

Физтех.Читалка

Блокчейн: инструкция по применению

Умеренков Валерий, 24 августа 2017





Что такое биткойн?



Как выглядит транзакция

2010-12-29 11:57:43

1JxDJCyWNakZ5kECKdCU9Zka6mh34mZ7B2

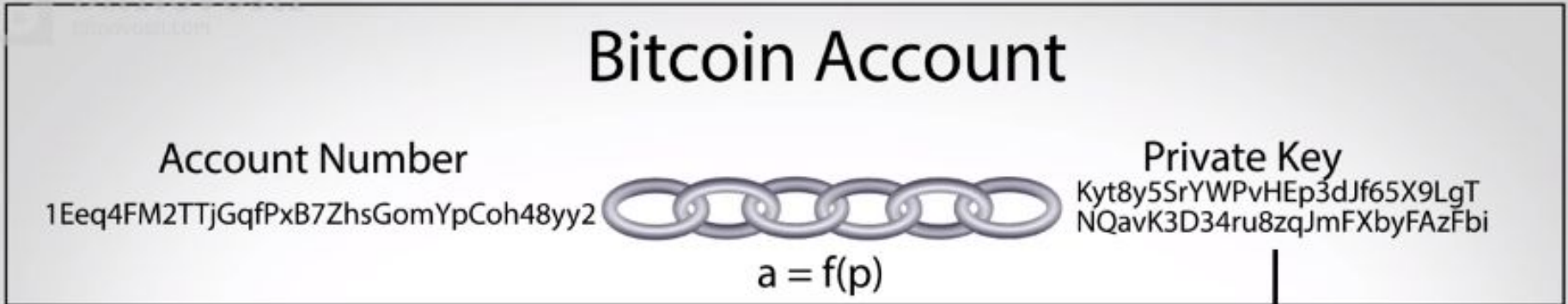


16FuTPaeRSPVxxCnwQmdyx2PQWxX6HWzhQ

0.01 BTC

0.01 BTC

Создание цифровой подписи

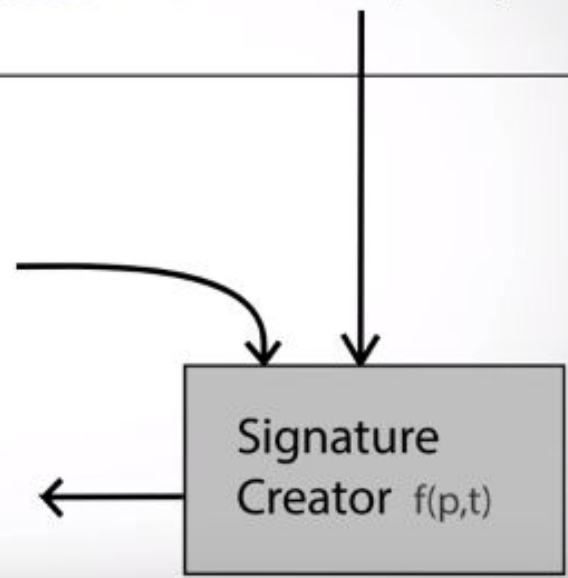


Transaction Message

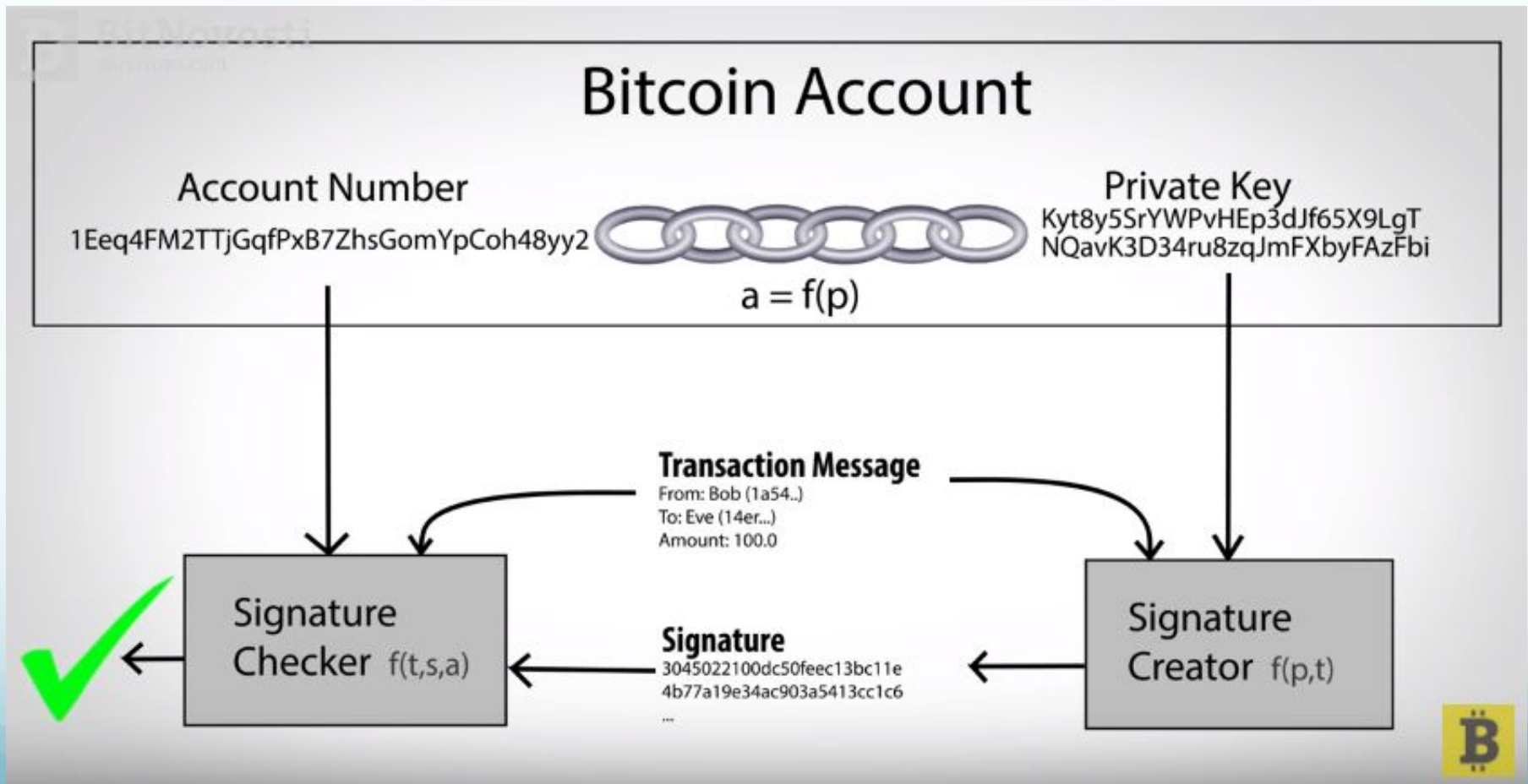
From: Bob (1a54...)
To: Eve (14er...)
Amount: 100.0

Signature

3045022100dc50feec13bc11e
4b77a19e34ac903a5413cc1c6
...



Проверка подписи по публичному ключу



Немного про хэш-функции

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

- невозможность восстановить исходную строку, исходный файл по результату
- при незначительно отличающемся входе совершенно разный выход
- отсутствие коллизий

Cryptographic Hash: text → short digest

SHA256("short sentence")

0x 0acdf28f4e8b00b399d89ca51f07fef34708e729ae15e85429c5b0f403295cc9

SHA256("The quick brown fox jumps over the lazy **dog**")

0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

SHA256("The quick brown fox jumps over the lazy **dog.**")

(extra period added)

0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

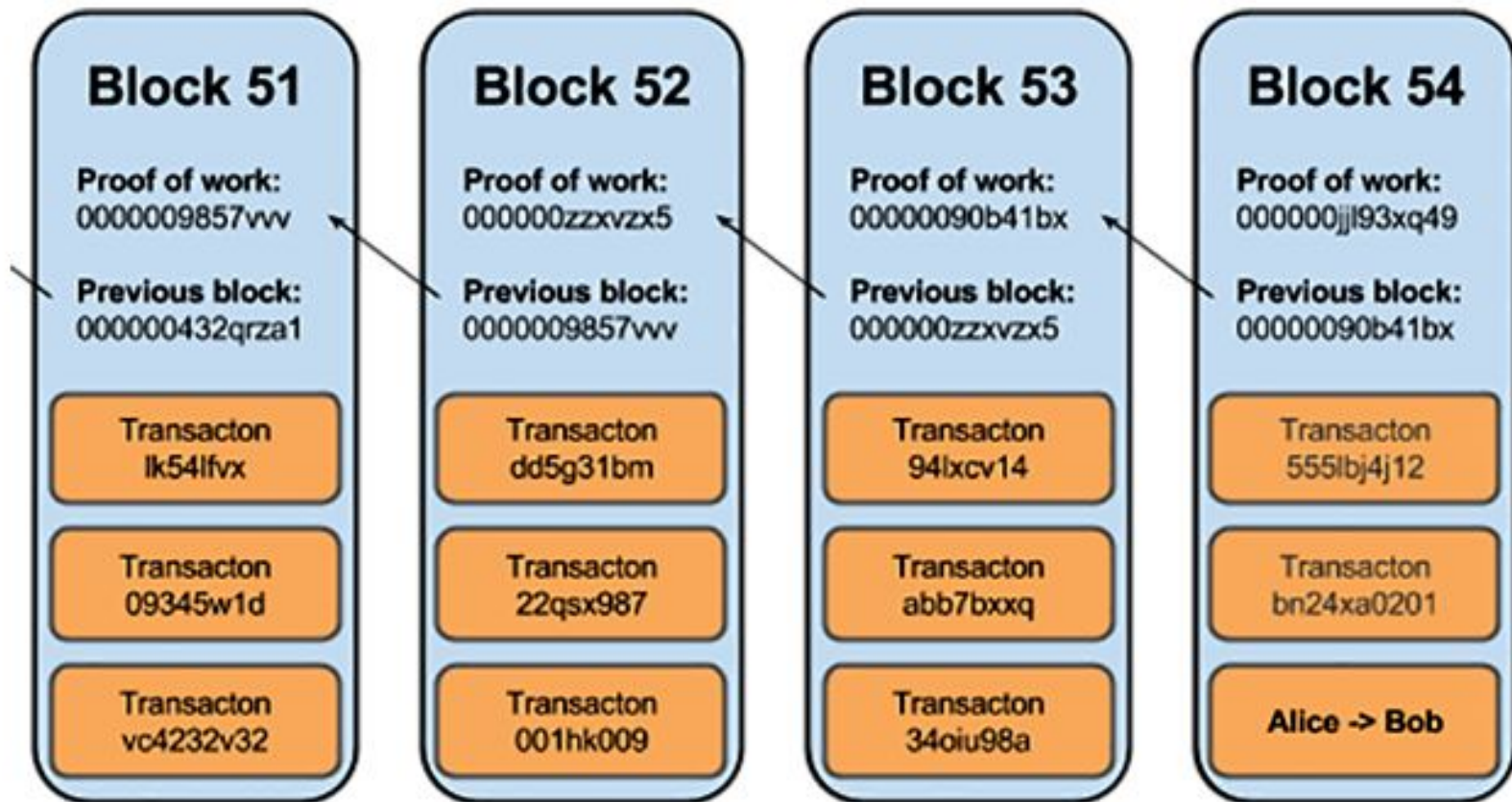
Математическая задача, позволяющая включить новые транзакции в цепочку

Crypto Hash Locks Blocks in Place

block contents		random	hash	?	target
prev block ID	transactions	guess (nonce)	result		
f(#78A..., tx#839, tx#a76, ...,		3001) = 438...	<	100...
f(#78A..., tx#839, tx#a76, ...,		3002) = 988...	<	100...
f(#78A..., tx#839, tx#a76, ...,		3003) = 587...	<	100...
f(#78A..., tx#839, tx#a76, ...,		3004) = 087...	<	100...



Блокчейн, цепочка блоков транзакций

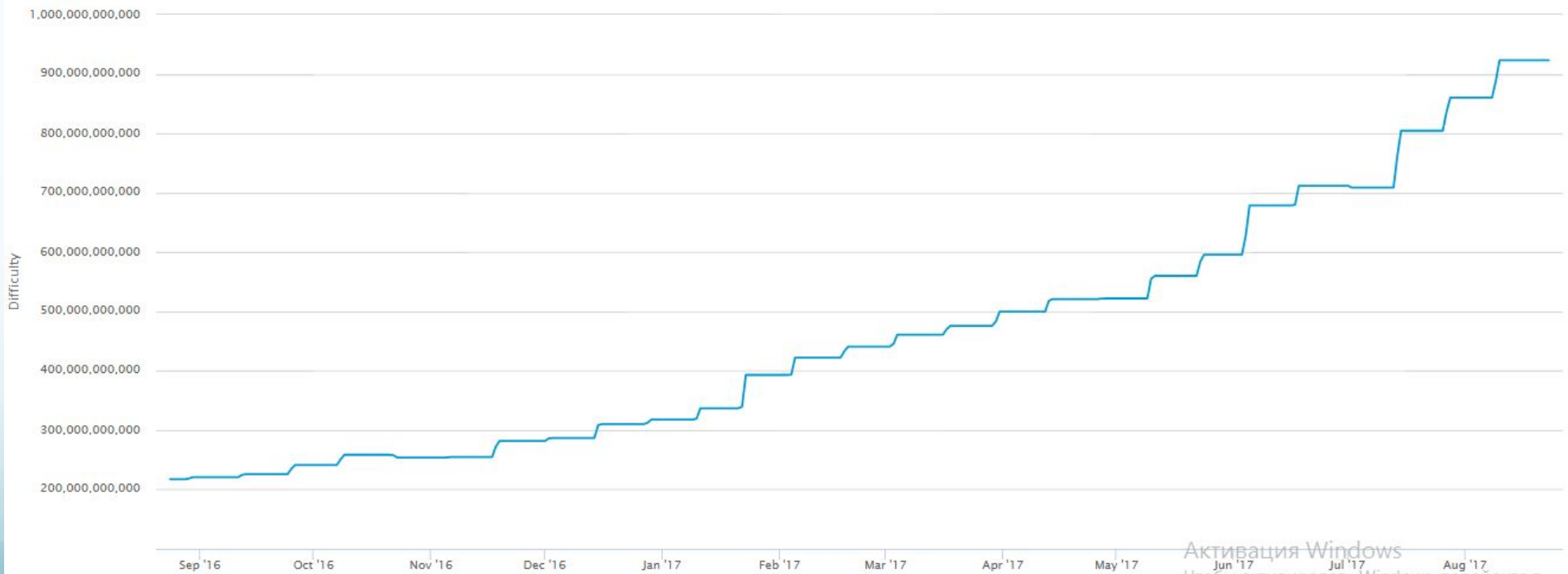


Сложность добычи блока от времени

Difficulty

A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

Source: blockchain.info



Активация Windows

Чтобы активировать Windows, перейдите в

Комиссия и награда

За каждую транзакцию отправитель платит в сеть комиссию, равную в среднем 0,001 BTC

Доход майнера = награда за нахождение блока (сейчас 12,5 BTC) + комиссии всех транзакций в блоке, который он нашёл.

Как бросить учёбу и начать добывать биткойны?

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

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

Или делают ботнет. :)

Если что, за создание ботнета предусмотрена уголовная ответственность.

Получается, биткойны будут печататься бесконечно?

Почти.

Сейчас какой-то счастливчик раз в 10 минут добывает 12,5 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?

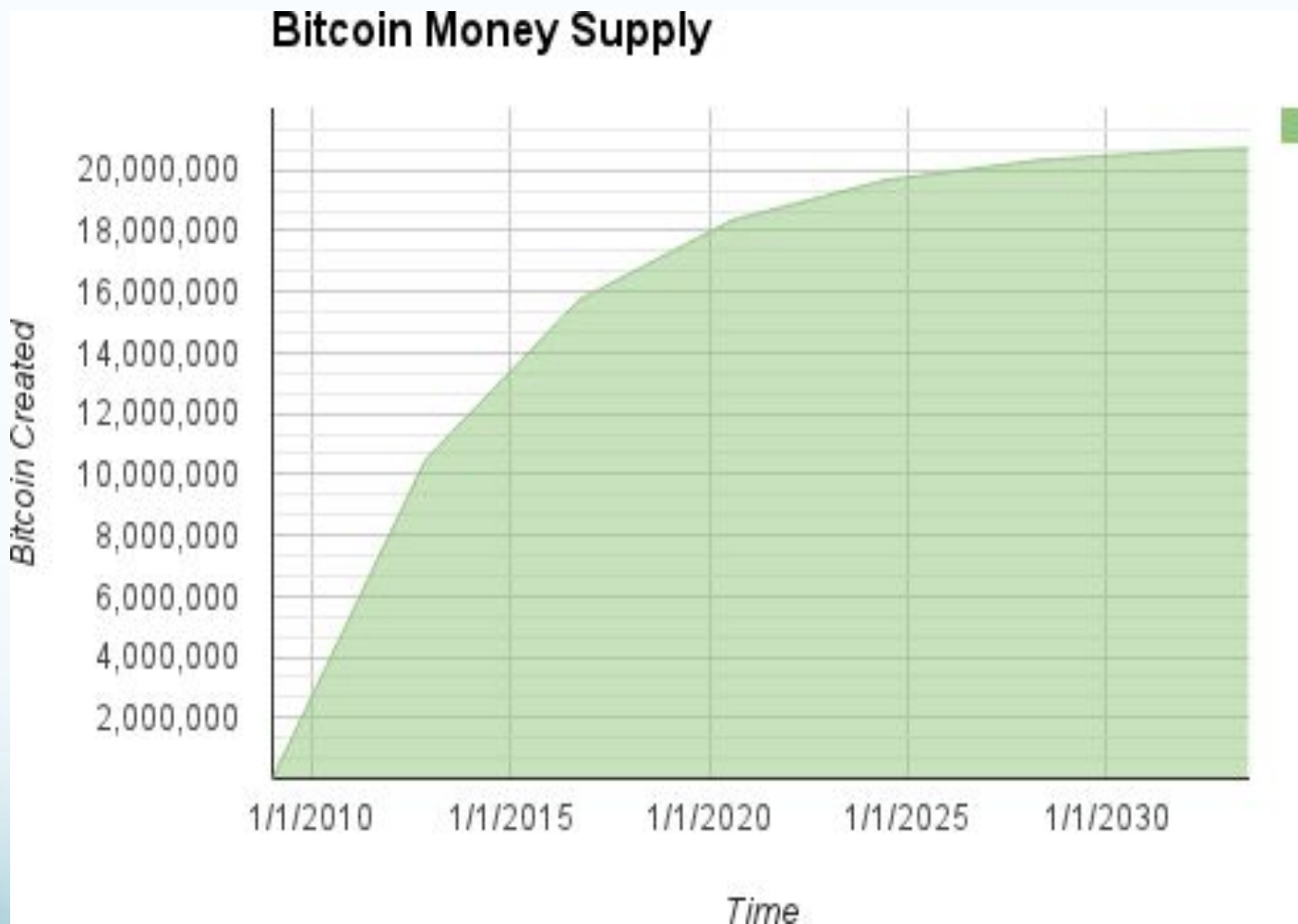
В действительности всё не так, как на самом деле. Уполовинивание награды происходит не раз в 4 года, а спустя каждые 210000 блоков.

Это, если мощность майнеров сильно не растёт, почти одно и то же (блоки добываются в среднем раз в 10 минут, а 4 года разделить на 10 минут равно 210384).

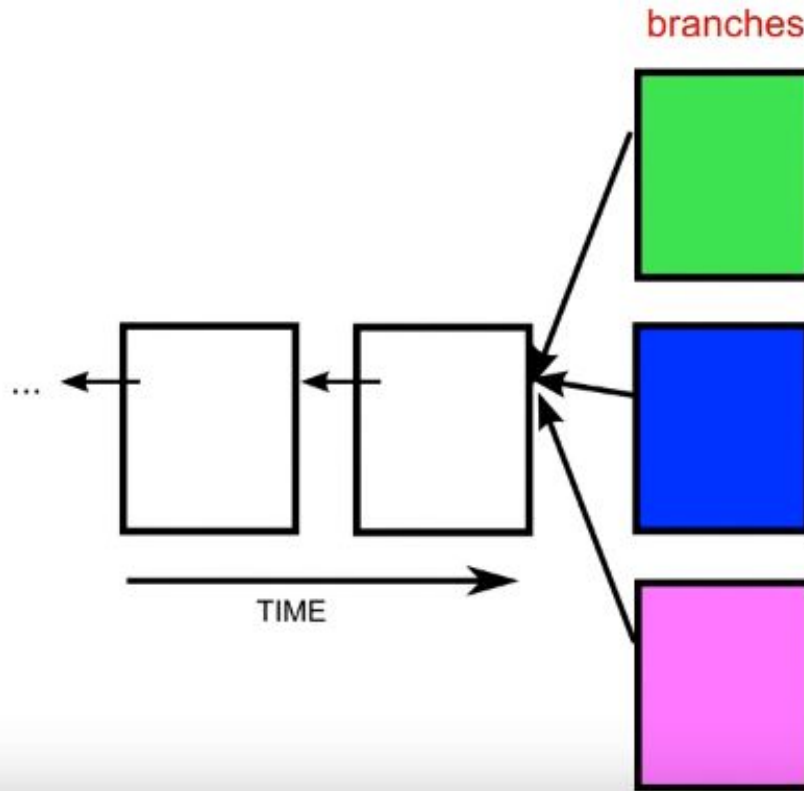
Кто умеет суммировать геометрическую прогрессию?

$$50 \cdot 210000 + 25 \cdot 210000 + 12,5 \cdot 210000 + \dots$$

Суммарно будет добыто 21 миллион биткойнов. Больше добыто не будет. Протокол неизменяем.

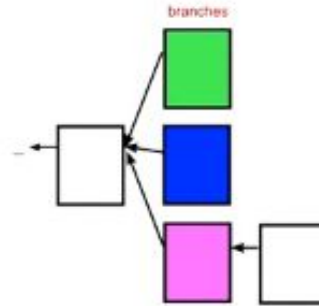


Одновременно найденные блоки

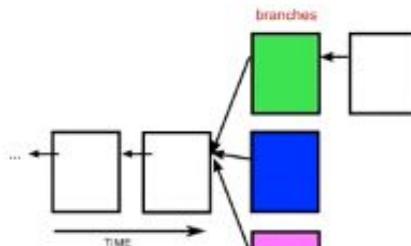


Выход из ситуации

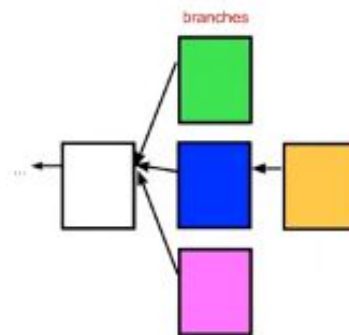
**Travis's
Block Chain**



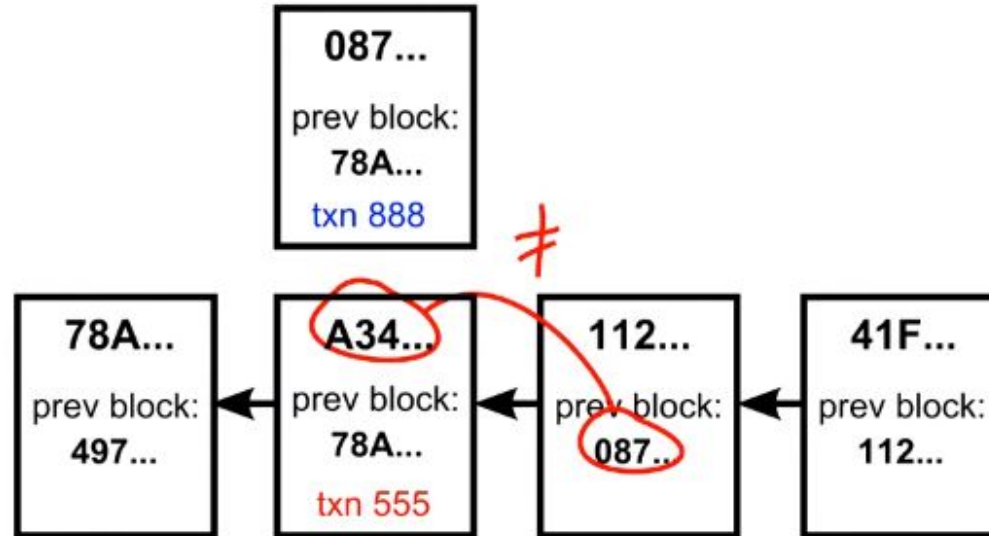
**Your
Block Chain**



**Carol's
Block Chain**



Транзакции блокчейна невозможно фальсифицировать



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 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;fíýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ā^ŠQ2:Ÿ_@
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 .....
00000060 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 ybàê.aP¶IÖ¼?Lİ8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.å.Á.P\8M÷ø..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

Также там был обнаружен
трибьют криптографу Len
Sassaman

```
:.: .: ' ' ' ' ' ' : :
:.: ' ' , , xiW, "4x, ' '
: , dWWWXXXXXi, 4WX,
' dWWWXXX7" `X,
lWWWXX7 X
:WWWXX7 ,xXX7' "^^X
lWWWX7, -:+, , -:+,
:WWW7, . ^"-" -^"
WW", X: X,
"7^^Xl. (_x7'
l ( :X:
~ . " XX ,xxWWWXX7
)X- " " 4X" .____.
,W X :Xi _/_/_
WW X 4XiyXWWXd
" " 4XWWWXX
, R7X, " ^447^
R, "4RXk, _/_/_
TWk "4RXXi, X',x
lTWk, "4RRR7' 4 XH
:lWWWk, ^" ^4
::TTXWWi, _ Xll :..
=====
LEN "rabbi" SASSAMA
1980-2011
Len was our friend.
A brilliant mind,
a kind soul, and
a devious schemer;
husband to Meredith
brother to Calvin,
son to Jim and
Dana Hartshorn,
```

Приколы, которые содержит блокчейн

Кроме того, блокчейн содержит тексты Бхагавада Гиты, длинный список цитат Нельсона Манделы, 1000 цифр числа Пи, стихотворения Шел Силверстайна, стихотворения Руми, файлы WikiLeaks, Python-код посвящённый добавлению информации в блокчейн и скачиванию её, два незаконных простых числа, огромное количество валентинок

Отличия от электронных денег

- Децентрализация
- Простота в использовании
- Анонимность
- Прозрачность и публичность
- Низкие комиссии
- Быстрые переводы 24/7/365
- Безотзывные транзакции

Другие преимущества

- Возможность отправлять микротранзакции
- Открытая технология
- Свободное рыночное ценообразование
- Вне государств, вне политики, вне санкций

Ethereum

Ethereum – это проект (успешно доведённый до запуска) коренного канадца по имени Vitalik Buterin.

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.

Динамика курса Bitcoin

Market Price (USD)

Average USD market price across major bitcoin exchanges.

Source: blockchain.info



Тотальная капитализация криптовалют

Total market cap: \$152,700,263,203



Bitcoin market cap: \$69,024M









Altcoin - market cap: \$83,676M



Место в списке фондового индекса S&P 500

Cryptocurrencies in the S&P 500

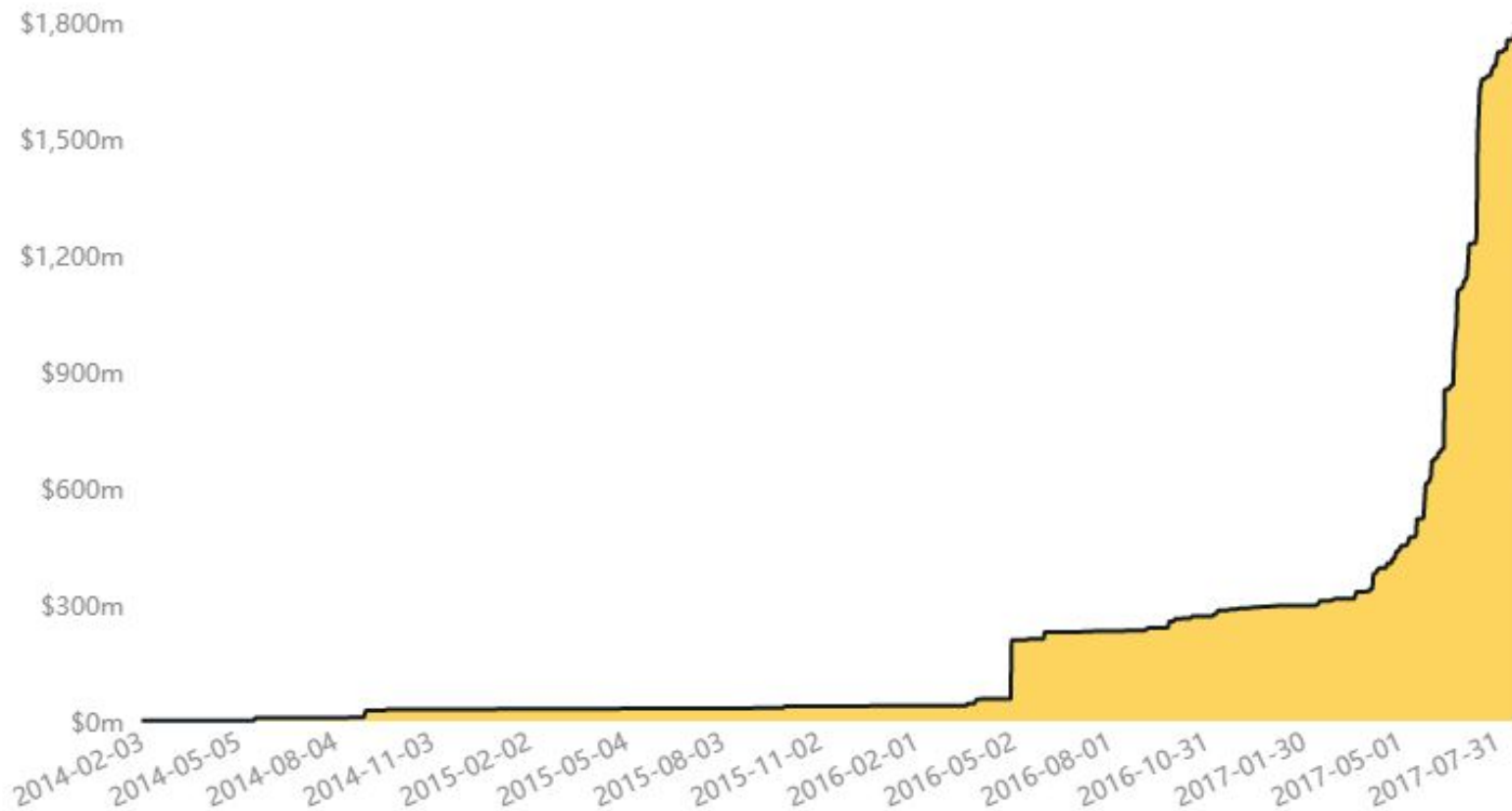
1		Apple Inc.	\$828,220M
29		Cisco Systems, Inc.	\$158,010M
30		The Walt Disney Comp.	\$157,720M
—	—	Cryptocurrencies	\$152,700M
31		Mastercard Inc.	\$141,430M
32		The Boeing Comp.	\$140,620M
500		Diamond Offshore Drilling, Inc.	\$1,490M

В каких областях можно применить

- Авторство и право владения
- Операции с товарами и сырьем
- Управление данными
- Цифровая идентичность, проверка подлинности и подтверждение прав доступа
- Средства электронного голосования
- Интернет вещей
- Ещё десятки примеров

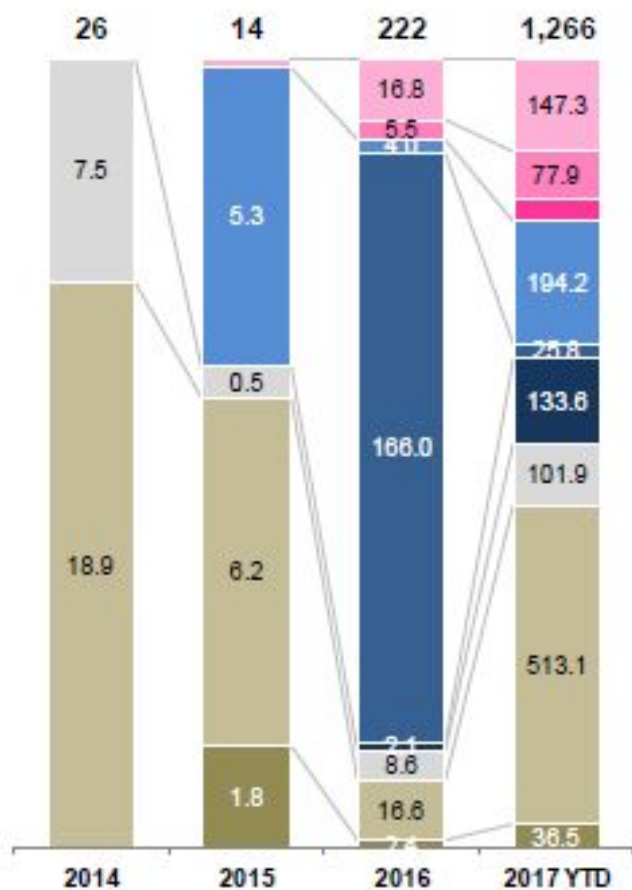
Общий объём привлечённых средств

All-Time Cumulative ICO Funding

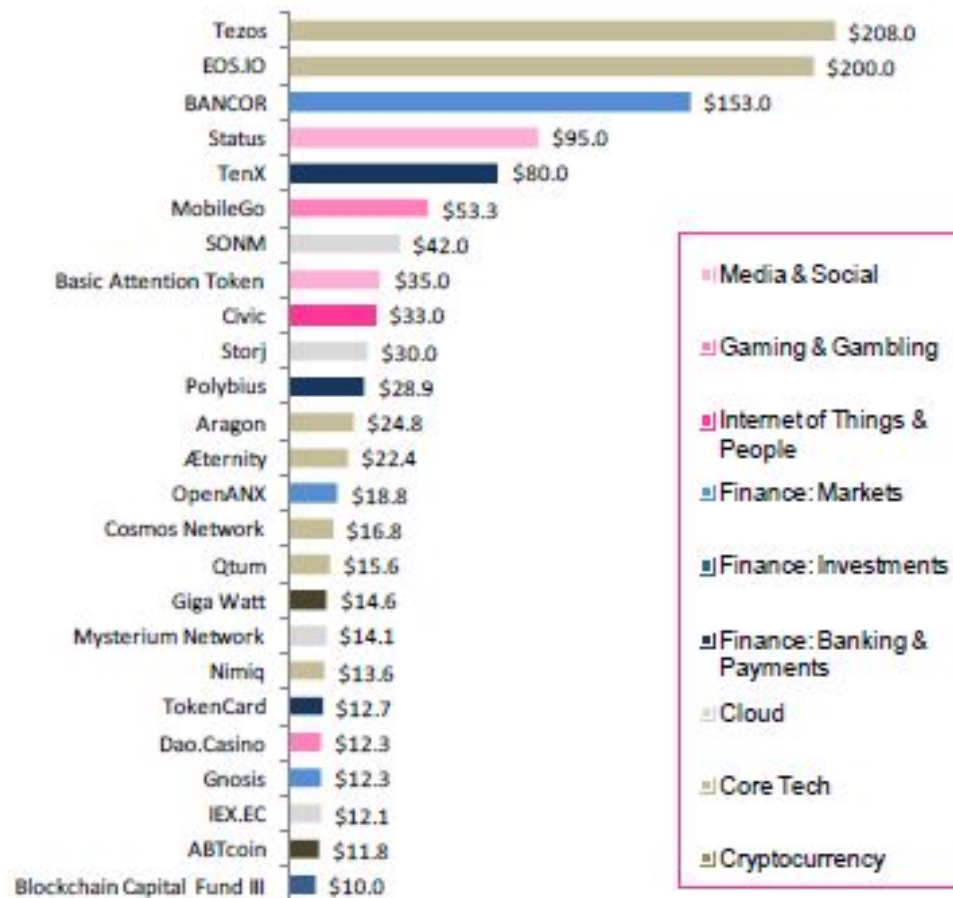


Ещё немного статистики

ICOs by Category (\$ millions)



Top 2017 ICOs by Category (\$ millions)



- Media & Social
- Gaming & Gambling
- Internet of Things & People
- Finance: Markets
- Finance: Investments
- Finance: Banking & Payments
- Cloud
- Core Tech
- Cryptocurrency

Контакты

- vk.com/umerenkov21
- t.me/umerenkov21
- Статья о нашей компании: vc.ru/p/modern-token

Буду рад ответить на вопросы и поделиться литературой по теме

Спасибо за внимание!