Биткойн

кто такой
с какого района

Что такое Биткойн?

Биткойн – это первая в истории человечества децентрализованная платёжная система.

По совместительству – ещё и валюта. Но это скорее побочный эффект.

Чем биткойны удобнее обычных денег?

Вы много знаете способов перевести 160 миллионов долларов из произвольной точки Земли в произвольную точку Земли за 10 минут без комиссии?

Вы много знаете способов перевести друг другу средства, при которых вас не попросят предъявить паспорт? При которых об этом вообще никто не узнает, кроме вас двоих?

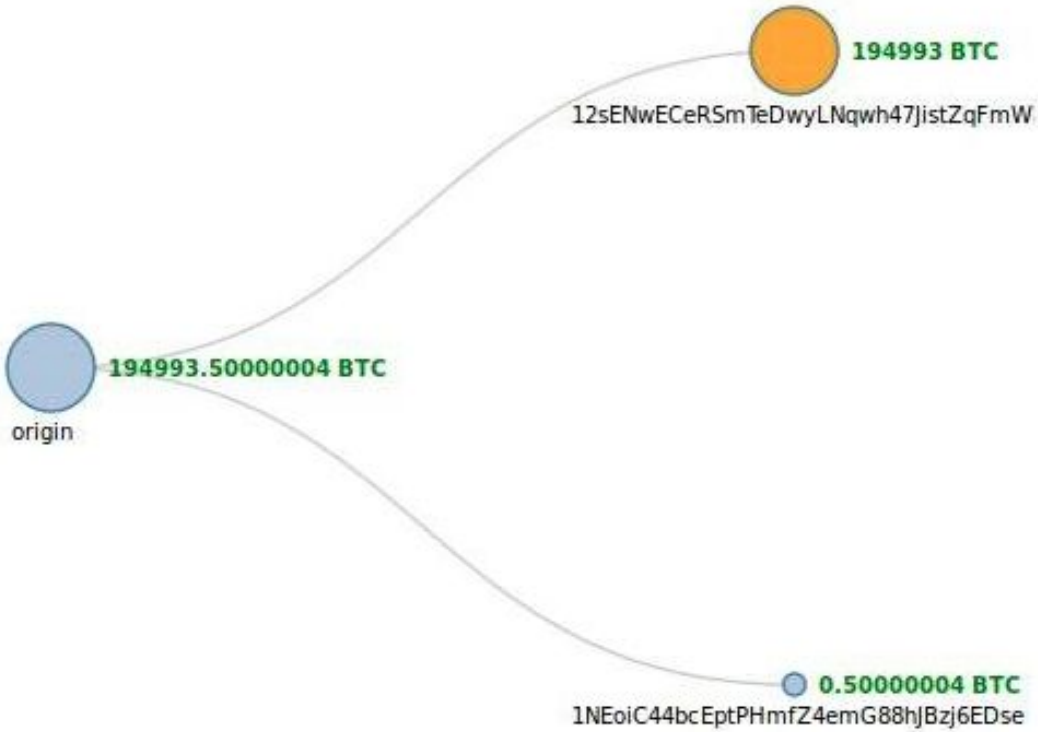
23 ноября 2013 в 18:31

Кто-то осуществил транзакцию биткоинов на $160 млн

Платежные системы*

Bitcoin-адрес с историей крупных транзакций прошлой ночью осуществил ещё один перевод на рекордную сумму 194 993 BTC, что составляет чуть более $160 млн в эквиваленте по текущему курсу.

Что характерно, владелец этой суммы заплатил **0 BTC** комиссионных за перевод. Только представьте, какова была бы комиссия при международном переводе 160 миллионов долларов через банковскую систему.



На сегодняшний день это самая крупная транзакция в сети Bitcoin.

Чем биткойны удобнее платёжных систем?

Чему равна комиссия в сети Биткойн?

Либо 0 BTC, либо 0.0001 BTC.

В переводе на российские реалии: либо 0 рублей, либо примерно 3 рубля.

Чем больше сумма перевода и чем более давно с этой суммой ничего не происходило, тем выше вероятность того, что комиссия составит 0 рублей.

Зачем нужна комиссия? И кому достаётся?

Комиссия нужна для того, чтобы мы с вами не хулиганили: чтобы, гоняя одни и те же монеты по кругу, не забивали сеть.

Достаётся она майнерам.
Майнеры – это те, кто занимается майнингом. Каждый может стать майнером.

Немного забегая вперёд, скажу, что доход майнера с найденного блока составляет 25 BTC + комиссии всех транзакций, попавших в этот блок.

И что, раньше электронных денег не существовало, что ли?

Децентрализованных электронных денег не существовало.

Как так? Интернет же существует столько лет!

Концепция децентрализованной цифровой валюты, а также альтернативных приложений, таких как реестры собственности, витала в воздухе десятилетиями. Протоколы "электронного кэша" 80-х и 90-х, по большей части опиравшиеся на широко известное в криптографии понятие слепой подписи (Chaumian blinding), предлагали валюту высокой степени анонимности – но не получили никакого распространения, так как принципиально зависели от централизованного посредника.

Как так? Интернет же существует столько лет!

Первым, кто предложил что-то подобное, был Wei Dai (1998).

Его концепция называлась b-money и в ней говорилось как про идею децентрализованного соглашения между участниками, так и про идею создания денег посредством решения вычислительных задач.

Однако он не привёл никаких деталей, а ограничился общими словами.

Как так? Интернет же существует столько лет!

Следующим был Hal Finney (2005).

Он предложил криптовалюту с концепцией RPOW (reusable proofs-of-work), которая использует идеи b-money вместе с Hashcash (прототипом proof-of-work системы Биткойн) – к сожалению, его идея также включала в себя посредника, которому пользователи должны были доверять.

Как так? Интернет же существует столько лет!

Люди, которые решали эту задачу до Биткойн, опирались на разные вариации задачи византийских генералов.

Задача византийских генералов

Византия. Ночь перед великим сражением с противником. Византийская армия состоит из легионов, каждым из которых командует свой генерал. Также у армии есть главнокомандующий, которому подчиняются генералы.

В то же самое время, империя находится в упадке, и любой из генералов и даже главнокомандующий могут быть предателями Византии, заинтересованными в её поражении.

Ночью каждый из генералов получает от предводителя приказ о варианте действий в 10 часов утра (время одинаковое для всех и известно заранее), а именно: «атаковать противника» или «отступать».

Задача византийских генералов

Возможные исходы сражения:

- Если все генералы атакуют — Византия уничтожит противника (благоприятный исход).
- Если все генералы отступят — Византия сохранит свою армию (благоприятный исход).
- Если некоторые генералы атакуют, а некоторые отступят — противник уничтожит всю армию Византии (неблагоприятный исход).

Задача византийских генералов

Также следует учитывать, что если главнокомандующий — предатель, то он может дать разным генералам противоположные приказы, чтобы обеспечить уничтожение армии. Следовательно, генералам лучше не доверять его приказам.

Если же каждый генерал будет действовать полностью независимо от других (например, сделает случайный выбор), то вероятность благоприятного исхода весьма низка.

Поэтому генералы нуждаются в обмене информацией между собой, чтобы прийти к единому решению.

Атака Сивиллы :3

Люди, которые решали эту задачу до Биткойн, опирались на разные вариации задачи византийских генералов.

Комментируя вопросы безопасности, они делали утверждения вида "наша система с N участниками безопасна, если не более N/4 участников — злоумышленники".

Атака Сивиллы улыбается и машет таким валютам.

Об авторе

Автор системы Биткойн называл себя Satoshi Nakamoto.

Имя satoshi переводится с японского как «мудрый», фамилия nakamoto – как «находящийся внутри сложной (закрытой) системы»

О дате

Запущена система Биткойн была 3 января 2009 года, в мой день рожденья.

Получается, биткойны будут печататься бесконечно?

Почти.
Сейчас какой-то счастливчик раз в 10 минут добывает 25 BTC. Протокол устроен так, что «награда за нахождение блока» раз в 4 года уполовинивается.

Первые 4 года (янв 2009 – янв 2013) награда составляла 50 BTC.

Получается, биткойны будут печататься бесконечно?

Первые 4 года (янв 2009 – янв 2013) награда майнера-победителя составляла 50 BTC.
Сейчас (янв 2013 – янв 2017) она составляет 25 BTC. В январе 2017 она снова уполовинится и окажется равной 12,5 BTC.

Получается, биткойны будут печататься бесконечно?

В действительности всё не так, как на самом деле. Уполовинивание награды происходит не раз в 4 года, а спустя каждые 210000 блоков.

Это, однако, почти одно и то же (блоки добываются в среднем раз в 10 минут, а 4 года разделить на 10 минут равно 210384).

Кто умеет суммировать геометрическую прогрессию?

$$50 \cdot 210000 + 25 \cdot 210000 + 12{,}5 \cdot 210000 + \ldots$$

Правильно!

Да, детка!
Суммарно будет добыто 21 миллион биткойнов.
Больше добыто не будет. Протокол неизменяем.

21 миллион!

На самом деле и это не совсем правда. В Биткойн денежные единицы делятся до восьми знаков после запятой. Дальше – не делятся.

Например, 3,14159265 BTC – отличная сумма для хранения в своём биткойн-кошельке.

21 миллион!

Для нас это сейчас означает, что в 2136 году выплаты полностью прекратятся.

Округление идёт вниз.

Поэтому на самом деле выплачено будет 20999999.99511055 биткойнов.

На практике это не имеет никакого значения хотя бы потому, что люди постепенно теряют биткойны.

И как тогда мотивировать людей продолжать заниматься майнингом?

Доход майнера = награда за нахождение блока + комиссии всех транзакций в блоке

9e638a289aef89ad7f2a710e82d60ca595738a4e2a3aa589bad40fbe5c3860e8 mined Feb 21, 2016 2:25:33 PM

No Inputs (Newly Generated Coins) → 1KFHE7w8BhaENAswwryaoccDb6qcT6DbYY 25.40668947 BTC (U)

1 CONFIRMATIONS 25.40668947 BTC

66e35114a51b51bdf604fe5e4aac06d4ffd4bff51948aad1dadc0734bb66c0c7 mined Feb 21, 2016 2:07:53 PM

No Inputs (Newly Generated Coins) → 1KM7w12SkjzJ1FYV2g1UCMzHjv3pkMgkEb 25.28137747 BTC (U)

1 CONFIRMATIONS 25.28137747 BTC

b7b21f8f661db8316d035c4ca3277327ceabea588031d98db03a01fb0962c1f7 mined Feb 21, 2016 2:00:14 PM

No Inputs (Newly Generated Coins) → 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE 25.20127458 BTC (U)

2 CONFIRMATIONS 25.20127458 BTC

97a49fa1e3180f12cf43ef1b97347488ef8823dcc12aad7af4e4fc7841d43bc5 mined Feb 21, 2016 1:53:30 PM

No Inputs (Newly Generated Coins) → 12i6Y6TZsmbFPJiQr6UXqTqmkL5j2FCXD3 25.05124169 BTC (U)

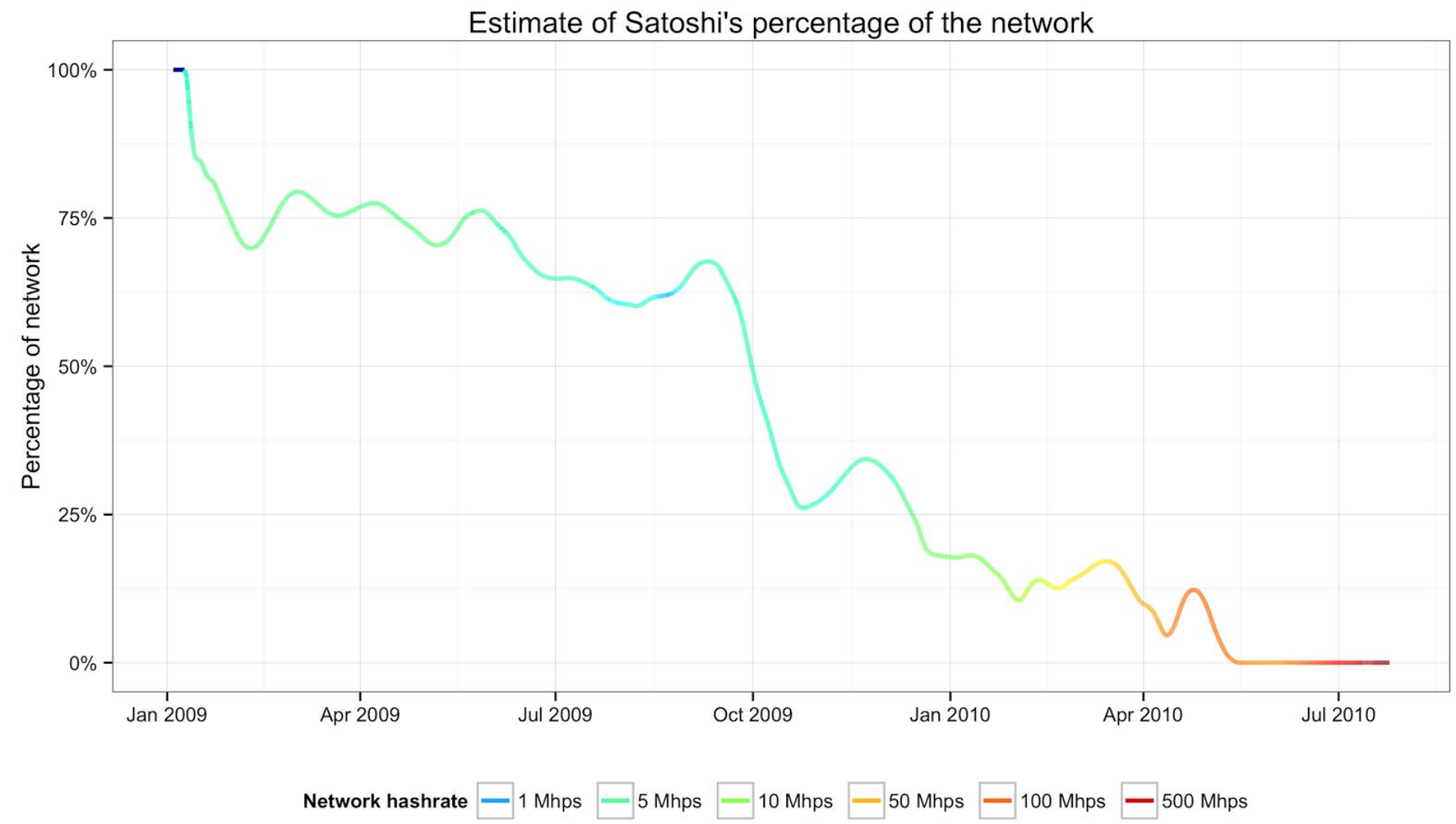
3 CONFIRMATIONS 25.05124169 BTC

О раннем майнинге

Принято считать, что Сатоши контролирует 988000 биткойнов.

По текущему курсу это свыше 400 миллионов долларов. Блокчейн абсолютно прозрачен, так что каждый может проверить – эти деньги, будучи добыты, ни разу никуда не перемещались.

Забавно, что в знак благодарности люди переслали ему 16 биткойнов.


Estimate of Satoshi's percentage of the network
Percentage of network
100%
75%
50%
25%
0%
Jan 2009
Apr 2009
Jul 2009
Oct 2009
Jan 2010
Apr 2010
Jul 2010
Network hashrate
1 Mhps
5 Mhps
10 Mhps
50 Mhps
100 Mhps
500 Mhps

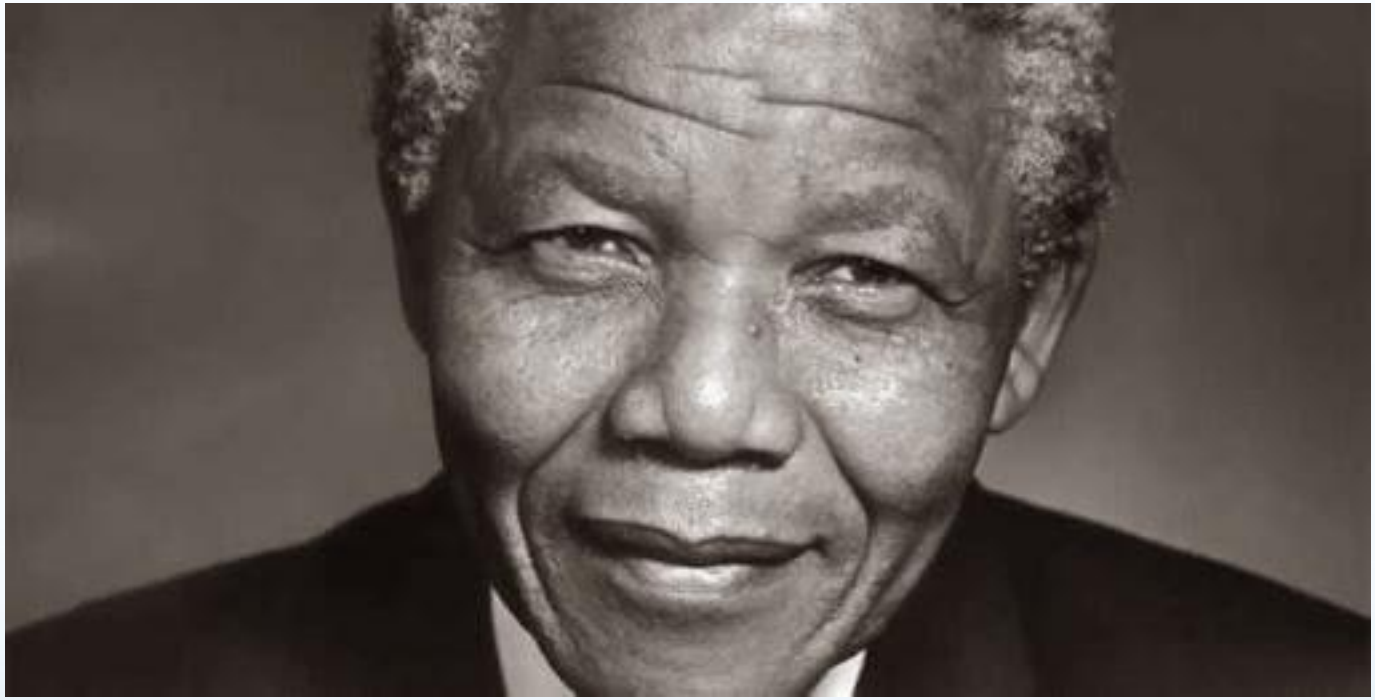
На каких сайтах всё это смотреть?

blockchain.info

blockexplorer.com

bitinfocharts.com

Приколы, которые содержит блокчейн



(+длинный список цитат Нельсона Манделы)

Приколы, которые содержит блокчейн

Хранится всё это в блокчейне в виде адресов, которые складываются в 16-ричные строки. На картинке ниже – кусок одной из транзакций, хранящей в себе эту штуку с Нельсоном Манделой. В этой транзакции незначительные биткойн-суммы пересылаются на несуществующие биткойн-адресы, такие как 15gHNr4TCKmhHDEG31L2XFNvpnEcnPSQvd

Приколы, которые содержит блокчейн

Этот адрес хранится в блокчейне в виде 16-ричного числа 334E656C736F6E2D4D616E64656C612E6A70673F.

Если теперь сконвертировать это число в Юникод, получится строка 3Nelson-Mandela.jpg?, означающая имя файла. Так же закодировано и само изображение. Таким образом, текст, картинки, и другой контент могут быть размещены в блокчейне Биткойн с помощью подходящих фейковых биткойн-адресов.

Genesis block содержит секретное сообщение

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

- Принято считать, что это доказательство того, что genesis block был создан 3 января 2009 года или позже; также это может означать скептическое отношение Сатоши к банковской системе. Кроме того, люди воспринимают это как свидетельство того, что Сатоши жил в Англии.
- Газета с этим заголовком стала коллекционной редкостью.

The raw hex version of the Genesis block looks like:

```
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   ....;£íýz{.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..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
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   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

Приколы, которые содержит блокчейн

Майнер Eligius начал добавлять католические молитвы в добытые им блоки. Примеры:

Benedictus Sanguis eius pretiosissimus. Benedictus Iesus in sanctissimo altaris Sacramento. Ave Maria, gratia plena, Dominus tecum. Benedicta tu in mulieribus, … ...and life everlasting, through the merits of Jesus Christ, my Lord and Redeemer. O Heart of Jesus, burning with love for us, inflame our hearts with love for Thee. Jesus, meek and humble of heart, make my heart like unto thine!

Приколы, которые содержит блокчейн

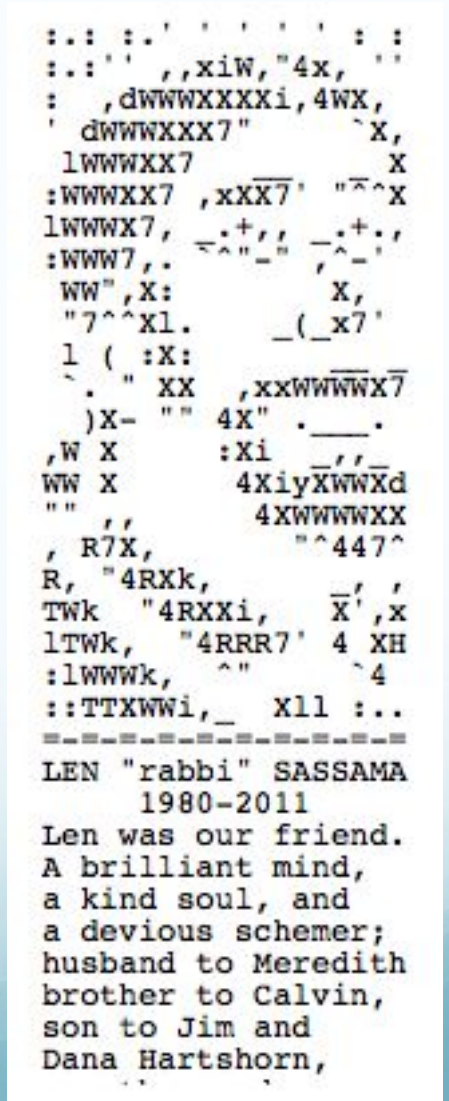
Другие майнеры начали возмущаться:

“Oh, and god isn't real, sucka. Stop polluting the blockchain with your nonsense.”, “FFS Luke-Jr leave the blockchain alone!”

В ответ они получили рикролл: “Militant atheists, http://bit.ly/naNhG2 -- happy now?”

Приколы, которые содержит блокчейн

Также там был обнаружен трибьют криптографу Len Sassaman



Приколы, которые содержит блокчейн

Кроме того, блокчейн содержит тексты Бхагавада Гиты, 1000 цифр числа Пи, стихотворения Шел Силверстайна, стихотворения Руми, файлы Викиликс, Python-код посвящённый добавлению информации в блокчейн и скачиванию её, два незаконных простых числа, три PGP-зашифрованных 86-килобайтных файла, огромное количество валентинок

Как устроена сеть Биткойн?

Самое главное – это блокчейн.

Самое главное – это блокчейн.

Самое главное – это блокчейн.

Что такое блокчейн?

Блокчейном называется большая бухгалтерская книга, в которой записаны все денежные переводы с самого начала существования сети. Понятно, что блокчейн непрерывно растёт.

Что такое блокчейн?

Блокчейн – это, как понятно из названия, цепочка блоков.

Таким образом, большая бухгалтерская книга выглядит как цепочка блоков.

Почему невозможна двойная трата монет?

Истинной (валидной) считается та цепочка, которая длиннее всех остальных. Совсем точно, истинна цепочка с наибольшей суммарной сложностью.

Денежные переводы, записанные во всех остальных цепочках, не имеют никакого значения.

Сложность и target

Самое главное, что нужно знать – что сложность вычислений подстраивается так, чтобы какой-то счастливчик «находил блок» раз в 10 минут.

Текущие значения target, diff и hashrate

Current hashrate = 1105 Phash/s

Current difficulty = 163491654908.95926

Current target = 00000000000000003f62e47ad7c42fc4f8e722e4decea3ae6a17d64844a5e91

График diff(t)

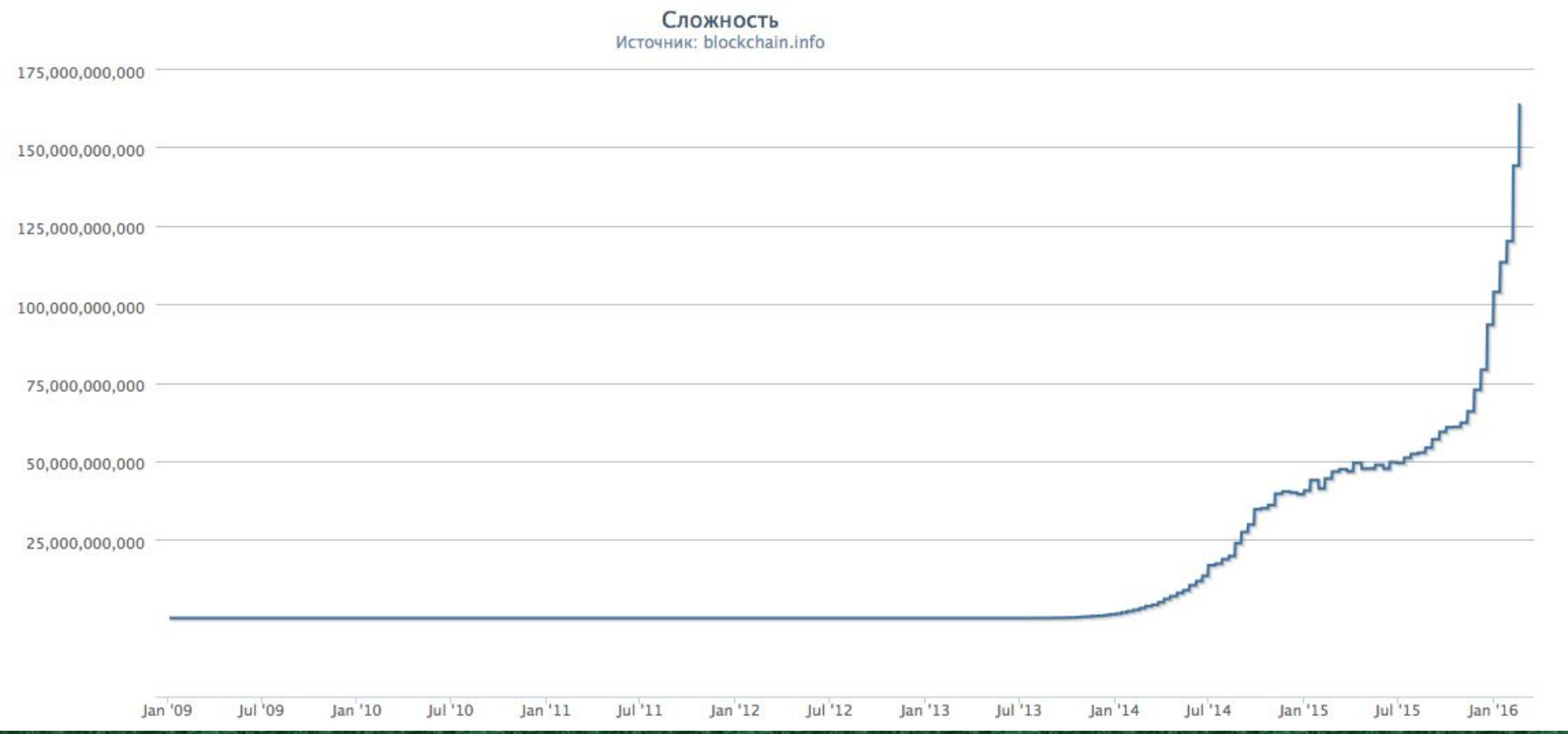
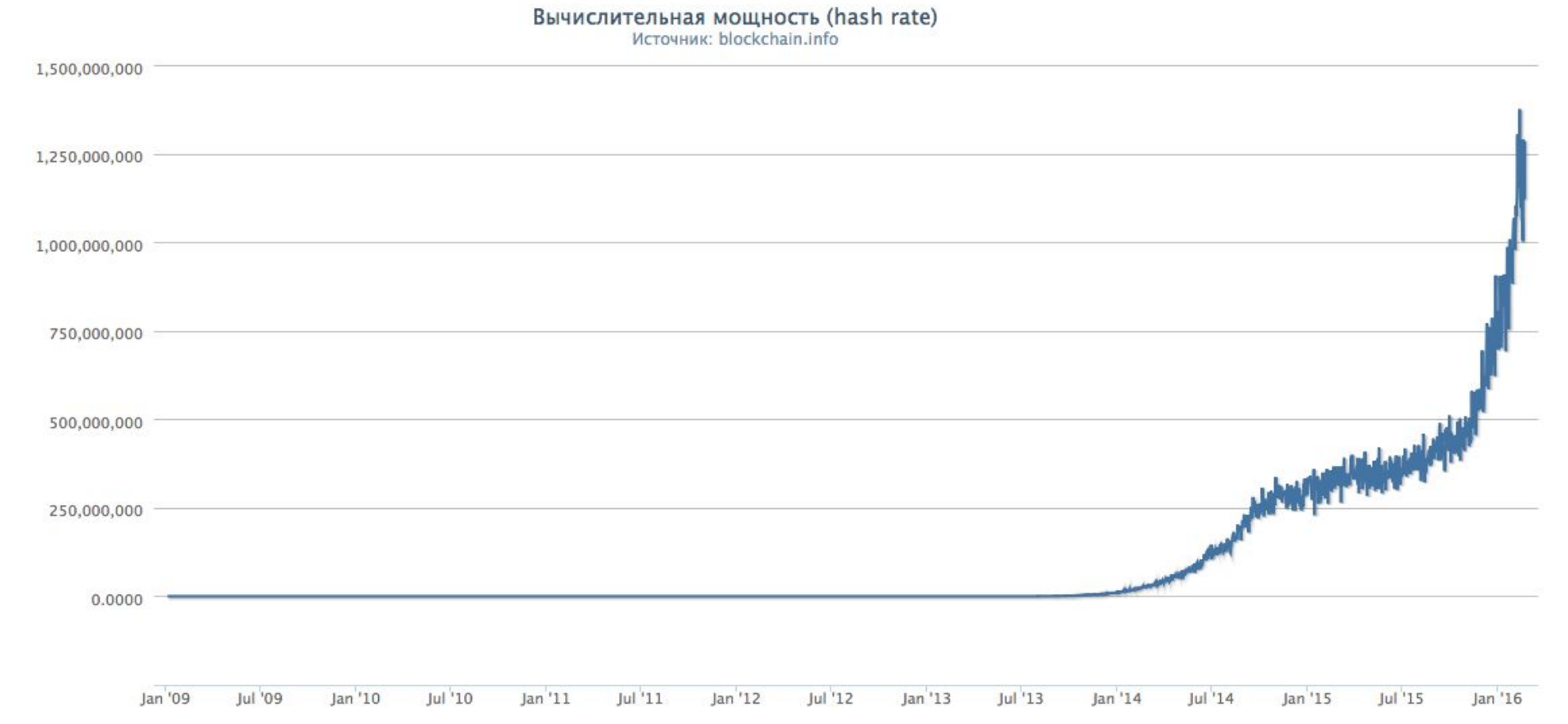


График hashrate(t)



Атака 51%

Но человек, который контролирует большую долю вычислительной мощности сети, может попробовать обогнать цепочку честных майнеров – сделать так, чтобы его нечестная была длиннее и воспринималась протоколом как честная.

Это называется атака 51%. Поговорим более детально об этой атаке.

Атака 51%

1. Переслать продавцу 100 BTC за некоторый продукт (лучше всего, цифровой)
2. Тут же молча начать майнить цепочку, в которой есть транзакция, переводящая эти 100 BTC на другой биткойн-кошелёк злоумышленника
3. Продавец ждёт z подтверждений и пересылает.
4. Обогнать честную цепочку блокчейна.

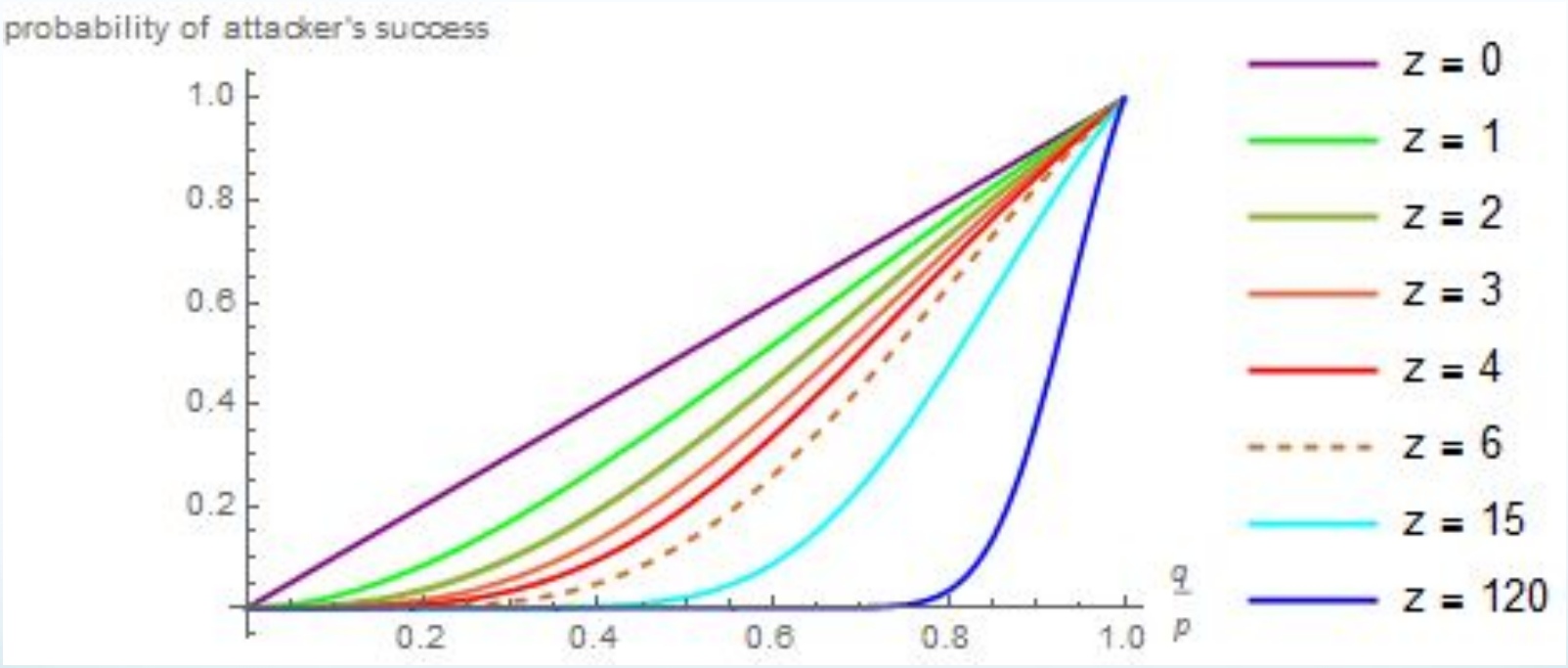
Как устроен обычный платёж?

1. Переводишь деньги с адреса 1KeatDCtrEnzaR42B2eUduYXmcM4U9jphB на адрес 1FTgzPJCbpCWYfF6VxPdmCMPUDBfygut2h
2. Продавец спустя некоторое время соглашается с тем, что платёж произошёл, и предоставляет тебе услугу. Принято дожидаться шести подтверждений.

Как устроен обычный платёж?

Каждый конкретный продавец решает сам, какого количества подтверждений ему ждать. Некоторые биржи считают биткойны зачисленными после трёх подтверждений.

Почему шесть подтверждений?



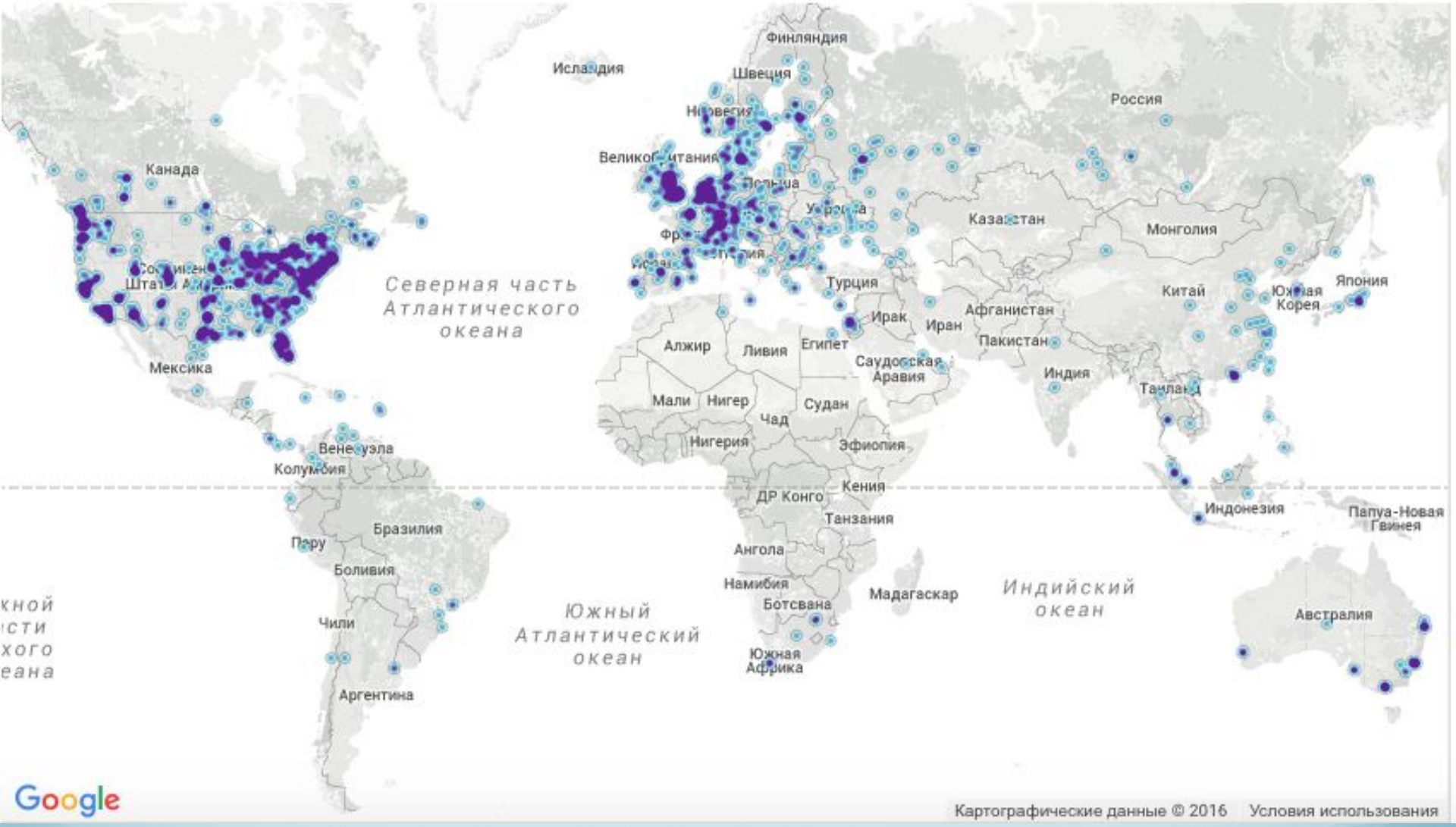
$$p_{\text{success}} = 1 - e^{-z\frac{q}{p}}\left(1 + z\frac{q}{p} + \frac{z^2}{2!}\left(\frac{q}{p}\right)^2 + \ldots + \frac{z^z}{z!}\left(\frac{q}{p}\right)^z - \left(\frac{q}{p}\right)^{z+1} - z\left(\frac{q}{p}\right)^{z+1} - \frac{z^2}{2!}\left(\frac{q}{p}\right)^{z+1} - \ldots - \frac{z^z}{z!}\left(\frac{q}{p}\right)^{z+1}\right)$$

Сколько всего людей держат полную ноду?

Веб-сайт bitnodes.21.co

сообщает нам, что на момент написания этой презентации активных полных нод было 6153.

То есть полная копия всего блокчейна хранится как минимум в 6153 местах на планете Земля.


Финляндия
Швеция
Россия
Канада
Казахстан
Монголия
Китай
Япония
Турция
Ирак
Иран
Афганистан
Пакистан
Индия
Египет
Ливия
Алжир
Мали
Нигер
Судан
Чад
Нигерия
Эфиопия
Кения
ДР Конго
Танзания
Ангола
Намибия
Ботсвана
Мадагаскар
Индонезия
Австралия
Мексика
Колумбия
Бразилия
Перу
Боливия
Чили
Аргентина
Северная часть Атлантического океана
Южный Атлантический океан
Индийский океан
Google
Картографические данные © 2016
Условия использования

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Fri Feb 19 2016 20:04:06 GMT+0300 (MSK).

6187 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2141 (34.60%)
2	Germany	803 (12.98%)
3	France	408 (6.59%)
4	Netherlands	357 (5.77%)
5	Canada	287 (4.64%)
6	United Kingdom	274 (4.43%)
7	Russian Federation	177 (2.86%)
8	Sweden	138 (2.23%)
9	China	120 (1.94%)
10	n/a	93 (1.50%)

Немного про хэш-функции

Хэш-функцией называется функция, берущая на вход строку произвольной длины и возвращающая строку фиксированной длины, удовлетворяющая трём свойствам:

- невозможность восстановить input (исходную строку, исходный файл) по output'у
- при незначительно отличающемся input'е совершенно разный output
- отсутствие коллизий

Немного про хэш-функции

К примеру, SHA3-хэш от "Saturday" даёт c38bbc8e93c09f6ed3fe39b5135da91ad1a99d397ef16948606cdcbd14929f9d

в то время как та же хэш-функция SHA3, взятая от "Caturday", приводит к результату b4013c0eed56d5a0b448b02ec1d10dd18c1b3832068fbbdc65b98fa9b14b6dbf

Output хэш-функции обычно используется как идентификатор того или иного документа и гарантирует то, что документ не был изменён или подделан.

Как устроен майнинг? (упрощённая версия)

Майнер перебором ищет такое число nonce (от английского «number used once»), что

$$hash(nonce) < target$$

Как устроен майнинг? (на самом деле)

Майнер перебором ищет такое число nonce (от английского «number used once»), что

sha256(sha256(version|hash_prev|merkle_root_hash|time stamp|bits|nonce)) < target

где | обозначает оператор конкатенации

То есть это вопрос удачи? То есть – либо 0 BTC, либо 25?

С точки зрения протокола сети – да. Однако майнеры года с 2010 стали объединяться в пулы – mining pools.

Это такие артели старателей, в которых важно не то, кто нашёл winning hash – а то, кто сколько вычислений в его поисках проделал.

Майнинг-пулы

Сейчас почти весь майнинг происходит на майнинг-пулах. Крупнейшие на данный момент – ghash.io, AntMiner, DiscusFish.

Ещё раз: пул «сглаживает» доход каждого майнера, который в этом пуле участвует, делает его равномерным.

Весь майнинг контролируют пулы? Как насчёт атаки 51%?

К примеру, пул ghash.io уже несколько раз на короткое время превышал величину 51%.

И они же собирали круглый стол. Им это невыгодно: доверие к сети падает, курс падает – а, как следствие, падает и суточный доход этих пулов.

Как бросить учёбу и начать добывать биткойны?

Это надо было делать раньше. В 2016 году майнинг – конкурентный бизнес.

Люди, которые решают заняться майнингом, накупают огромное количество специализированного оборудования, арендуют склад, следят за тем, чтобы не случилась перегрузка электросети.

Как бросить учёбу и начать добывать биткойны?

Или делают ботнет. :)

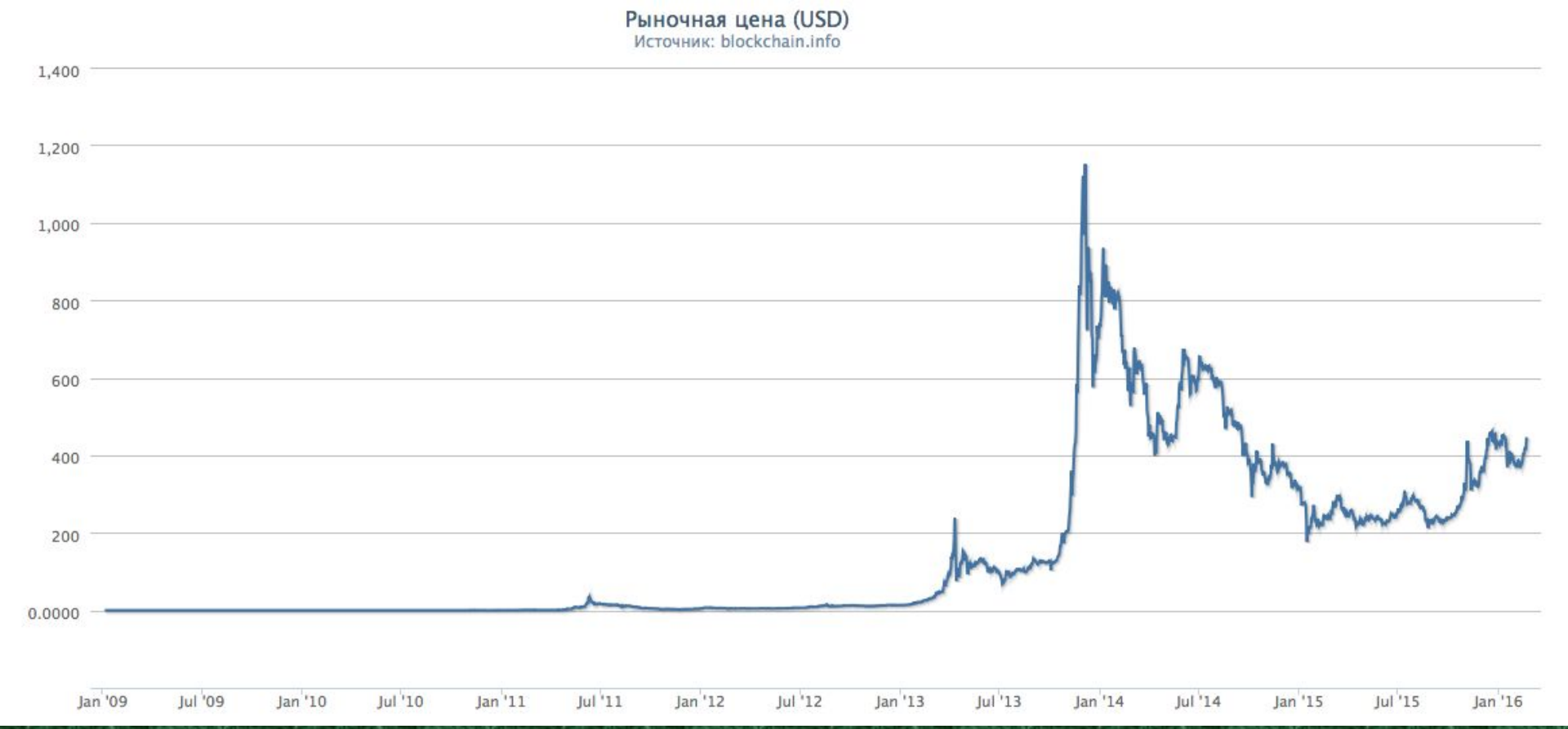
Если что, за создание ботнета предусмотрена уголовная ответственность.

Что ещё за АСИКи?

Application-specific integrating circuit (ASIC).

CPU → GPU → FPGA → ASIC

Динамика курса биткойна за всю историю



Мемасики!

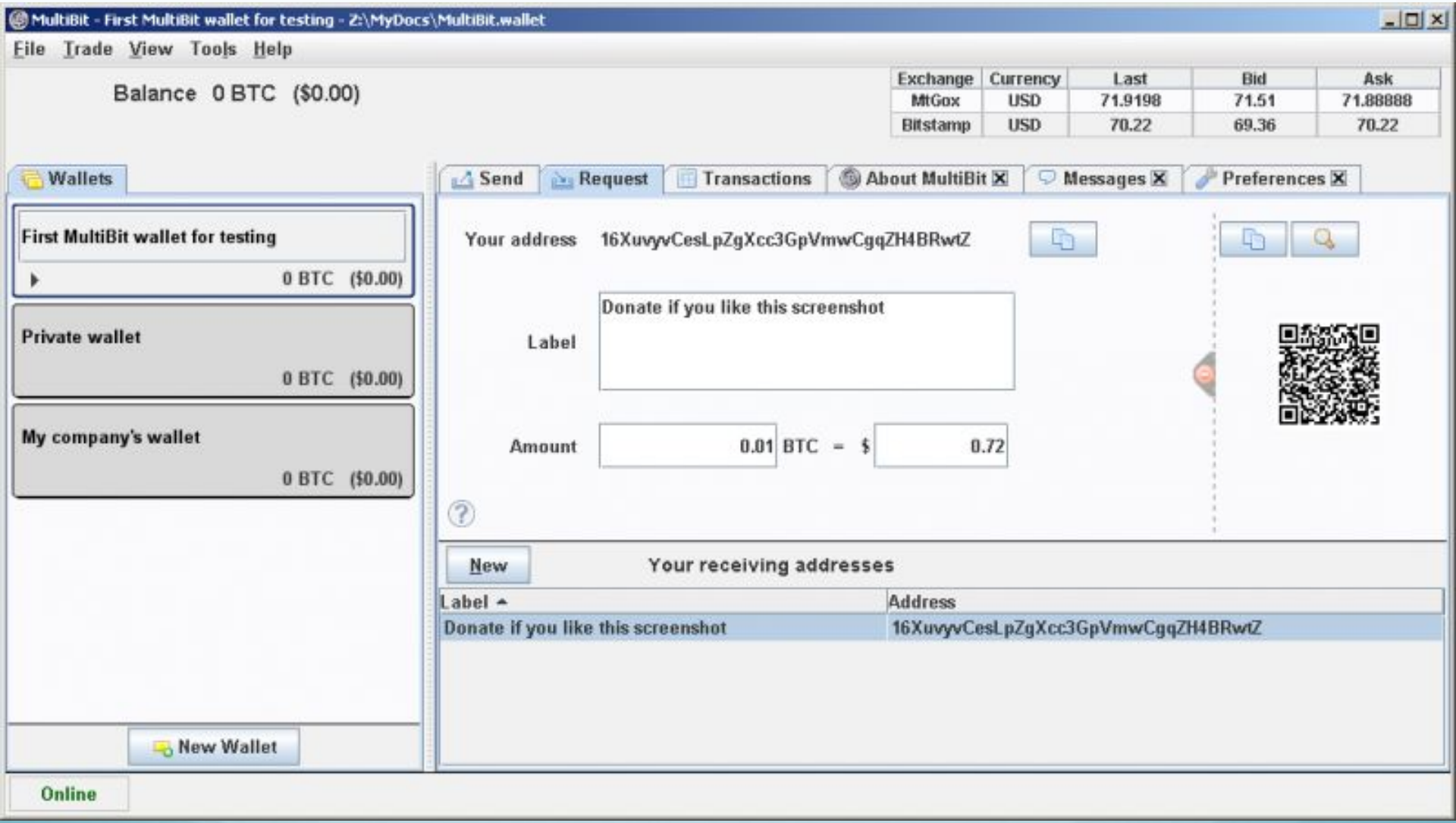
- Пицца стоимостью 12 миллионов долларов
- Писавший в 2009 курсач в универе по электронным валютам норвежский счастливчик
- Выброшенный на помойку жёсткий диск в Лондоне

Как завести биткойн-кошелёк?

Правильный способ: установить на свой компьютер официальный биткойн-клиент. Он загрузит на ваш компьютер весь блокчейн (56 Гб сейчас).

Другие способы: MultiBit, Electrum, Armory

Кошелёк MultiBit



Из чего состоит биткойн-кошелёк?

Наивно, он состоит из двух строк:

публичного ключа и *приватного ключа*

(public key, private key)

Публичный ключ, приватный ключ

Публичный ключ легко вычисляется по приватному.

Публичный ключ, грубо говоря, является хэшем приватного.

Это означает, что кража приватного ключа означает потерю денег.

Публичный ключ, приватный ключ

В то же время, подобрать приватный ключ с большой суммой денег невозможно за всё время жизни Вселенной. Вероятность ничтожно мала. Сейчас мы её подсчитаем.

Публичный ключ, приватный ключ

Хэш публичного ключа 160 бит.

Чтобы получить доступ ко всем биткойн-кошелькам, придётся перебрать 2^{160} пар ключей ($2^{160} \approx 1{,}46 \cdot 10^{48}$)

Теперь давайте поймём, сколько всего непустых адресов есть.

Balance	Addresses	% Addresses (Total)	Coins	$USD	% Coins (Total)
0 - 0.0001	3883164	51.16% (100%)	624.69 BTC	275,318 USD	0% (100%)
0.001 - 0.01	1162450	15.32% (48.84%)	4,173 BTC	1,839,328 USD	0.03% (100%)
0.01 - 0.1	1313660	17.31% (33.52%)	40,918 BTC	18,033,919 USD	0.27% (99.97%)
0.1 - 1	719960	9.49% (16.22%)	245,997 BTC	108,418,741 USD	1.61% (99.7%)
1 - 10	372102	4.9% (6.73%)	1,026,590 BTC	452,450,063 USD	6.7% (98.1%)
10 - 100	121771	1.6% (1.83%)	4,099,629 BTC	1,806,834,128 USD	26.77% (91.39%)
100 - 1,000	15308	0.2% (0.23%)	3,492,038 BTC	1,539,049,602 USD	22.8% (64.62%)
1,000 - 10,000	1703	0.02% (0.02%)	3,363,454 BTC	1,482,378,801 USD	21.96% (41.82%)
10,000 - 100,000	104	0% (0%)	2,617,061 BTC	1,153,420,055 USD	17.09% (19.86%)
100,000 - 1,000,000	3	0% (0%)	424,807 BTC	187,225,719 USD	2.77% (2.77%)

Как видно, их число не превышает $8 \cdot 10^6$

Давайте отрядим на это самый крутой суперкомпьютер мира – китайский Tianhe-2 с мощностью 33,86 petaFLOPS.

Этот компьютер – а вернее, кластер из 16000 машин – составляет 3120000 процессорных ядер.

Будем генерировать 100 пар ключей в секунду на одном ядре – то есть, всего будем генерировать 312 миллионов пар ключей в секунду.

Даже нет, давайте заставим все вычислительные мощности, занятые в биткойн-майнинге, заниматься этим. Вычислительная мощность сети Биткойн сейчас 14788703.98 petaFLOPS, что в 436760 раз больше этого вашего китайского суперкомпьютера.

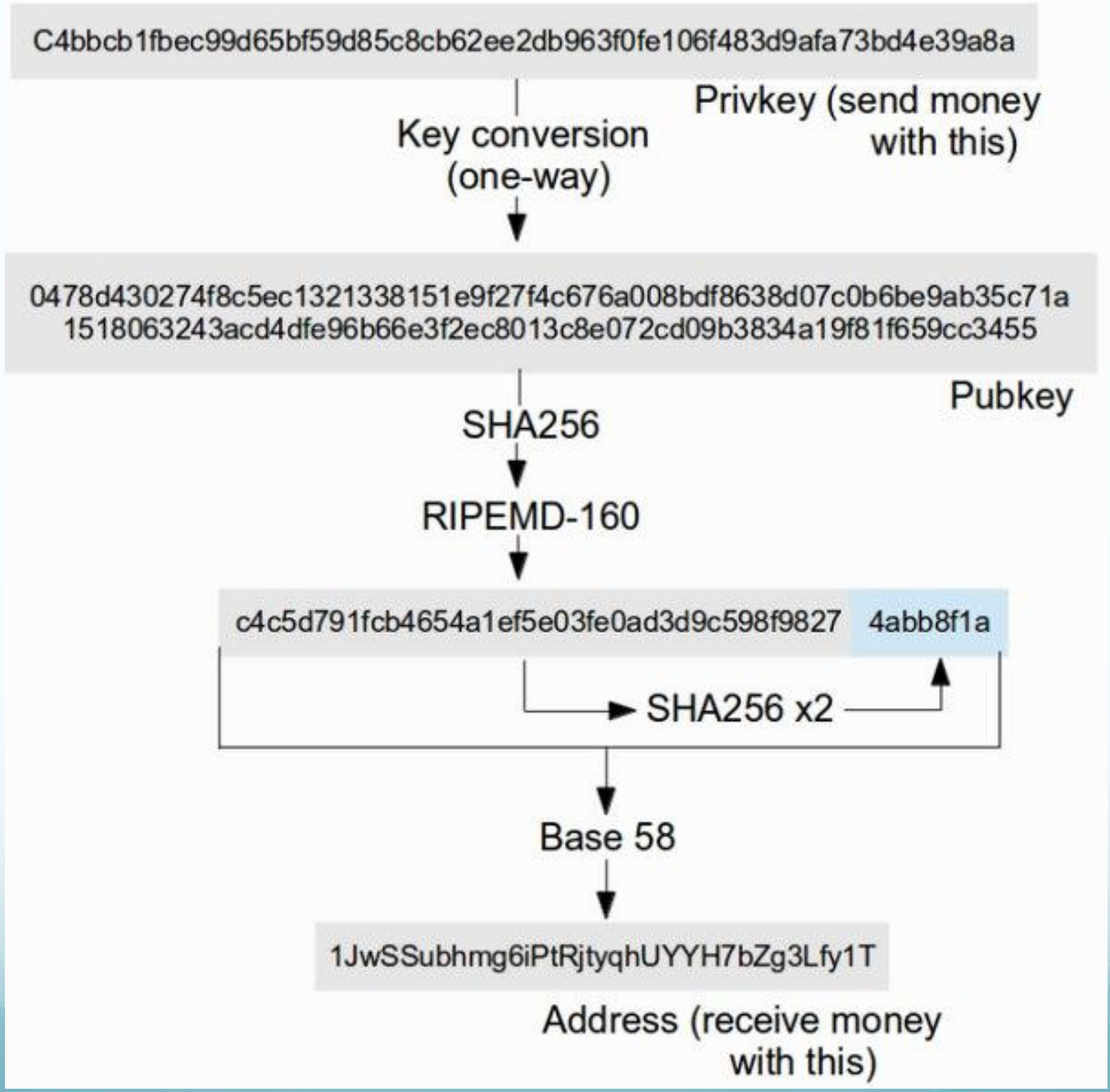
Тогда нам удастся генерировать 312 миллионов $\cdot$ 436760 = 136,2 $\cdot$ 10^{12} пар ключей в секунду.

Это означает, что за год мы переберём 136,2 $\cdot$ 10^{12} $\cdot$ 3,15576 $\cdot$ 10^{7} = 430 $\cdot$ 10^{19} пар ключей

Вероятность встретить таким перебором непустой кошелёк равна

$$(8 \cdot 10^{6}) \cdot (430 \cdot 10^{19})/(1{,}46 \cdot 10^{48}) = 2{,}36 \cdot 10^{-20}$$

Через 5 миллиардов лет Солнце станет красным гигантом.


C4bbcb1fbec99d65bf59d85c8cb62ee2db963f0fe106f483d9afa73bd4e39a8a
Privkey (send money with this)
Key conversion (one-way)
0478d430274f8c5ec1321338151e9f27f4c676a008bdf8638d07c0b6be9ab35c71a
1518063243acd4dfe96b66e3f2ec8013c8e072cd09b3834a19f81f659cc3455
Pubkey
SHA256
RIPEMD-160
c4c5d791fcb4654a1ef5e03fe0ad3d9c598f9827
4abb8f1a
SHA256 x2
Base 58
1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T
Address (receive money with this)

«Красивые» биткойн-адреса

Во-первых, ещё раз повторю, что биткойн-адрес = пара публичный ключ + приватный ключ.

Во-вторых, можно генерировать красивые пары. Каждый может сам написать скрипт, который бы брал случайную строку, вычислял вот всё это и получал публичный ключ.

К счастью, такая утилита есть. Она называется vanitygen

«Красивые» биткойн-адреса

Большое количество человек в начале 2014 получали маленькие спам-платежи от адресов 1Enjoy… и 1Sochi…

Эти платежи обычно не брались майнерами в блоки, и смысл их не особенно ясен.

Богатые биткойн-адреса

Top 100 Richest Addresses Bitcoin

	Address	Balance	Percent of coins	First Input	Last Input
1	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v	162,232 BTC ($72,519,003 USD)	1.07%	2015-10-16 17:43:06	2016-02-13 09:40:01
2	3Kg7Cmooris7cLErTsijq6qR1FH3cTiK2G	157,996 BTC ($70,625,706 USD)	1.04%	2014-12-21 02:50:32	2016-02-13 09:40:01
3	3KBUuGko4H5ke7EVsq9B7PLK1c5Askdd7y	104,579 BTC ($46,747,703 USD)	0.6870%	2014-10-20 11:39:39	2016-02-18 06:19:41
4	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	79,957 BTC ($35,741,511 USD)	0.5253%	2011-03-01 13:26:19	2016-02-13 09:40:01
5	1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx	69,370 BTC ($31,009,028 USD)	0.4557%	2013-04-10 01:03:36	2016-02-13 09:40:01

Богатые догекойн-адреса

Top 100 Richest Addresses Dogecoin

	Address	Balance	Percent of coins	First Input	Last Input
1	D6ReVJuZLoAf1KDbGWe2mVqru482ZJ5vnz	13,000,000,022 DOGE ($3,735,299 USD)	12.61%	2016-01-11 13:33:05	2016-01-27 10:45:08
2	D8EyEfuNsfQ3root9R3ac54mMcLmoNBW6q	9,550,000,821 DOGE ($2,744,009 USD)	9.26%	2014-03-01 20:55:03	2016-01-17 15:18:03
3	DDTtqnuZ5kfRT5qh2c7sNtqrJmV3iXYdGG	5,031,000,838 DOGE ($1,445,561 USD)	4.88%	2014-01-11 13:15:27	2016-01-09 14:11:55
4	D8pr3ZhjeAWYeXMW7KAspbKRETdkowaUG2	2,778,737,754 DOGE ($798,417 USD)	2.69%	2016-02-19 11:32:39	2016-02-19 11:32:39
5	DDogepartyxxxxxxxxxxxxxxxxxxw1dfzr	1,854,576,459 DOGE ($532,877 USD)	1.80%	2014-08-12 21:30:39	2015-12-22 12:09:30

Как выглядит валидный биткойн-адрес?

Он начинается с единицы, длится. При одном условии: если он не начинается с тройки. Если он начинается с тройки – это кошелёк с мультиподписью.

BitcoinEaterDontSend

Поскольку приватный ключ для таких адресов неизвестен, биткойны, отправленные на него, потеряны навсегда.

1BitcoinEaterAddressDontSendf59kuE

имеет чуть более 2.1 BTC на нём

1111111111111111111114oLvT2

имеет 47 биткойнов

Proof-of-burn

Counterparty использовала proof-of-burn вместо майнинга, предлагая переслать на свой адрес

1CounterpartyXXXXXXXXXXXXXXXUWLpVr

Этот адрес получил 2130 BTC, которые теперь потеряны навсегда. Взамен Counterparty выпустили свою валюту тем, кто «сжёг» таким образом свои биткойны.

Как обзавестись биткойнами?

Ура! У нас есть кошелёк.
Правда, в нём ровно 0,00000000 BTC. Как обрести первые биткойны в своей жизни?

- Принимать в дар (обнародовать свой публичный ключ и сказать людям «пересылайте деньги по этому адресу»)
- Принимать в качестве оплаты за услуги

Как обзавестись биткойнами?

- Заняться майнингом (нереально в 2016 году)
  - Открыть сайт любой биржи и купить

Сайты бирж:

- btc-e.com (самая лучшая, BTC/RUR)

Дневной объём торгов превышает 3 миллиона долларов, и при комиссии 0.2% дневная выручка создателей биржи составляет $6000. ДНЕВНАЯ.

- Bitstamp
- Bitfinex
- OkCoin

Не храните большие суммы денег на биржах!

(история про MtGox)

Есть ли у биткойна клоны?

Исходный код протокола Биткойн открыт – поэтому, конечно, да.

Биткойн – всего лишь первопроходец.

Самые знаменитые форки:

- Litecoin (block time = 2.5 minutes; 84 миллиона монет; хэш-функция не sha256, а scrypt)
- Dogecoin (всё то же, что и лайткойн, но на эмблеме монеты – мем с собачкой)
- Primecoin (полезная версия майнинга: вычисляет цепочки Куннингема)

Litecoin

Dogecoin


wow much coin how money so crypto
very currency wow
wow
plz mine v rich very

Dogecoin


100
THE UNITED STATES OF DOGELAND
Ð
such cash
wow
many doge
rich shibe
awesome
100
DogeCoin
Ð
100

Dogecoin и ямайские бобслеисты в Сочи

Капитан ямайской команды по бобслею на олимпиаде в Сочи в интервью телеканалу BBC пожаловался на недостаток финансирования:

«По правде говоря, мы не знаем, достаточно ли у нас сейчас денег, чтобы полететь в Сочи. Как получится. В первую очередь нам нужно позаботиться о наших семьях»

Слова спортсмена растревожили сердца создателей виртуальной валюты, и они объявили о начале сбора пожертвований для ямайских бобслеистов.

Dogecoin и ямайские бобслеисты в Сочи

18 января сообщество Reddit неожиданно решило поддержать ямайцев, пожертвовав денег в догкойнах на общую сумму около 33 тысяч долларов. Организация Dogecoin Foundation запустила специальный сайт, на котором публиковалась интерактивная информация о состоянии счёта.

Dogecoin и ямайские бобслеисты в Сочи

Необходимая сумма набралась на кошельке за сутки. Один из участников сообщества на Reddit с ником dogefreedom заявлял, что пожертвует 20 миллионов догкоинов (около 19 тысяч долларов), если ему объяснят, можно ли доверять Dogecoin Foundation.

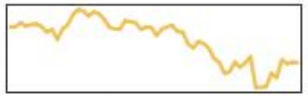
Собрав необходимую сумму, Dogecoin Foundation обменяли её на 35 биткойнов из-за опасений резкого изменения курса догкойна.

Биткойн – он такой один?

Исходный код биткойн-клиента открыт – поэтому валют, похожих на него, наклепали уже больше тысячи. Каждый день какой-нибудь школьник клепает новую.

Pump&DumpCoin

Неполный список можно посмотреть на coinmarketcap.com

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 6,388,105,406	$ 419.44	15,229,900 BTC	$ 55,950,200	-0.21 %	
2	Ethereum	$ 341,674,415	$ 4.43	77,154,925 ETH	$ 8,496,220	2.25 %	
3	Ripple	$ 279,627,399	$ 0.008202	34,090,841,338 XRP *	$ 839,971	3.41 %	
4	Litecoin	$ 145,099,749	$ 3.26	44,564,626 LTC	$ 1,547,380	0.44 %	
5	Dogecoin	$ 30,566,136	$ 0.000296	103,148,278,981 DOGE	$ 407,285	7.79 %	
6	Dash	$ 23,167,794	$ 3.72	6,233,800 DASH	$ 100,931	8.69 %	

Какие есть интересные валюты, помимо биткойна?

Самые знаменитые:

- Namecoin (децентрализованная система DNS-серверов)
- Dash (раньше назывался Darkcoin)
- Ripple (хавала)
- ETHEREUM

Ethereum

Ethereum – это проект (успешно доведённый до запуска) коренного канадца по имени Vitalik Buterin. Суть его вот в чём.

В Биткойн есть только один тип аккаунтов – «кошелёк, управляемый человеком».

В сети Эфириум есть ещё один:
«кошелёк, управляемый программным кодом»

«Кошелёк, управляемый программным кодом»

Таким кошельком управляешь не ты, человек. Один раз написав код и нажав «Отправить в сеть», такой кошелёк начинает жить своей жизнью.

При этом код общедоступен – точно так же, как общедоступны все записи в блокчейне.

Ethereum

Во время продажи своей криптовалюты они собрали 31 килобиткойн. По курсу на тот момент это составляло 20 миллионов долларов. Типичный пример того, как легко сделать в интернете огромные деньги.

Проблемы Биткойна

- Централизация майнинга
- Неполная анонимность
- Масштабируемость

Биткойн через сеть Tor

На arxiv.org есть статья «Bitcoin over Tor isn’t a good idea»

Биткойн через сеть Tor

Пустогаров и Бирюков выявили возможность подобной манипуляции, сфокусировавшись на малоизвестном аспекте протокола Биткойн: встроенной защите от DoS-атак (атака отказа в обслуживании). В целях самозащиты, биткойн-серверы присваивают баллы пользователям, генерирующим проблемные транзакции. В том случае, если количество баллов превышает 100, сервер блокирует пользователя на 24 часа.

Биткойн через сеть Tor

Авторы поясняют, что, когда пользователь Тора подсоединяется к Биткойну, его IP-адрес никак не фигурирует в сети. Вместо этого адреса Биткойн-сеть видит только адреса выходного Тор-узла. Таким образом, злоумышленники могут заблокировать все выходные узлы Тора, инициировав большое количество невалидных транзакций через Тор. Благодаря принципу работы защитной системы на серверах Биткойна через какое-то время после начала спам-атаки все выходные узлы Тора попадут в “черные списки”.

Биткойн через сеть Tor

Сообразительный взломщик в силах настроить ряд биткойн-серверов и выходных узлов таким образом, чтобы система защиты Биткойн-сети от DoS-атак блокировала доступ всех выходных Tor-узлов, за исключением нескольких, над которыми у злоумышленника есть контроль.

Когда жертва начнет использовать Tor для подключения к Биткойну, ей ничего не остается, кроме как подсоединиться к тем биткойн-серверам, которые уже захвачены взломщиком, так как все остальные заблокированы. С этой секунды, вся информация о биткойн-транзакциях жертвы проходит через руки злоумышленника.

Биткойн через сеть Tor

Это MITM-атака, и с её помощью можно выявить IP-адрес пользователя и проследить связь с другими биткойн-адресами.

В результате атаки транзакции и блоки запущенные истинным владельцем биткойн-адреса тоже подвергаются рискам, поскольку взломщик может отложить их или вовсе отменить.

При самом неблагоприятном сценарии злоумышленник может даже одурачить жертву, создав иллюзию, что на счет пользователя зачислены биткойны, в то время как на самом деле это не соответствует действительности (атака под названием «двойная трата»).

Биткойн и квантовый компьютер

Квантовым компьютером не ломается та часть системы, которая гласит о невозможности по публичному ключу вычислить приватный.

Всё благодаря тому, что биткойн-адрес – хэш публичного ключа, а не ключ – помните картинку?..

Видите какой мудрый вождь наш Сатоши Накамото!

Биткойн и квантовый компьютер

Квантовым компьютером не ломается также и майнинг – по-видимому, перебор значений nonce не является той операцией, в которой квантовый компьютер позволяет достичь убыстрения вычислений.

Единственное что – нужно будет пользоваться каждым биткойн-адресом только один раз.

Задача на миллиард долларов

Биткойн испытывает две проблемы:

- неполной анонимности
- централизации майнинга

Проблема неполной анонимности решается добавлением слепых подписей в протокол.

Задача
на миллиард долларов

Проблема централизации майнинга не решается пока что никак.

Предложение: обойтись совсем без майнинга. Придумать систему, в которой локально подмену за несколько времён жизни Вселенной произвести было б нельзя.

Без этих ваших децентрализованных соглашений.

Ну хорошо, а как мне на всём этом заработать?

Есть несколько сервисов под названием DoubleYourBitcoins,

один из них даже в сети TOR.

Про сам процесс пересылки им ваших монет они говорят «invest».

Кроме шуток, биткойн-банк вполне можно сделать.

Ну хорошо, а как мне на всём этом заработать?

Другая идея: Bitcoin Faucets. Faucet = кран.

freebitco.in

Краны зарабатывают на контекстной рекламе гораздо больше, чем выплачивают вам.

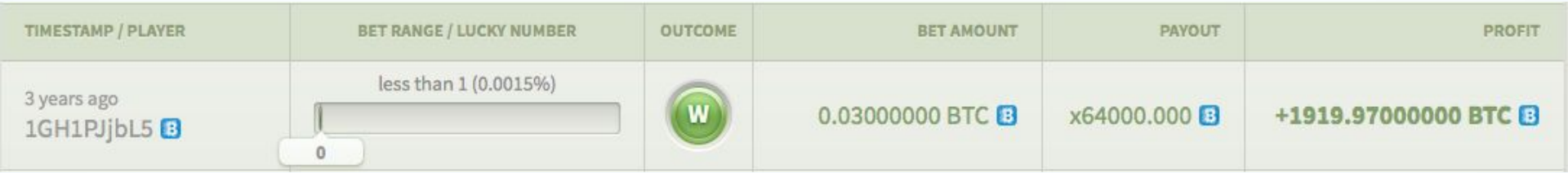
Как заработать?

Есть знаменитый сервис SatoshiDice

Вероятность выигрыша равна 48.1%, вероятность проигрыша – 51.9%

Тем не менее, есть четверо человек за всю историю сервиса, которые-таки сорвали куш!

Как заработать?



Как заработать?

Но вообще – btc-e.com нам всем служит примером. Сделай какую-нибудь игрушку. Сделай какой-нибудь развлекательный сайт.

Где читать новости биткойн-мира?

- bitnovosti.com (лютейшая пропаганда!)
- coinmarketcap.com
- en.bitcoin.it – биткойн-википедия
- bitcoin.org

Donate me

1DJ79KPAqhJ77kuQWLRgbcA2fMMKJhW4W5