования в цифровой сфере. В то же время, являясь цифровой собственностью, биткойн можно хранить, не полагаясь на третьих лиц (банки). Таким образом, вы можете буквально хранить биткойн под матрасом,

храня закрытые ключи там, где это кажется наиболее безопасным.

Подходящее время

Биткойн был создан в разгар мирового финансового кризиса 2008/09 года. На первом блоке блокчейна биткойна, который также называется блоком Genesis, Сатоши Накамото оставил четкое послание. Там он цитирует заголовок в газете The Times со словами: „Канцлер на грани второго спасения банков“.

Этим поступком Сатоши выразил критическую по отношению к государству философию киберпанков. Во время

Bitcoin Genesis Block Raw Hex Version

00000000	01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	;f1ýz{.²zÇ,>
00000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.È.Ã^ŠQ2:Ÿ,ª
00000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_IŸŸ...¬+
00000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ŸŸŸŸM.ŸŸ..
00000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Times 03/
00000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 Chancel
000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brink of
000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bailout f
000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksŸŸŸŸ..ð.
000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠŸ°pUH'
000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"(à9.
000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybâê.aB¶IÖ¿?Lİ8Ä
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.â.Á.ß\8M+ø..W
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._¬....

финансового кризиса 2008 года центральные банки выпустили в обращение огромное количество новых денег, чтобы спасти банки. Однако косвенно за это заплатили сберегатели, поскольку их сбережения потеряли в цене из-за наплыва денег. Этот факт утвердил киберпанков в их недоверии к государству и укрепил их убежденность в том, что срочно необходимы независимые от государства деньги.

Та же игра, только в еще больших масштабах, повторилась после начала пандемии Ковид-19. Только в 2020 году денежная масса США была увеличена на 50 процентов, а в других странах - включая Швейцарию - цифровой печатный станок работает постоянно. Прямым следствием этого являются рекордно низкие процентные ставки - в Швейцарии даже отрицательные процентные ставки - и высокая инфляция активов.

Хеджирование от девальвации валюты

Поэтому биткоин был запущен в самое подходящее время. Редко когда денежный вопрос был более актуальным, а знаки вопроса - более значительными, чем сегодня. С его абсолютно ограниченным предложением 21 миллион биткоинов представляет собой приятный контраст с бесконечно растущими балансами центральных банков. Его ограниченное предложение обеспечивает защиту от

размывания собственного капитала, как это происходило со всеми валютами мира в последние десятилетия.

Благодаря своей специфической конструкции биткоин должен обеспечивать сохранение покупательной способности в течение длительных периодов времени. Поскольку биткоин абсолютно дефицитен, он должен справляться с этой задачей даже лучше, чем золото, приток которого составляет 1-2% каждый год. Кроме того, затраты на хранение и транспортировку биткоина также значительно ниже по сравнению с золотом, что также позволяет лучше сохранять стоимость.

Защита собственности

Еще одна проблема, которую облегчает биткойн, - это защита собственности. В то время как золото или наличные деньги обычно приходится надежно хранить с большими затратами, чтобы защитить их от кражи, биткойн можно хранить и перевозить практически без затрат. Даже значительные суммы могут быть доставлены в любую точку мира с помощью кода, состоящего из двенадцати или двадцати четырех слов. После запоминания и физического уничтожения этот код не может быть украден никем, а значит, активы, стоящие за кодом, находятся в абсолютной безопасности и при желании могут быть унесены их владельцем в могилу.

КУПИТЬ БИТКОИН

В основном существует два способа завладеть биткоином. Либо вы становитесь майнером, либо покупаете биткоин у другого человека. Поскольку в настоящее время майнинг с помощью домашних устройств стал практически невозможен, у новичков остается только один путь - покупка.

Криптовалютные биржи

Самый простой способ купить биткоин - через торговую биржу. Они работают аналогично платформам для торговли акциями. После открытия личного счета швейцарские франки, евро или доллары США можно перевести банковским переводом или кредитной картой. После того как деньги поступили на личный счет на торговой бирже, Bitcoin можно купить несколькими щелчками мыши

Peer-to-peer

В качестве альтернативы криптовалютным биржам биткоин

также можно приобрести непосредственно у других участников рынка без участия биржи через платформы peer-to-peer. Это позволяет обеспечить большую анонимность, поскольку для такой сделки не нужно предоставлять личные данные.

Биткойн-банкоматы

Существует также возможность снятия биткойнов через банкоматы. Они уже доступны во многих странах, включая Швейцарию, Германию и Австрию. В биткойн-банкоматах биткойн можно анонимно снять наличными или кредитной картой. При этом не требуется ни счет, ни существующий криптокошелек.

Безопасное хранение биткоина

После приобретения биткойнов встает вопрос об их безопасном обращении и хранении. Биткойн и криптовалюты подчиняются принципу: „не твои ключи, не твои монеты“. Чтобы действительно владеть биткоином, вы должны обладать соответствующими

закрытыми ключами. Это несколько техническое выражение означает, что вы действительно имеете контроль над своими Bitcoin, если вы храните их в личном цифровом кошельке, к которому у вас есть закрытые ключи.

Пока биткойны хранятся на криптовалютной бирже, они находятся под контролем биржи. Если биржа будет взломана, обанкротится или окажется мошеннической, биткойны могут быть потеряны навсегда “.

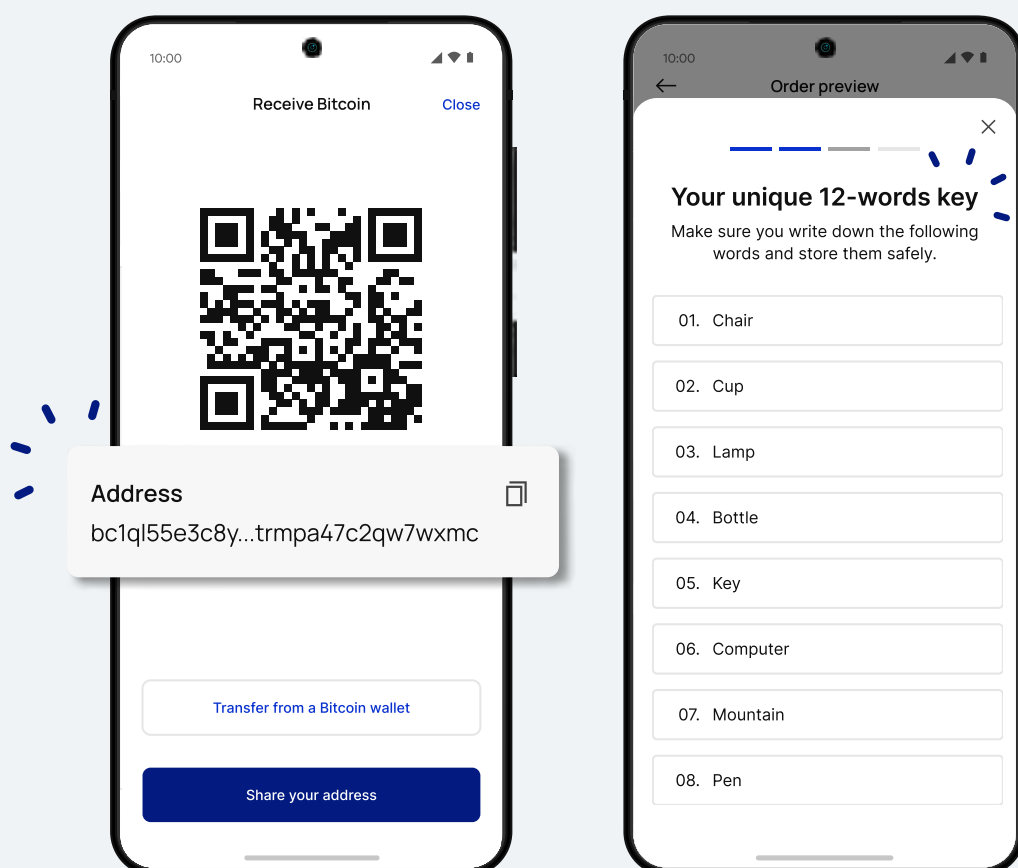
Биткоин-банкоматы

В отличие от банковского счета, с

биткойном у вас есть возможность хранить свои денежные единицы на личном кошельке. Это позволяет вам быть своим собственным банком. Преимущество этого способа заключается в том, что вы имеете абсолютный контроль над своим Bitcoin. И наоборот, это также влечет за собой личную ответственность. Закрытый ключ, который часто бывает в виде двенадцати или двадцати четырех слов, должен хранить сам владелец соответствующего биткойна. Неправильное или небрежное обращение может привести к безвозвратной потере биткойна.

Кошельки: цифровые кошельки

Кошельки, то есть цифровые



кошельки, помогают надежно хранить Bitcoin, а точнее, закрытые ключи. Сами биткойны всегда находятся в блокчейне и не могут быть переведены в кошелек. В кошельке могут храниться только ключи доступа к биткоину.

Поэтому были созданы кошельки для безопасного и удобного хранения закрытых ключей. Они также позволяют отправлять и получать Bitcoin с помощью всего нескольких щелчков мыши. Таким образом, кошельки являются полезным инструментом для работы с Bitcoin.

Программный кошелек

Наиболее распространенными кошельками являются программные кошельки. Программные кошельки могут быть установлены как настольные приложения или как приложение для смартфонов. При настройке закрытые ключи к кошельку перечисляются в виде двенадцати или двадцати четырех слов. Эти слова являются синонимом биткойна в этом кошельке. Тот, кто знает эти слова, обладает властью распоряжаться монетами. Поэтому слова должны быть записаны в аналоговой форме, предпочтительно на бумаге, в тайне и храниться в безопасности. Если мобильный телефон потерян, кошелек можно восстановить в любое время с помощью этих слов.

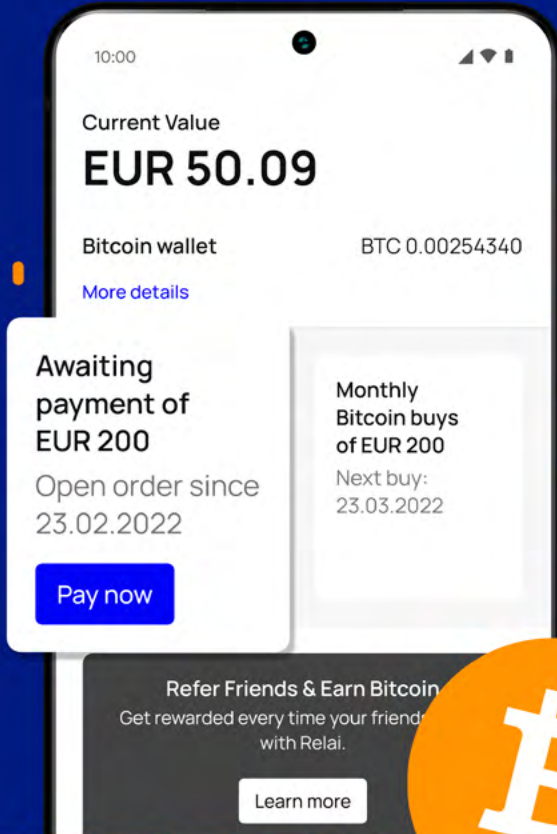
Преимущество программных кошельков заключается в том, что их можно быстро настроить и они просты в использовании. Однако, поскольку программные кошельки устанавливаются на устройство в виде компьютерных программ и напрямую подключены к Интернету, всегда существует риск хакерских атак.

Аппаратный кошелек

Если вы цените максимальную безопасность, вам следует использовать аппаратный кошелек. Эти небольшие устройства хранят коды доступа к биткоину на USB-накопителе, который подключается к компьютеру только при необходимости. Устройство сконструировано таким образом, что даже компьютер, зараженный вредоносным программным обеспечением, не может получить доступ к кодам.

При настройке этих устройств также указываются двенадцать или двадцать четыре слова, которые необходимо записать по аналогии и хранить в безопасности. Если аппаратный кошелек утерян, его можно восстановить с помощью слов. Примерами поставщиков аппаратных кошельков являются BitBox и Trezor.

 Made in Switzerland



EUROPE'S EASIEST BITCOIN APP



Received Bitcoin
24.09.2021

BTC 0.00254340
CHF 50.65

Relai



 Download on the
App Store

 GET IT ON
Google Play

Buy bitcoin in 1 minute from as little
as 10 EUR/CHF without verification.



Отправлять и получать Bitcoin

Отправка и получение Bitcoin - это детская забава. Каждый кошелек Bitcoin имеет свой публичный адрес, который генерируется на основе так называемого публичного ключа. Это служит адресом получения, аналогично номеру IBAN. Любой, у кого есть этот адрес, может отправить Bitcoin на соответствующий кошелек. Адрес часто также отображается в виде QR-кода, что упрощает работу с ним. Если вы хотите отправить кому-то биткоин, вы можете либо ввести биткоин-адрес получателя в поле „отправить“ в своем личном кошельке, либо отсканировать соответствующий QR-код. Понесенные комиссионные за транзакцию автоматически списываются с кошелька

отправителя. Размер комиссии за транзакцию зависит от загруженности сети и может быть уточнен здесь. Перевод доходит до получателя в среднем за 10 минут. Однако это может занять и больше времени, в зависимости от суммы комиссии за транзакцию, которую вы готовы заплатить.

Если вы хотите отправить кому-то биткоин, вы можете либо ввести биткоин-адрес получателя в поле „отправить“ в своем личном кошельке, либо отсканировать соответствующий QR-код. Понесенные комиссионные за транзакцию автоматически списываются с кошелька отправителя. Размер комиссии за транзакцию зависит от загруженности сети и может быть уточнен [здесь](#). Перевод доходит до

получателя в среднем за 10 минут. Однако это может занять и больше времени, в зависимости от суммы комиссии за транзакцию, которую вы готовы заплатить.

Оплата с помощью Bitcoin

Во время появления биткойна была надежда, что однажды биткойн можно будет использовать для оплаты повседневных вещей. И в принципе, это возможно уже сегодня. Отдельные налоговые службы, некоммерческие организации и компании принимают Bitcoin в качестве платежного средства. Но поскольку сегодня транзакции через сеть Bitcoin могут стоить несколько франков и занимать не менее 10 минут, это имеет смысл только для больших сумм. Поэтому для дешевой и быстрой отправки Bitcoin необходимо альтернативное решение.

Молниеносная сеть - быстрее и дешевле

Поэтому поверх сети Bitcoin была построена дополнительная сеть. Эта сеть, называемая Lightning, позволяет проводить платежи с помощью Bitcoin за считанные секунды при минимальных затратах. В таких странах, как Эль-Салавдор, сеть Lightning уже

активно и успешно используется. Поэтому в будущем оплата повседневных товаров с помощью Биткойна будет осуществляться в основном через сеть Lightning. Разработки в этой области также идут полным ходом. Например, Twitter недавно ввел функцию „чаевых“, которая также работает через сеть Lightning. Кроме того, приложение Strike предлагает платежи по всему миру в различных валютах по нулевой цене через сеть Lightning. Поэтому следует ожидать, что в будущем только крупные суммы будут рассчитываться непосредственно через сеть Биткойн, а все остальные транзакции будут проходить через сеть Lightning.

Поскольку в сети Lightning часто пересылаются меньшие суммы, в качестве единицы измерения используется не биткойн, а сатоши, или сокращенно саты. 1 биткойн равен 100 000 000 сатов. Для использования сети Lightning необходимо создать кошелек Lightning.

ВЗГЛЯД В БУДУЩЕЕ

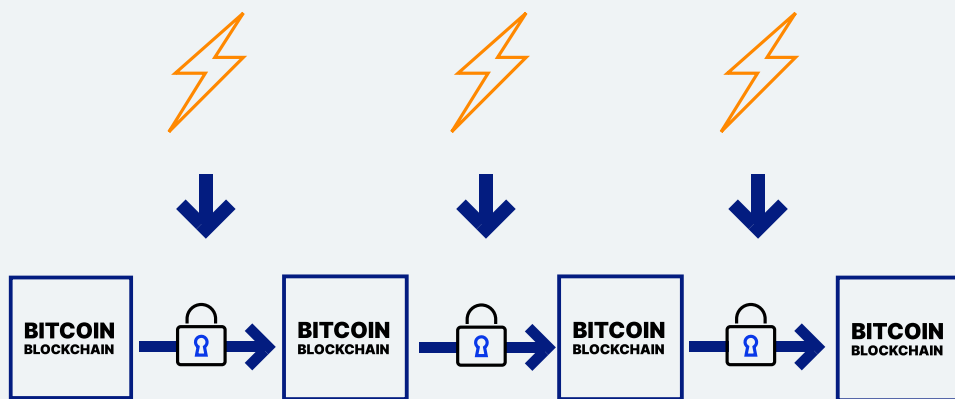
За более чем десять лет своего существования биткойн многое пережил и перетерпел. Несколько раз цифровая валюта объявлялась мертвой или забывалась широкой публикой после сильных ценовых потерь. Но биткойн неумолимо распространяется по всему миру.

Биткойн и энергетика

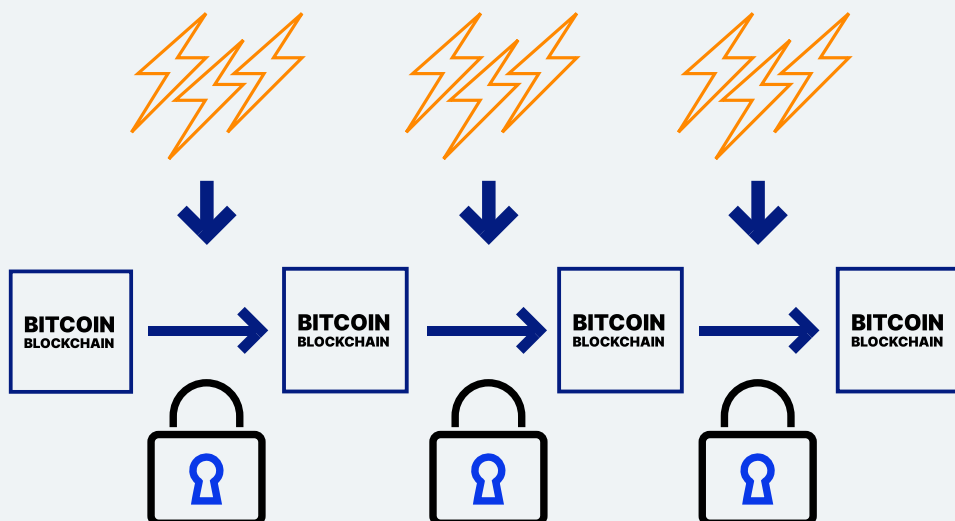
Один из первых вопросов,

который всегда поднимается в связи с развитием Биткойна, - это энергопотребление сети Биткойна. Майнинг биткойна уже потребляет большое количество электроэнергии во всем мире. И это потребление, вероятно, будет расти в будущем по мере того, как все больше людей будут заниматься майнингом биткойна.

Чем меньше энергии в виде вычислительных мощностей используется для создания блокчейна Биткойна, тем легче его потом изменить.



Чем больше энергии в виде вычислительной мощности используется для создания блокчейна Биткойна, тем сложнее его потом изменить.



Важно понимать, что количество энергии, поступающей в сеть Bitcoin, имеет решающее значение для безопасности сети. Чем больше энергии поступает в сеть, тем она надежнее. Это связано с тем, что для последующего изменения блокчейна Bitcoin необходимо использовать то же количество вычислительной мощности - а значит, и энергии, - которое уже было вложено в создание блокчейна. Но поскольку миллионы компьютеров по всему миру обеспечивают вычислительную мощность сети Bitcoin, практически невозможно, чтобы отдельный

человек, организация или государство когда-либо собрали достаточно вычислительной мощности для внесения даже самых незначительных изменений в блокчейн. Поэтому хэш-мощность и связанное с ней потребление энергии является важной характеристикой безопасности сети Bitcoin.

Кроме того, преимущество компьютеров для майнинга биткоинов заключается в том, что они могут находиться в любой точке мира. Поскольку шахтерам для получения прибыли требуется

как можно более дешёвая электроэнергия, они часто размещаются в местах, где много избыточной и, следовательно, дешёвой энергии. В долгосрочной перспективе это, скорее всего, будет особенно заметно там, где много возобновляемых источников энергии, поскольку они производят самую дешёвую электроэнергию.

По данным Совета по майнингу биткоина, в настоящее время майнеры биткоина используют около 56 % возобновляемой энергии, и эта тенденция растёт. Многие эксперты по биткоину считают, что в будущем майнинг биткоина будет осуществляться с использованием до 100% возобновляемой энергии.

Однако до тех пор, пока это не произойдёт, потребление энергии биткойном сводится к вопросу о том, стоят ли безопасные и не подделываемые деньги и хранилище стоимости таких затрат энергии - или нет.

Сальвадор - биткоин в качестве национальной валюты

Уже несколько лет назад провидцы считали возможным, что биткойн однажды будет признан национальными государствами в качестве законного платёжного средства. Летом 2021 года пришло время: Сальвадор стал первой страной в мире, которая

ввела биткоин в качестве законного платёжного средства. В магазинах, ресторанах и у поставщиков услуг всех видов теперь можно расплачиваться не только долларами США, но и биткойнами. Для этого жителям был предоставлен кошелек Bitcoin, который позволяет проводить платежи через сеть Lightning в считанные секунды и с минимальными затратами.

Другие страны, такие как Украина, Бразилия и Панама, в настоящее время обсуждают подобные законопроекты. Если другие страны последуют примеру Сальвадора, это, с одной стороны, ещё больше увеличит спрос на биткоин, а с другой стороны, прежде всего, подкрепит доверие к нему как к „деньгам“. Поэтому принятие биткоина в качестве законного платёжного средства во все большем количестве стран является важнейшим этапом в процессе глобальной адаптации биткоина.

Законы и нормативные акты

Это означает, что государства, центральные банки и компании вынуждены интенсивно работать с криптовалютами. Различные государства, в том числе Швейцария, выпустили первые нормативные акты и руководства, касающиеся криптовалют. Этот шаг приветствуется многими

участниками рынка, поскольку он создает правовую определенность как для криптопроектов, так и для вовлеченных в них компаний.

В США, которые до сих пор придерживались довольно экономически либерального подхода, также на горизонте появляются нормативные акты. За тем, какую именно форму они примут, внимательно следит мировое криптосообщество, поскольку они окажут серьезное влияние на весь криптосектор.

Другие криптовалюты

Биткойн - далеко не единственная криптовалюта в наши дни. В настоящее время существует более 16 000 различных криптовалют и ценностей. Все эти валюты имеют различные характеристики и способы функционирования, и не все они долгое время воспринимались как „валюты“ или деньги. Некоторые из них больше похожи на акции, поскольку их стоимость отражает успех криптопроекта. Другие необходимы для использования определенной услуги. А другие - так называемые „токены мемов“ - являются в первую очередь веселыми валютами.

Поэтому, чтобы избежать потерь, рекомендуется внимательно изучить соответствующую валюту и стоящий за ней проект, прежде

чем делать какие-либо инвестиции.

Цифровые валюты центрального банка (CBDC)

Криптовалюты находятся на этапе перехода от первоначальной нерегулируемой фазы Дикого Запада к регулируемому, более упорядоченному криптофинансовому миру. Такое развитие событий не оставило центральные банки в стороне, и появились идеи о том, что центральные банки должны выпускать собственные криптовалюты. Эти „цифровые валюты Центрального банка“, или сокращенно CBDC, по мнению сторонников, будут сочетать в себе стабильность государственной валюты с преимуществами валюты на основе блокчейна. Короче говоря, они создадут, так сказать, цифровую наличность.

Однако, в зависимости от конструкции, CBDC может иметь принципиально разные характеристики.

В разных странах начались пилотные испытания различных типов CBDC, а в нескольких странах CBDC уже запущены. Однако с нетерпением ожидается, запустят ли свои CBDC и в какой форме экономически сильные валютные зоны, такие как США, ЕС или Китай.

Денежная конкуренция

За последние десятилетия наше общество настолько привыкло к государственным валютам, что другие виды денег для многих до недавнего времени были немыслимы. Но не так давно параллельное обращение различных видов денег было частью повседневной жизни. Существовали банкноты различных банков, монеты из различных драгоценных металлов и другие денежные ценности, которые можно было использовать в качестве платежных средств.

С появлением биткойна негосударственные валюты вновь стали доступной альтернативой. До сих пор большинство правительств относились к ней терпимо, в том числе благодаря ее децентрализации, что делает эту валюту трудно атакуемой. Для граждан это означает, что помимо золота и серебра теперь доступна цифровая альтернатива государственным деньгам. Влияние этой дополнительной денежной конкуренции будет интересно наблюдать в будущем.

БИТКОЙН, ЧТО ТЕПЕРЬ?

Если вы задаетесь вопросом, что делать со всей этой информацией, позвольте мне сделать предложение. Вход в мир биткойна практически ничего не стоит - ни времени, ни денег. Но вы познакомитесь с технологией, которая вот-вот изменит наш мир и его будущее.

Поэтому: загрузите кошелек на свой мобильный телефон и купите Bitcoin один раз за 50 CHF. Или попросите коллегу отправить вам Bitcoin на ваш личный кошелек. Но

хотя бы раз вступайте в контакт с Bitcoin. После этого вам больше никогда не придется прикасаться к кошельку, обещаю.

Потому что если биткойн совершит прорыв и станет таким же вездесущим, как интернет, после этой брошюры вы будете не только теоретически знать о нем, но и сами использовать биткойн. Эти практические знания помогут вам быстрее сориентироваться в новом мире цифровых валют.

О САЙТЕ ОБ АВТОРЕ

Даниэль Юнген - экономист и финансовый журналист, специализирующийся на криптоактивах. Даниэль является соучредителем InsightDeFi, исследовательского бутика, специализирующегося на вопросах криптовалют. Вместе со

своими партнерами из InsightDeFi он каждые две недели публикует немецкий информационный бюллетень InsightDeFi, в котором предлагает читателям ознакомиться с актуальными темами, связанными с биткоином, DeFi и криптовалютами.

RELAI

Компания Relai была основана Джулианом Линигером и Адемом Биликаном в Швейцарии, поскольку два основателя испытывали трудности с поиском безопасного и простого места для покупки биткоина. Благодаря Relai, сбережение и инвестирование в биткоин теперь доступно каждому. Приложение Bitcoin разработано простым и интуитивно понятным, позволяя любому человеку в Европе покупать и продавать

Bitcoin в течение нескольких минут, без необходимости регистрации, верификации или банковского перевода. Независимо проверенная и уже инвестировавшая через платформу более 35 миллионов швейцарских франков в биткоинах, Relai предлагает клиентам возможность изучить новые способы сбережения и инвестирования.

Узнайте больше на сайте [Relai.app](https://relai.app).

Спасибо @[Bitcoinbleibt](https://twitter.com/Bitcoinbleibt) за перевод этой электронной книги с английского на русский язык