CBP Prep Course (overview)

by Andreas M. Antonopoulos

Download these slides: bit.ly/aantonopworkshop

Course Contents

During the course we’ll discuss all of these topics (and more):

History of Bitcoin

Units & Issuance

Monetary Characteristics

Transaction Basics

Keys & Addresses

Blockchain Explorers

Price Discovery & Markets

Transaction Fees & Confirmations

Basics of Mining

Consensus

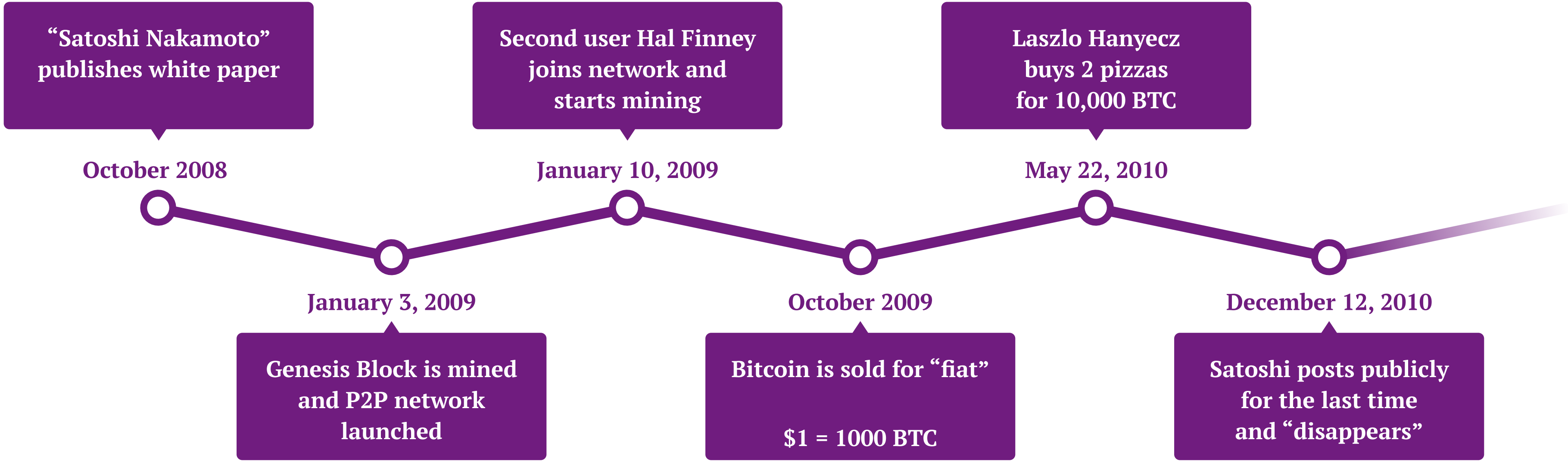
WARNING

Do not send bitcoin to the addresses in these slides.
These addresses are only for display purposes.
Any bitcoin sent to them will be **LOST**

If you want to test, send small amounts of bitcoin to a colleague's wallet

History of Bitcoin & What is Bitcoin

History of Bitcoin
The first “steps”



October 2008

“Satoshi Nakamoto” publishes white paper

January 3, 2009

Genesis Block is mined and P2P network launched

January 10, 2009

Second user Hal Finney joins network and starts mining

October 2009

Bitcoin is sold for “fiat”

$1 = 1000 BTC

May 22, 2010

Laszlo Hanyecz buys 2 pizzas for 10,000 BTC

December 12, 2010

Satoshi posts publicly for the last time and “disappears”

Bitcoin / bitcoin / blockchain

Bitcoin

A protocol for a decentralized peer-to-peer network that creates consensus without needing a central authority to provide trust.

bitcoin

The currency (token) issued as a reward in the proof-of-work mining process.

blockchain

The public ledger where the network records (transactions) are written.

User Stories

Storyline

Alice

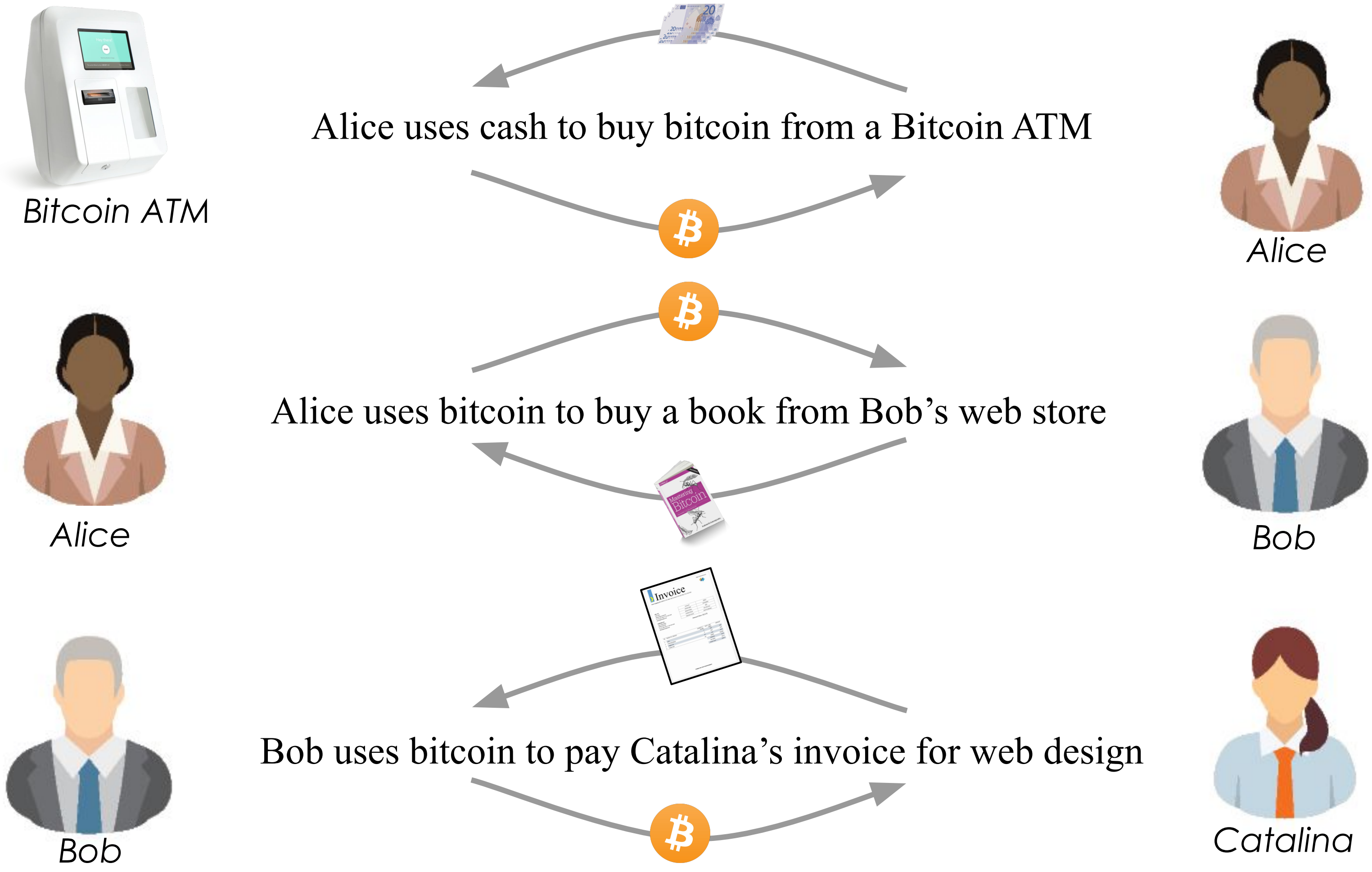
Bob

Catalina

Alice lives in Europe and she’s fairly new to bitcoin. In this course, we’ll see Alice purchase her first bitcoin and use that bitcoin to buy a book from a US bookseller.

Bob lives in the US and runs an online bookstore. He has a lot of customers outside of the US and he accepts many currencies for payment, including bitcoin.

Catalina is an Argentinian web developer with clients all around the world. Bob is one of her clients.



Bitcoin ATM

Alice uses cash to buy bitcoin from a Bitcoin ATM

Alice

Alice

Alice uses bitcoin to buy a book from Bob's web store

Bob

Bob

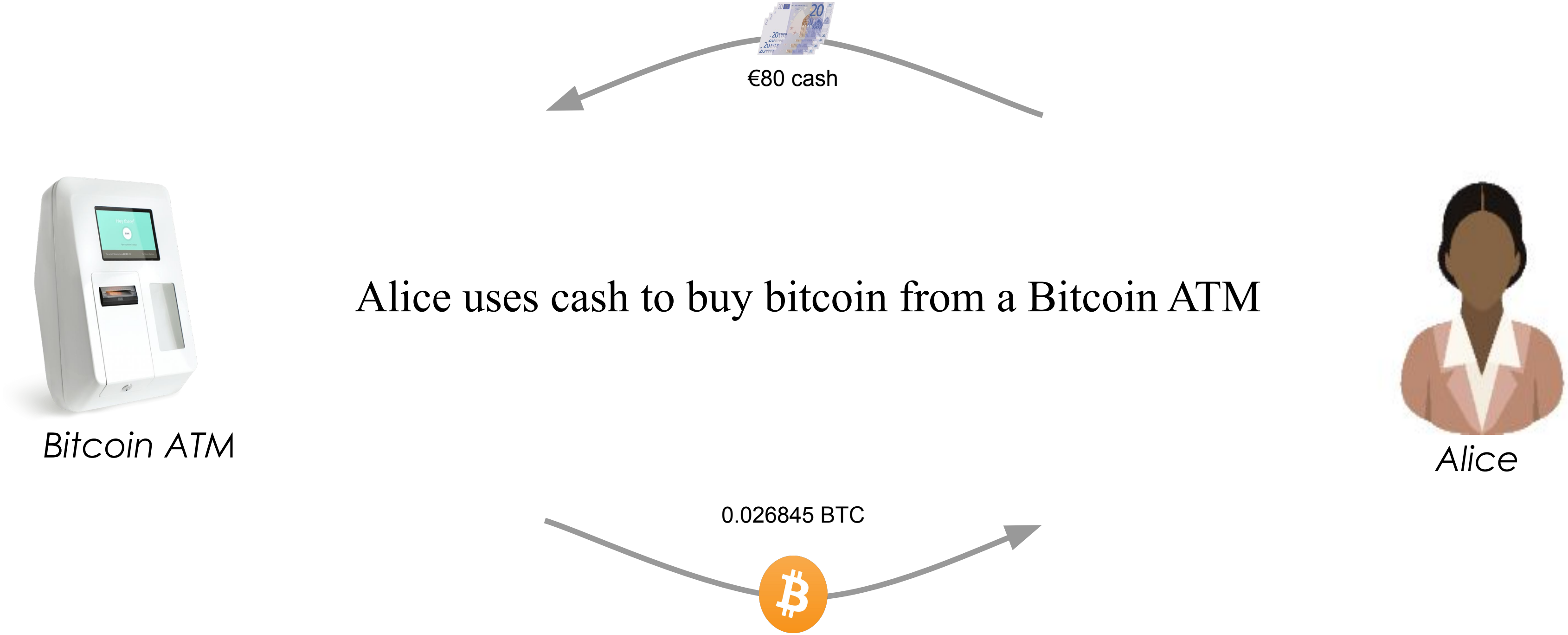
Bob uses bitcoin to pay Catalina's invoice for web design

Catalina

Alice buys bitcoin from a Bitcoin ATM

How do people acquire bitcoin?

- **Earn - Get paid in bitcoin**
    - □ Offer a service - cut hair, wash cars, drive taxi
    - □ Sell a product - homemade baklava, gourmet coffee, keychains
    - □ Wages - ask your employer to pay part of your wages in bitcoin - bitwage.com
- **Buy - Exchange national money (fiat) for bitcoin.**
    - □ From an exchange - a company offering a service for buying and selling bitcoin
    - □ From a bitcoin ATM - a vending machine selling bitcoin for cash
    - □ From another person directly, for cash - find them at a meetup or a site like localbitcoin.com
- **Trade - Trade your belongings for bitcoin**
    - □ Sell your car for bitcoin
    - □ Sell your house for bitcoin



€80 cash

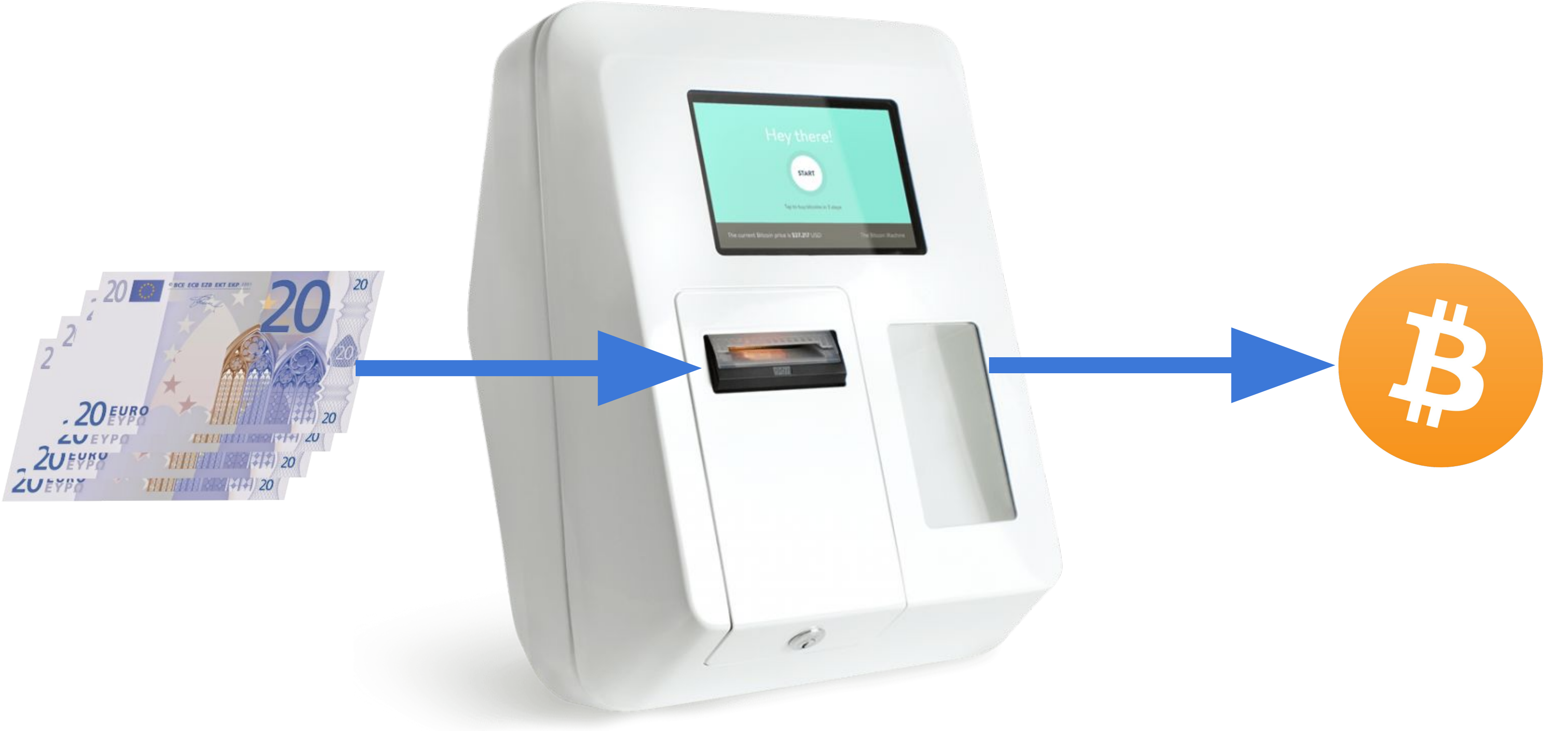
Alice uses cash to buy bitcoin from a Bitcoin ATM

Bitcoin ATM

Alice

0.026845 BTC

Bitcoin ATM Vending Machine

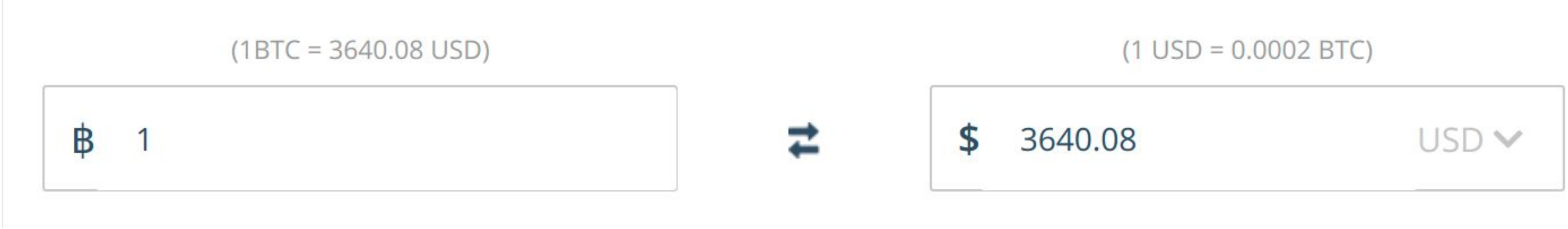


=

? BTC

How much bitcoin does 80 EUR buy?

Bitcoin’s “Price”



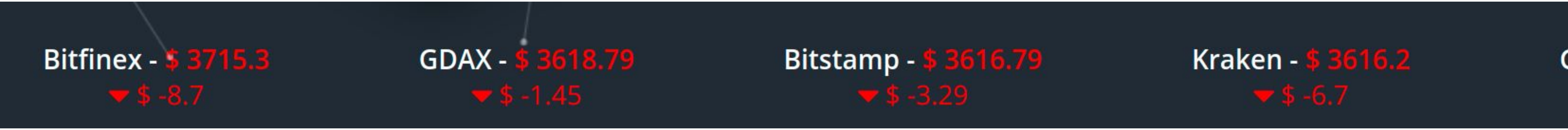
(1BTC = 3640.08 USD)

(1 USD = 0.0002 BTC)

฿ 1

$ 3640.08 USD

See: bitcoinaverage.com



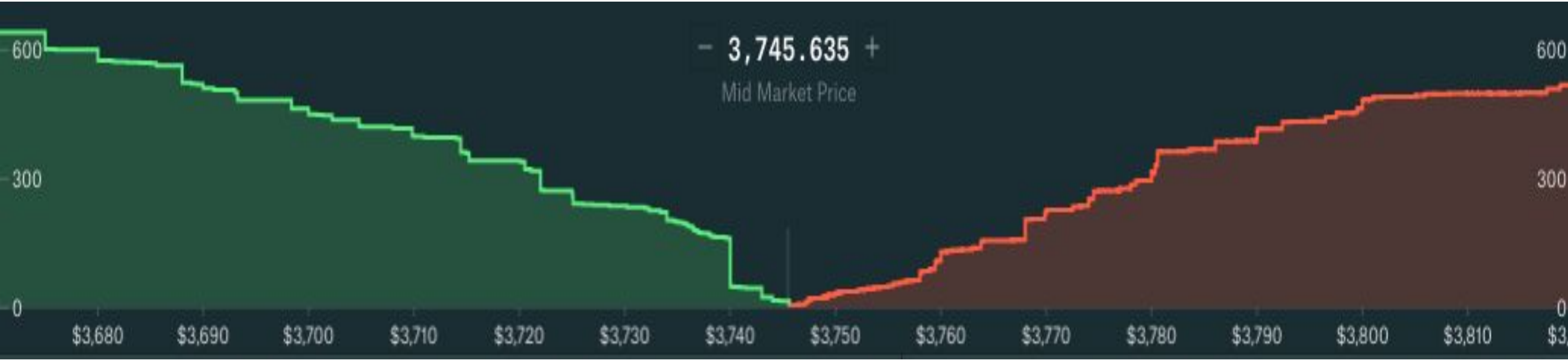
Bitfinex - $ 3715.3
▼ $ -8.7

GDAX - $ 3618.79
▼ $ -1.45

Bitstamp - $ 3616.79
▼ $ -3.29

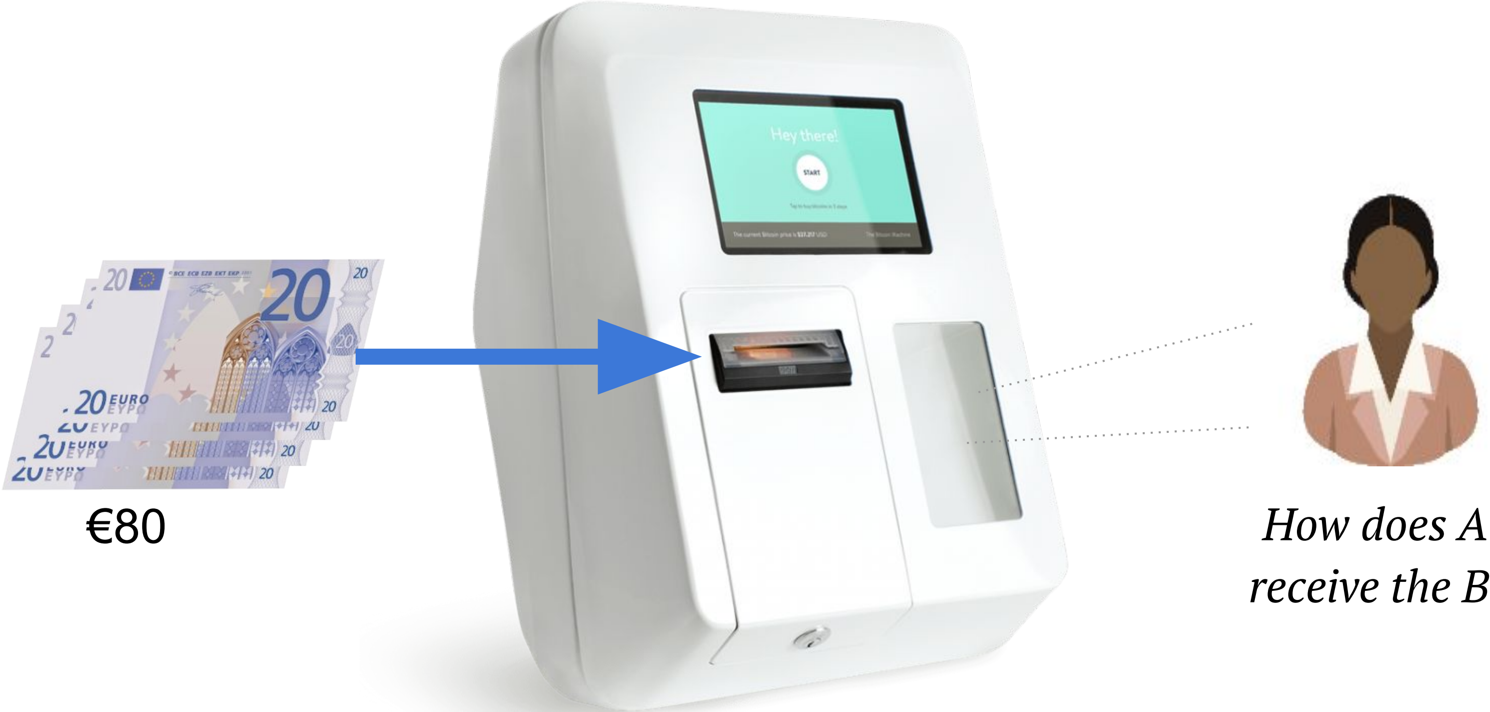
Kraken - $ 3616.2
▼ $ -6.7

Price Discovery and Markets



Order Book: Hundreds of orders at different prices

Bitcoin ATM calculates the exchange rate



€80

1 BTC ≅ €3,000

How does Alice receive the BTC?

Bitcoin
A public deposit box

Anyone can deposit

Private Key

Like a very long PIN,
only the owner can unlock

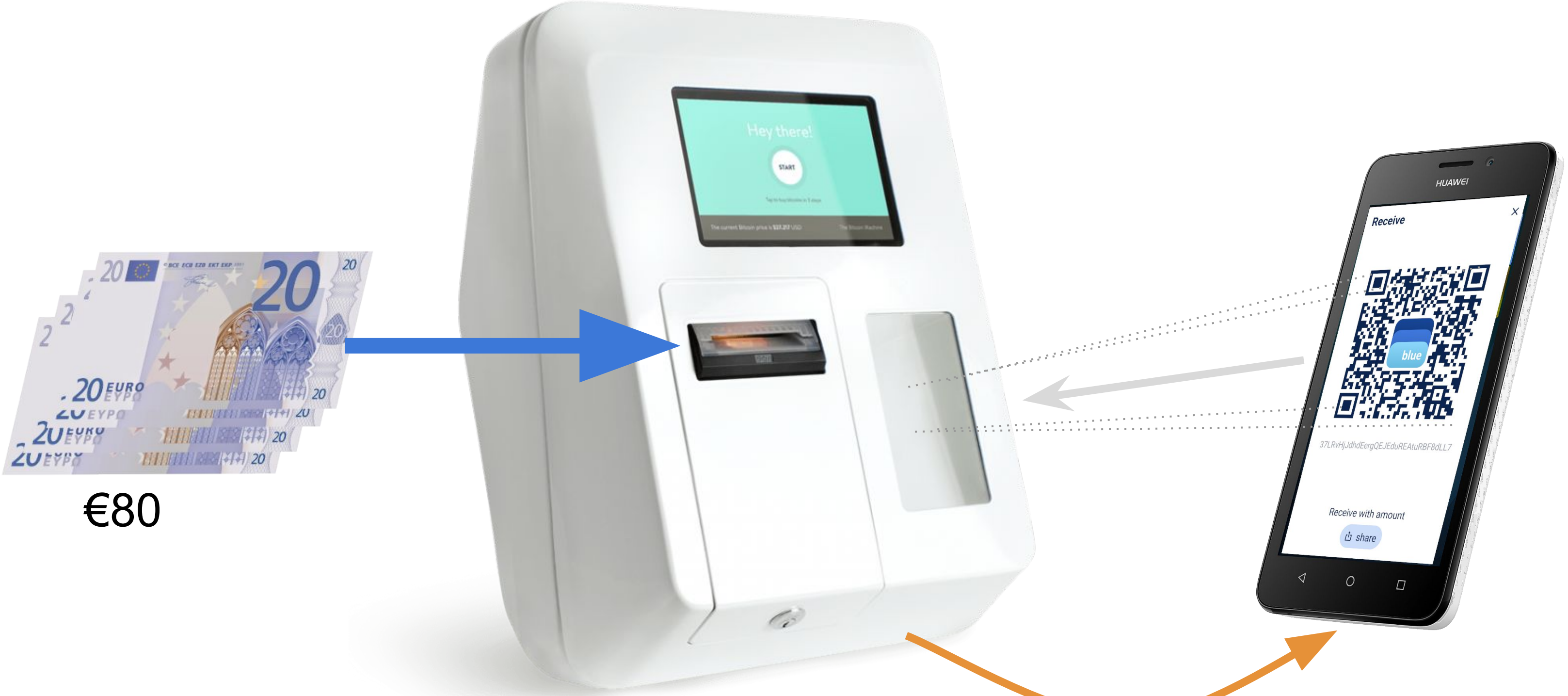
A Bitcoin Address

Used to identify where
to deposit the payment

37LRvHjJdhdEergQEJEduREAtuRBF8dLL7

Alice shows a bitcoin address to the ATM

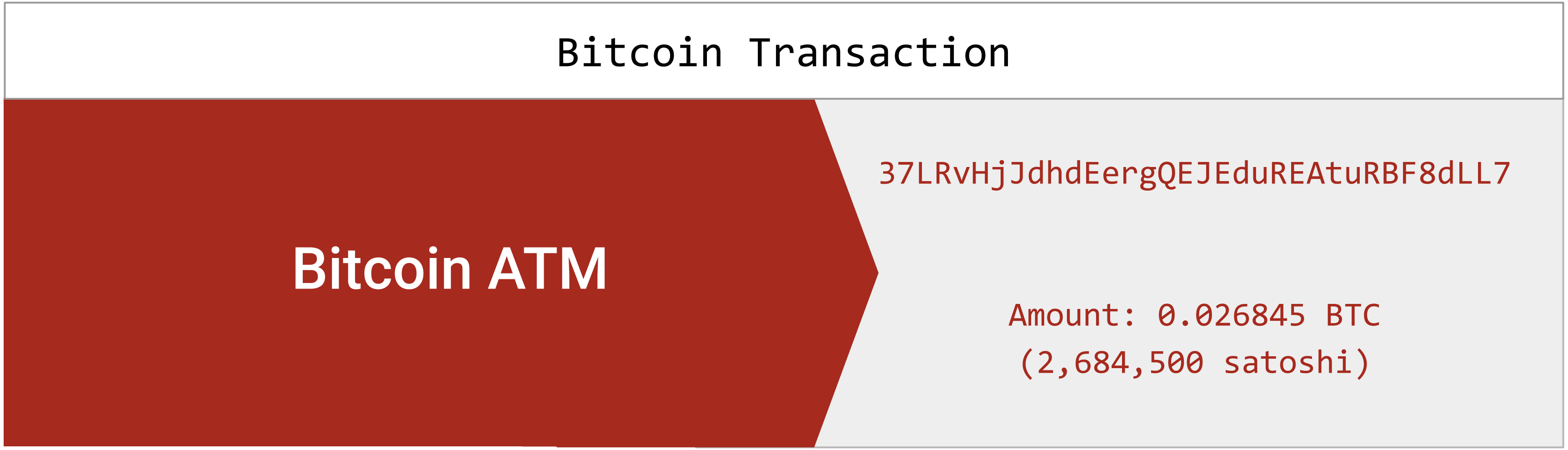
Alice buys Bitcoin from a Bitcoin ATM



€80

1 BTC ≅ €3,000

0.026845 BTC



Bitcoin Transaction

Bitcoin ATM

37LRvHjJdhdEergQEJEduREAtuRBF8dLL7

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

ATM sends 0.026845 BTC to Alice's wallet

Bitcoin Units

The only unit that exists in the system is the satoshi

Everything is stored as amounts of satoshis

One bitcoin = 100 million satoshis

Converting Units

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

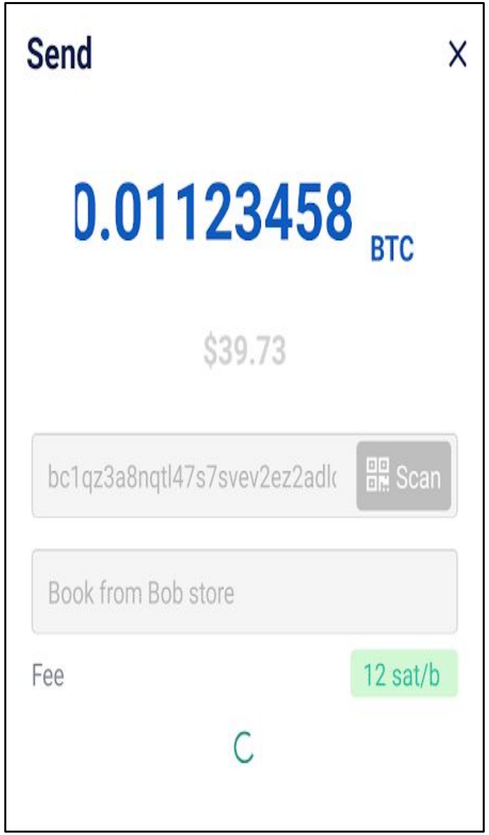
Alice buys a book from Bob's online store

0.01123458 BTC
Alice
Bob
Mastering Bitcoin

Alice uses bitcoin to buy a book from Bob's web store

Mastering Bitcoin
0.01123458 BTC
$40 USD

Alice’s wallet constructs a transaction



Send

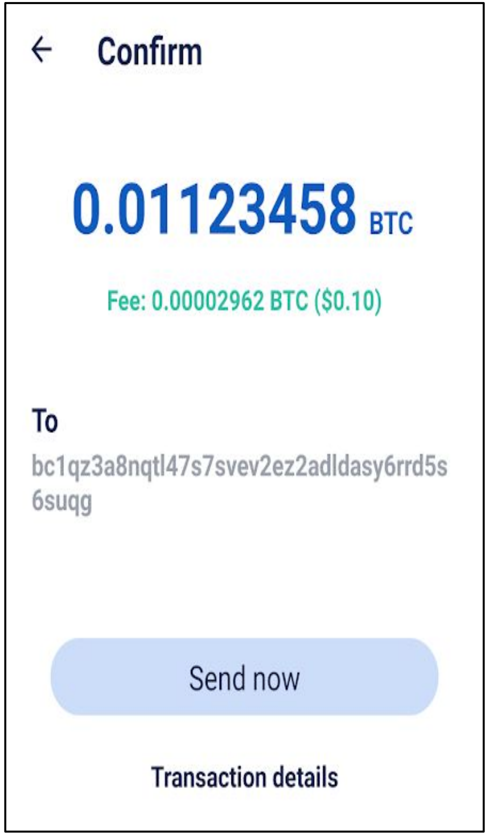
0.01123458 BTC

$39.73

bc1qz3a8nqtl47s7svev2ez2adl

Book from Bob store

Fee 12 sat/b

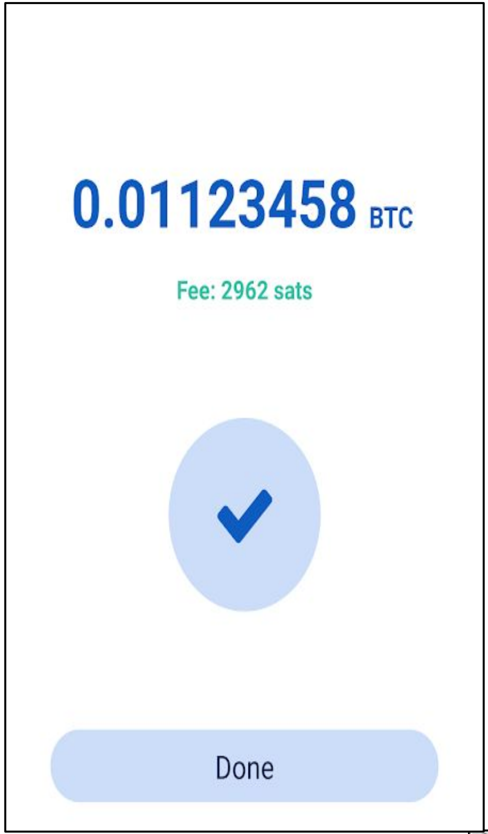


Confirm

0.01123458 BTC

Fee: 0.00002962 BTC ($0.10)

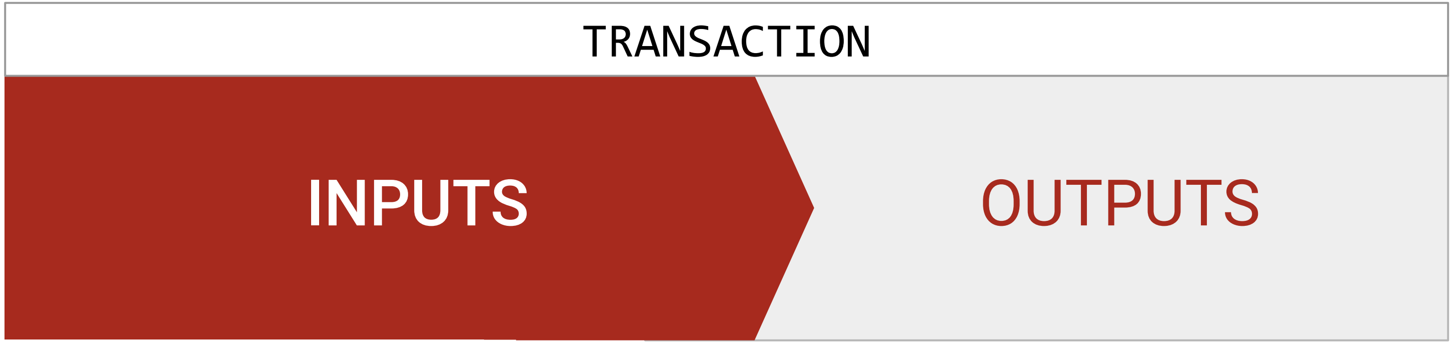
To
bc1qz3a8nqtl47s7svev2ez2adldasy6rrd5s6suqg



0.01123458 BTC

Fee: 2962 sats

Transaction Basics

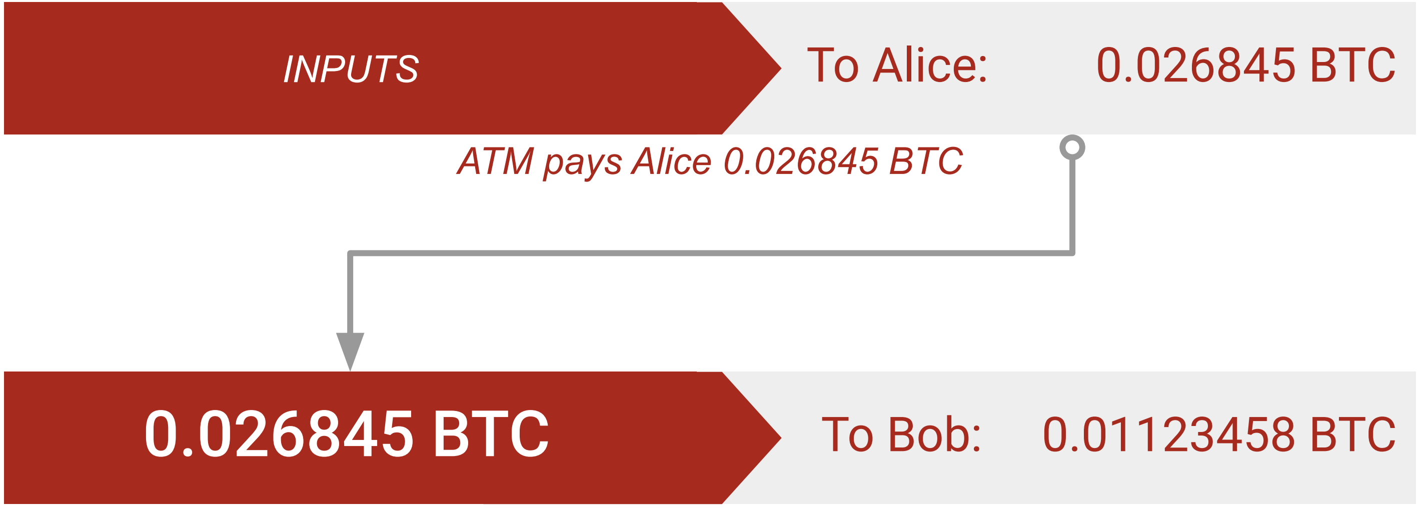


TRANSACTION

INPUTS

OUTPUTS

Transaction Basics



INPUTS

To Alice: 0.026845 BTC

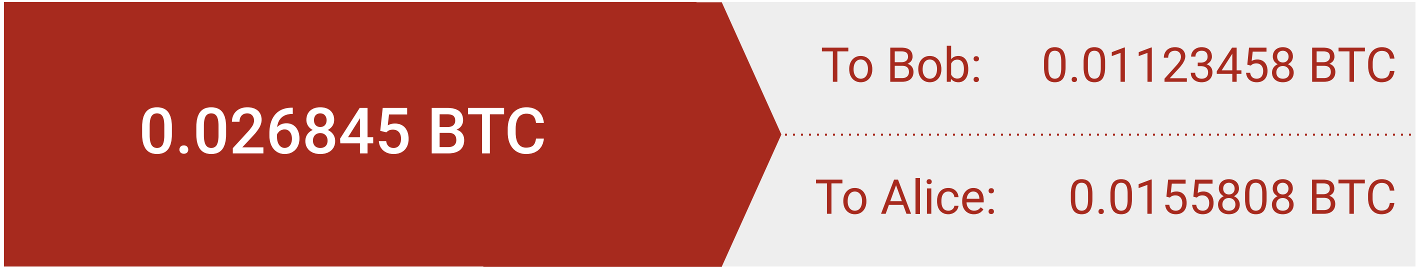
ATM pays Alice 0.026845 BTC

0.026845 BTC

To Bob: 0.01123458 BTC

Alice pays Bob 0.01123458

Transactions and Change

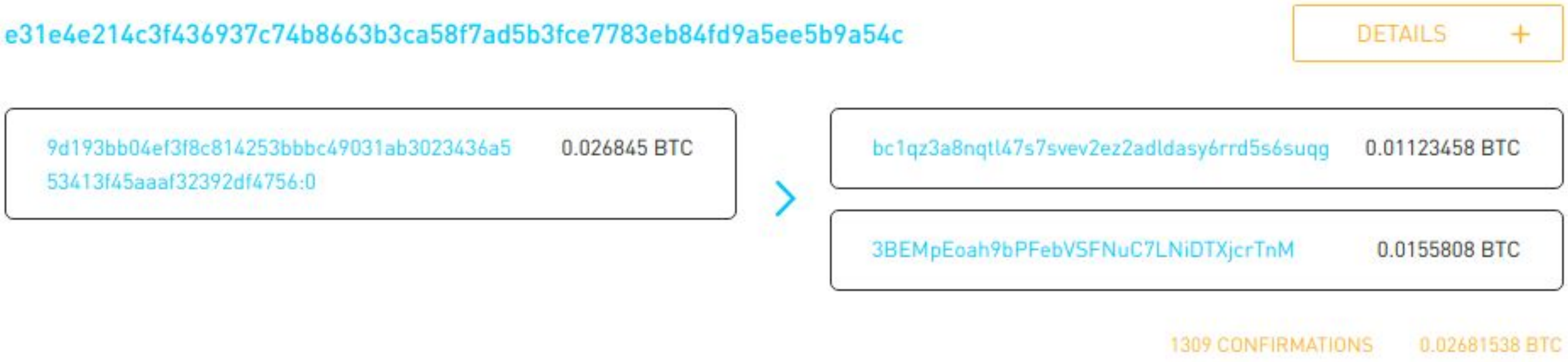


0.026845 BTC

To Bob: 0.01123458 BTC

To Alice: 0.0155808 BTC

Alice’s transaction, on the blockchain



e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c

9d193bb04ef3f8c814253bbbc49031ab3023436a553413f45aaaf32392df4756:0 0.026845 BTC

bc1qz3a8nqtl47s7svev2ez2adldasy6rrd5s6suqg 0.01123458 BTC

3BEMpEoah9bPFebVSFNuC7LNiDTXjcrTnM 0.0155808 BTC

1309 CONFIRMATIONS 0.02681538 BTC

Browse (case sensitive):
bit.ly/**A**lice**T**x

Part One Recap

We’ve learned about

- Bitcoin history
- Keys and addresses
- Markets, exchanges, and bitcoin pricing
- Units of account (satoshis)
- Transaction basics: inputs, outputs, change
- Using block explorers

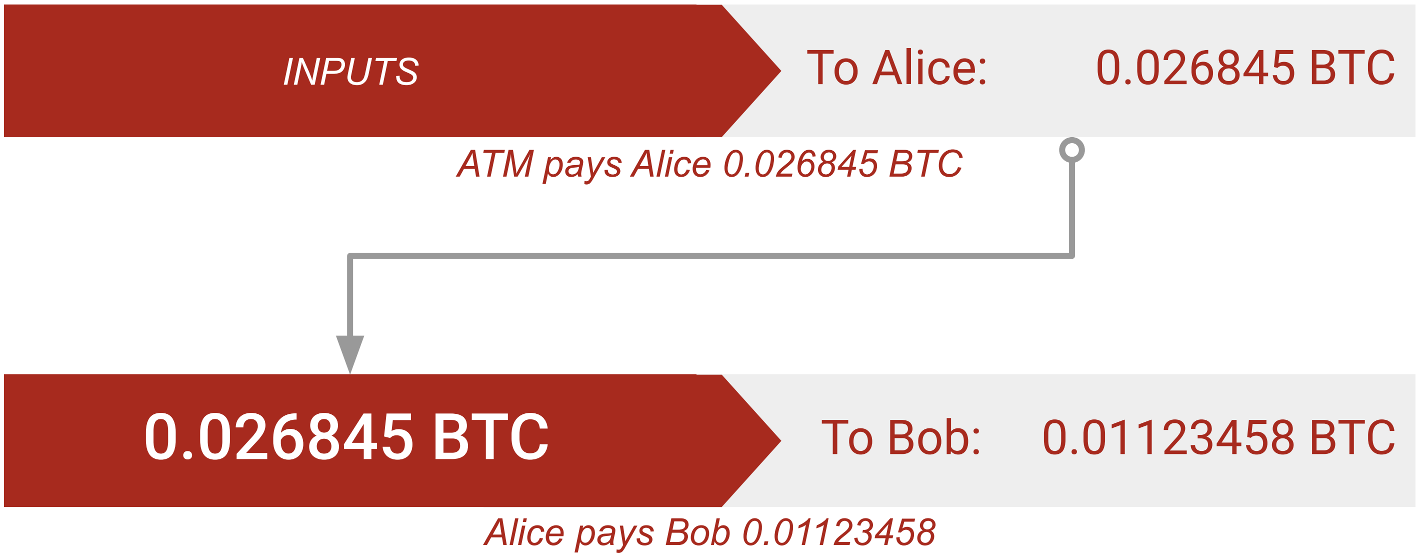
Part Two

In the next part we'll cover:

- Transaction fees
- Aggregating transaction inputs
- Issuance and monetary policy
- Mining and blockchain basics
- Consensus
- Forks

Alice buys a book from Bob’s online store (continued)

Outputs and Inputs (review)



INPUTS

To Alice: 0.026845 BTC

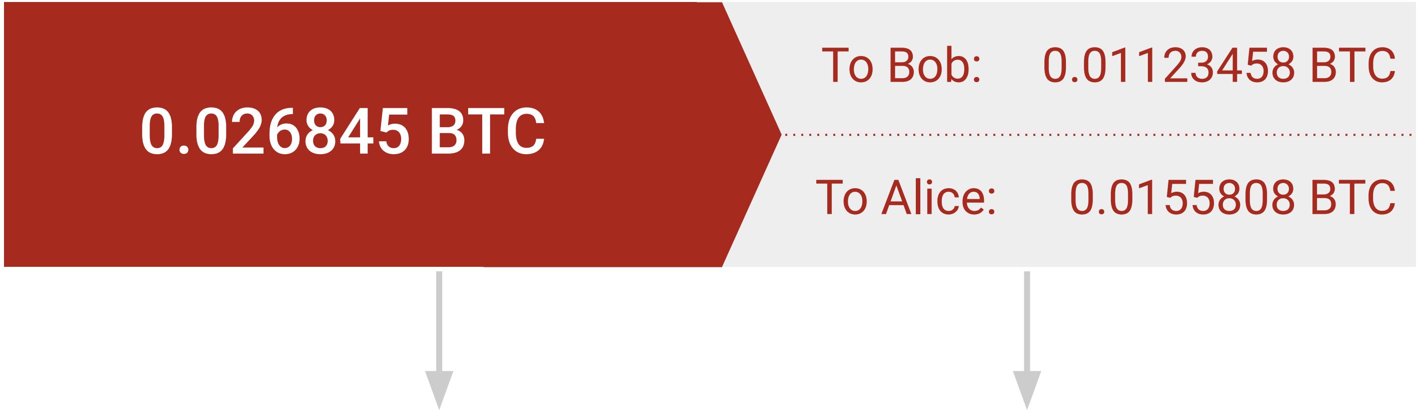
ATM pays Alice 0.026845 BTC

0.026845 BTC

To Bob: 0.01123458 BTC

Alice pays Bob 0.01123458

Transactions and Fees



0.026845 BTC

To Bob: 0.01123458 BTC

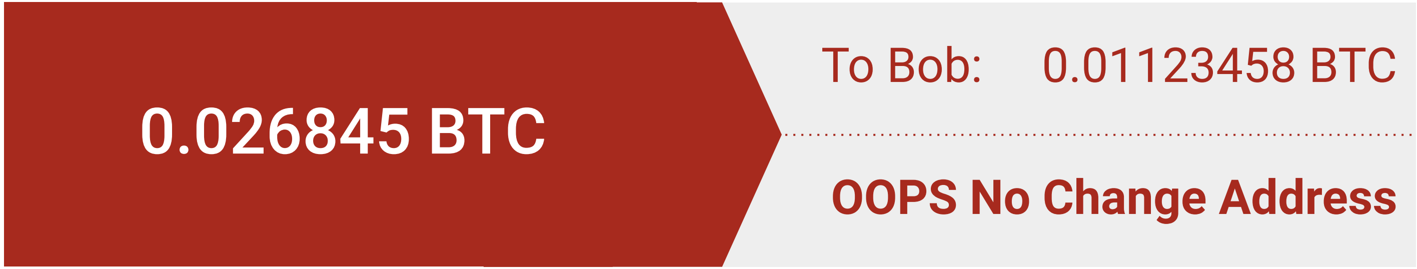
To Alice: 0.0155808 BTC

```
Inputs: 0.02684500 - Outputs 0.02681538 = Fees 0.00002962
```

“Miners, keep the rest of the change as a fee”

Change and Fees

What if Alice’s wallet didn’t include a change address for her change?



0.026845 BTC

To Bob: 0.01123458 BTC

OOPS No Change Address

```
Inputs: 0.02684500 - Outputs 0.01123458 = Fees 0.01561042
```

Transaction Fees

Why are there transaction fees?

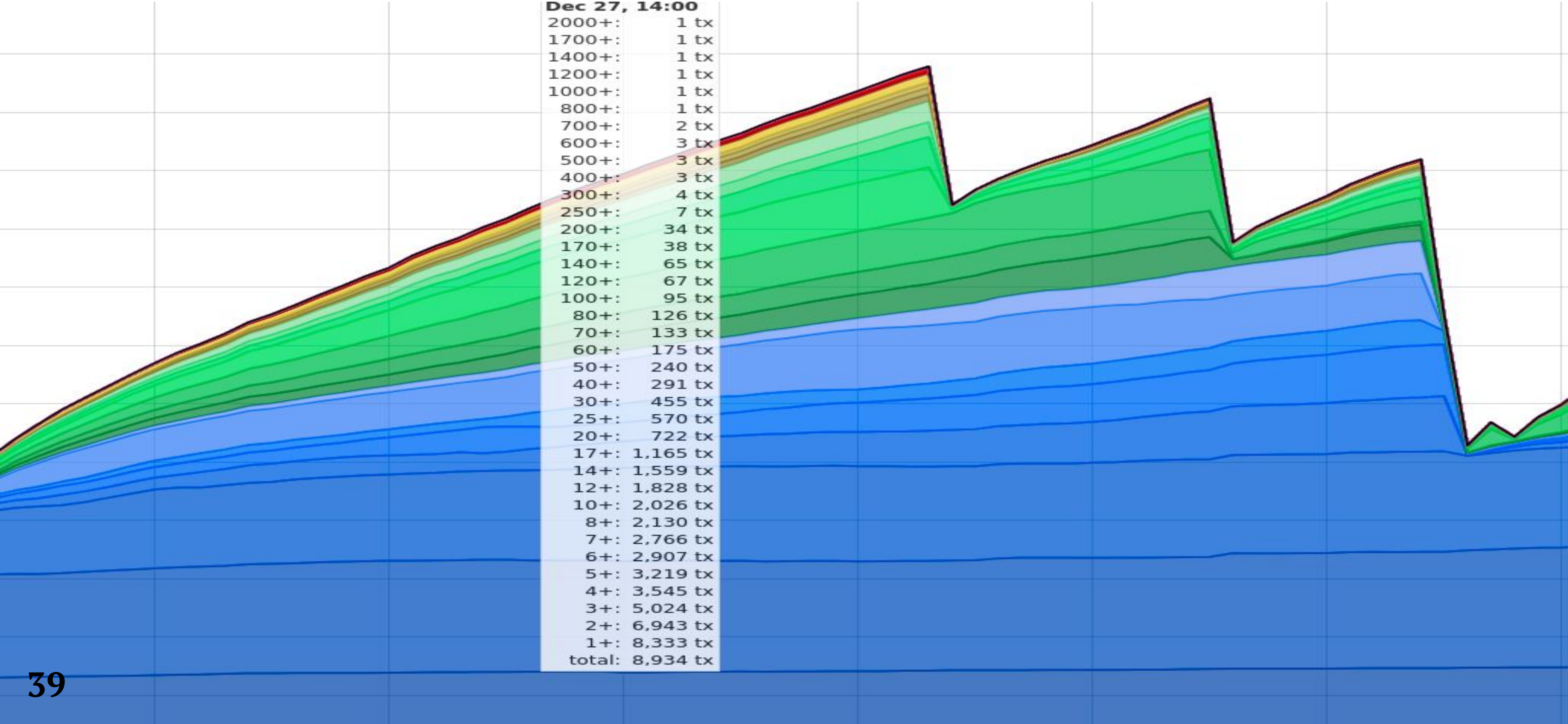
- ◻ Space for transactions is limited
- ◻ Fees determine who values their transaction
- ◻ Fees support mining as issuance declines

Are transaction fees static or dynamic?

- ◻ Is there a minimum required fee?

How do transaction fees affect the time it takes for my transaction to settle?

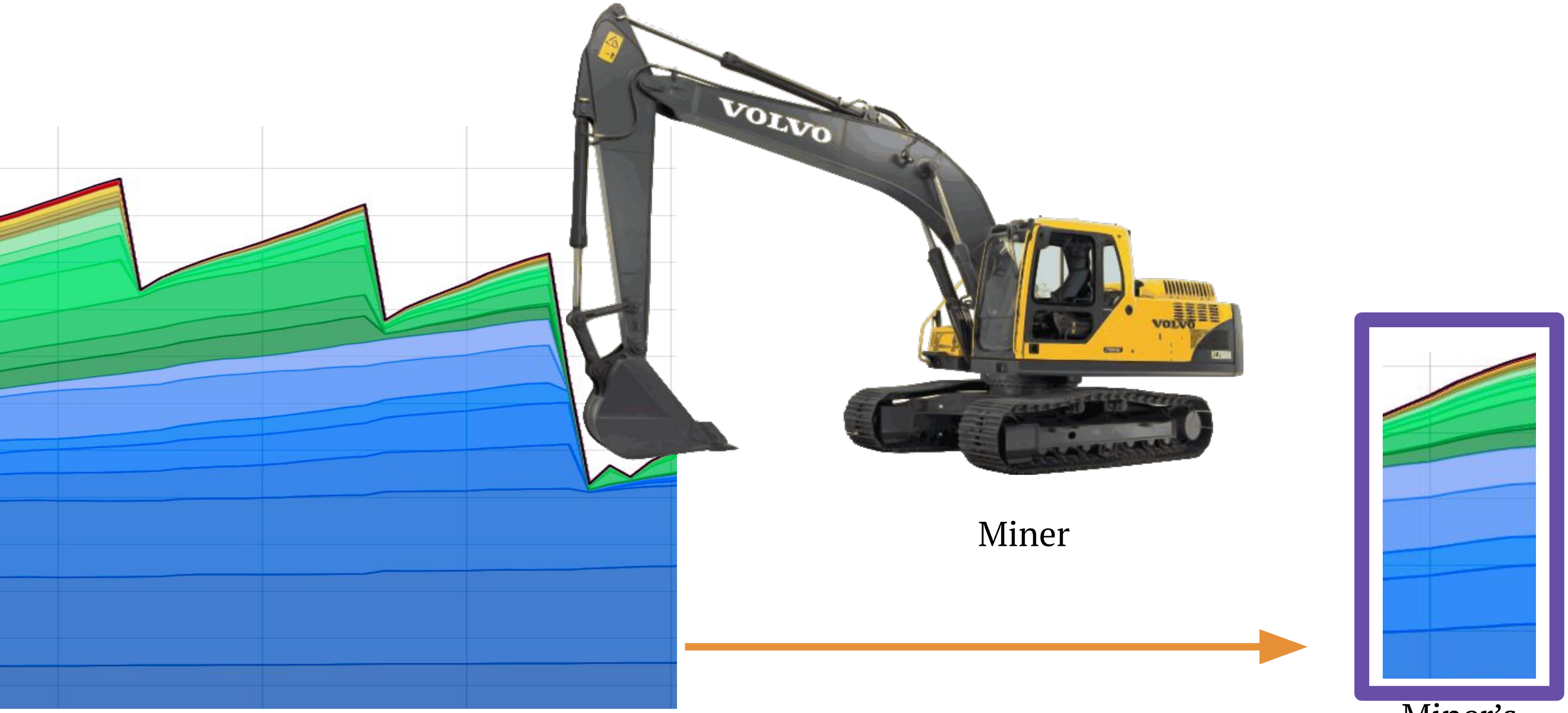
Transaction Fees



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

Miners Add Transactions to Blocks

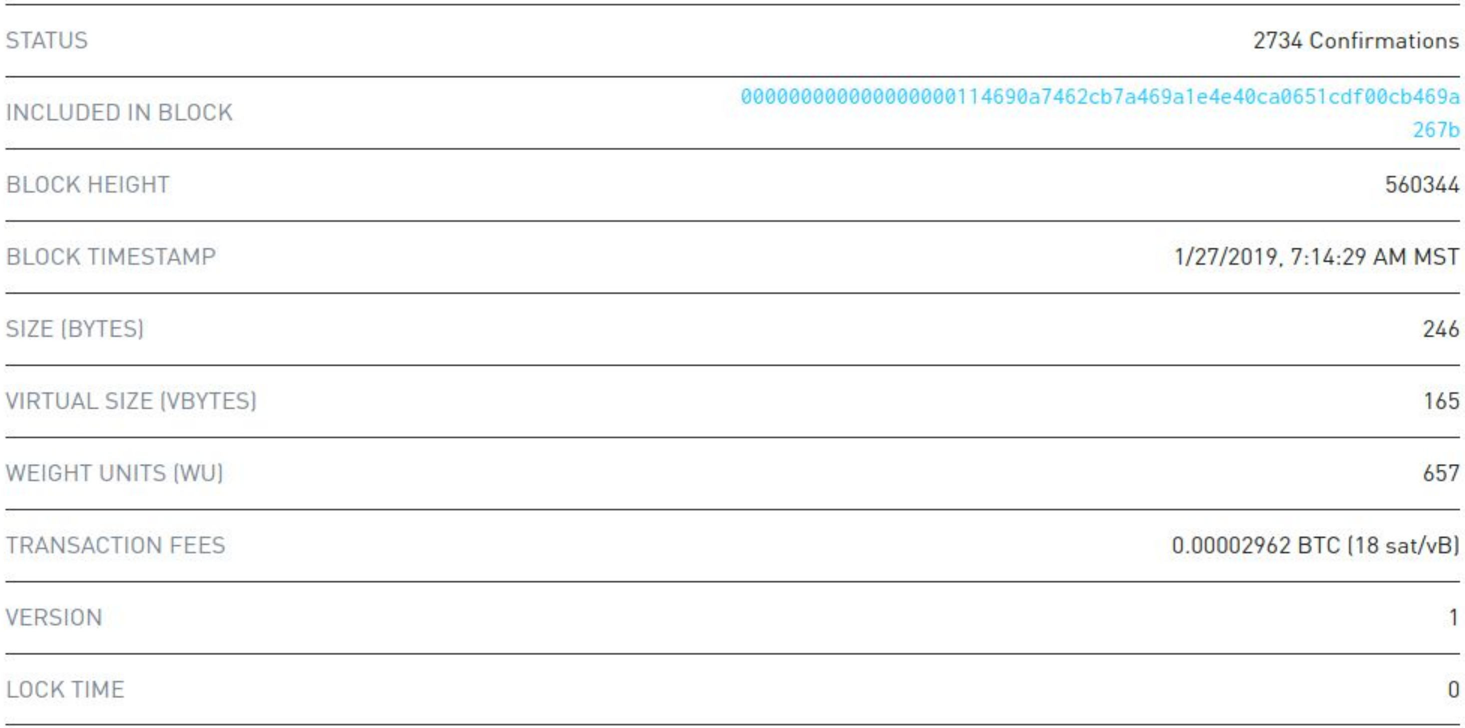


Miner

Miner’s Mem-Pool
Of Unconfirmed Transactions

Miner’s
Candidate Block

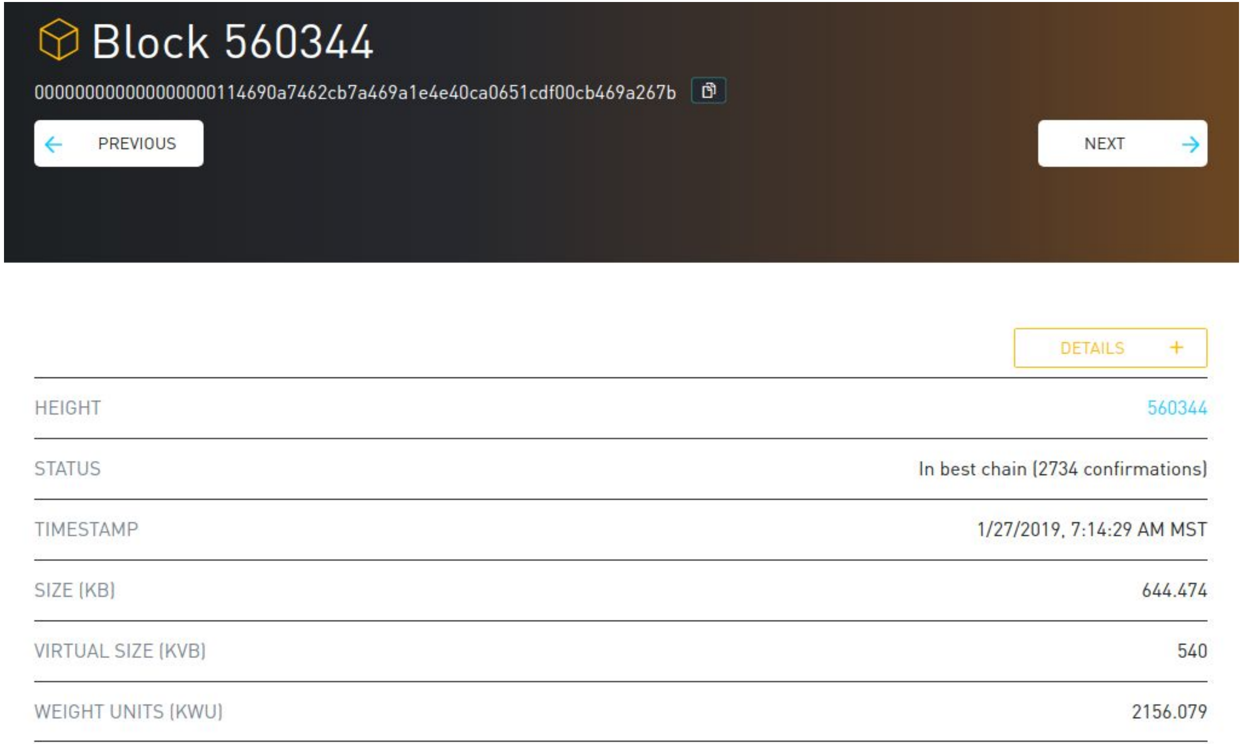
Alice’s transaction on the Bitcoin blockchain



STATUS	2734 Confirmations
INCLUDED IN BLOCK	000000000000000000114690a7462cb7a469a1e4e40ca0651cdf00cb469a267b
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

Alice’s transaction on the Bitcoin blockchain



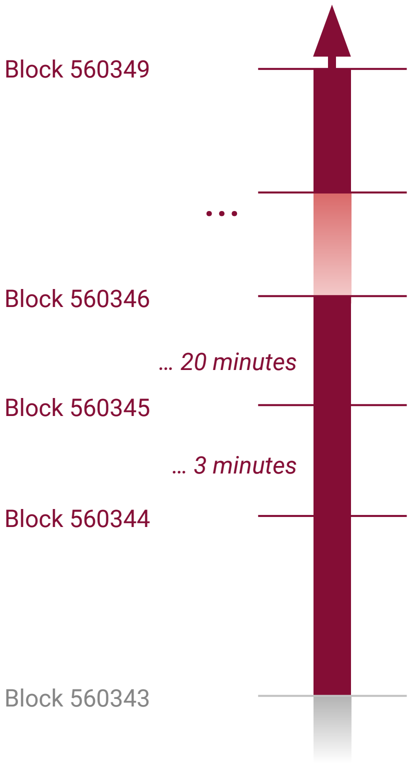
Block 560344

000000000000000000114690a7462cb7a469a1e4e40ca0651cdf00cb469a267b

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

Alice's transaction on the Bitcoin blockchain



Block Mined on 1/27/2019, 12:53:18 PM GMT-3
Bob ships Alice's book 6 confirmations after her transaction is mined.
In this case, 6 blocks took 1hr 39min to mine

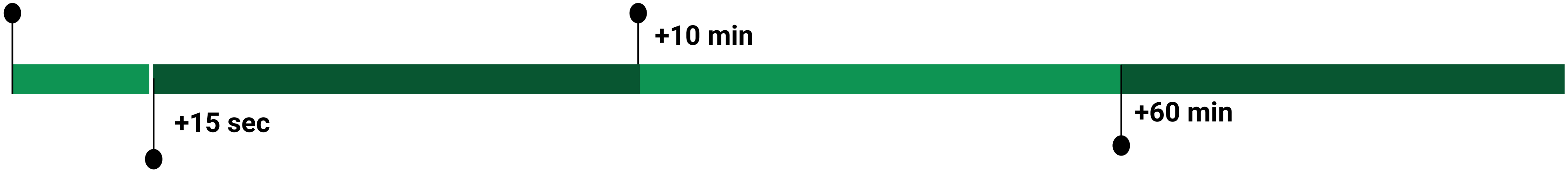
Block Mined on 1/27/2019, 11:37:17 AM GMT-3

Block Mined on 1/27/2019, 11:17:11 AM GMT-3

Block Mined on 1/27/2019, 11:14:29 AM GMT-3
Alice's Transaction
e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c

Browse:
bit.ly/Block344

Alice Tx Timeline



Alice's Wallet

Creates, signs and transmits transaction paying Bob's address $40, or 0.01123458 BTC

+15 sec

Bob's Wallet

Bob's wallet receives the transaction from the Bitcoin network.

The transaction is unconfirmed (not mined in a block yet)

+10 min

Miner

A miner successfully mines a new block, which contains Alice's transaction.

Alice's transaction has "1 confirmation"

+60 min

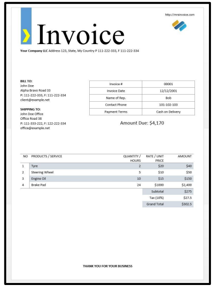
Bob's Wallet

Bob's wallet receives 5 more blocks, mined on top of the one containing Alice's transaction.

Bob's store policy is to ship books after 6 confirmations. Bob now ships the book to Alice.

Bob pays Catalina’s invoice for web development work

Bob’s Payment Options



http://mrsinvoice.com

Invoice

Your Company LLC Address 123, State, My Country P 111-222-333, F 111-222-334

BILL TO:
John Doe
Alpha Bravo Road 33
P: 111-222-333, F: 111-222-334
client@example.net

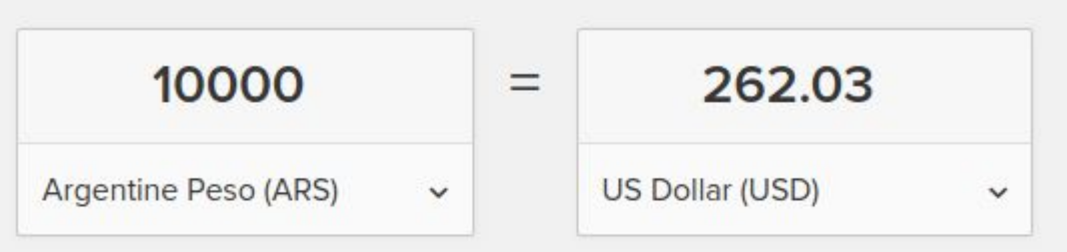
SHIPPING TO:
John Doe Office
Office Road 38
P: 111-333-222, F: 122-222-334
office@example.net

Invoice #	00001
Invoice Date	12/12/2001
Name of Rep.	Bob
Contact Phone	101-102-103
Payment Terms	Cash on Delivery

Amount Due: $4,170

NO	PRODUCTS / SERVICE	QUANTITY / HOURS	RATE / UNIT PRICE	AMOUNT
1	Tyre	2	$20	$40
2	Steering Wheel	5	$10	$50
3	Engine Oil	10	$15	$150
4	Brake Pad	24	$1000	$2,400
			Subtotal	$275
			Tax (10%)	$27.5
			Grand Total	$302.5

THANK YOU FOR YOUR BUSINESS



10000 = 262.03

Argentine Peso (ARS)

US Dollar (USD)

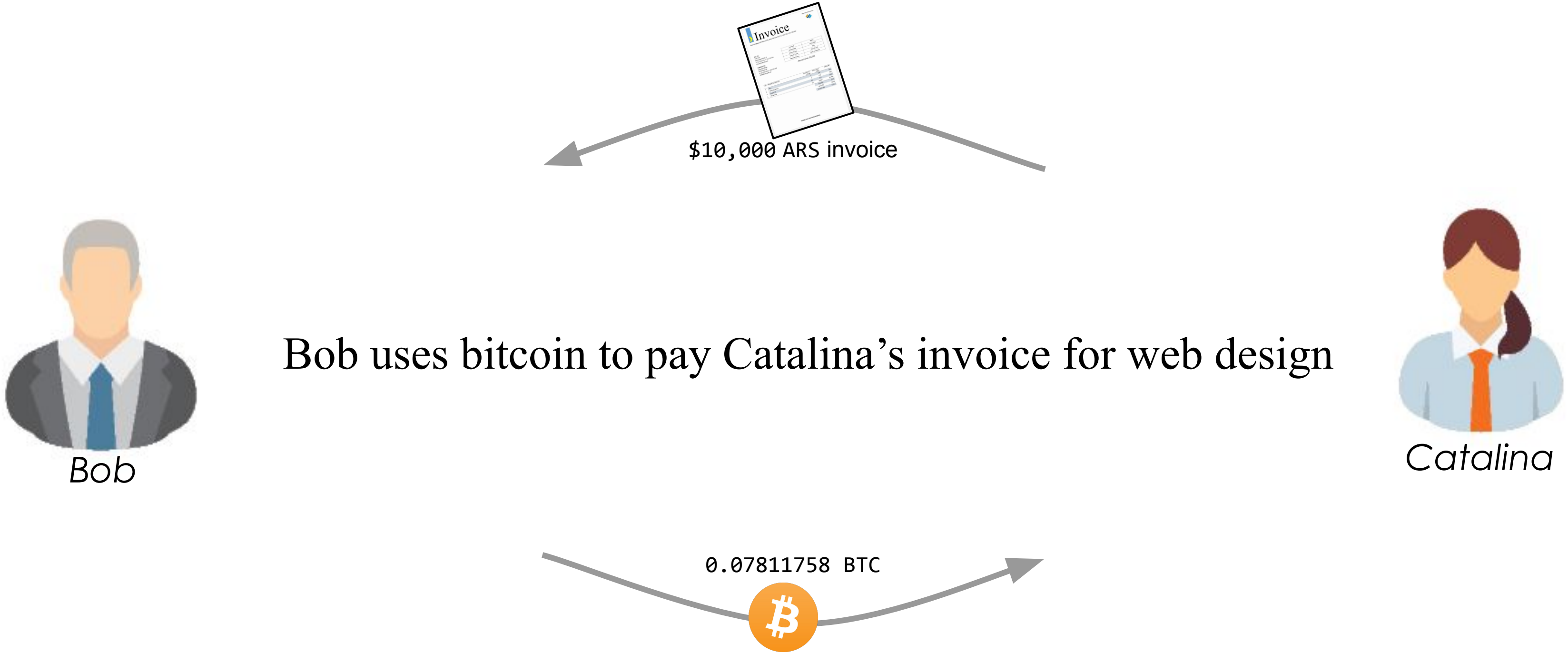
International Wire Transfer (bank)

Western Union

Paper check?

Bitcoin

Bob uses bitcoin to pay Catalina’s invoice for web design



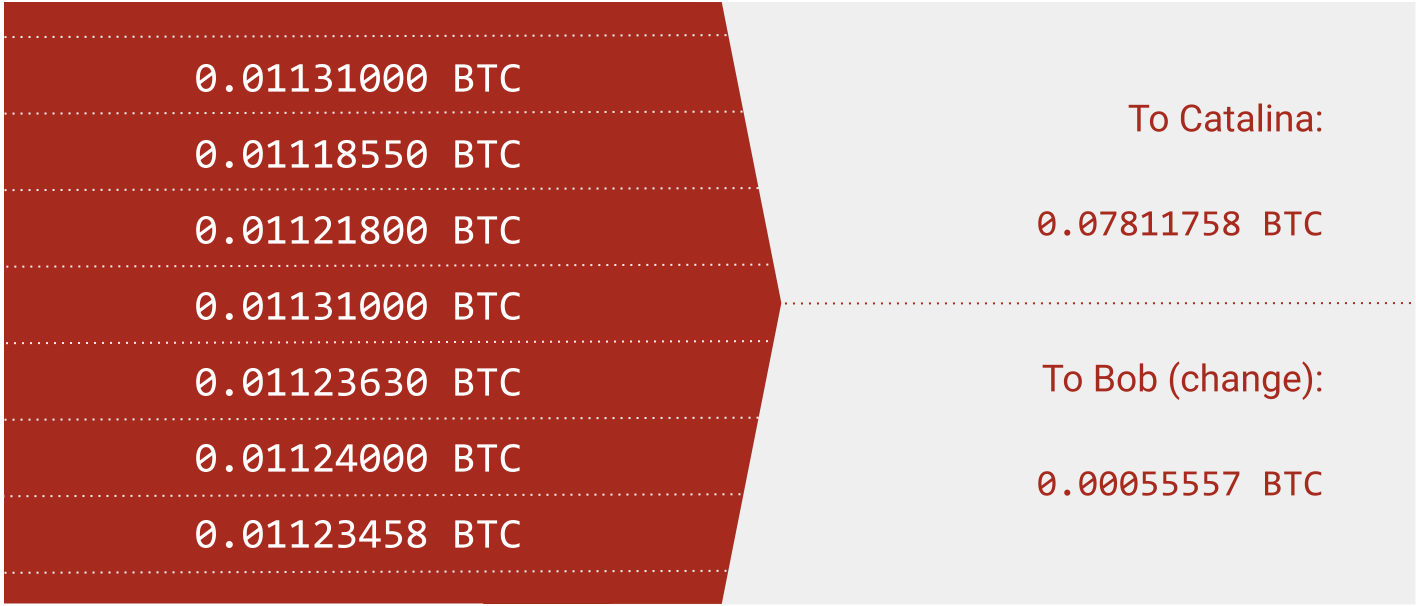
$10,000 ARS invoice

Bob

Catalina

0.07811758 BTC

Aggregating Transaction



0.01131000 BTC

0.01118550 BTC

0.01121800 BTC

0.01131000 BTC

0.01123630 BTC

0.01124000 BTC

0.01123458 BTC

To Catalina:

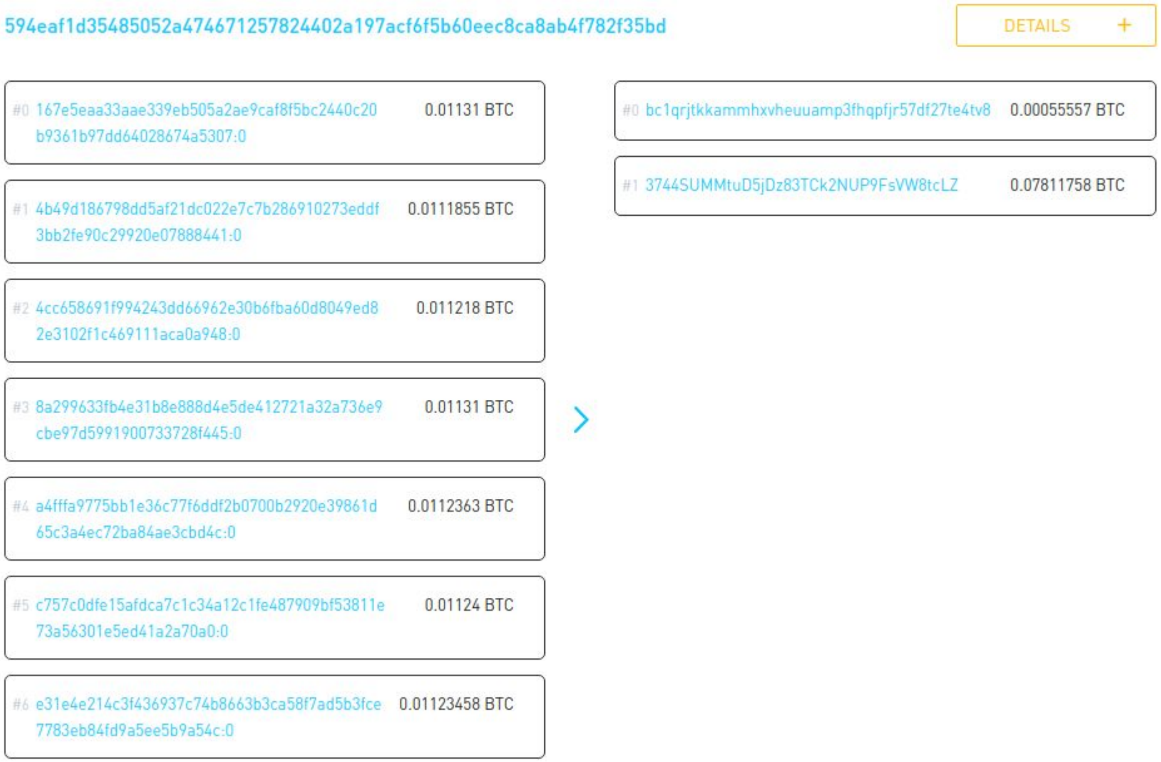
0.07811758 BTC

To Bob (change):

0.00055557 BTC

Bob pays Catalina 0.07811758 BTC

Aggregating Transaction



594eaf1d35485052a474671257824402a197acf6f5b60eec8ca8ab4f782f35bd

#0 167e5eaa33aae339eb505a2ae9caf8f5bc2440c20b9361b97dd64028674a5307:0 0.01131 BTC

#1 4b49d186798dd5af21dc022e7c7b286910273eddf3bb2fe90c29920e07888441:0 0.0111855 BTC

#2 4cc658691f994243dd66962e30b6fba60d8049ed82e3102f1c469111aca0a948:0 0.011218 BTC

#3 8a299633fb4e31b8e888d4e5de412721a32a736e9cbe97d5991900733728f445:0 0.01131 BTC

#4 a4fffa9775bb1e36c77f6ddf2b0700b2920e39861d65c3a4ec72ba84ae3cbd4c:0 0.0112363 BTC

#5 c757c0dfe15afdca7c1c34a12c1fe487909bf53811e73a56301e5ed41a2a70a0:0 0.01124 BTC

#6 e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c:0 0.01123458 BTC

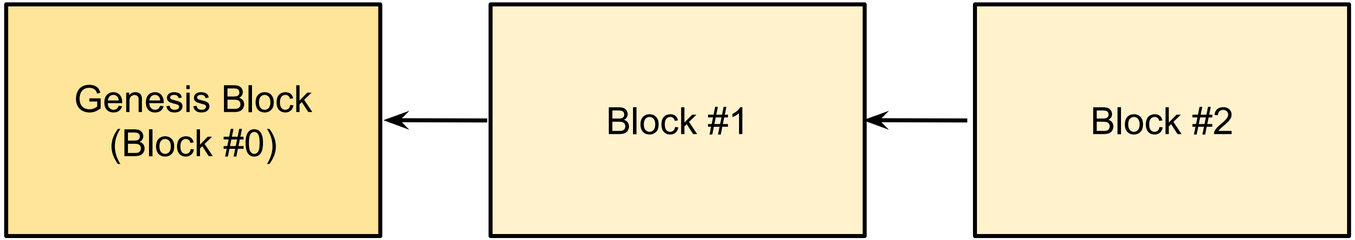
#0 bc1qrjtkkammhxvheuuamp3fhqpfjr57df27te4tv8 0.00055557 BTC

#1 3744SUMMtuD5jDz83TCk2NUP9FsVW8tcLZ 0.07811758 BTC

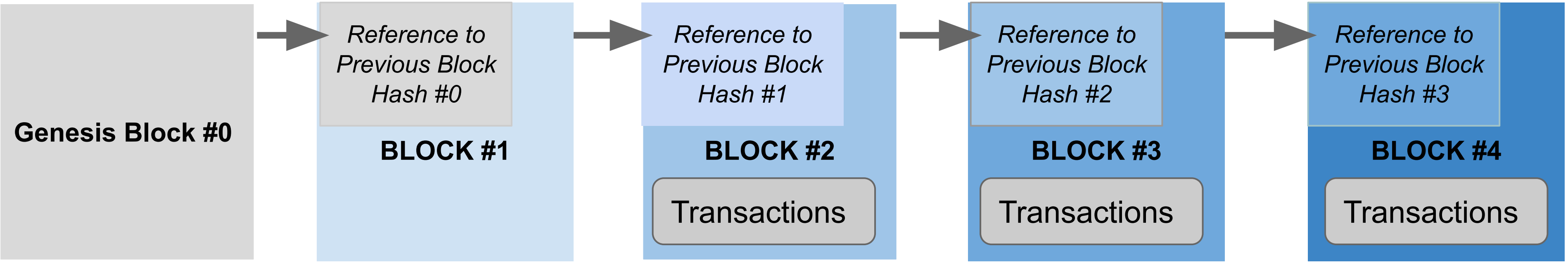
Bob pays Catalina 0.07811758 BTC

The Blockchain

History of the Bitcoin Blockchain

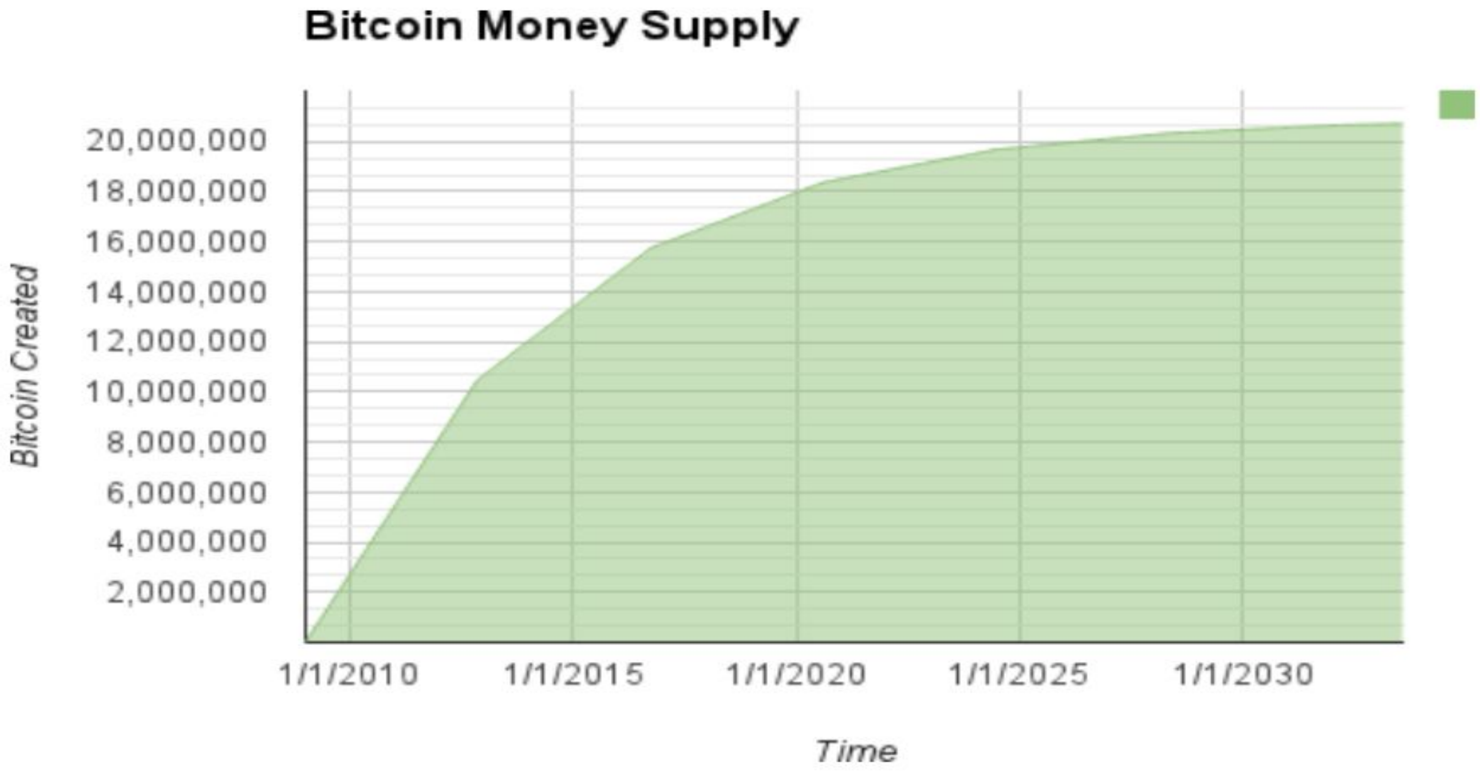


Chained Blocks

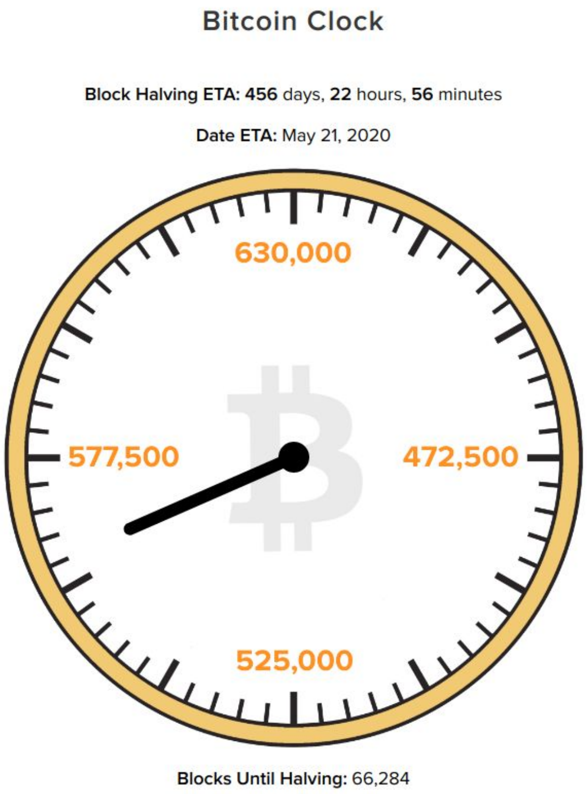

Genesis Block #0
Reference to Previous Block Hash #0
BLOCK #1
Reference to Previous Block Hash #1
BLOCK #2
Transactions
Reference to Previous Block Hash #2
BLOCK #3
Transactions
Reference to Previous Block Hash #3
BLOCK #4
Transactions

- □ Each block references the hash of the previous, or “parent,” block
- □ The sequence of hashes linking each block to its parent creates a chain
- □ Creates a tamper-evident log; combined with proof-of-work (i.e. an energy cost for making changes) results in the characteristic of **immutability**

Monetary Policy



Halving



Bitcoin Clock

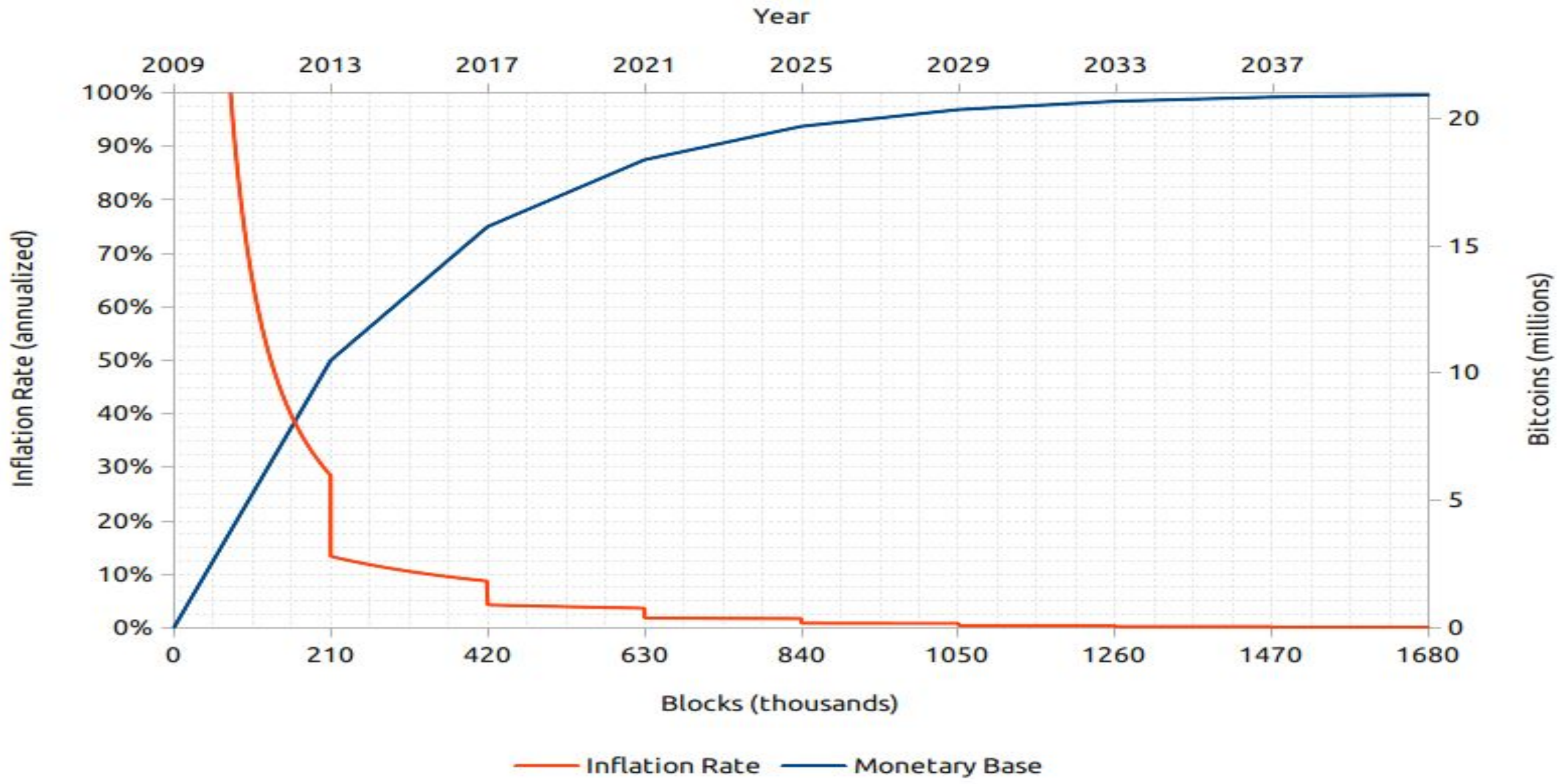
Block Halving ETA: 456 days, **22** hours, **56** minutes

Date ETA: May 21, 2020

Blocks Until Halving: 66,284

- Every 210,000 blocks
- Bitcoin issuance is “halved”
- 2009-2012: 50 BTC per block
- 2012-2016: 25 BTC per block
- 2016-2020: 12.5 BTC per block
- 2020-2024: 6.25 BTC per block
- …

Bitcoin Inflation vs. Time

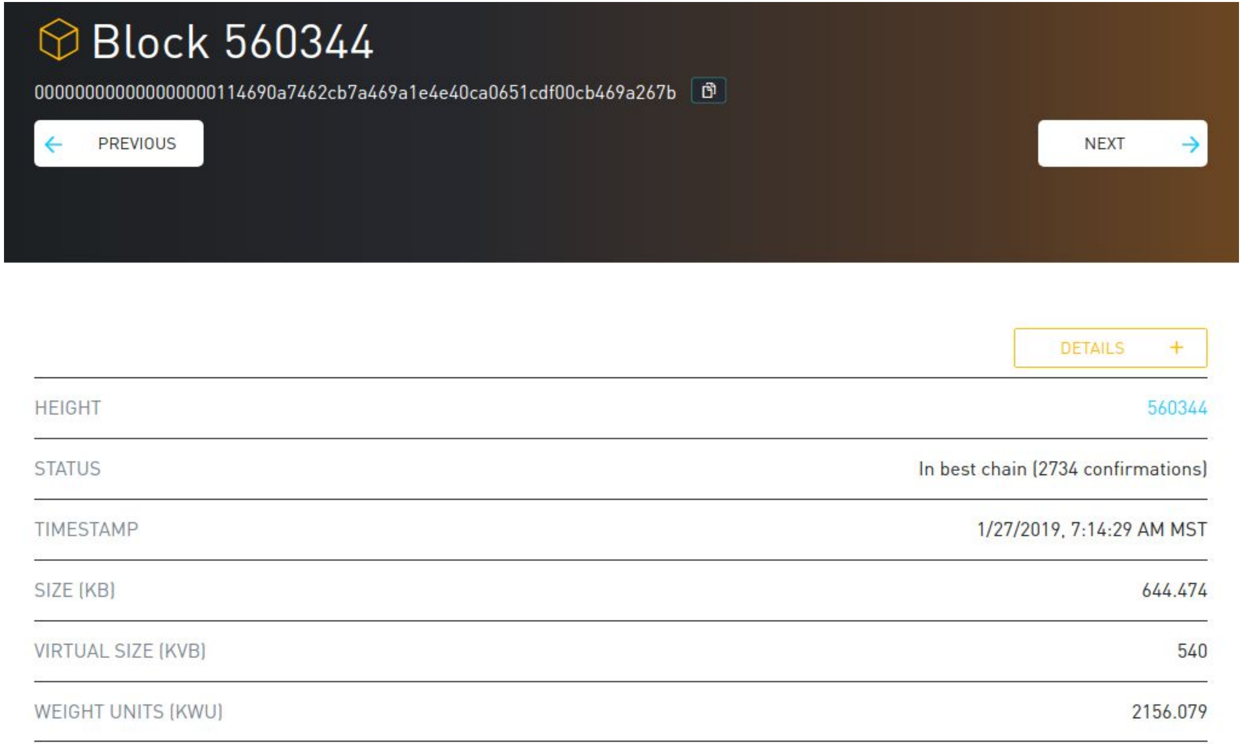


Mining Incentives

Miners currently receive two types of rewards in return for the security provided by mining:

(1) new coins created with each new block, and
(2) transaction fees from all the transactions included in the block.

Alice’s transaction on the Bitcoin blockchain



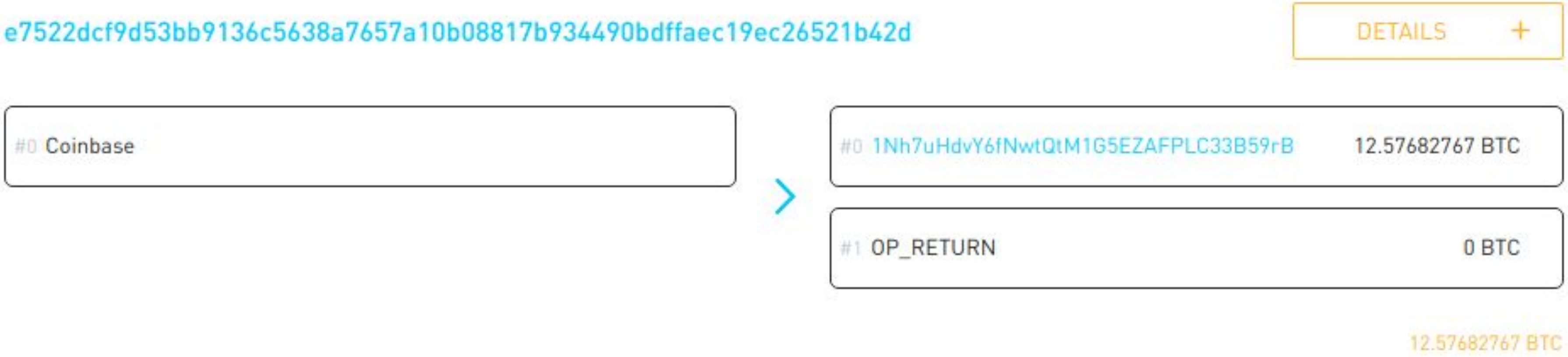
Block 560344

0000000000000000000114690a7462cb7a469a1e4e40ca0651cdf00cb469a267b

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

Coinbase Transaction



e7522dcf9d53bb9136c5638a7657a10b08817b934490bdffaec19ec26521b42d

#0 Coinbase

#0 1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB 12.57682767 BTC

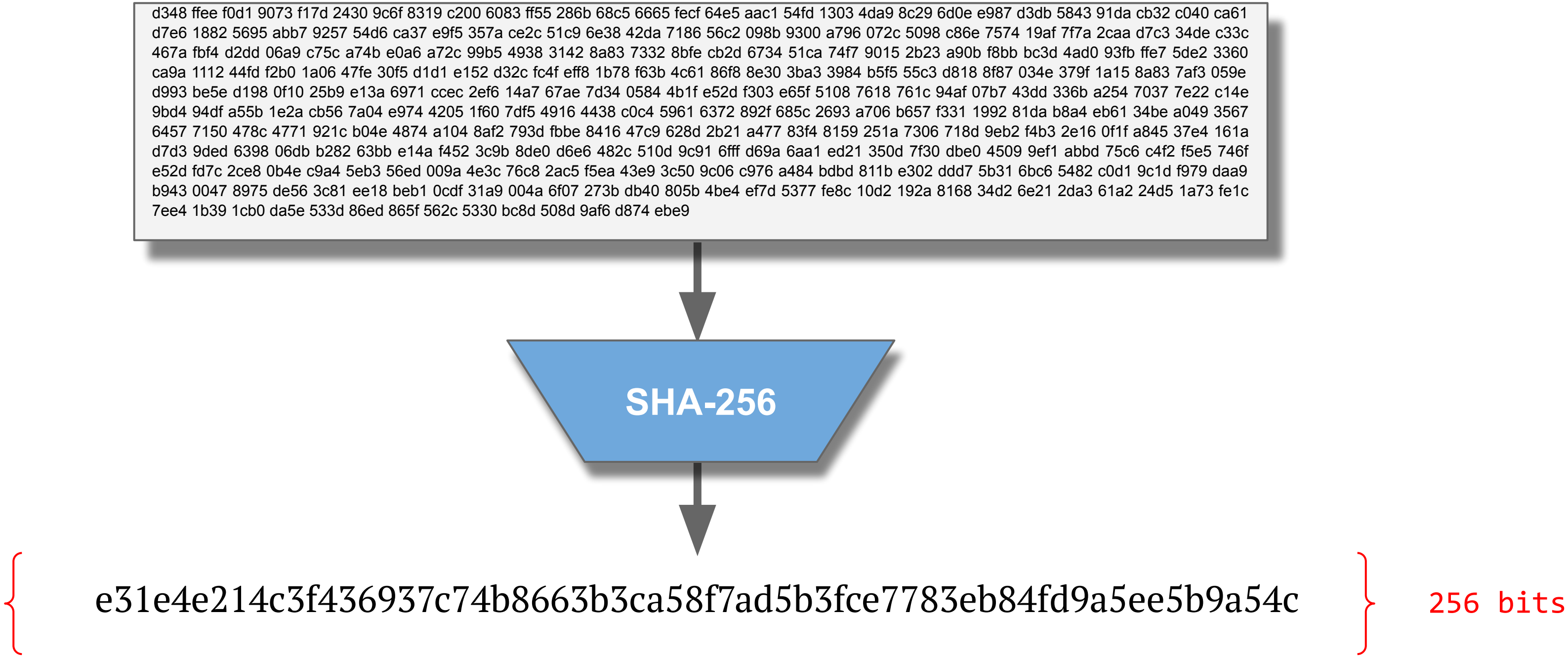
#1 OP_RETURN 0 BTC

12.57682767 BTC

Mining

SHA-256 Hash Algorithm

Hash Algorithm: Compresses any amount of data into a fixed-length "fingerprint".



```
d348 ffee 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 fbf4 d2dd 06a9 c75c a74b e0a6 a72c 99b5 4938 3142 8a83 7332 8bfe 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
```

e31e4e214c3f436937c74b8663b3ca58f7ad5b3fce7783eb84fd9a5ee5b9a54c

256 bits

Small change in input
Big change in output

“I am Satoshi” => ef2cdaa37271e1bea8e95b2b9ec15209f84e5eb3583449b4b4b8e7f2a18d72b9

“I am Satoshi!” => 1da78803987e56886194d1e1b9ba8bfd216be4c607b0cfef7eeb05689871b8a7

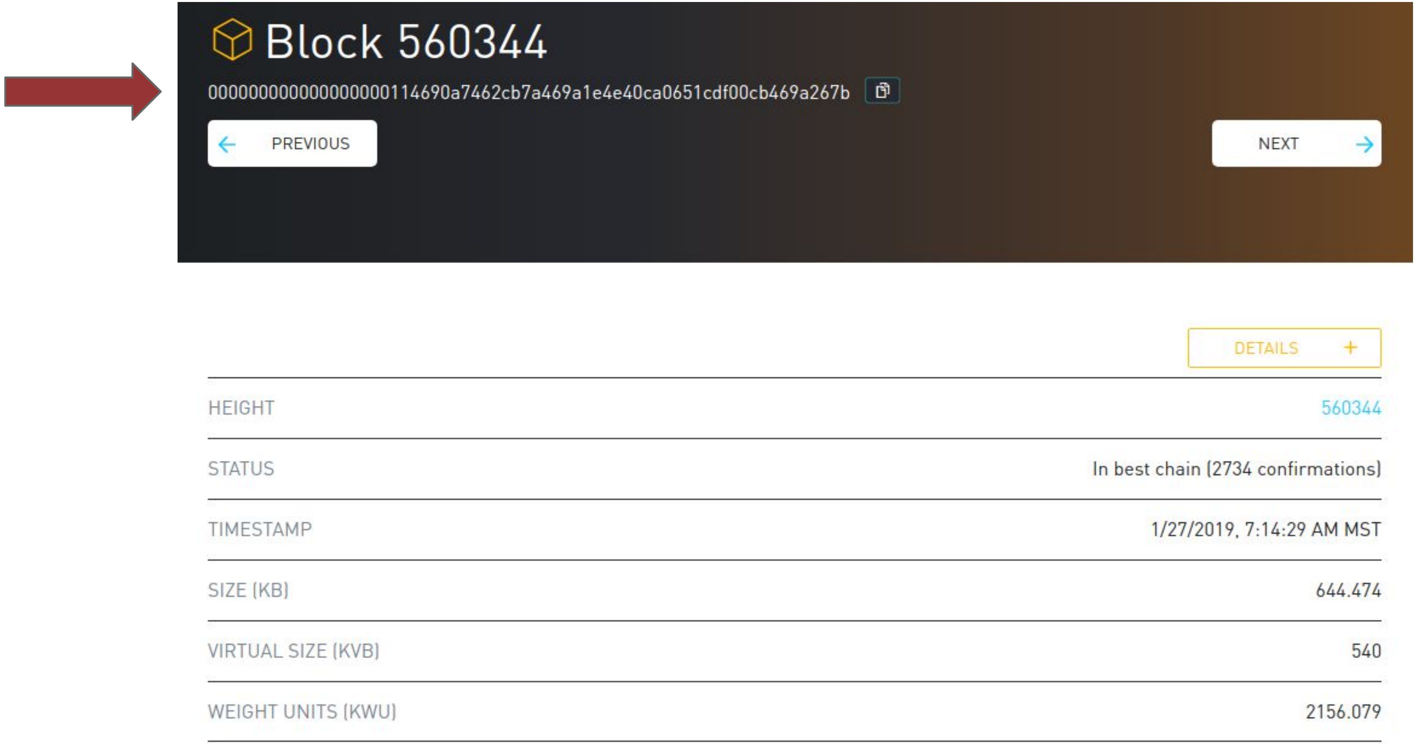
"I am Satoshi 0" => 972c421e91226b24a7a08b3099e3cebe893e5d111804d0f464f8cf472d09e1c9
"I am Satoshi 1" => 7b1b1f24624ef8821c7fb6c95a4e0efeb4d68dac80953cdf903b3b77f086af4b
"I am Satoshi 2" => 36c99755599d8b4bc21616c9e770c873885ad3fd4b2e4094abe9f19ce983d4cd

Hashing to a target pattern

```
"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 1116500145"     =>       000000000bbe916434baf4521260f5ba1e860d9ccc16a7566eee03663bc12741
```

Mining Farm

The Block Hash



Block 560344

000000000000000000114690a7462cb7a469a1e4e40ca0651cdf00cb469a267b

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

Q & A

Thank you!

CBP Prep Course

Find a study guide at cryptoconsortium.org

Exercises

Using a block explorer look up Alice’s transaction to Bob (bit.ly/**A**lice**T**x)

- □ How many inputs and outputs does Alice’s transaction have?
- □ Which output is the change output? How can you tell?
- □ How much change did Alice get in BTC?
- □ How much is Alice’s change in satoshi?

Click on the input of Alice’s transaction to find Alice’s transaction with the Bitcoin ATM

- □ How many inputs and outputs does this transaction have?
- □ How many milibits did Alice receive from the ATM?
- □ What was the effective exchange rate that Alice received for her 80EUR?

What was the price of 1 bitcoin on the day you started working here?

Answers

- Alice’s Tx has _____ input(s) and _____ output(s)
- The #___ output is change
- Alice received ____________________ BTC as change
- Alice received ____________________ satoshi as change
- The Bitcoin ATM Tx has _____ input(s) and ______ output(s)
- Alice received ____________________ millibits from the ATM
- The effective exchange rate Alice got was 1 BTC = ____________ EUR
- According to __________________ the price of 1 bitcoin on the day I started working was _______________________.

Answers

- Alice’s Tx has **1** input(s) and **2** output(s)
- The **2nd** output is change
- Alice received **0.0155808** BTC as change
- Alice received **1,558,080** satoshi as change
- The Bitcoin ATM Tx has **1** input(s) and **2** output(s)
- Alice received **26.845** millibits from the ATM
- The effective exchange rate Alice got was **1 BTC = 2980.07 EUR**
- According to ____________________ the price of 1 bitcoin on the day I started working was __________________________.

Advanced Exercises

- How many inputs does Bob’s payment to Catalina contain?
- How much fee did Bob pay for that transaction?
- Which block contained Bob’s payment to Catalina (ie. 1 confirmation)?
- How much time did it take until that transaction had 6 confirmations?
- How many other transactions were in the same block as Bob’s payment to Catalina?
- What was the amount paid to the miner in the coinbase transaction of the block containing Bob’s payment to Catalina?
- What was the block hash of that block?
- How many zeroes (in hex) in the beginning of the block hash of that block?
- What was the amount of the block subsidy and how much were the fees in that block?