Bitcoin Basics Workshop

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

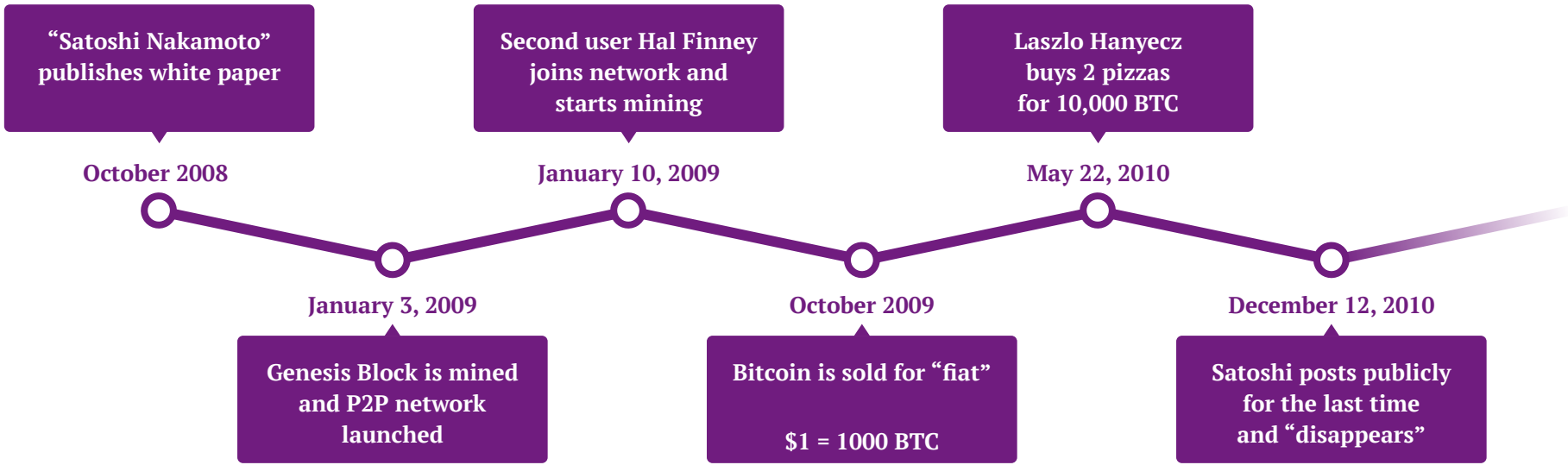
WARNING

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”



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

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

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

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 uses bitcoin to pay Catalina's invoice for web design

Bob

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

Bitcoin ATM

Alice uses cash to buy bitcoin from a Bitcoin ATM

Alice

Bitcoin ATM Vending Machine

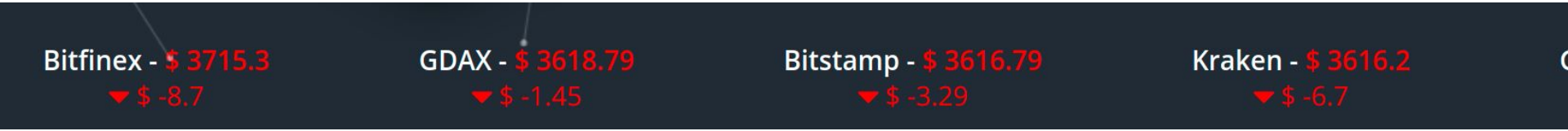
=

? BTC

How much bitcoin does 80 EUR buy?

Bitcoin’s “Price”

See: bitcoinaverage.com



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

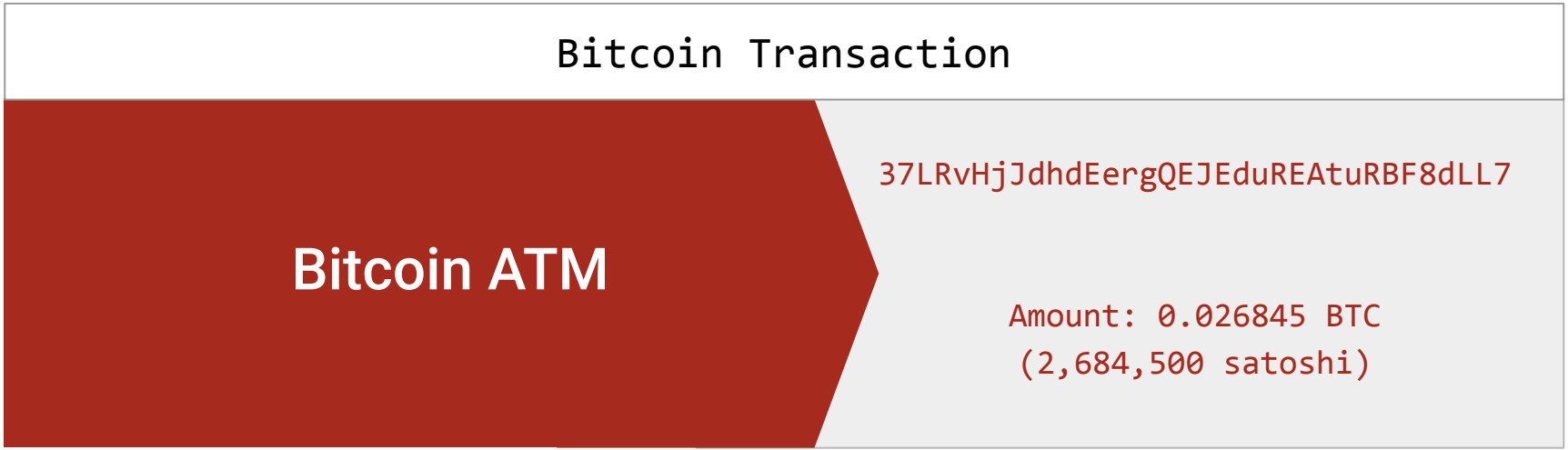
Alice shows a bitcoin address to the ATM

Alice buys Bitcoin from a Bitcoin ATM

€80

1 BTC ≅ €3,000

0.026845 BTC



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

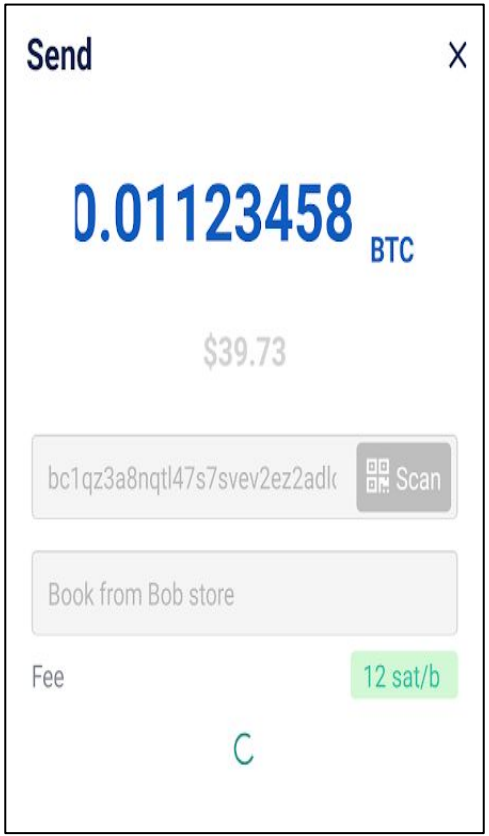
Alice

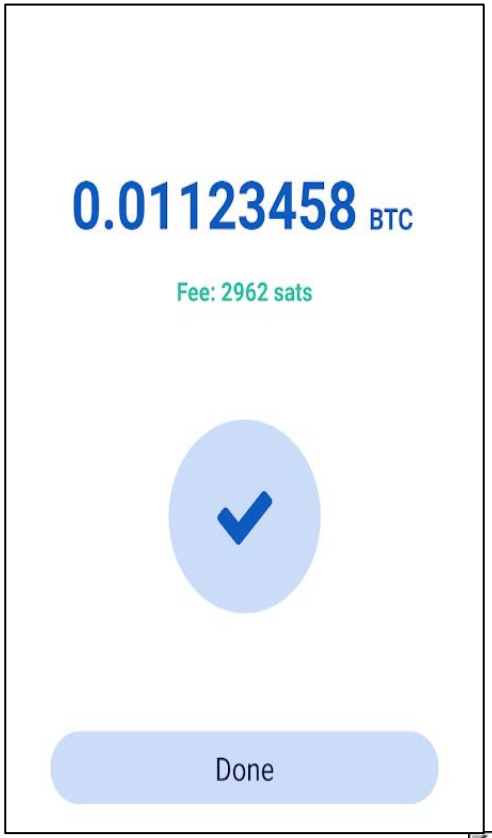
Alice uses bitcoin to buy a book from Bob's web store

Bob

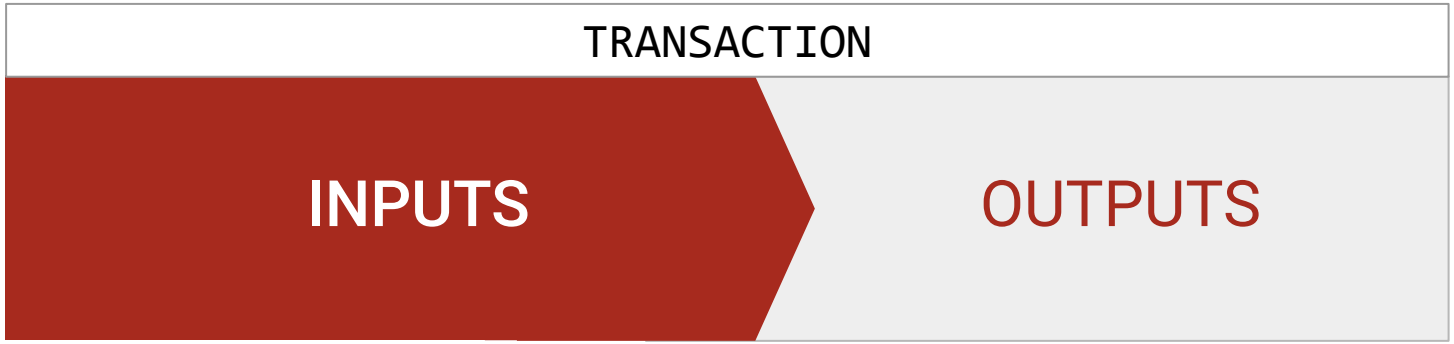

Mastering
Bitcoin
0.01123458 BTC
$40 USD

Alice's wallet constructs a transaction





Transaction Basics



Transaction Basics

Transactions and Change

Alice's transaction, on the blockchain

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

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)

Transactions and Fees


```
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?


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

Transaction Fees

Why are there transaction fees?

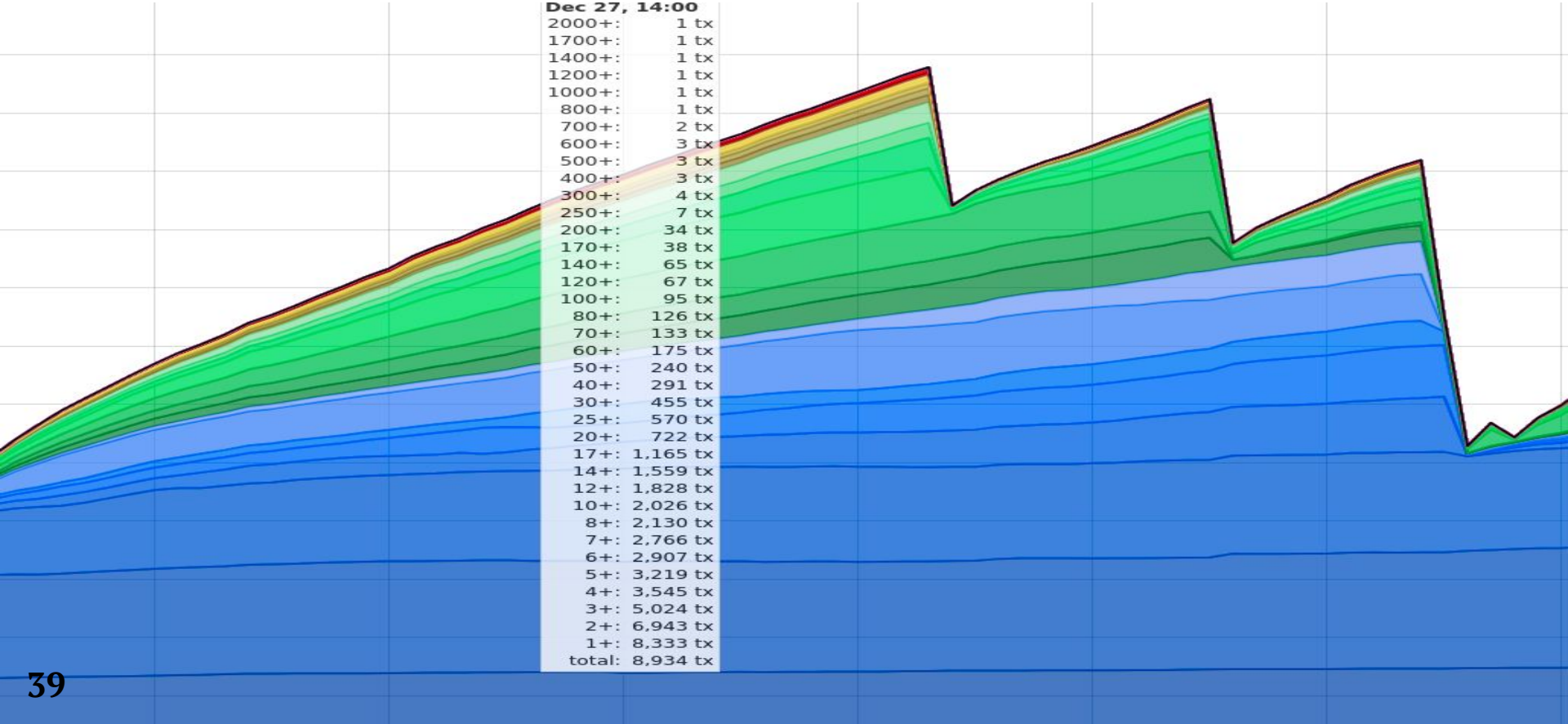
- Space for transactions is limited
- Fees determine who values their transaction
- Fees support mining as issuance declines

Are transaction fees static or dynamic?

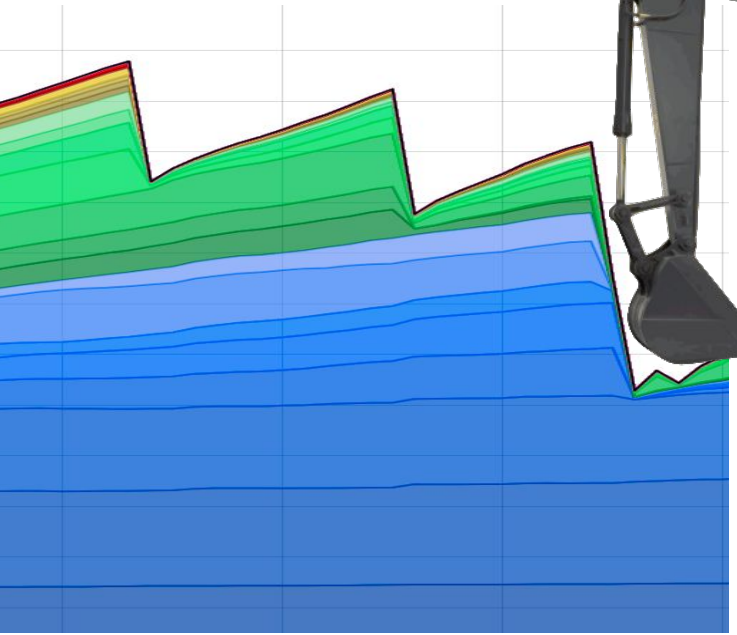
- Is there a minimum required fee?

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

Transaction Fees

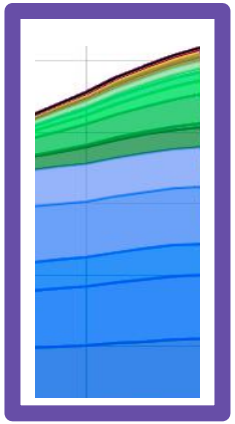


Miners Add Transactions to Blocks



Miner’s Mem-Pool
Of Unconfirmed Transactions

Miner



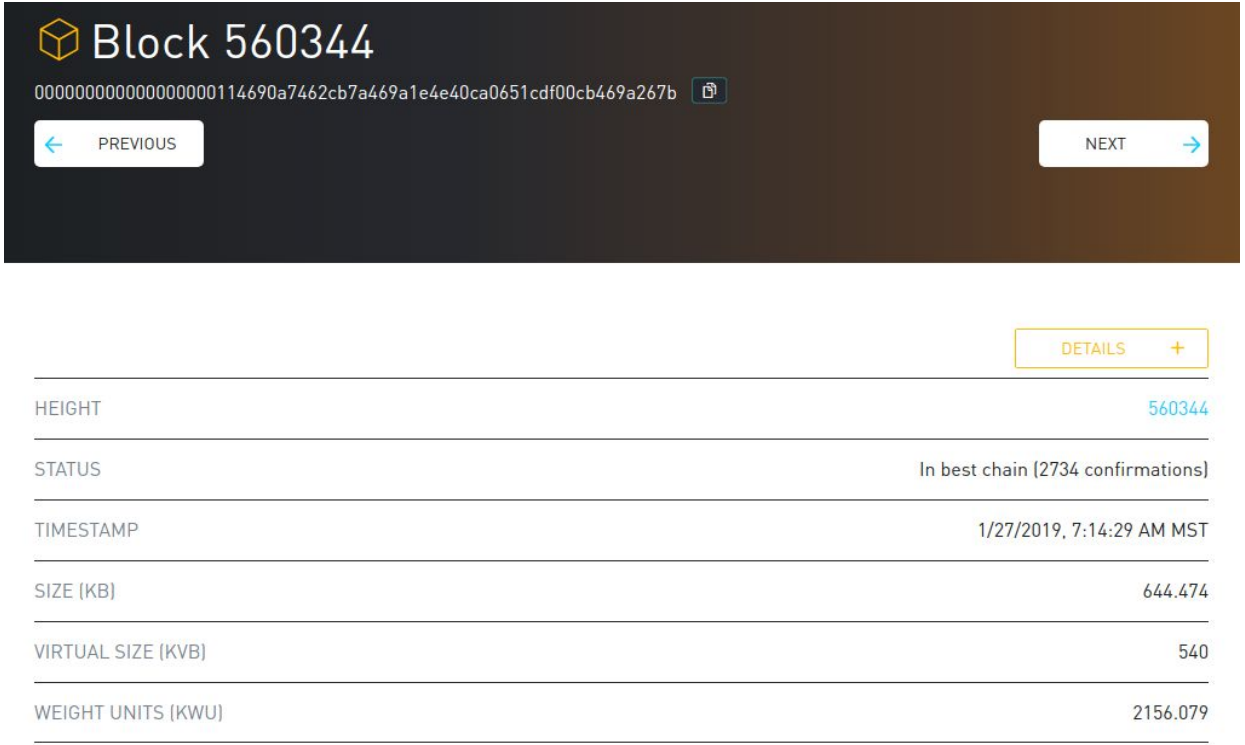
Miner’s
Candidate Block

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

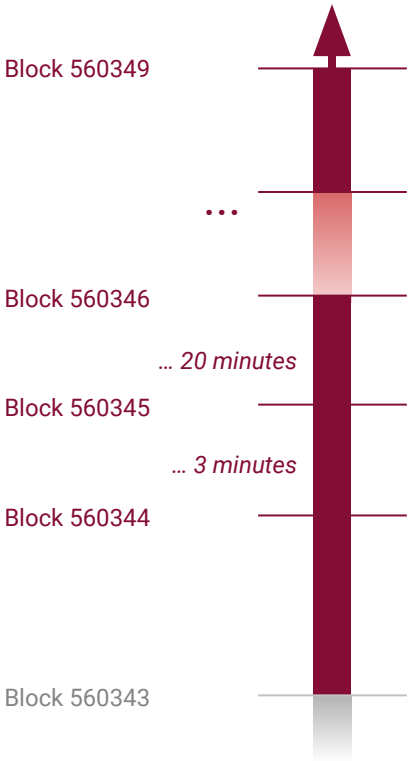
Browse: bit.ly/**B**lock344

Alice's transaction on the Bitcoin blockchain



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

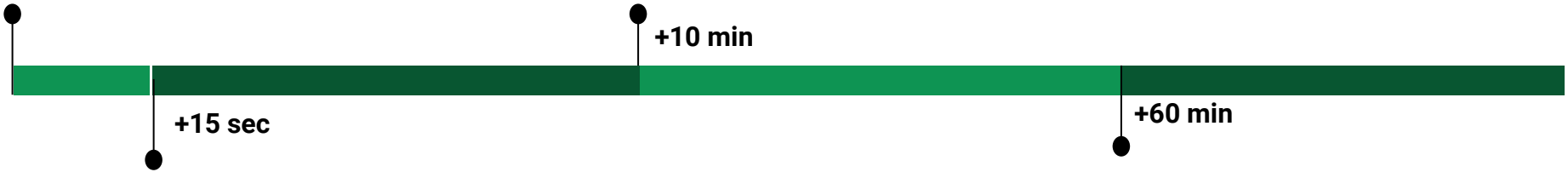
Alice's Wallet

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

Miner

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

Alice's transaction has "1 confirmation"



Bob's Wallet

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

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

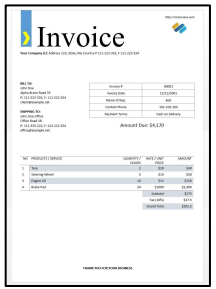
Bob's Wallet

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


Invoice

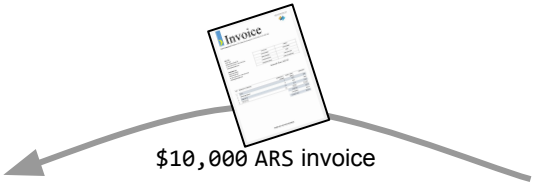
10000	=	262.03
Argentine Peso (ARS)		US Dollar (USD)

International Wire Transfer (bank)

Western Union

Paper check?

Bitcoin

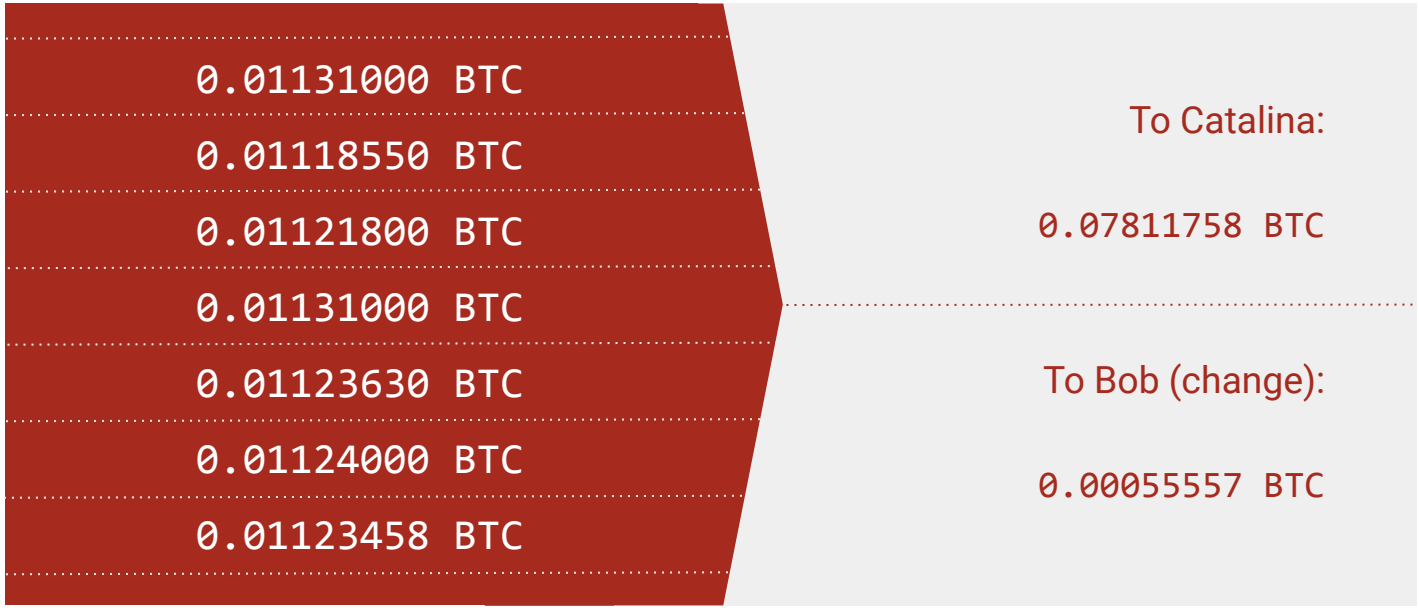


Bob

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

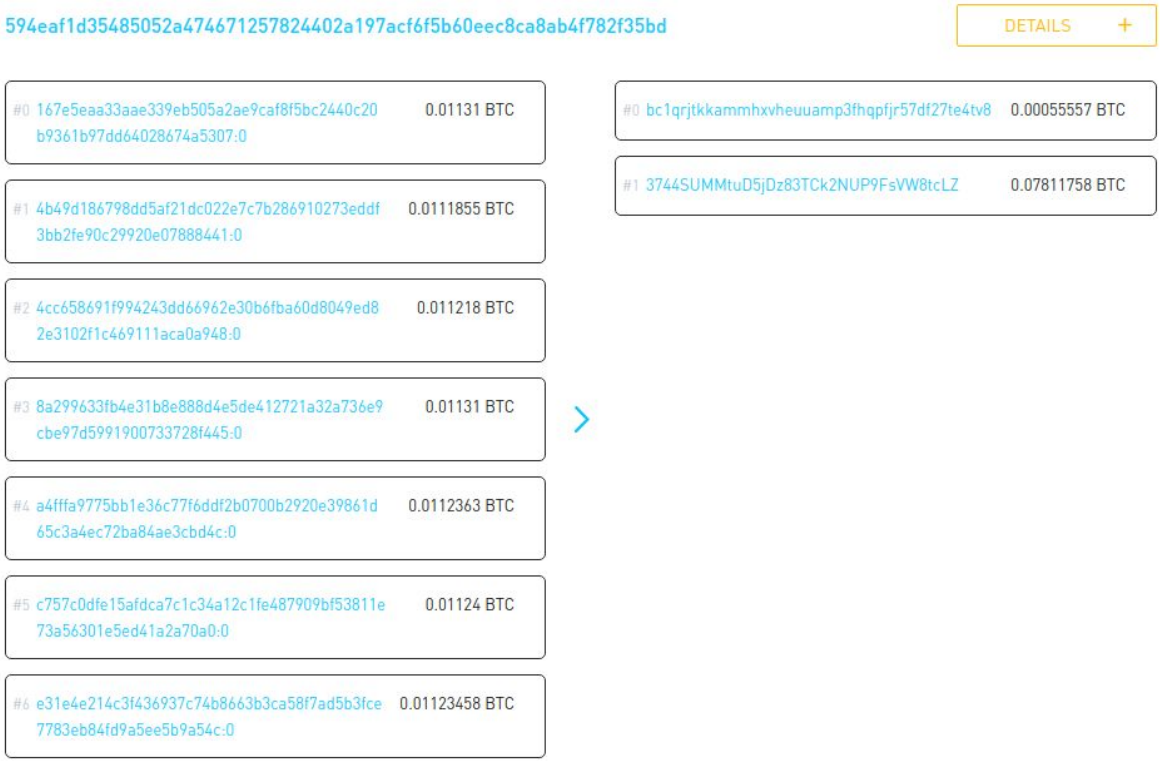
Catalina

Aggregating Transaction



Bob pays Catalina 0.07811758 BTC

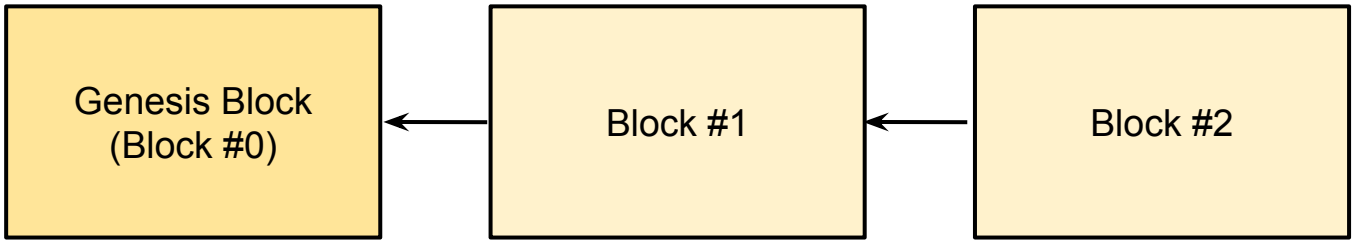
Aggregating Transaction



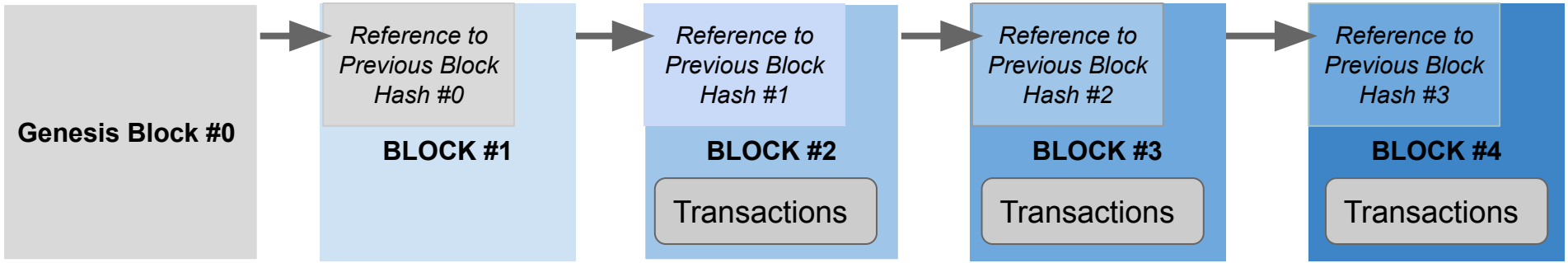
Bob pays Catalina 0.07811758 BTC

The Blockchain

History of the Bitcoin Blockchain



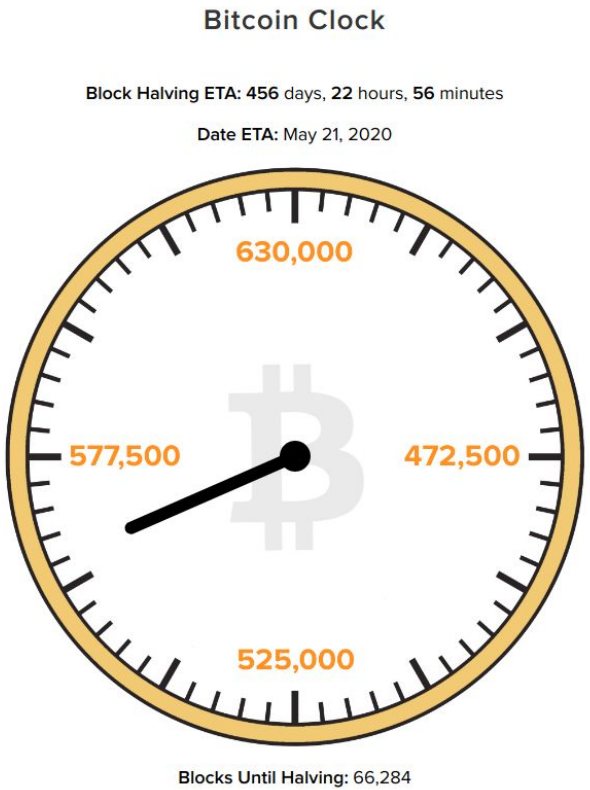
Chained Blocks



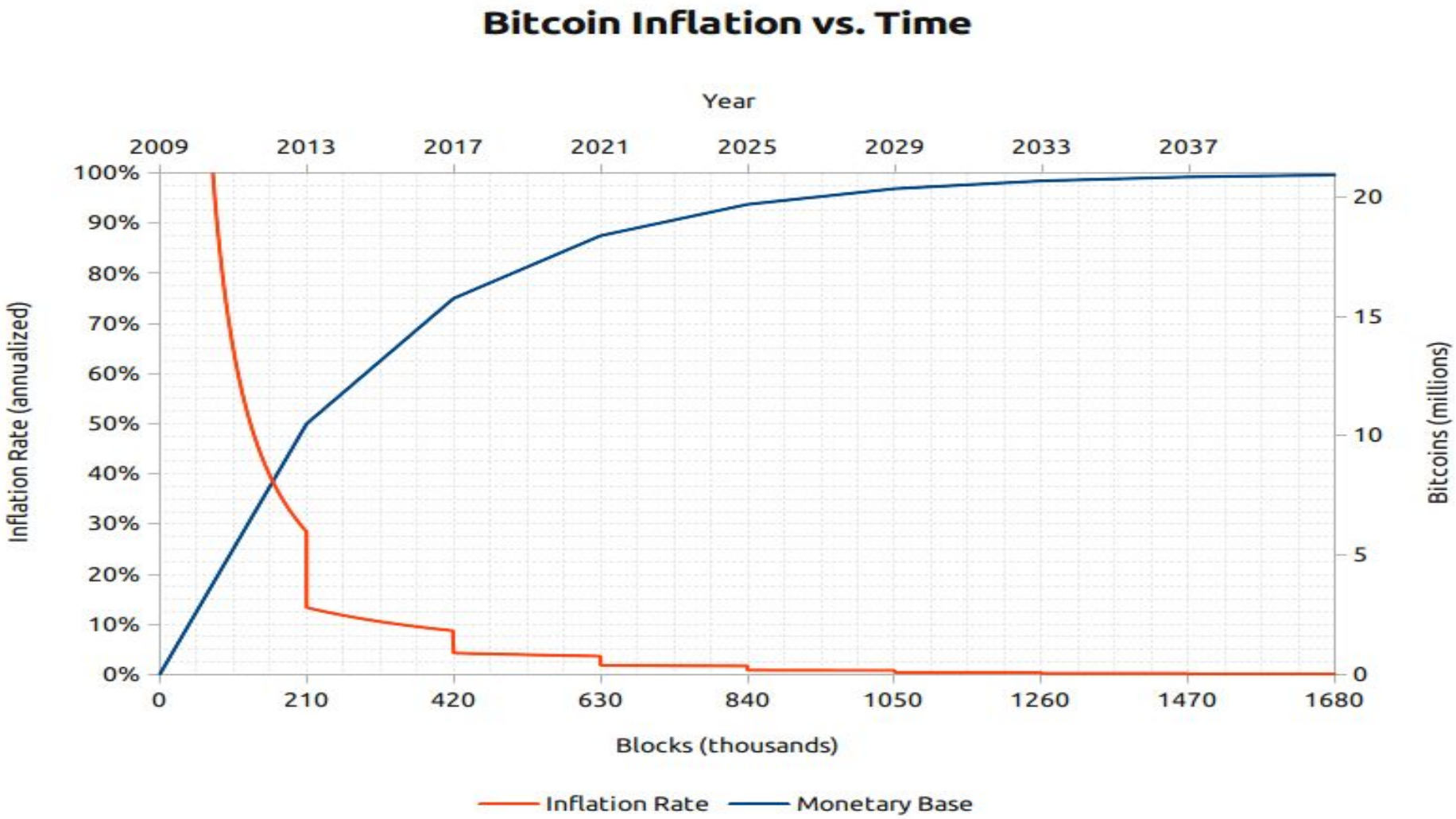
- Each block references the hash of the previous, or "parent," block
- The sequence of hashes linking each block to its parent creates a chain
- Creates a tamper-evident log; combined with proof-of-work (i.e. an energy cost for making changes) results in the characteristic of **immutability**

Monetary Policy

Halving



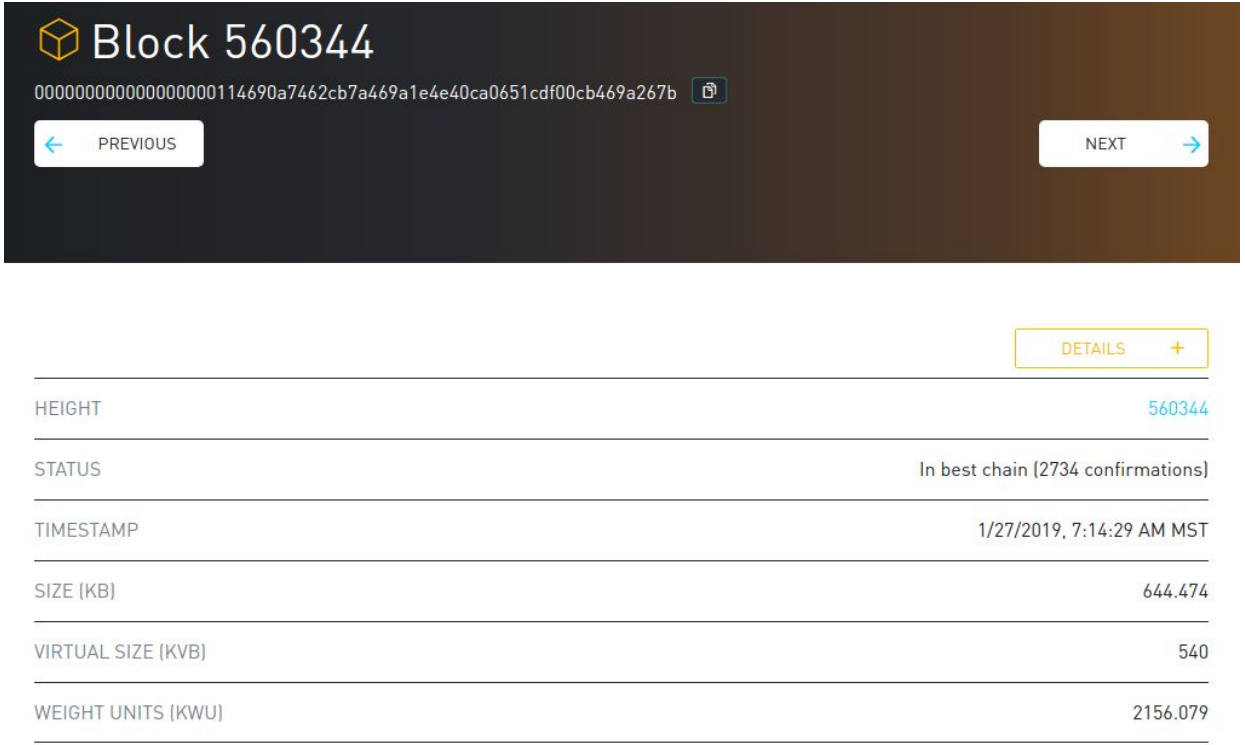
- Every 210,000 blocks
- Bitcoin issuance is “halved”
- 2009-2012: 50 BTC per block
- 2012-2016: 25 BTC per block
- 2016-2020: 12.5 BTC per block
- 2020-2024: 6.25 BTC per block
- …


Bitcoin Inflation vs. Time
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

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



Browse: bit.ly/Block344

Coinbase Transaction

e7522dcf9d53bb9136c5638a7657a10b08817b934490bdffaec19ec26521b42d

DETAILS +

#0 Coinbase

#0 1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB 12.57682767 BTC

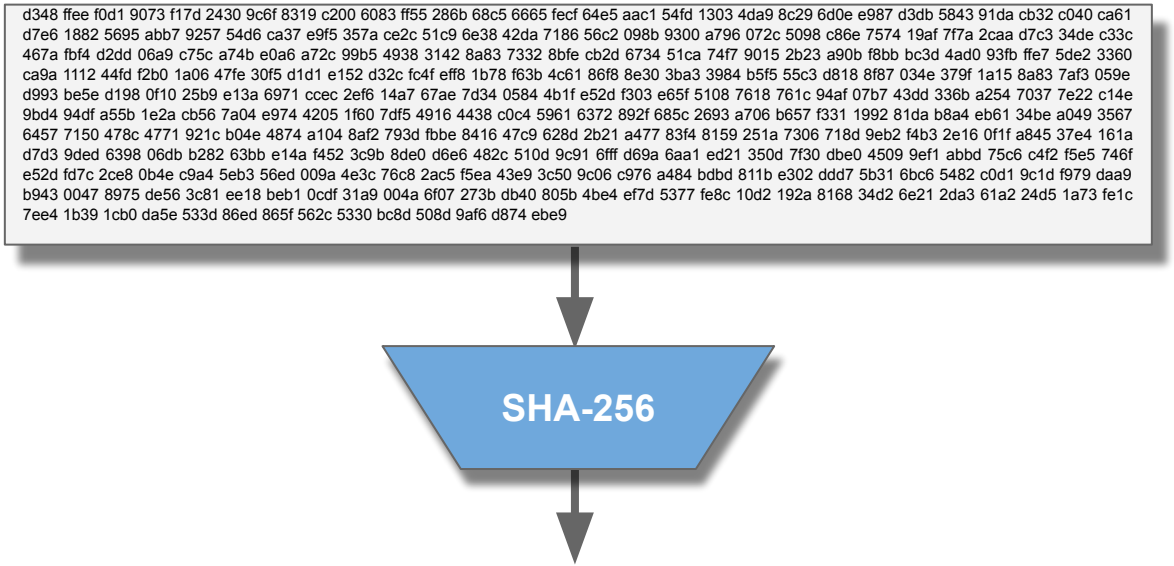
#1 OP_RETURN 0 BTC

12.57682767 BTC

Mining

SHA-256 Hash Algorithm

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



Small change in input
Big change in output

“I am Satoshi” => `ef2cdaa37271e1bea8e95b2b9ec15209f84e5eb3583449b4b4b8e7f2a18d72b9`

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

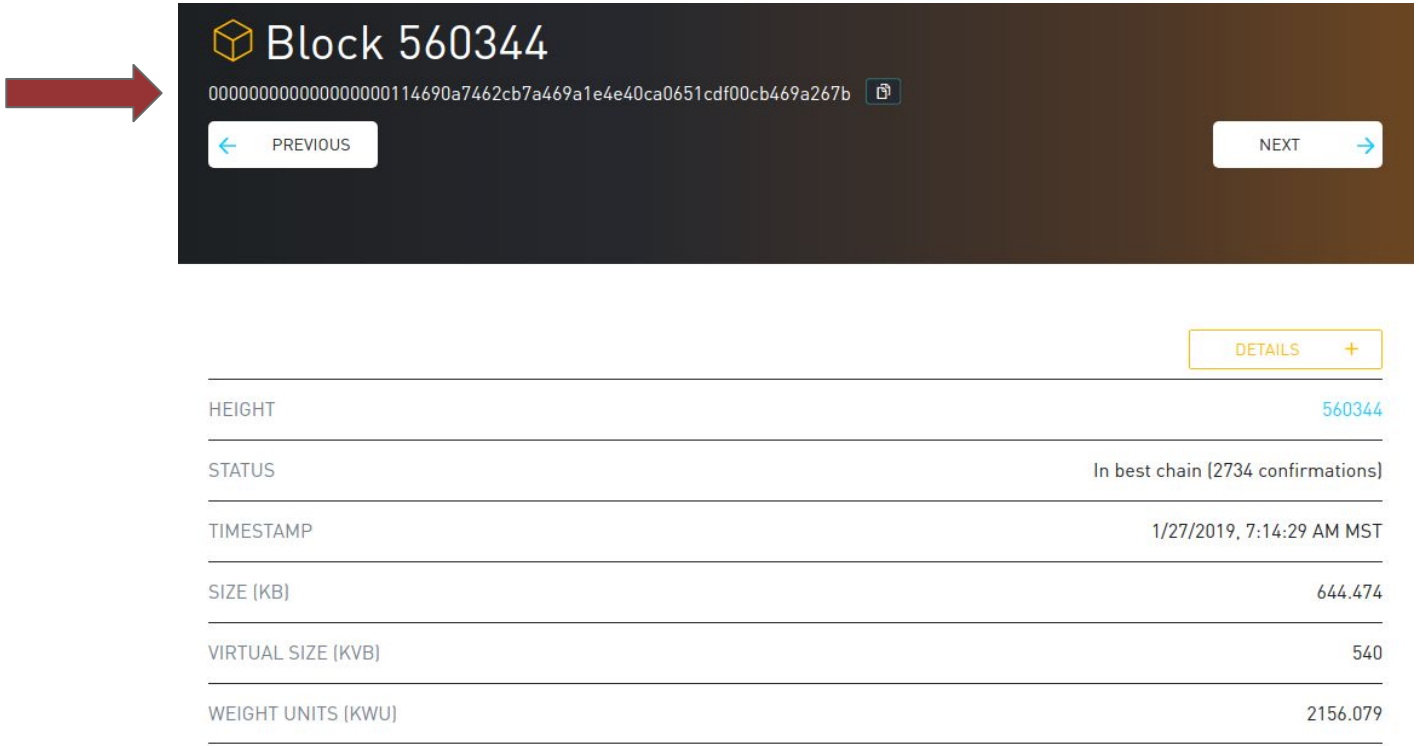
"I am Satoshi 0" => `972c421e91226b24a7a08b3099e3cebe893e5d111804d0f464f8cf472d09e1c9`
"I am Satoshi 1" => `7b1b1f24624ef8821c7fb6c95a4e0efeb4d68dac80953cdf903b3b77f086af4b`
"I am Satoshi 2" => `36c99755599d8b4bc21616c9e770c873885ad3fd4b2e4094abe9f19ce983d4cd`

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 11116500145" =>  000000000bbe916434baf4521260f5ba1e860d9ccc16a7566eee03663bc12741
```

Mining Farm

The Block Hash



Browse: bit.ly/Block344

Q & A

Thank you!

Bitcoin Basics Workshop

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?