



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

Ключи и адреса

Основы майнинга

Единицы и эмиссия

Обозреватели блоков

Консенсус

**Монетарные
характеристики**

Ценообразование и рынки

Основы транзакций

**Комиссии и
подтверждения**

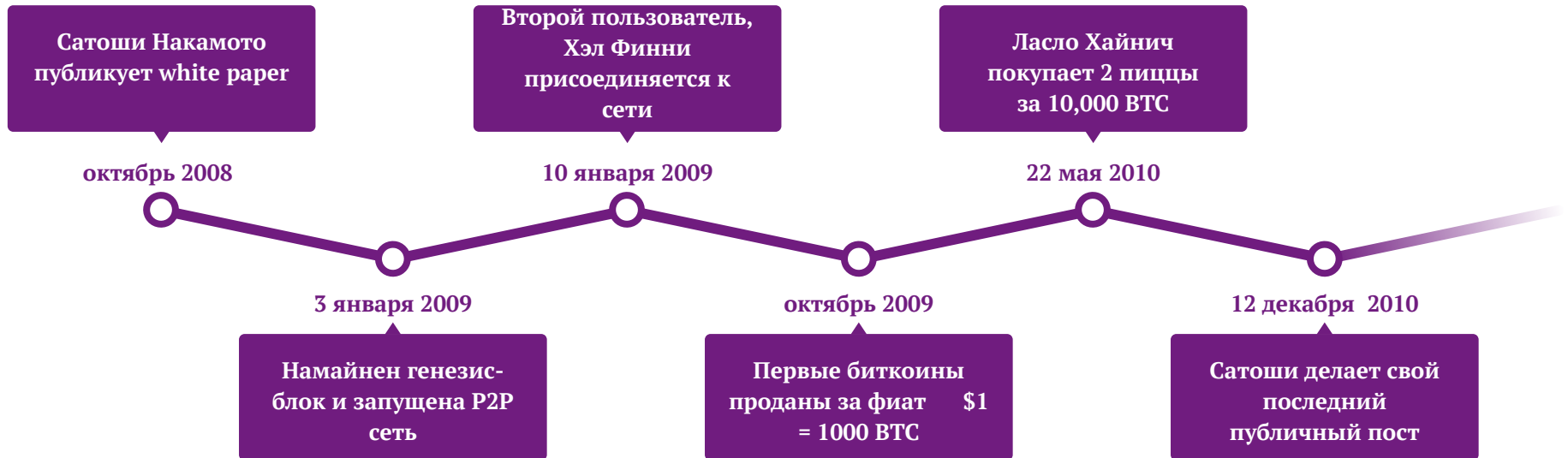
ВНИМАНИЕ

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.

История Биткойна и Что такое Биткойн

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.



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

Алиса покупает биткойны в Биткойн- банкомате

Как получить 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



Биткоин-банкомат

Алиса использует наличные для покупки биткоина в
биткоин-банкомате



Алиса



Биткоин-банкомат





=

? BTC

*Сколько биткоинов можно
купить на 80 евро?*

“Цена” биткоина

(1BTC = 3640.08 USD)

฿ 1



(1 USD = 0.0002 BTC)

\$ 3640.08

USD ▼

Обратите внимание на: bitcoinaverage.com

Bitfinex - \$ 3715.3

▼ \$ -8.7

GDAX - \$ 3618.79

▼ \$ -1.45

Bitstamp - \$ 3616.79

▼ \$ -3.29

Kraken - \$ 3616.2

▼ \$ -6.7

Ценообразование и рынки



Книга ордеров: Сотни ордеров на различных
ценовых уровнях

Биткоин-банкомат рассчитывает обменный курс



€80

Как Алиса
получает BTC?

1 BTC $\approx$ €3,000



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



37LRvHjJdhdeEergQEJEduREAtuRBF8dLL7

*Алиса показывает свой Биткоин-
адрес банкомату*

Алиса покупает биткоин в банкомате



Биткоин-транзакция

Биткоин-банкомат

37LRvHjJdhdEergQEJEduREAtuRBF8dLL7

Сумма: 0.026845 BTC
(2,684,500 satoshi)

*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

Алиса покупает книгу в интернет-магазине Боба





Кошелек Алисы создает транзакцию

Send

X

0.01123458

BTC

\$39.73

bc1qz3a8nqtl47s7svev2ez2adlk

Scan

Book from Bob store

Fee

12 sat/b

C

←

Confirm

0.01123458

BTC

Fee: 0.00002962 BTC (\$0.10)

To

bc1qz3a8nqtl47s7svev2ez2adldasy6rrd5s6suqg

Send now

Transaction details

0.01123458

BTC

Fee: 2962 sats

✓

Done

Основы транзакций



Основы транзакций



Транзакции и сдача

0.026845 BTC

Бобу: 0.01123458 BTC

Алисе: 0.0155808 BTC

Транзакция алисы в блокчейне

e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c

DETAILS +

9d193bb04ef3f8c814253bbbc49031ab3023436a5 0.026845 BTC
53413f45aaaf32392df4756:0



bc1qz3a8nqtl47s7svev2ez2adldasy6rrd5s6suqq 0.01123458 BTC

3BEMpEoah9bPFebVSFNuC7LNI DTXjcrTnM 0.0155808 BTC

1309 CONFIRMATIONS 0.02681538 BTC

Найти транзакцию можно по ссылке (чувствительно к регистру):
bit.ly/AliceTx

Итог первой части

Мы узнали о:

- История Биткойна
- Ключи и адреса
- Рынки, биржи, ценообразование биткойна
- 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

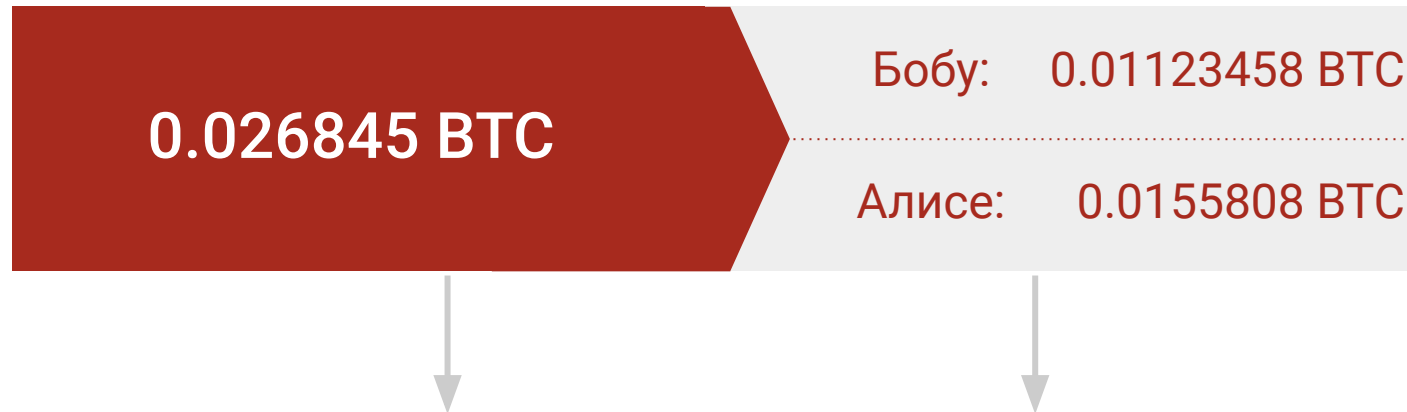
Алиса покупает книгу в интернет-магазине Боба

(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?

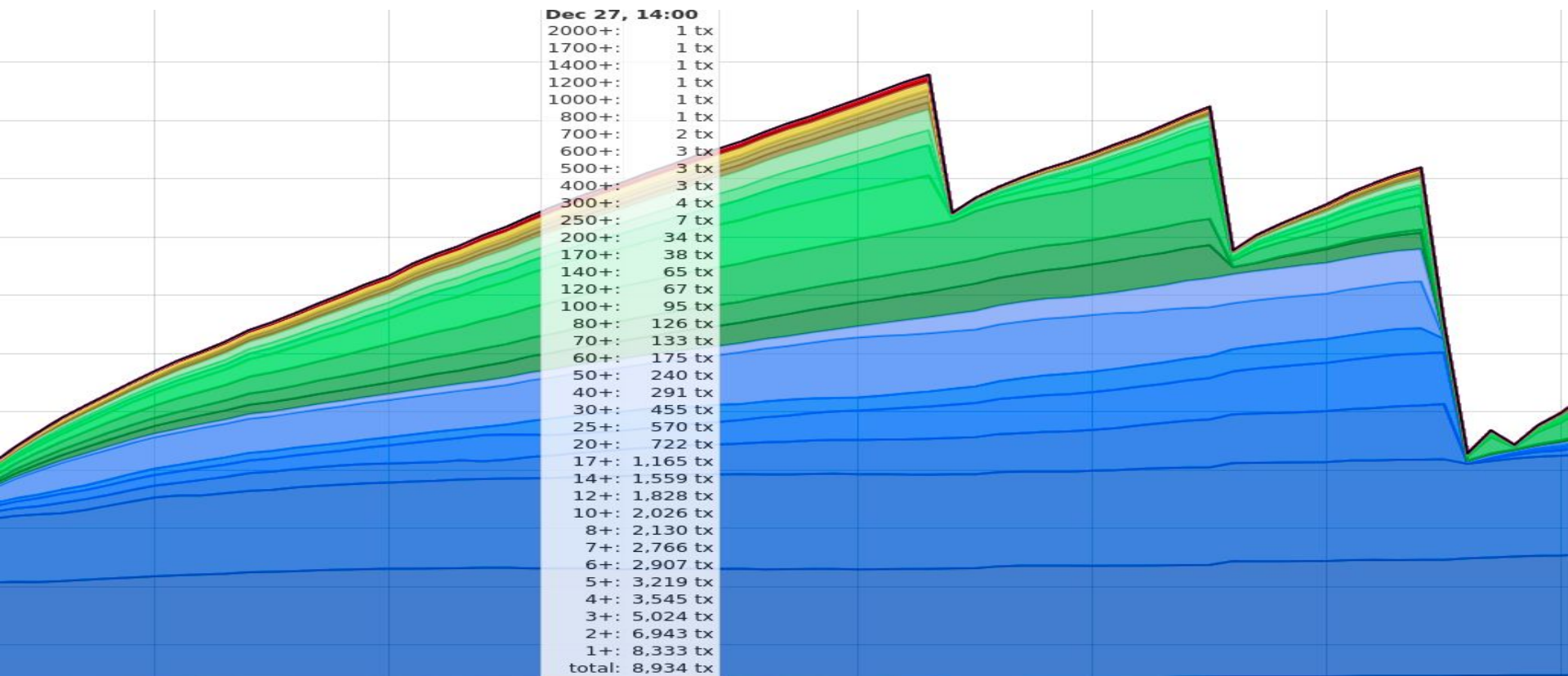
- Свободное место для транзакций ограничено
- Комиссии определяют насколько каждый ценит свою транзакцию
- Комиссии стимулируют майнинг по мере того, как эмиссия замедляется

Комиссии статичны или они меняются?

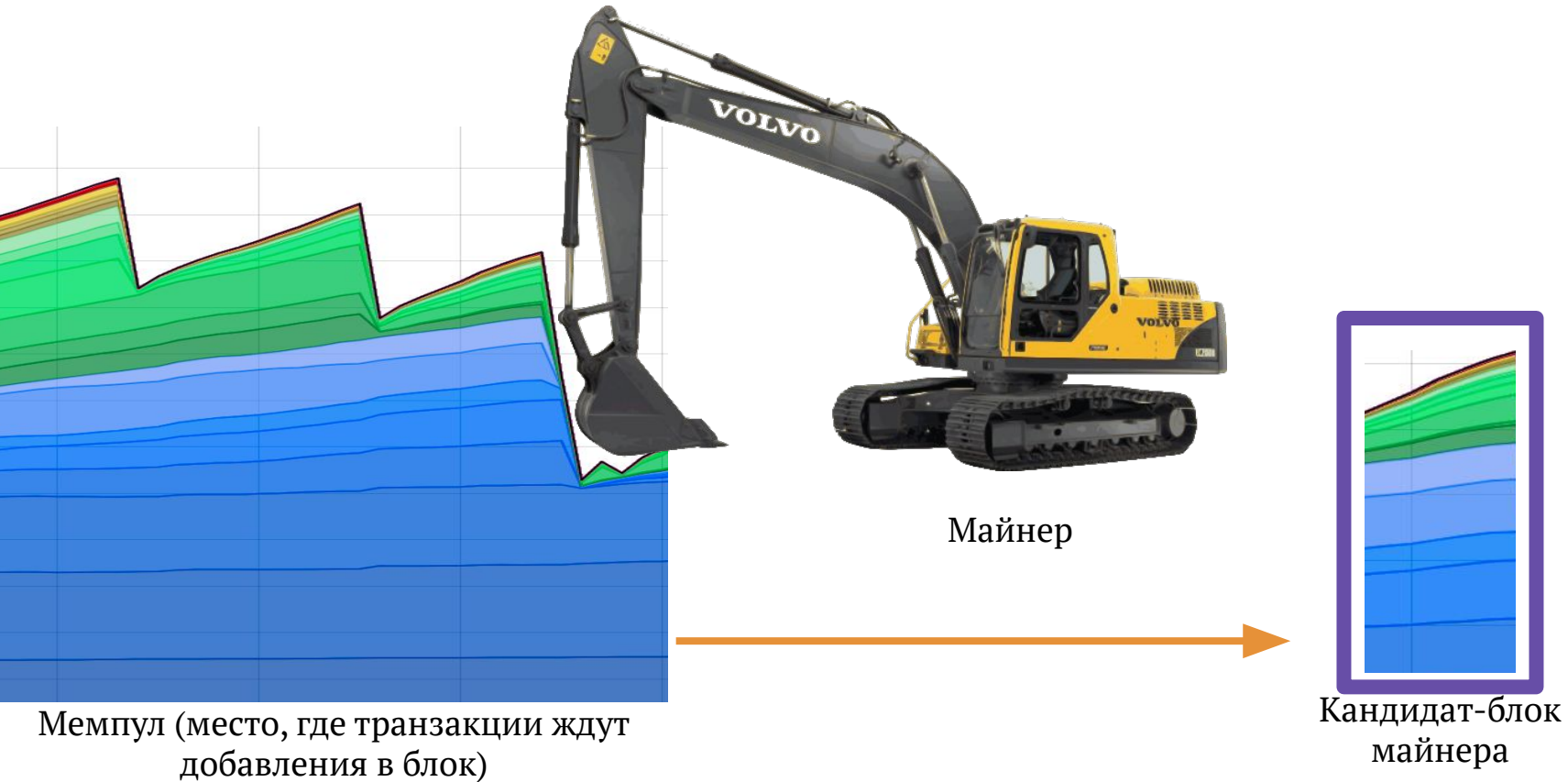
- Какова минимальная возможная комиссия?

Как комиссии влияют на скорость подтверждения транзакции?

Комиссии



Майнеры добавляют транзакции в блоки





Browse: bit.ly/Block344

[illegible]

[← PREVIOUS](#)

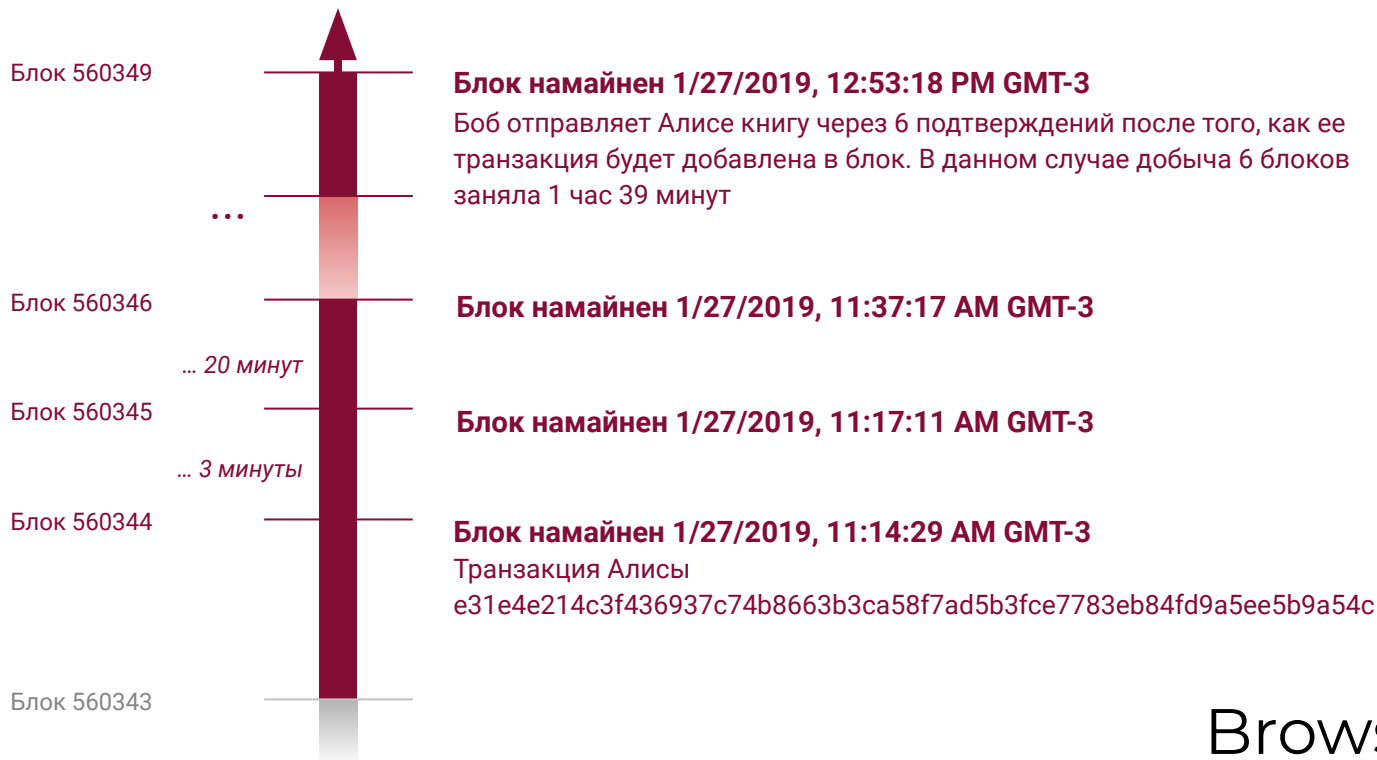
NEXT

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



Browse:
bit.ly/Block344

Таймлайн транзакции Алисы

Кошелек Алисы

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

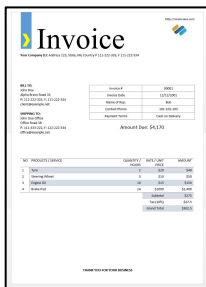
Майнер

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



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

Варианты оплаты



10000	=	262.03
Argentine Peso (ARS) ▼		US Dollar (USD) ▼

Международный перевод (банк)

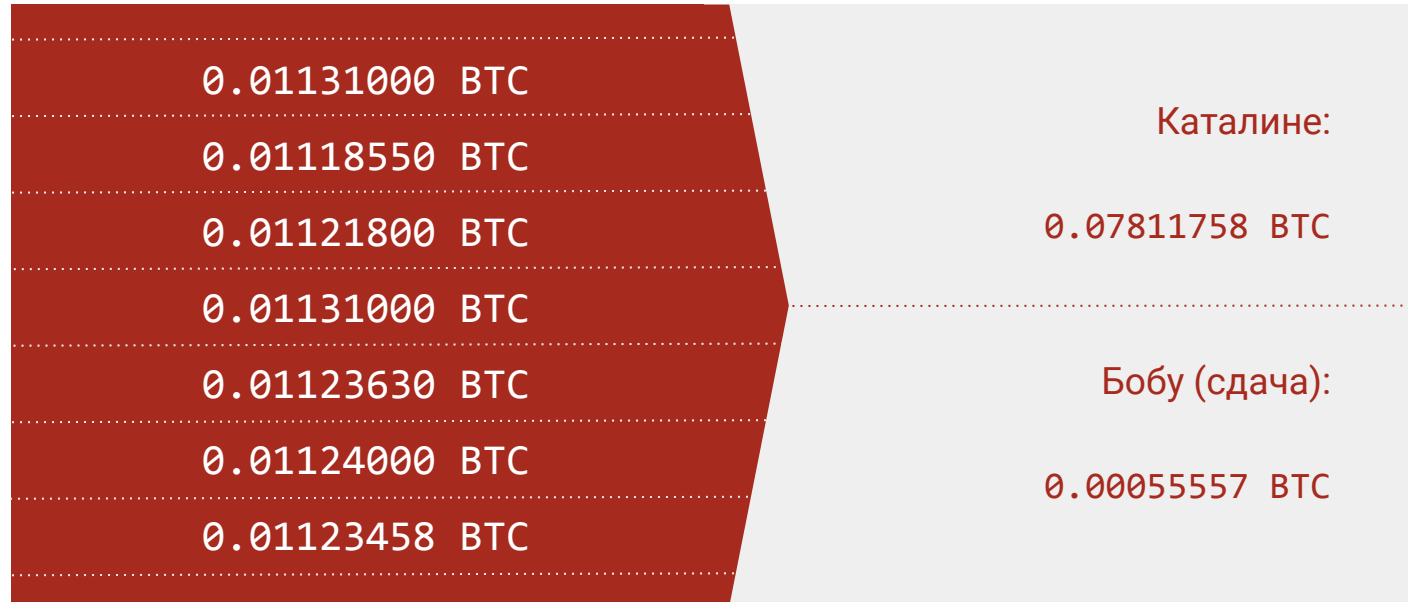
Western Union

Чек?

БИТКОИН



Создание транзакции



Боб платит Каталине 0.07811758 BTC

Создание транзакции

594eaf1d35485052a474671257824402a197acf6f5b60eec8ca8ab4f782f35bd

DETAILS



#0 167e5eaa33aae339eb505a2ae9caf8f5bc2440c20 0.01131 BTC
b9361b97dd64028674a5307:0

#1 4b49d186798dd5af21dc022e7c7b286910273eddf 0.0111855 BTC
3bb2fe90c29920e07888441:0

#2 4cc658691f994243dd66962e30b6fba60d8049ed8 0.011218 BTC
2e3102f1c469111aca0a948:0

#3 8a299633fb4e31b8e88d4e5de412721a32a736e9 0.01131 BTC
cbe97d5991900733728f445:0

#4 a4fffa9775bb1e36c77f6ddf2b0700b2920e39861d 0.0112363 BTC
65c3a4ec72ba84ae3cbd4c:0

#5 c757c0dfe15afdca7c1c34a12c1fe487909bf53811e 0.01124 BTC
73a56301e5ed41a2a70a0:0

#6 e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce 0.01123458 BTC
7783eb84fd9a5ee5b9a54c:0



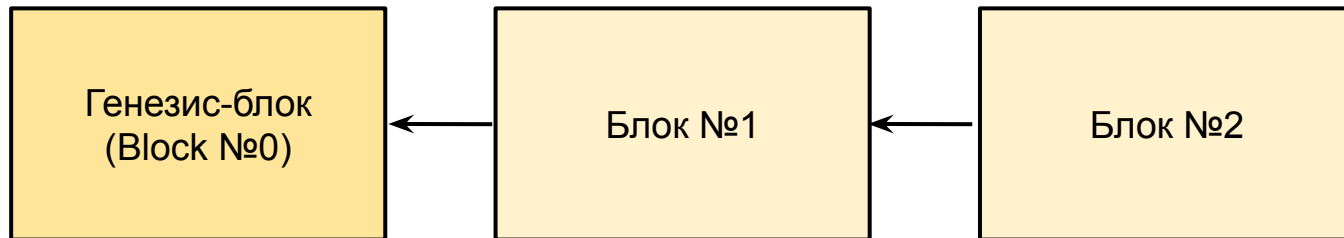
#0 bc1qrijtkkammhxvheuuamp3fhqpfjr57df27te4tv8 0.00055557 BTC

#1 3744SUMMtUD5jDz83TCk2NUP9FsVW8tcLZ 0.07811758 BTC

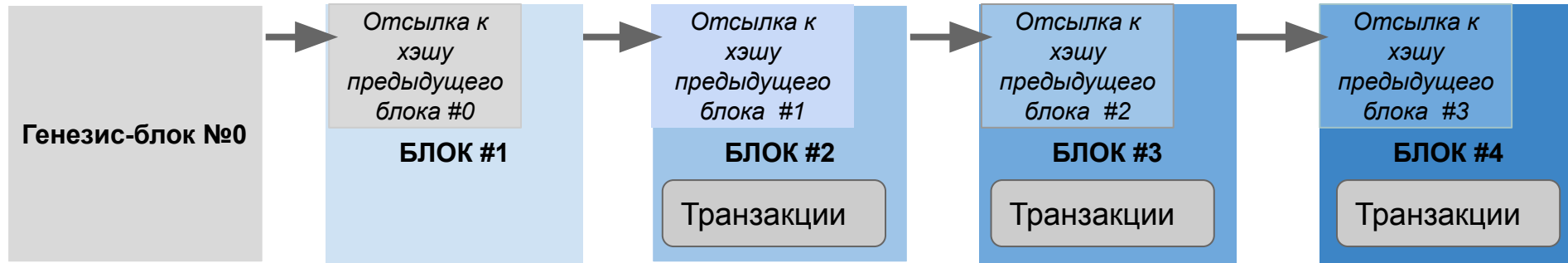
Боб платит Каталине 0.07811758 BTC

Блокчейн

История Биткоин-блокчейна

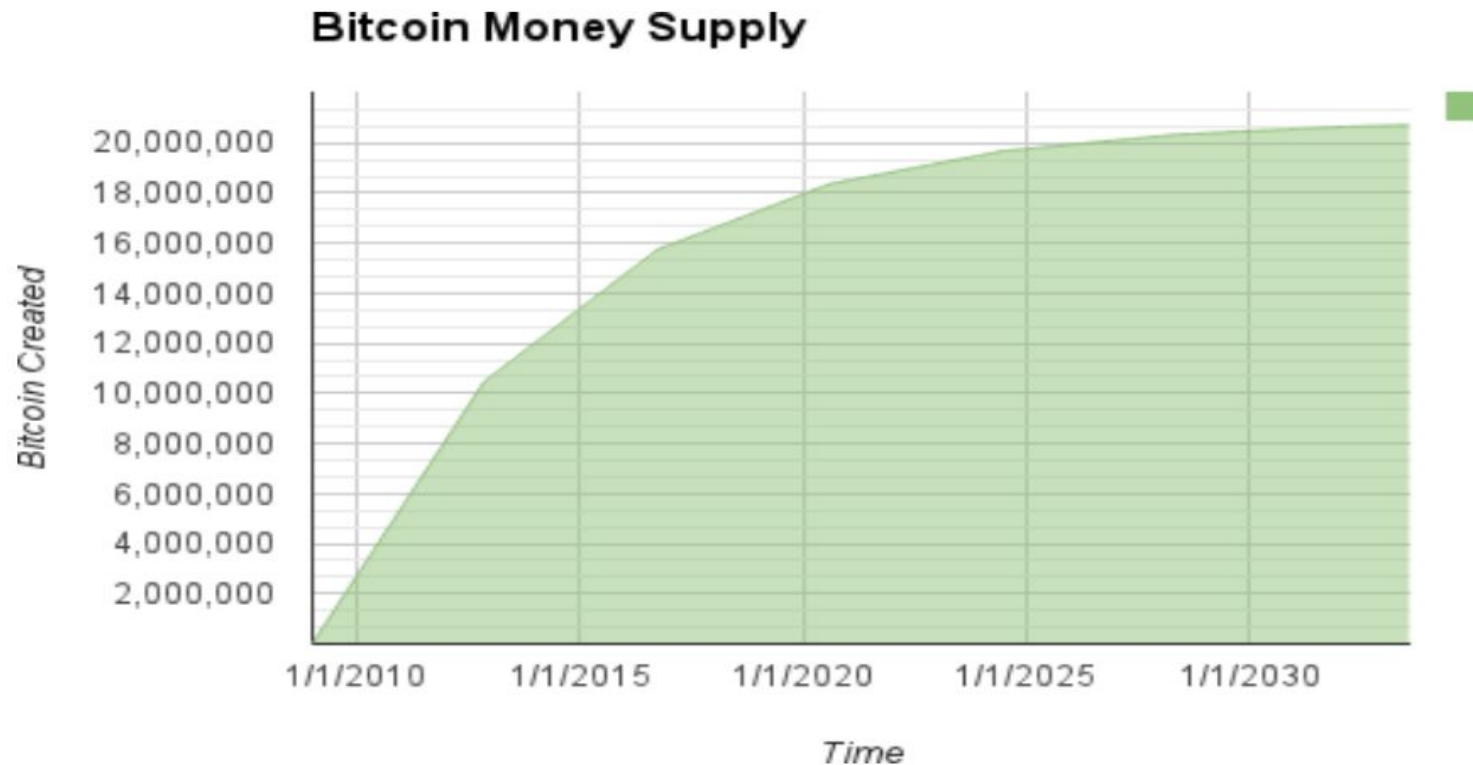


Цепь блоков

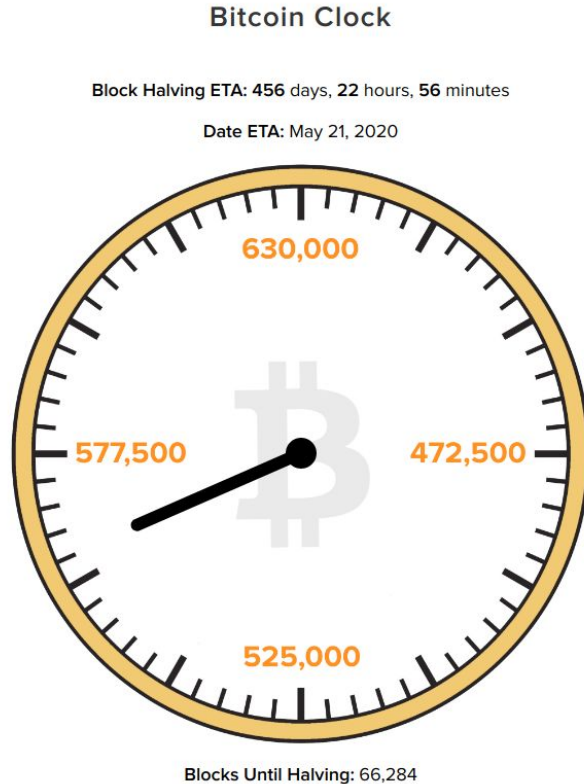


- Каждый блок ссылается на хэш предыдущего, так называемого "родительского" блока
- Последовательность хэшей, связывающих каждый блок с его родителем, создает цепочку
- Создает защищенный от взлома реестр; в сочетании с Proof-of-Work (т.е. затраты энергии для внесения изменений) гарантирует необратимость

Монетарная политика

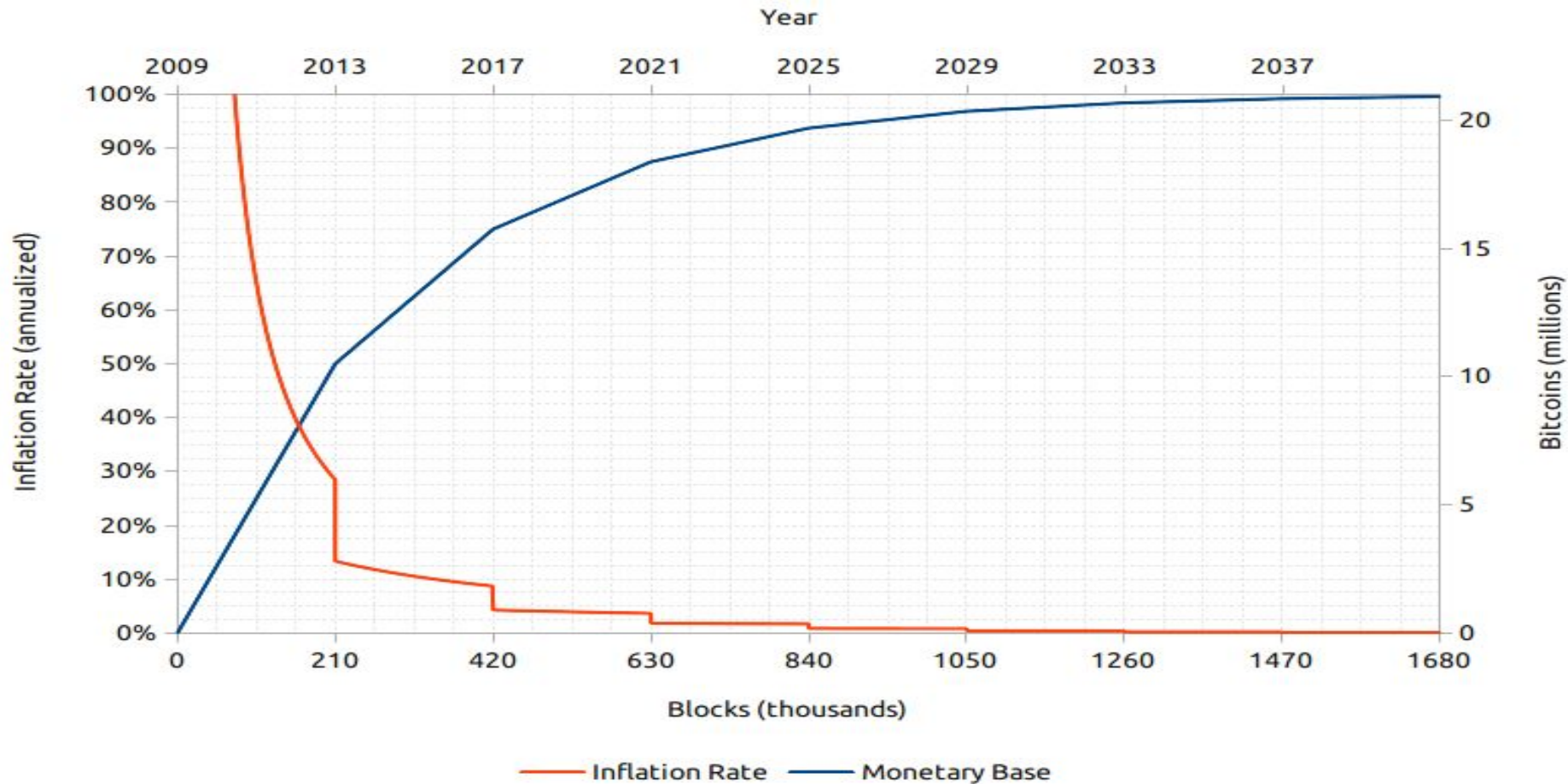


Халвинг



- 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



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.

`000000000000000000000000114690a7462cb7a469a1e4e40ca0651cdf00cb469a267b`

[← PREVIOUS](#)

NEXT

DETAILS

+

560344

In best chain (2734 confirmations)

1/27/2019, 7:14:29 AM MST

644.474

540

2156.079

Browse: bit.ly/Block344

Транзакция Coinbase

e7522dcf9d53bb9136c5638a7657a10b08817b934490bdffaec19ec26521b42d

DETAILS



#0 Coinbase



#0 1Nh7uHdvY6fNwtQtM1G5EZAFLC33B59rB

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”.

```
d348 fee f0d1 9073 f17d 2430 9c6f 8319 c200 6083 ff55 286b 68c5 6665 fecf 64e5 aac1 54fd 1303 4da9 8c29 6d0e e987 d3db 5843 91da cb32 c040 ca61  
d7e6 1882 5695 abb7 9257 54d6 ca37 e9f5 357a ce2c 51c9 6e38 42da 7186 56c2 098b 9300 a796 072c 5098 c86e 7574 19af 7f7a 2caa d7c3 34de c33c  
467a fb4d d2dd 06a9 c75c a74b e0a6 a72c 99b5 4938 3142 8a83 7332 b8fe cb2d 6734 51ca 74f7 9015 2b23 a90b f8bb bc3d 4ad0 93fb ffe7 5de2 3360  
ca9a 1112 44fd f2b0 1a06 47fe 30f5 d1d1 e152 d32c fc4f eff8 1b78 f63b 4c61 86f8 8e30 3ba3 3984 b5f5 55c3 d818 8f87 034e 379f 1a15 8a83 7af3 059e  
d993 be5e d198 0f10 25b9 e13a 6971 ccec 2ef6 14a7 67ae 7d34 0584 4b1f e52d f303 e65f 5108 7618 761c 94af 07b7 43dd 336b a254 7037 7e22 c14e  
9bd4 94df a55b 1e2a cb56 7a04 e974 4205 1f60 7df5 4916 4438 c0c4 5961 6372 892f 685c 2693 a706 b657 f331 1992 81da b8a4 eb61 34be a049 3567  
6457 7150 478c 4771 921c b04e 4874 a104 8af2 793d fbbe 8416 47c9 628d 2b21 a477 83f4 8159 251a 7306 718d 9eb2 f4b3 2e16 0f1f a845 37e4 161a  
d7d3 9ded 6398 06db b282 63bb e14a f452 3c9b 8de0 d6e6 482c 510d 9c91 6fff d69a 6aa1 ed21 350d 7f30 dbe0 4509 9ef1 abbd 75c6 c4f2 f5e5 746f  
e52d fd7c 2ce8 0b4e c9a4 5eb3 56ed 009a 4e3c 76c8 2ac5 f5ea 43e9 3c50 9c06 c976 a484 bdbd 811b e302 ddd7 5b31 6bc6 5482 c0d1 9c1d f979 daa9  
b943 0047 8975 de56 3c81 ee18 beb1 0cdf 31a9 004a 6f07 273b db40 805b 4be4 ef7d 5377 fe8c 10d2 192a 8168 34d2 6e21 2da3 61a2 24d5 1a73 fe1c  
7ee4 1b39 1cb0 da5e 533d 86ed 865f 562c 5330 bc8d 508d 9af6 d874 ebe9
```

SHA-256

e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c

256 bits

Незначительное изменение при вводе Большая разница при выводе

Переведено проектом
21ideas.org

“I am Satoshi” => ef2cdaa37271e1bea8e95b2b9ec15209f84e5eb3583449b4b4b8e7f2a18d72b9

“I am Satoshi!” => 1da78803987e56886194d1e1b9ba8bfd216be4c607b0cfef7eeb05689871b8a7

"I am Satoshi 0" => 972c421e91226b24a7a08b3099e3cebe893e5d111804d0f464f8cf472d09e1c9

"I am Satoshi 1" => 7b1b1f24624ef8821c7fb6c95a4e0efeb4d68dac80953cdf903b3b77f086af4b

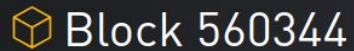
"I am Satoshi 2" => 36c99755599d8b4bc21616c9e770c873885ad3fd4b2e4094abe9f19ce983d4cd

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"	=>	00696441ac9b9ec853eb288f3c33e31daddcc1857a88bcfe4efebbb4b4385fd9d
"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





[← PREVIOUS](#)

NEXT

DETAILS

+

560344

In best chain (2734 confirmations)

1/27/2019, 7:14:29 AM MST

644.474

540

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/AliceTx)

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

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

- ☐ Сколько у этой транзакции входов и выходов?
- ☐ Сколько миллибит 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 _____ миллибит 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** миллибит 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?