Bitcoin, Blockchain and the Boogeyman behind it

http://knowledge.wharton.upenn.edu/article/is-this-the-end-of-money/

Prof. Sara Billey

University of Washington

Happy Mathday!

March 19, 2018

Outline

- History of Money
- The Double Spending Problem
- Electronic Currency: Bitcoin
- Encoding Monetary Transactions: Blockchain
- Satoshi Nakamoto: The Boogeyman behind it

- References for more info

Money makes the world go around

https://www.google.com/search?q=currency+images

Wikipedia: History of Money

- The **shekel** was the unit of weight and currency, first recorded c. 3000 BCE, referring to a specific weight of barley, and equivalent amounts of silver, bronze, copper, etc.

An electrum Carthaginian shekel, c. 310–290 BC, bearing the image of Tanit, consort of Baʿal Hammon.

http://www.cngcoins.com/Coin.aspx?CoinID=156634

Wikipedia: History of Money/Math

- “The **history of money** concerns the development of means of carrying out transactions involving a medium of exchange.”

- **“Money is any clearly identifiable object of value** that is generally accepted as payment for goods and services and repayment of debts within a market, or which is legal tender within a country.”

- The oldest known **tally stick** is dated to the Aurignacian, about 30,000 years ago.
- The most recent form of money is **cryptocurrency.**

Peer to Peer
Electronic Cash Transactions

Elmo makes iPhone apps.   Kiki wants to pay $1 for Elmo's app, but Apple takes a 30% cut. Elmo wants to avoid paying Apple!

Solution: Elmo takes cryptocurrency!

http://www.easydrawingtutorials.com/index.php/86-sesame-street/76-draw-elmo?start=2

https://madlibbs.deviantart.com/art/Kiki-371677944

Cryptocurrency

- My definition: An electronic payment system where transactions use cryptography to build trust instead of a central bank.
- Wikipedia: A **cryptocurrency** (or **crypto currency**) is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

Experiment

- “Face to face cash transactions” versus
- “Remote electronic cash transactions.”

Double Spending Problem

- Elmo has X cryptocoins in a ledger.
- Merchants Harry and Hermione verify that Elmo has X and sells Elmo their services.
- Both H+H use their Elmo profits to buy other services, etc.
- Eventually someone finds out that Elmo spent the same cryptocoins twice!
- How can the final merchants collect?

Introduce Bitcoin

- “Bitcoin: A peer-to-peer Electronic Cash System” by Satoshi Nakamoto. (ca 2008)

- Def: A **bitcoin** is an electronic record with a timestamp for its last transaction which is recorded in a world wide ledger stored in many different computer memories.

Introduce Bitcoin

“Bitcoin: A peer-to-peer Electronic Cash System” by Satoshi Nakamoto. (ca 2008)

Stated Goals: Create an electronic cash system so

1. No double spending allowed.
2. Extremely hard for a thief to modify the ledger.
3. Use the power of the public witness, crowd sourcing, and cryptography to build trust.
4. Incentivize honest behavior.

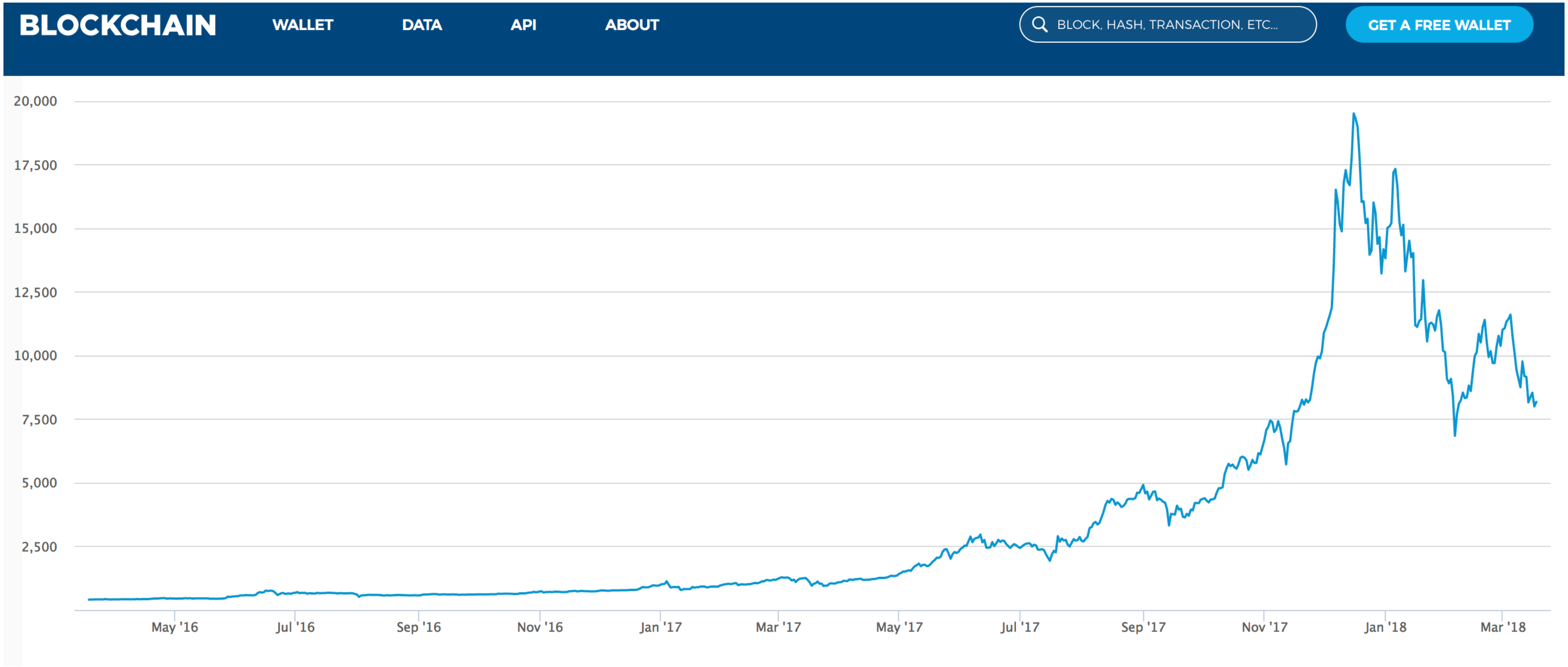
Introduce Bitcoin

Question: Did Satoshi Nakamoto succeed in creating a trusted peer-to-peer electronic cash system?

Bitcoin Current Value

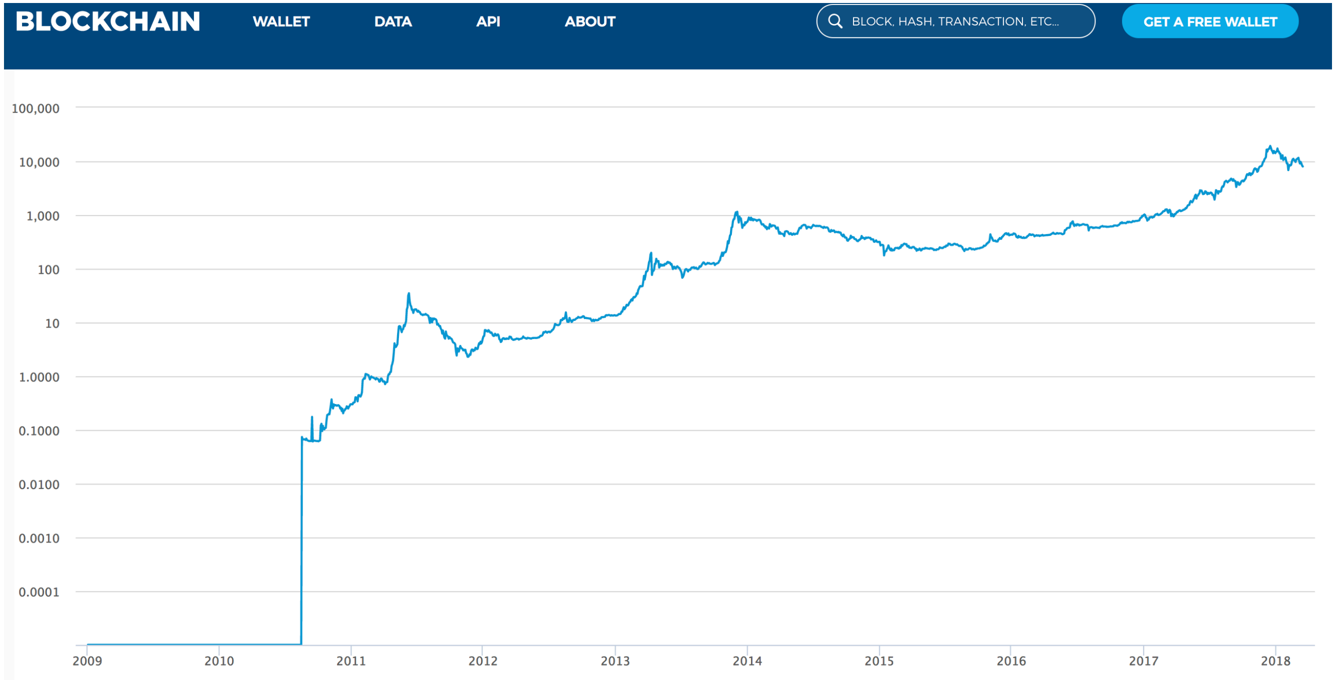
- 1 Bitcoin (BTC) = 8,155.32 USD   2018-03-18
- 1 Satoshi = 0.00000001 Bitcoins

Bitcoin value over time



https://blockchain.info/charts/market-price?timespan=all

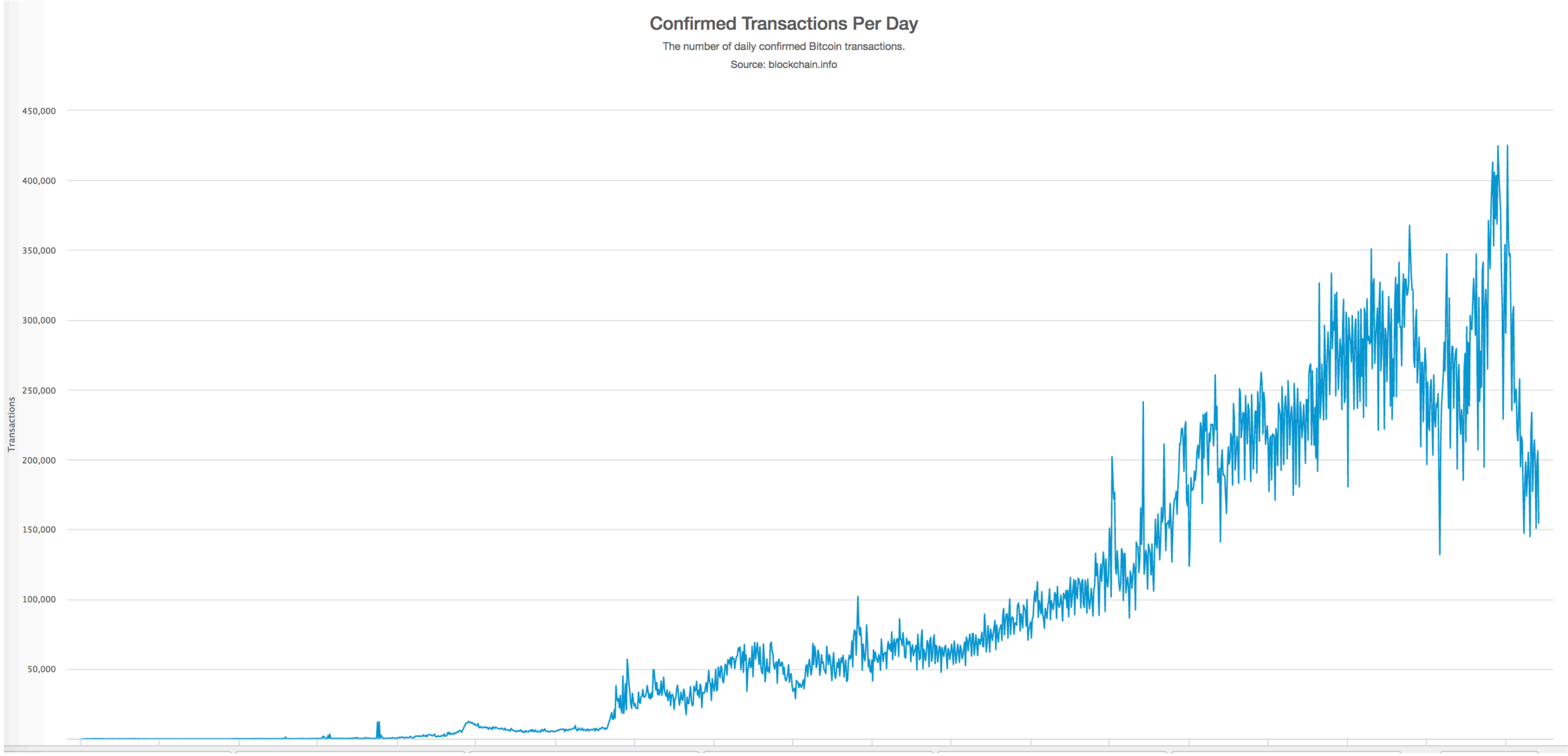
Bitcoin value log scale



1 Bitcoin (BTC) = .067 USD on 2010-08-23

https://blockchain.info/charts/market-price?timespan=all&scale=1

169,059 Confirmed Transactions on Sunday March 18, 2018



Confirmed Transactions Per Day

The number of daily confirmed Bitcoin transactions.

Source: blockchain.info

https://blockchain.info/

Introduce Bitcoin

Question: Did Satoshi Nakamoto succeed in creating a trusted peer-to-peer electronic cash system?

My Answer: **Yes! It’s brilliant!**

We need to understand how it works and how it builds on math that is understand.

Timestamp Ledger

Example Timestamp Ledger:

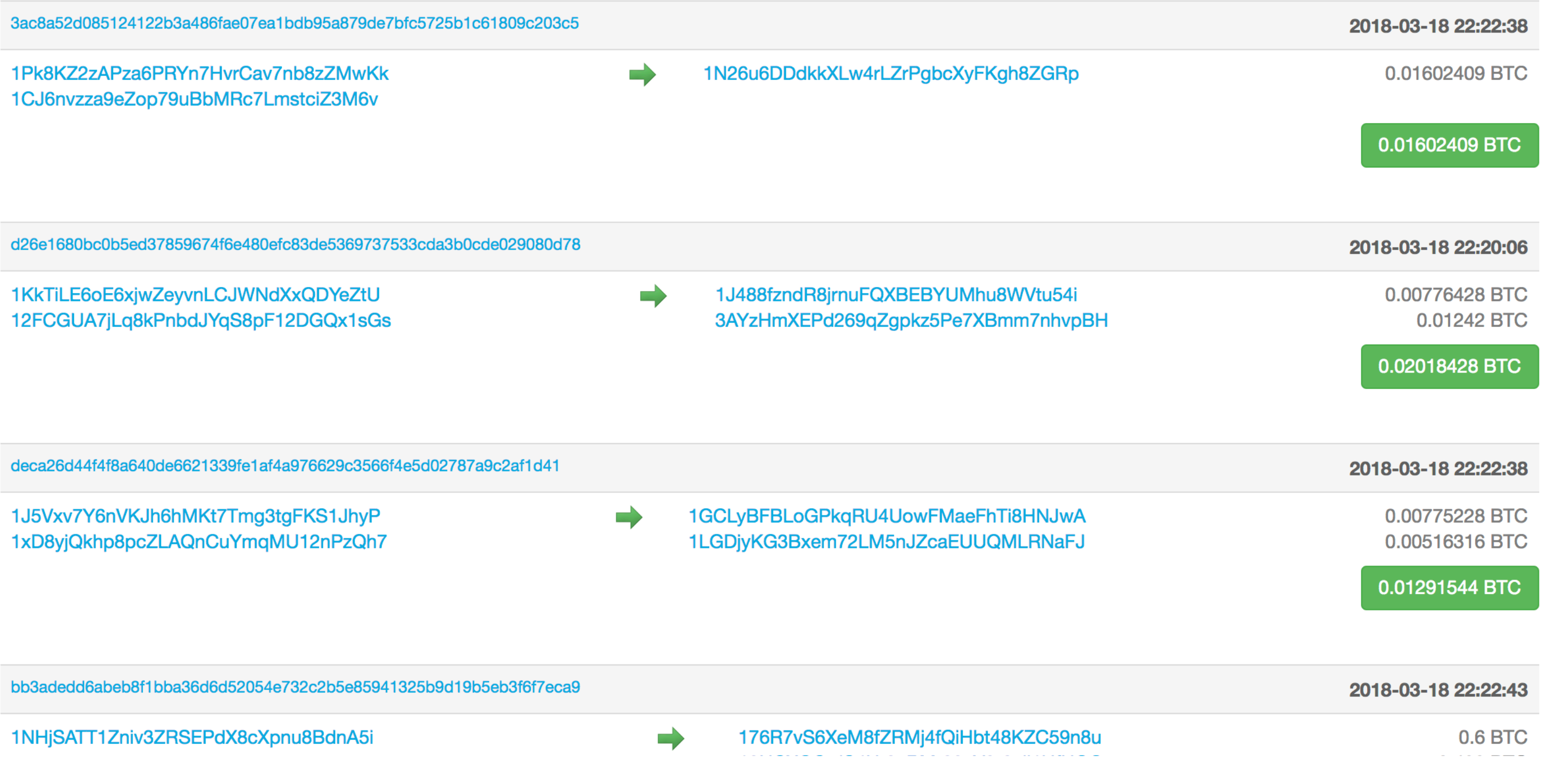
Owner	Acquired
B1: 002391	2018-03-18 22:24:13
B2: 308937	2018-03-18 22:27:08
B3: 100273	2018-03-18 22:29:03
…	

Example New Transactions :

B2 sold to 100273 at 2018-03-19 02:29:03

B7 sold to 308937 at 2018-03-19 10:49:03

Real Transactions Yesterday



3ac8a52d085124122b3a486fae07ea1bdb95a879de7bfc5725b1c61809c203c5 **2018-03-18 22:22:38**

1Pk8KZ2zAPza6PRYn7HvrCav7nb8zZMwKk
1CJ6nvzza9eZop79uBbMRc7LmstciZ3M6v → 1N26u6DDdkkXLw4rLZrPgbcXyFKgh8ZGRp 0.01602409 BTC

0.01602409 BTC

d26e1680bc0b5ed37859674f6e480efc83de5369737533cda3b0cde029080d78 **2018-03-18 22:20:06**

1KkTiLE6oE6xjwZeyvnLCJWNdXxQDYeZtU → 1J488fzndR8jrnuFQXBEBYUMhu8WVtu54i 0.00776428 BTC
12FCGUA7jLq8kPnbdJYqS8pF12DGQx1sGs 3AYzHmXEPd269qZgpkz5Pe7XBmm7nhvpBH 0.01242 BTC

0.02018428 BTC

deca26d44f4f8a640de6621339fe1af4a976629c3566f4e5d02787a9c2af1d41 **2018-03-18 22:22:38**

1J5Vxv7Y6nVKJh6hMKt7Tmg3tgFKS1JhyP → 1GCLyBFBLoGPkqRU4UowFMaeFhTi8HNJwA 0.00775228 BTC
1xD8yjQkhp8pcZLAQnCuYmqMU12nPzQh7 1LGDjyKG3Bxem72LM5nJZcaEUUQMLRNaFJ 0.00516316 BTC

0.01291544 BTC

bb3adedd6abeb8f1bba36d6d52054e732c2b5e85941325b9d19b5eb3f6f7eca9 **2018-03-18 22:22:43**

1NHjSATT1Zniv3ZRSEPdX8cXpnu8BdnA5i → 176R7vS6XeM8fZRMj4fQiHbt48KZC59n8u 0.6 BTC

https://blockchain.info/block/0000000000000000000131bdc80aa7b7f5f77a57330198b9d9f66549b38558003

Encoded Timestamp Ledger: Blockchain

A hash function is any function that takes any typed message as input and outputs a number in a specific range.

Toy example: Count words(Sara owes Paul 5 kidcoins)=5

Real example using SHA-256 hash function:

```
bash-3.2$ more test.message.1
Sara owes Paul 5 kidcoins.
bash-3.2$ shasum test.message.1
1a5313f03a23ea9f5f3638f40e07ab95eac6dbee
```

Encoded Timestamp Ledger: Blockchain

Real example using SHA-256 hash function:

```
bash-3.2$ more test.message.1
Sara owes Paul 5 kidcoins.
bash-3.2$ shasum test.message.1
1a5313f03a23ea9f5f3638f40e07ab95eac6dbee

bash-3.2$ more test.message.2
Sara owes Paul 5 kidcoins. Blueberry.
bash-3.2$ shasum test.message.2
73cd28117281780d12f06d3633fb4f7a651ab1c3
```

Encoded Timestamp Ledger: Blockchain

A nunce is any extra phrase that when added to a message gives a hash value with a fixed number of 0’s at the beginning or end.

Example: One required initial 0

```
bash-3.2$ more test.message.3; shasum test.message.3
Sara owes Paul 5 kidcoins. 7.
06805c616152a28933ccf43c9c23579d34958662
```

The nunce is “7.”

Encoded Timestamp Ledger: Blockchain

A nunce is any extra phrase that when added to a message gives a hash value with a fixed number of 0’s at the beginning or end.

Example: Two required initial 0’s:

```
bash-3.2$ more test.message.3; shasum test.message.3
Sara owes Paul 5 kidcoins. 10.
007a67a09e125c3ec891bb998b4b89331ae63ca5
```

Now the nunce is “10.”

Blockchain: Worldwide Competition

1. Use a hash function like SHA-256 on the file which contains all the current Bitcoins, Owners, and Timestamps to verify it gives the current hash value.

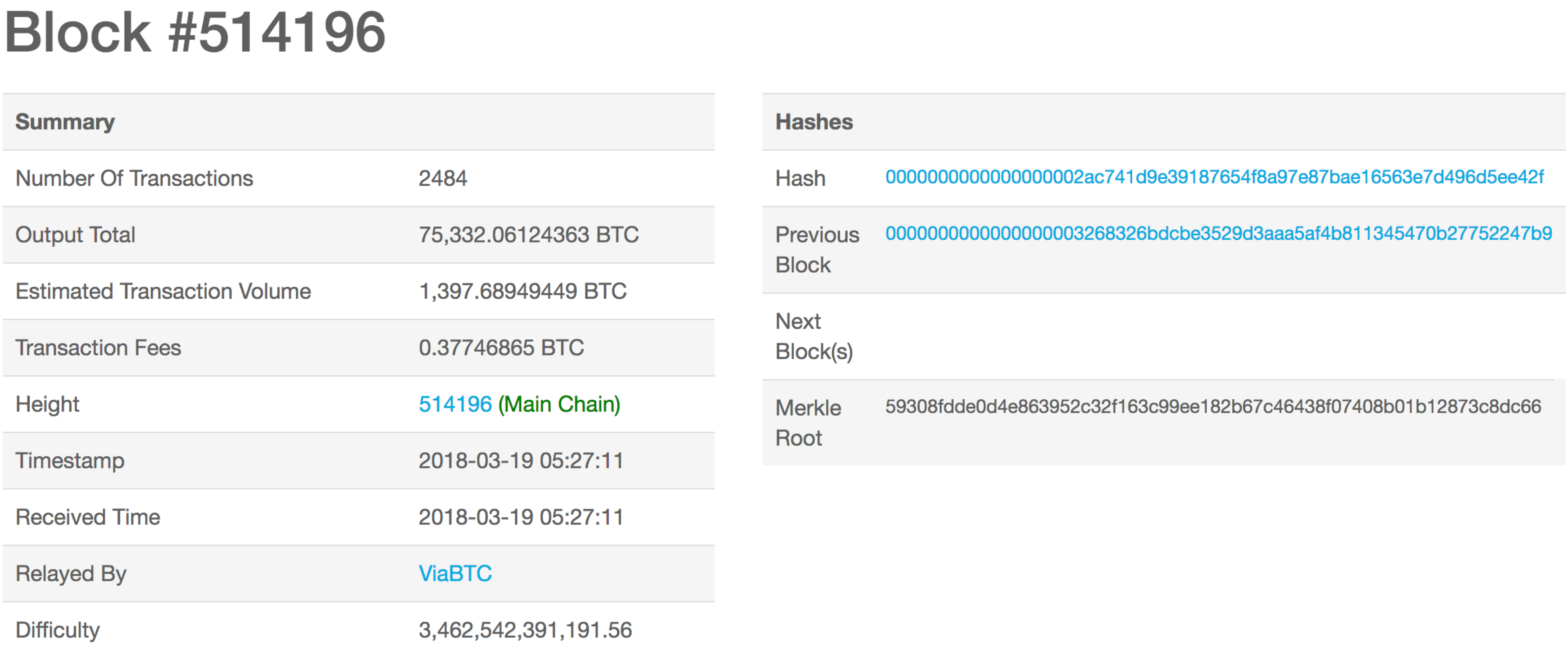
2. Test each new transaction to see if anyone has attempted to double spend a bitcoin.

3. If not, add all new transactions to the ledger.

4. Goal: Find a nunce to add to the updated file so that it has enough initial zeros to meet the current challenge.

5. First computer to find a nunce, wins 1 BTC.

Blockchain: Competition



Block #514196

Summary	
Number Of Transactions	2484
Output Total	75,332.06124363 BTC
Estimated Transaction Volume	1,397.68949449 BTC
Transaction Fees	0.37746865 BTC
Height	514196 (Main Chain)
Timestamp	2018-03-19 05:27:11
Received Time	2018-03-19 05:27:11
Relayed By	ViaBTC
Difficulty	3,462,542,391,191.56

Hashes	
Hash	0000000000000000002ac741d9e39187654f8a97e87bae16563e7d496d5ee42f
Previous Block	0000000000000000003268326bdcbe3529d3aaa5af4b811345470b27752247b9
Next Block(s)	
Merkle Root	59308fdde0d4e863952c32f163c99ee182b67c46438f07408b01b12873c8dc66

Bitcoin and Blockchaining

Where is the math?

- Game Theory: logical set of rules and incentive.
- Cryptography: used to digitally sign transfers and in the creation of the hash function.
- Probability: The trust factor comes from the probabilistic proof-of-work needed to get the longest blockchain.

Bitcoin and the Boogeyman Behind it

“Bitcoin: A peer-to-peer Electronic Cash System” by Satoshi Nakamoto. (ca 2008)

1,000,000BTC Question: Who is Satoshi Nakamoto?

We don’t know! “He” is a mythical team of people who set up the bitcoin decentralized software and set it running. He/She/They are boogeypeople.

References

- **Bitcoin: A peer-to-peer Electronic Cash System** by Satoshi Nakamoto. https://bitcoin.org/en/
- **How the Bitcoin protocol actually works** by Michael Nielsen on December 6, 2013. http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/
- **Letter to Jamie Dimon; And anyone else still struggling to understand cryptocurrencies.** Oct 16, 2017 https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80