Переведено проектом
21ideas.org

CBP Prep Course

(введение в Биткоин)

Андреас Антонопулос

Оригинал слайдов: bit.ly/aantonopworkshop

Содержание Курса

В ходе курса мы обсудим все эти темы (и многое другое):

История Биткоина

Единицы и эмиссия

Монетарные характеристики

Основы транзакций

Ключи и адреса

Обозреватели блоков

Ценообразование и рынки

Комиссии и подтверждения

Основы майнинга

Консенсус

ВНИМАНИЕ

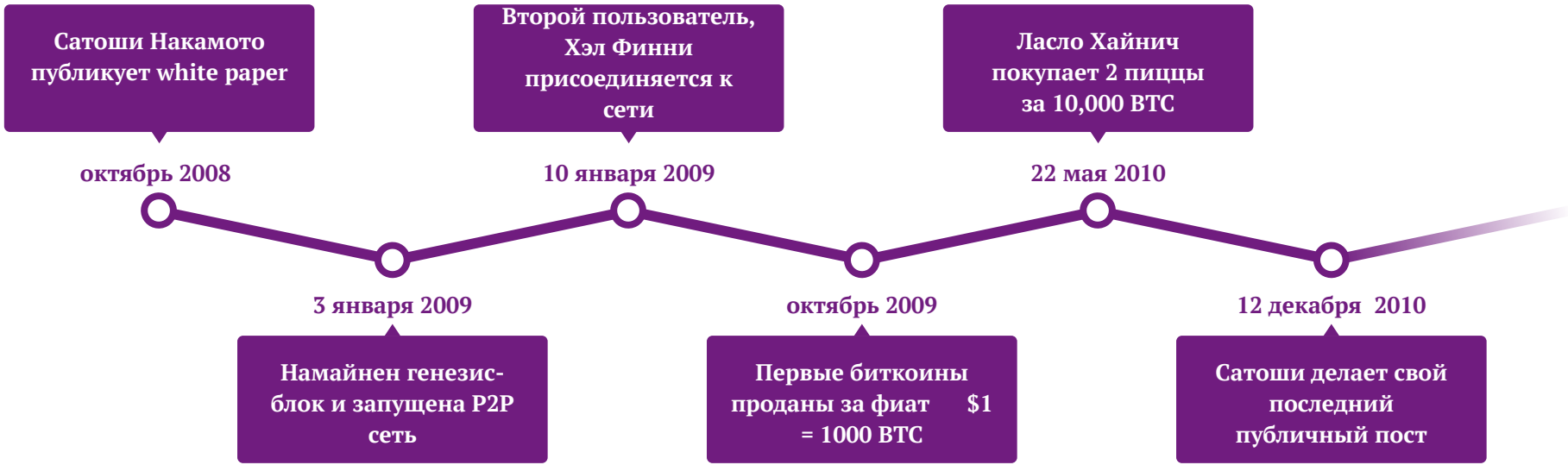
Не отправляйте биткоины на адреса в этой презентации. Эти адреса продемонстрированы исключительно для наглядности. Все биткоины, отправленные на эти адреса будут **УТЕРЯНЫ**

Если вы хотите попробовать, отправьте немного биткоина своему коллеге.

Переведено проектом
21ideas.org

История Биткоина и Что такое Биткоин

История Биткоина
“первые шаги”



Биткоин / биткоин / блокчейн

Биткоин

Протокол для децентрализованной одноранговой сети, который создает консенсус, не нуждаясь в центральном органе для обеспечения доверия.

биткоин

Валюта (токен), выпускаемая в качестве вознаграждения в процессе майнинга proof-of-work.

блокчейн

Публичный реестр, в который записываются транзакции.

Реальные истории

Сюжетная линия

Алиса

Алиса живет в Европе, и она совсем недавно познакомилась с биткоином. В этом курсе мы увидим, как Алиса купит свой первый биткоин и использует его для покупки книги у американского продавца.

Боб

Боб живет в США и управляет книжным интернет-магазином. У него много покупателей за пределами США, и он принимает к оплате многие валюты, включая биткоин.

Каталина

Каталина — веб-разработчик из Аргентины с клиентами по всему миру. Боб — один из ее клиентов.

Переведено проектом
21ideas.org

Биткоин-банкомат

Алиса использует наличные для покупки биткоина в биткоин-банкомате

Алиса

Алиса использует биткоин для покупки книги в интернет-магазине Боба

Алиса

Боб

Боб использует биткоин для оплаты работы Каталины над веб-дизайном магазина

Боб

Каталина

Переведено проектом
21ideas.org

Алиса покупает биткоины в Биткоин-банкомате

Как заполучить свои первые биткоины

- **Зарабатывай - Принимай оплату в биткоинах**
  - Предоставляй услуги - стрижка, мойка машин, извоз
  - Продавай товары - домашняя пахлава, изысканный кофе, брелки
  - Зарплата - попроси своего работодателя оплачивать часть твоей заработной платы в биткоинах - bitwage.com
- **Покупай - Обменивай национальную валюту (фиат) на биткоины**
  - На бирже - компания, которая предлагает покупать и продавать биткоины
  - В банкомате - вендинговая машина, продающая биткоины за наличные
  - Напрямую заинтересованного продавца, за наличку - их можно встретить на митапе или на сайте, таком как localbitcoin.com
- **Обменивай - Trade your belongings for bitcoin**
  - Продай свою машину за биткоины
  - Продай свой дом за биткоины

€80
наличными

Биткоин-банкомат

Алиса использует наличные для покупки биткоина в биткоин-банкомате

Алиса

0.026845 BTC

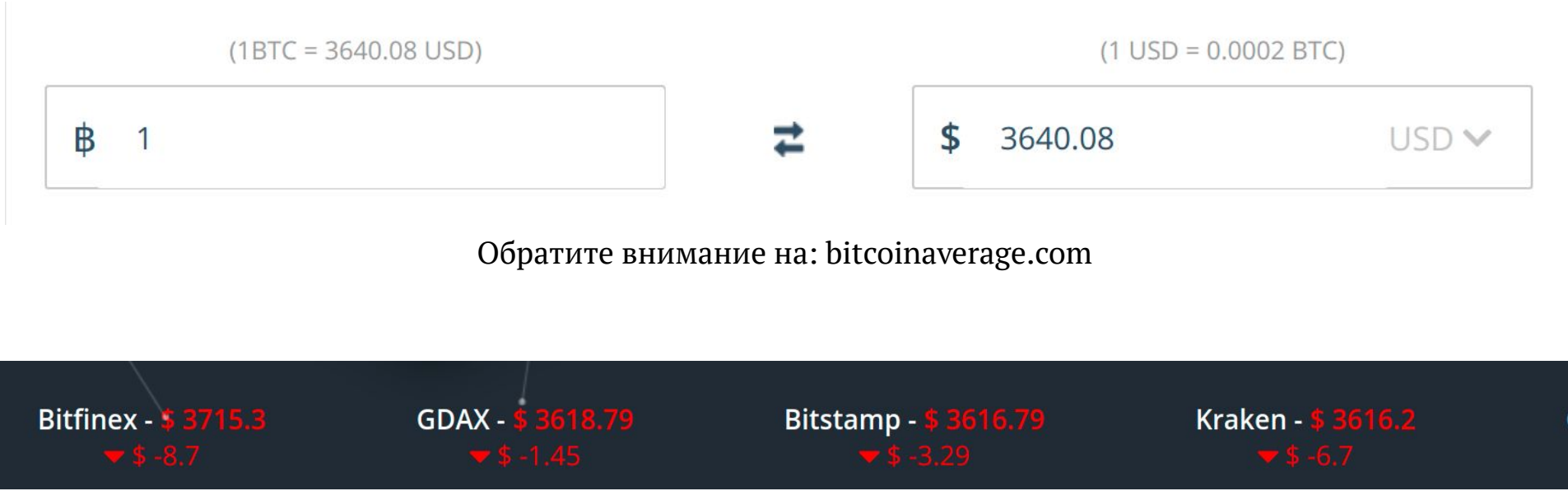
Биткоин-банкомат

=

? BTC

Сколько биткоинов можно купить на 80 евро?

“Цена” биткоина



Обратите внимание на: bitcoinaverage.com

Ценообразование и рынки

Книга ордеров: Сотни ордеров на различных ценовых уровнях

Биткоин-банкомат рассчитывает обменный курс

€80

1 BTC ≅ €3,000

Как Алиса получает BTC?

Биткоин
Публичный депозитный ящик
Кто угодно может внести средства

Приватный ключ

Что-то наподобие очень длинного PIN-кода, только хозяин может разблокировать

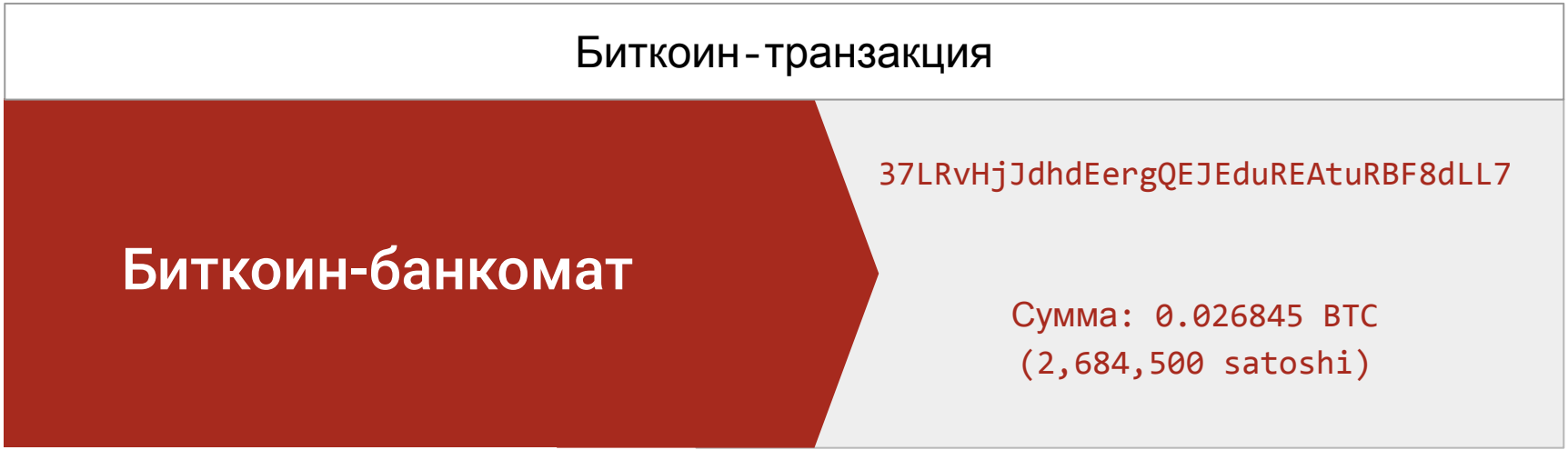
Биткоин-адрес

Используется, чтобы указать куда вносить платеж

37LRvHjJdhdEergQEJEduREAtuRBF8dLL7

Алиса показывает свой Биткоин-адрес банкомату

Алиса покупает биткоин в банкомате



Банкомат отправляет 0.026845 BTC на кошелек Алисы

Единицы в Биткоине

Единственная существующая в сети Биткоин единица исчисления — это сатоши

Все хранится как определенное количество сатоши

Один биткоин = 100 миллионов сатоши

Конвертация единиц

	bitcoin	millibit (mbit)	bit	satoshi
1 bitcoin =	1	1,000	1,000,000	100,000,000
1 millibit =	0.001	1	1000	100,000
1 bit =	0.000001	0.001	1	100
1 satoshi =	0.00000001	0.000001	0.001	1

Переведено проектом
21ideas.org

Алиса покупает книгу в интернет-магазине Боба

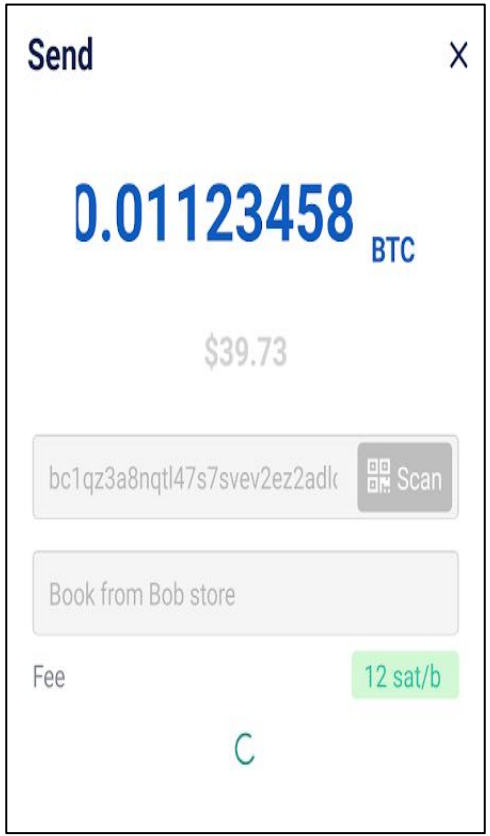
Алиса

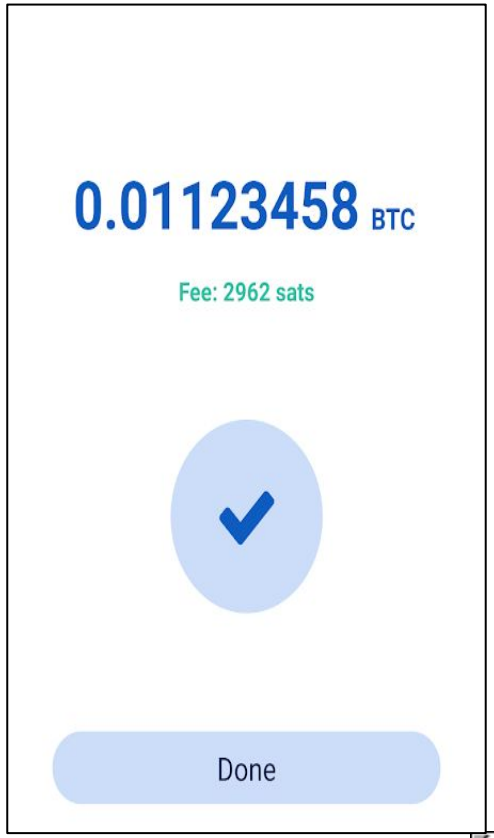
Алиса использует биткоин для покупки книги в интернет-магазине Боба

Боб

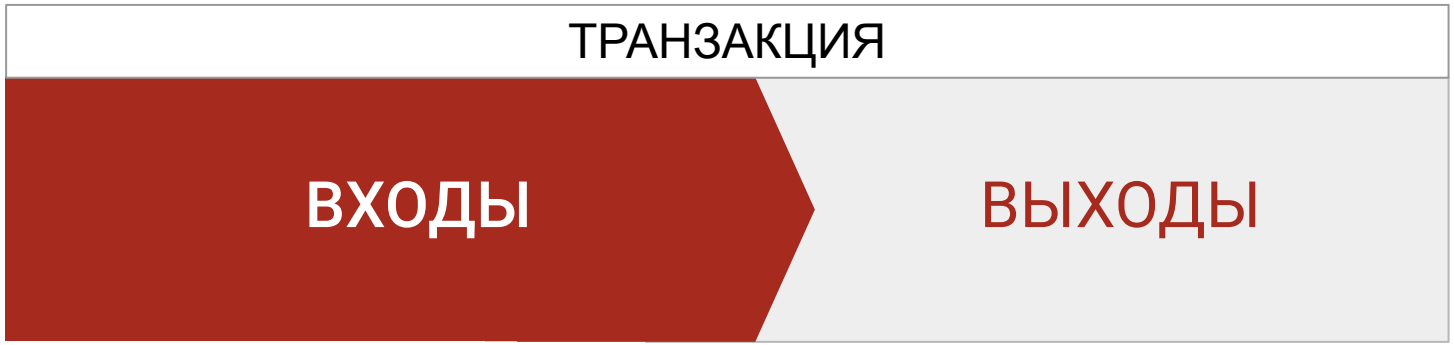

Mastering
Bitcoin
0.01123458 BTC
$40 USD

Кошелек Алисы создает транзакцию



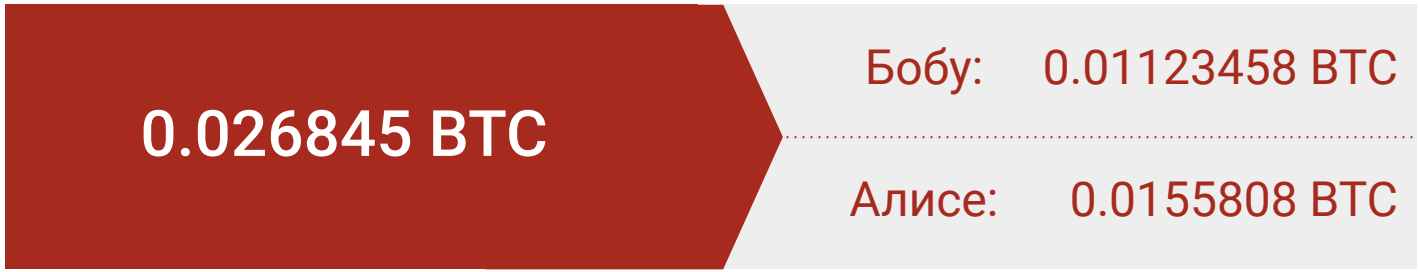


Основы транзакций



Основы транзакций

Транзакции и сдача



Транзакция алисы в блокчейне

Найти транзакцию можно по ссылке (чувствительно к регистру):
bit.ly/**A**lice**T**x

Итог первой части

Мы узнали о:

- История Биткоина
- Ключи и адреса
- Рынки, биржи, ценообразование биткоина
- Единицы учета (сатоши)
- Основы транзакций: входы, выходы, сдача
- Использование обозревателей блоков

Часть вторая

В следующей части мы остановимся на:

- Комиссии за транзакции
- Совмещение транзакционных выводов
- Эмиссия и монетарная политика
- Майнинг и основы блокчейна
- Консенсус
- Форки

Переведено проектом
21ideas.org

Алиса покупает книгу в интернет-магазине Боба
(продолжение)

Входы и выходы (повторение)

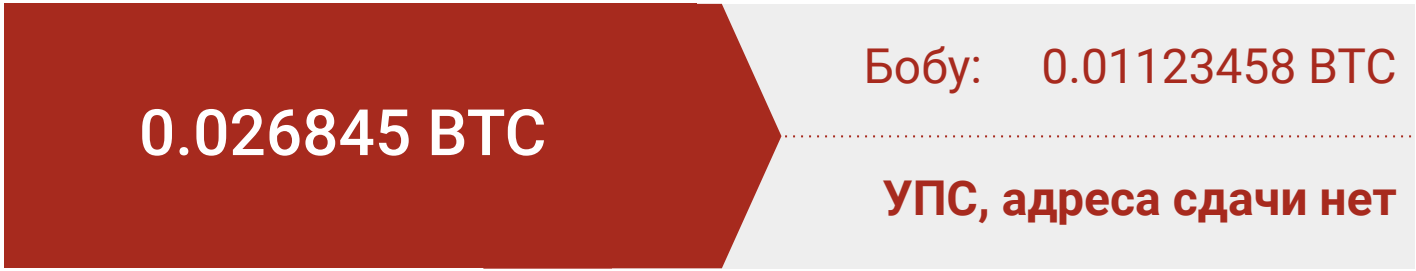
Транзакции и комиссии

Входы: `0.02684500` - Выходы `0.02681538` = Комиссии `0.00002962`

“Майнеры, оставшееся после сдачи — ваша комиссия”

Сдача и комиссии

Что если кошелек Алисы не предоставил адрес сдачи?



Входы: `0.02684500` - Выходы `0.01123458` = **Комиссия `0.01561042`**

Комиссии за транзакции

Зачем нужны комиссии?

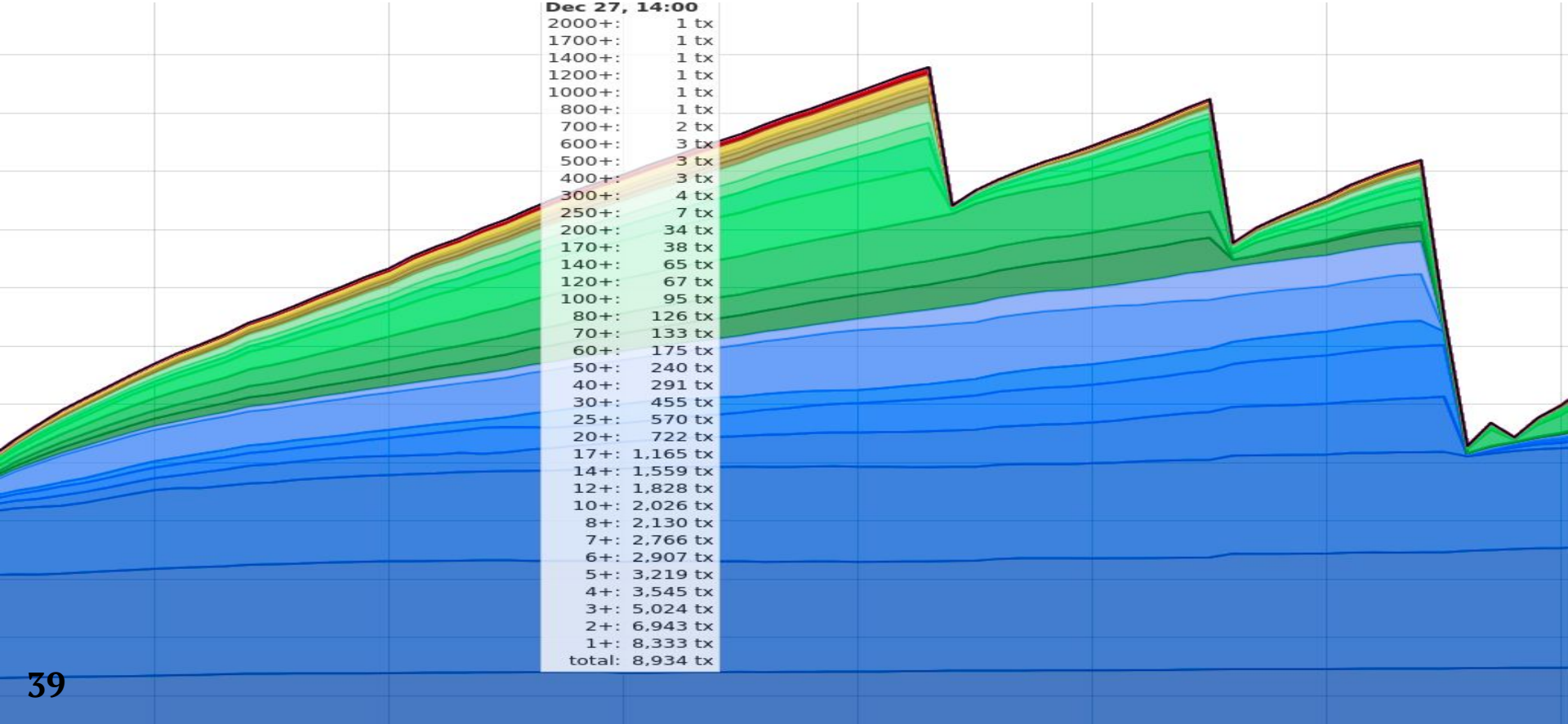
- Свободное место для транзакций ограниченно
- Комиссии определяют насколько каждый ценит свою транзакцию
- Комиссии стимулируют майнинг по мере того, как эмиссия замедляется

Комиссии статичны или они меняются?

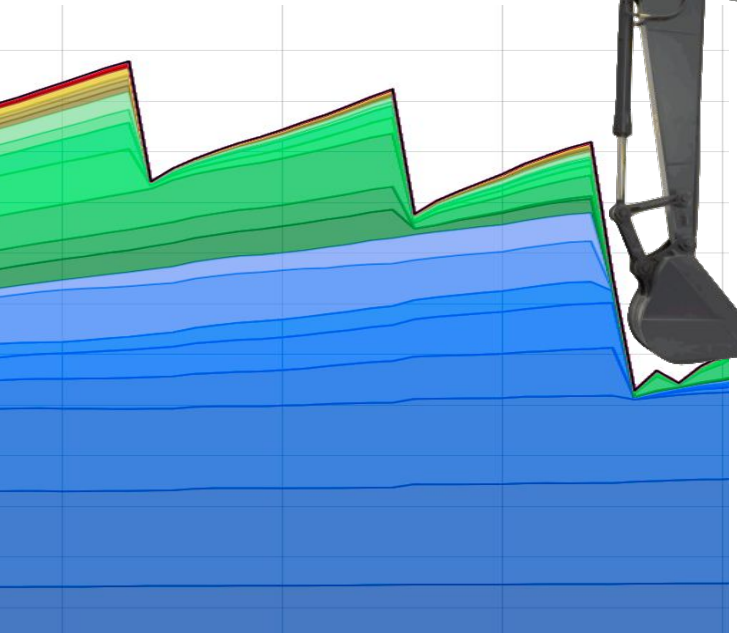
- Какова минимальная возможная комиссия?

Как комиссии влияют на скорость подтверждения транзакции?

Комиссии

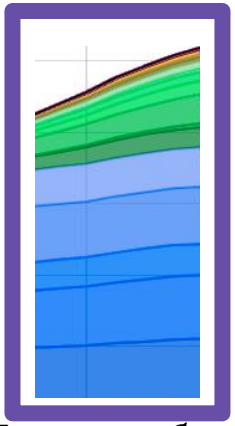

Dec 27, 14:00
2000+: 1 tx
1700+: 1 tx
1400+: 1 tx
1200+: 1 tx
1000+: 1 tx
800+: 1 tx
700+: 2 tx
600+: 3 tx
500+: 3 tx
400+: 3 tx
300+: 4 tx
250+: 7 tx
200+: 34 tx
170+: 38 tx
140+: 65 tx
120+: 67 tx
100+: 95 tx
80+: 126 tx
70+: 133 tx
60+: 175 tx
50+: 240 tx
40+: 291 tx
30+: 455 tx
25+: 570 tx
20+: 722 tx
17+: 1,165 tx
14+: 1,559 tx
12+: 1,828 tx
10+: 2,026 tx
8+: 2,130 tx
7+: 2,766 tx
6+: 2,907 tx
5+: 3,219 tx
4+: 3,545 tx
3+: 5,024 tx
2+: 6,943 tx
1+: 8,333 tx
total: 8,934 tx

Майнеры добавляют транзакции в блоки



Мемпул (место, где транзакции ждут добавления в блок)

Майнер



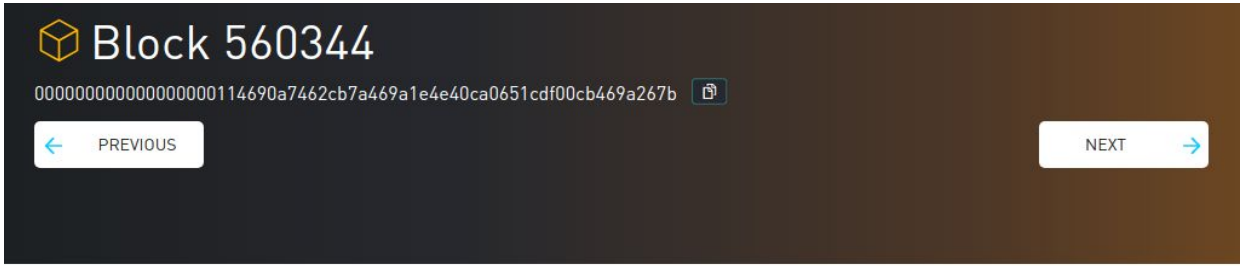
Кандидат-блок майнера

Транзакция Алисы на Биткоин-блокчейне

STATUS	2734 Confirmations
INCLUDED IN BLOCK	00000000000000000114690a7462cb7a469a1e4e40ca0651cdf00cb469a267b
BLOCK HEIGHT	560344
BLOCK TIMESTAMP	1/27/2019, 7:14:29 AM MST
SIZE (BYTES)	246
VIRTUAL SIZE (VBYTES)	165
WEIGHT UNITS (WU)	657
TRANSACTION FEES	0.00002962 BTC (18 sat/vB)
VERSION	1
LOCK TIME	0

Browse: bit.ly/**B**lock344

Транзакция Алисы на Биткоин-блокчейне

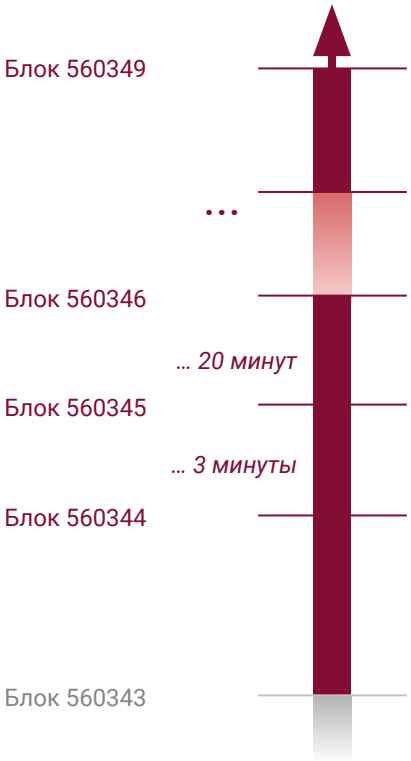


DETAILS +

HEIGHT	560344
STATUS	In best chain (2734 confirmations)
TIMESTAMP	1/27/2019, 7:14:29 AM MST
SIZE (KB)	644.474
VIRTUAL SIZE (KVB)	540
WEIGHT UNITS (KWU)	2156.079

Browse: bit.ly/Block344

Транзакция Алисы на Биткоин-блокчейне



Блок намайнен 1/27/2019, 12:53:18 PM GMT-3

Боб отправляет Алисе книгу через 6 подтверждений после того, как ее транзакция будет добавлена в блок. В данном случае добыча 6 блоков заняла 1 час 39 минут

Блок намайнен 1/27/2019, 11:37:17 AM GMT-3

Блок намайнен 1/27/2019, 11:17:11 AM GMT-3

Блок намайнен 1/27/2019, 11:14:29 AM GMT-3

Транзакция Алисы
e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c

Browse:
bit.ly/Block344

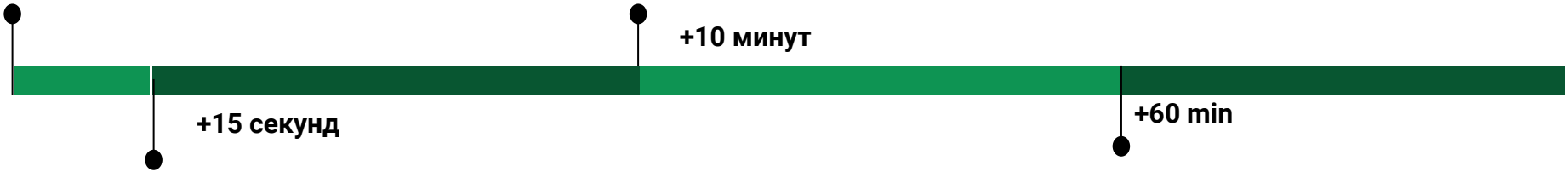
Таймлайн транзакции Алисы

Кошелек Алисы

Создает, подписывает и передает транзакцию, пополняя адрес Боба $40, или 0,01123458 BTC

Майнер

Майнер успешно добывает новый блок, который содержит транзакцию Алисы. У транзакции Алисы теперь "1 подтверждение"



Кошелек Боба

Кошелек Боба получает транзакцию в Биткоин-сети.

Транзакция еще не подтверждена (еще не добавлена в блок)

Кошелек Боба

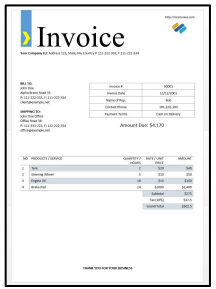
Кошелек Боба видит еще 5 блоков, добытых поверх блока, содержащего транзакцию Алисы.

Политика магазина Боба заключается в отправке книг после 6 подтверждений. Теперь Боб отправляет книгу Алисе.

Переведено проектом
21ideas.org

Боб оплачивает счет Каталины за ее работу над веб-дизайном магазина

Варианты оплаты


Invoice

Amount Due $4,130

Международный перевод (банк)

Western Union

Чек?

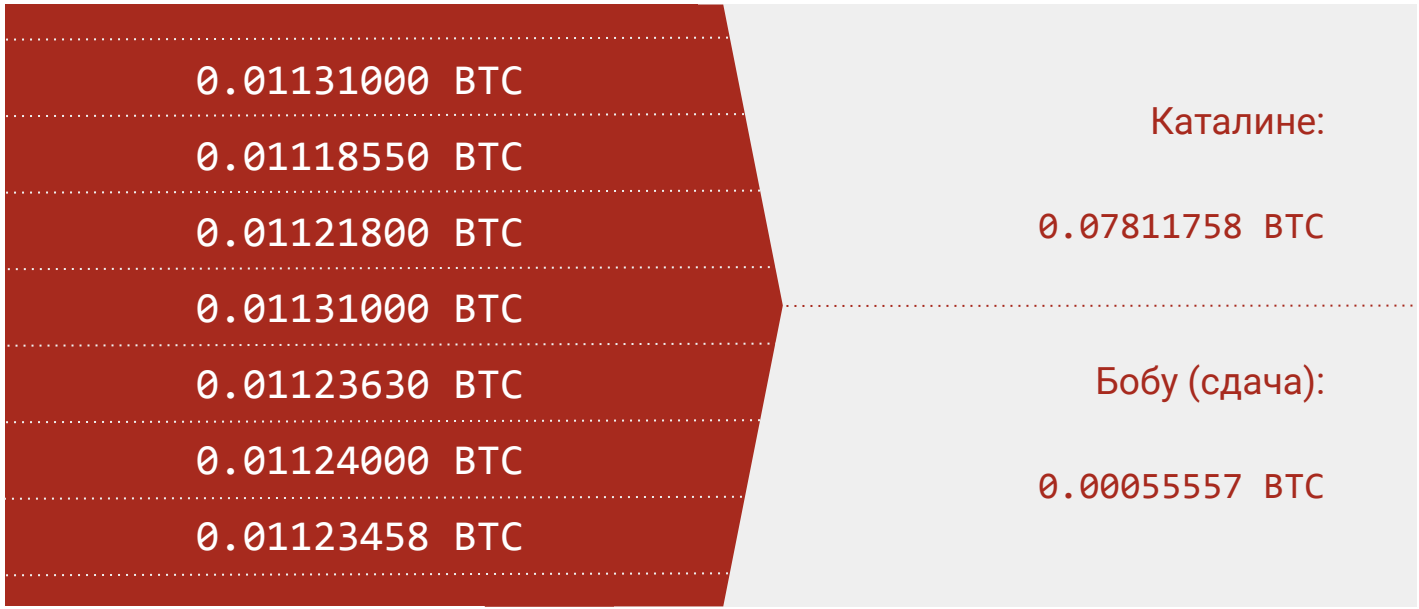
Биткоин

Боб

Боб использует биткоин для оплаты счета Каталины за веб-дизайн

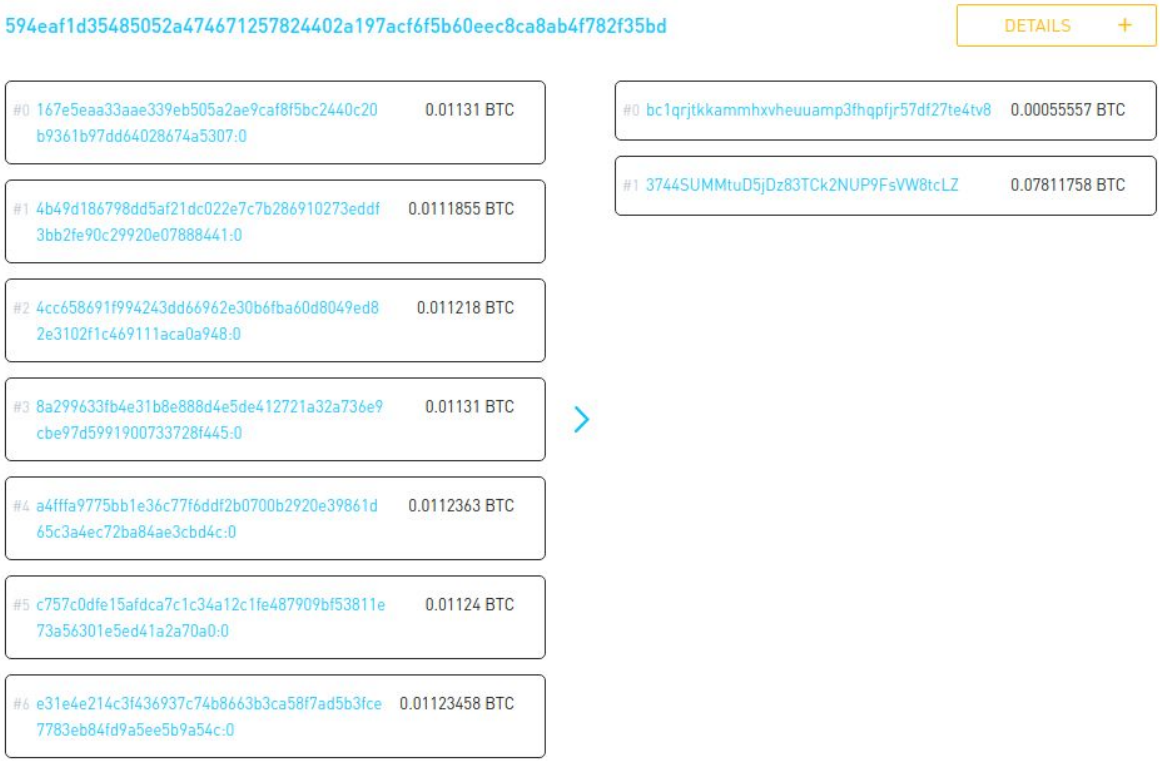
Каталина

Создание транзакции



Боб платит Каталине 0.07811758 BTC

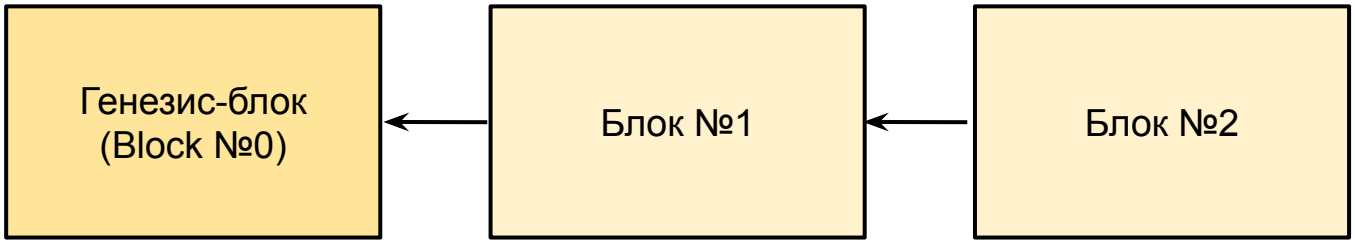
Создание транзакции



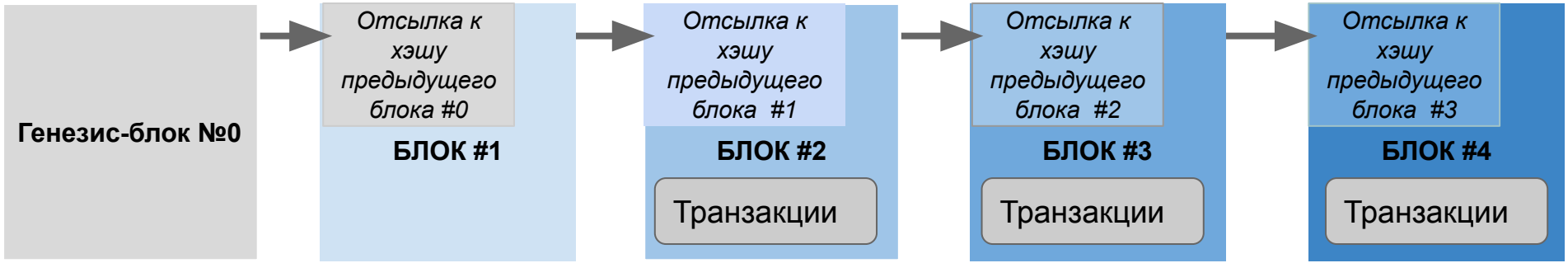
Боб платит Каталине 0.07811758 BTC

Блокчейн

История Биткоин-блокчейна



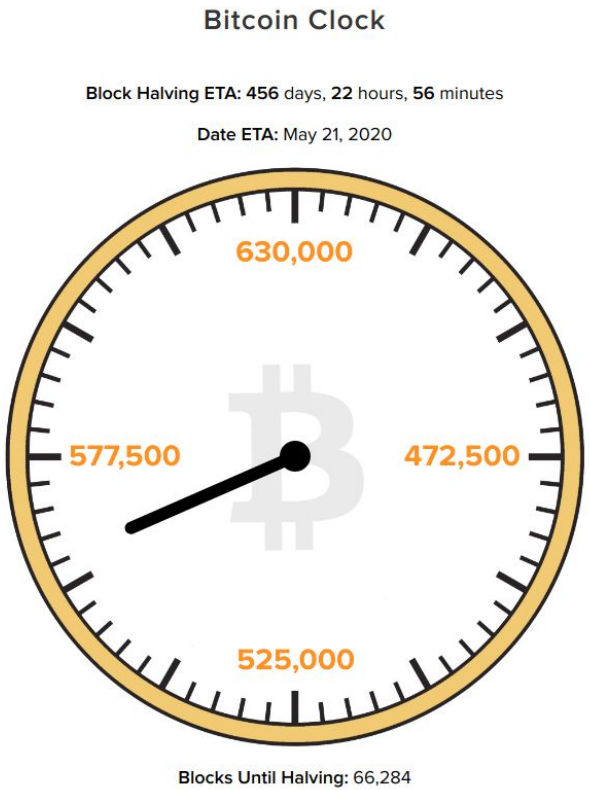
Цепь блоков



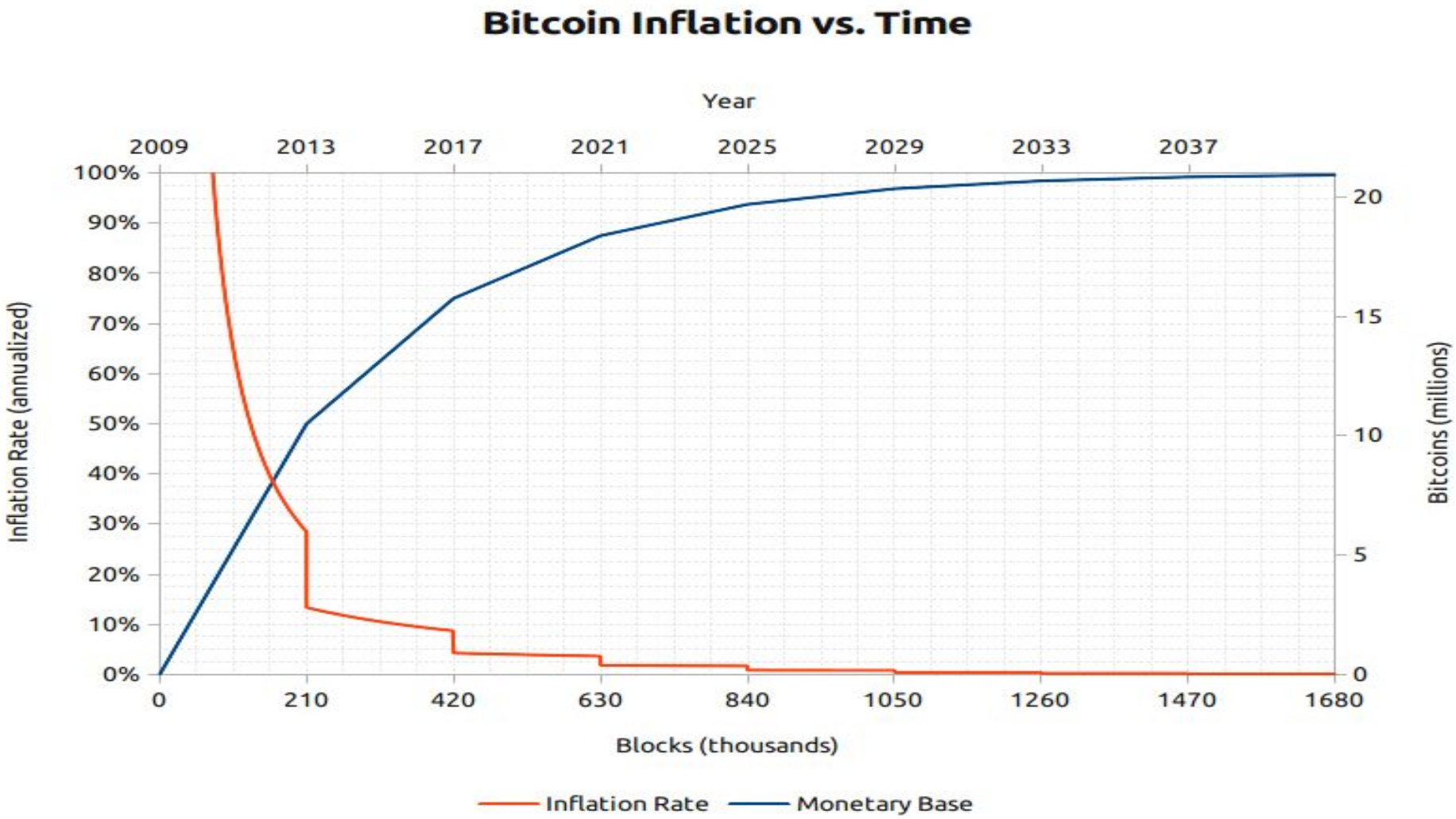
- Каждый блок ссылается на хэш предыдущего, так называемого "родительского" блока
- Последовательность хэшей, связывающих каждый блок с его родителем, создает цепочку
- Создает защищенный от взлома реестр; в сочетании с Proof-of-Work (т.е. затраты энергии для внесения изменений) гарантирует необратимость

Монетарная политика

Халвинг



- Каждые 210,000 блоков
- Эмиссия биткоинов уменьшается вдвое
- 2009-2012: 50 BTC за блок
- 2012-2016: 25 BTC за блок
- 2016-2020: 12.5 BTC за блок
- 2020-2024: 6.25 BTC за блок
- …

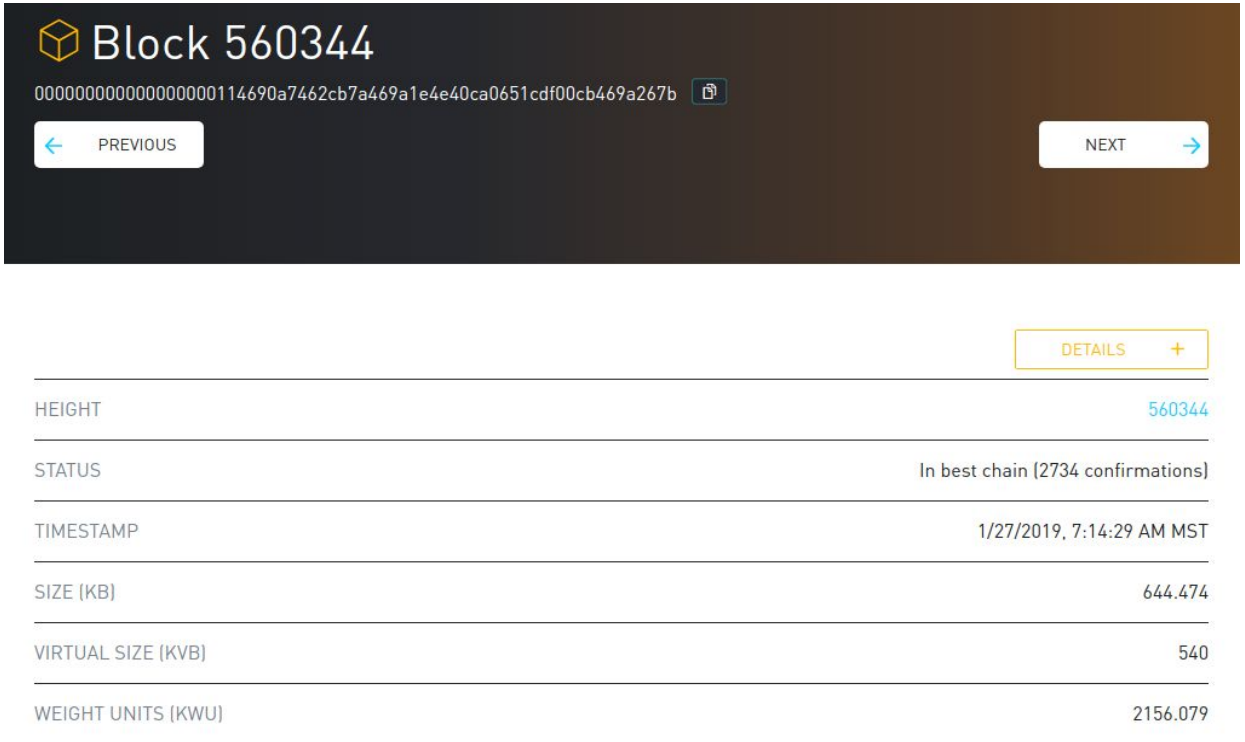

Bitcoin Inflation vs. Time
Year
2009
2013
2017
2021
2025
2029
2033
2037
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Inflation Rate (annualized)
20
15
10
5
0
Bitcoins (millions)
0
210
420
630
840
1050
1260
1470
1680
Blocks (thousands)
Inflation Rate
Monetary Base

Стимулы майнеров

В настоящее время майнеры получают два вида вознаграждения в обмен на обеспечение безопасности сети:

(1) новые монеты, появляющиеся с каждым блоком и
(2) комиссии за все транзакции, включенные в блок.

Транзакция Алисы на Биткоин-блокчейне



Browse: bit.ly/Block344

Транзакция Coinbase

e7522dcf9d53bb9136c5638a7657a10b08817b934490bdffaec19ec26521b42d

DETAILS +

#0 Coinbase

#0 1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB 12.57682767 BTC

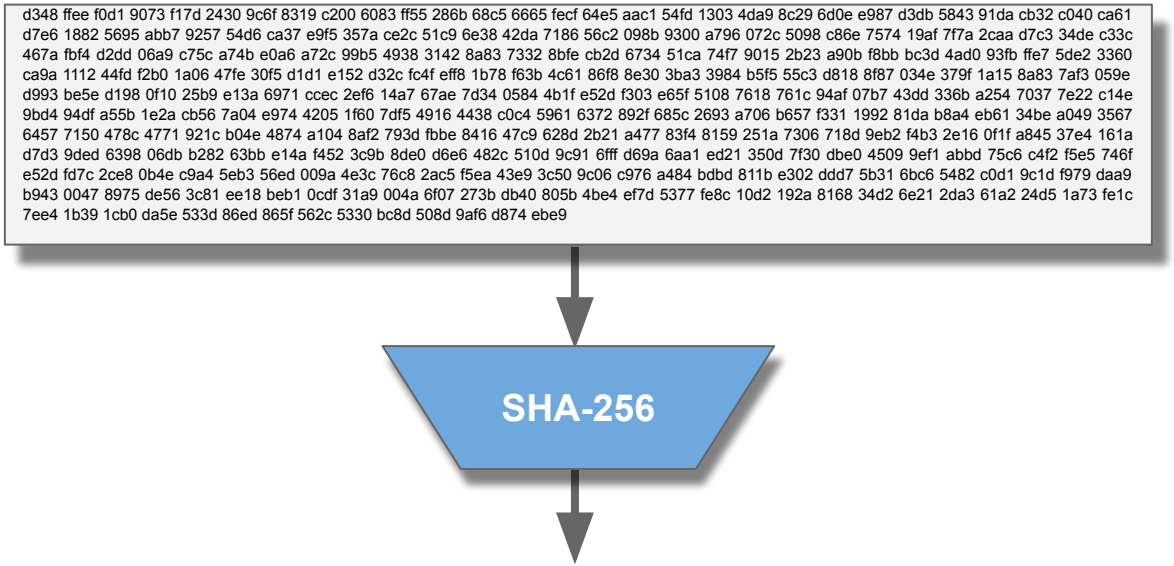
#1 OP_RETURN 0 BTC

12.57682767 BTC

Майнинг

Алгоритм SHA-256

Алгоритм хэширования: Сжатие любого количества информации в ограниченный по длине “отпечаток”.



Незначительное изменение при вводе
Большая разница при выводе

“I am Satoshi” => `ef2cdaa37271e1bea8e95b2b9ec15209f84e5eb3583449b4b4b8e7f2a18d72b9`

“I am Satoshi!” => `1da78803987e56886194d1e1b9ba8bfd216be4c607b0cfef7eeb05689871b8a7`

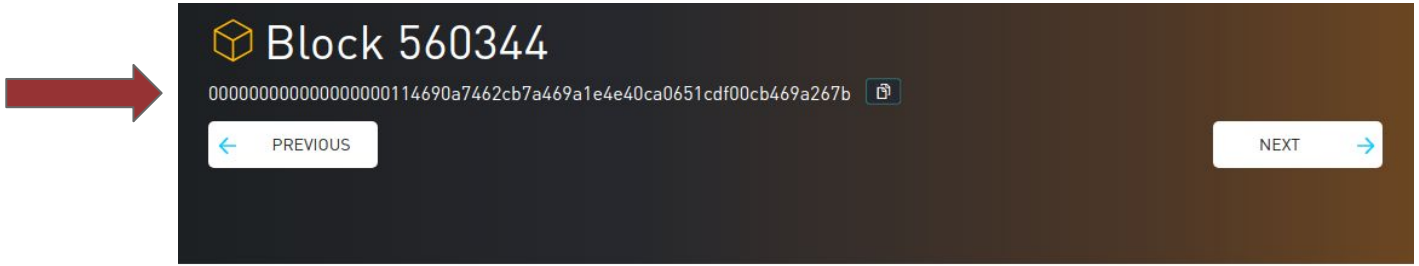
"I am Satoshi 0" => `972c421e91226b24a7a08b3099e3cebe893e5d111804d0f464f8cf472d09e1c9`
"I am Satoshi 1" => `7b1b1f24624ef8821c7fb6c95a4e0efeb4d68dac80953cdf903b3b77f086af4b`
"I am Satoshi 2" => `36c99755599d8b4bc21616c9e770c873885ad3fd4b2e4094abe9f19ce983d4cd`

Нацеленное хэширование

```
"I am Satoshi 0"          =>  972c421e91226b24a7a08b3099e3cebe893e5d111804d0f464f8cf472d09e1c9
"I am Satoshi 1"          =>  7b1b1f24624ef8821c7fb6c95a4e0efeb4d68dac80953cdf903b3b77f086af4b
"I am Satoshi 2"          =>  36c99755599d8b4bc21616c9e770c873885ad3fd4b2e4094abe9f19ce983d4cd
"I am Satoshi 3"          =>  a3a63c129e48e8874b4a31492436da50383cee7141d528cd1b02840e2d5a7e73
"I am Satoshi 15"         =>  0197a2cd275bf35803843b24f8260d8a842ae0a397e46bd4d8c81b9a8abe00e7
"I am Satoshi 34"         =>  0256b62b457a82abd81b4bb5039716f03a967997ca7e8bae9bddf13bbdb617a4
"I am Satoshi 35"         =>  0990b62dd5583aa77949353eb2e91e19a778f2ad5c69248b4d5c252db4576347
"I am Satoshi 48"         =>  0ba9d296d586e859eaa3f4edbde4b89e6bfcec349ea7747de6fb1451b6fd0733

"I am Satoshi 303"        =>  00696441ac9b9ec853eb288f3c33e31daddcc1857a88bcfe4efebb4b4385fd9d

"I am Satoshi 3485"       =>  0003ed2483cc7a0e192ca396ccb6cc3e2c962435da299001aa7f98f6bc6da5f2

"I am Satoshi 141789"     =>  0000d30318e5e56d9decc69ea6ca7059ac28966b8d95c95add9c08e538aa957d

"I am Satoshi 843944"     =>  000009a332e0ca596a776fd656ca9cb277cf84bd596dbf1fde6e25eddb740d31

"I am Satoshi 60994009"   =>  0000009a8895b9260a2f4dd5147f932acb64091ad28a3087b2e6f764f32d68af

"I am Satoshi 94203058"   =>  0000000013b2a9b2db111be18f7fbe4bd68cf0a885bce051c6ec6f260f446e46

"I am Satoshi 11116500145" =>  000000000bbe916434baf4521260f5ba1e860d9ccc16a7566eee03663bc12741
```

Майнинг-ферма

Хэш блока



DETAILS +

HEIGHT	560344
STATUS	In best chain (2734 confirmations)
TIMESTAMP	1/27/2019, 7:14:29 AM MST
SIZE (KB)	644.474
VIRTUAL SIZE (KVB)	540
WEIGHT UNITS (KWU)	2156.079

Browse: bit.ly/Block344

Спасибо за внимание!

CBP Prep Course

Find a study guide at cryptoconsortium.org

Q & A

Exercises

Используя блокчейн-обозреватель, изучите транзакции Алисы Бобу (bit.ly/**A**lice**T**x)

- Сколько входов и выходов у транзакции Алисы?
- Какой из выходов является сдачей? Как вы это определили?
- Сколько сдачи в BTC получила Алиса?
- Сколькиа сатоши равна сдача Алисы?

Кликните на вход транзакции Алсиы, чтобы открыть транзакцию Алисы с Биткоин-банкоматом

- Сколько у этой транзакции входов и выходов?
- Сколько милибит Алиса получила от банкомата?
- Какой был обменный курс на момент получения Алисой BTC в обмен на 80 евро?

Ответы

- У транзакции Алисы _____ вход(а/ов) и _____ выход(а/ов)
- Выход номер ___ является сдачей
- Алиса получила _____ сдачи в BTC
- Алиса получила _____ сдачи в сатах
- У транзакции с банкоматом _____ вход(а/ов) и _____ выход(а/ов)
- Алиса получила _____ милибит от банкомата
- Обменный курс на момент покупки биткоинов был 1 BTC = _____ EUR

Ответы

- У транзакции Алисы **1** вход и **2** выхода
- Выход номер **2** является сдачей
- Алиса получила **0.0155808** BTC в качестве сдачи
- Алиса получила **1,558,080** сатоши в качестве сдачи
- У транзакции с банкоматом **1** вход и **2** выхода
- Алиса получила **26.845** милибит от банкомата
- Обменный курс на момент покупки биткоинов был **1 BTC = 2980.07 EUR**

Продвинутый уровень

- Сколько входов содержит платеж Боба в адрес Каталины?
- Какую комиссию заплатил Боб за эту транзакцию?
- Какой блок содержал платеж Боба в пользу Каталины (1 подтверждение)?
- Сколько времени потребовалось, чтобы эта транзакция получила 6 подтверждений?
- Сколько других транзакций было в том же блоке, что и платеж Боба Каталине?
- Какая сумма была выплачена майнеру в coinbase-транзакции блока, содержащего платеж Боба Каталине?
- Каков был хэш этого блока?
- Сколько нулей (в шестнадцатеричном формате) в начале хэша этого блока?
- Какова была сумма субсидии блока и сколько составляли комиссии в этом блоке?