

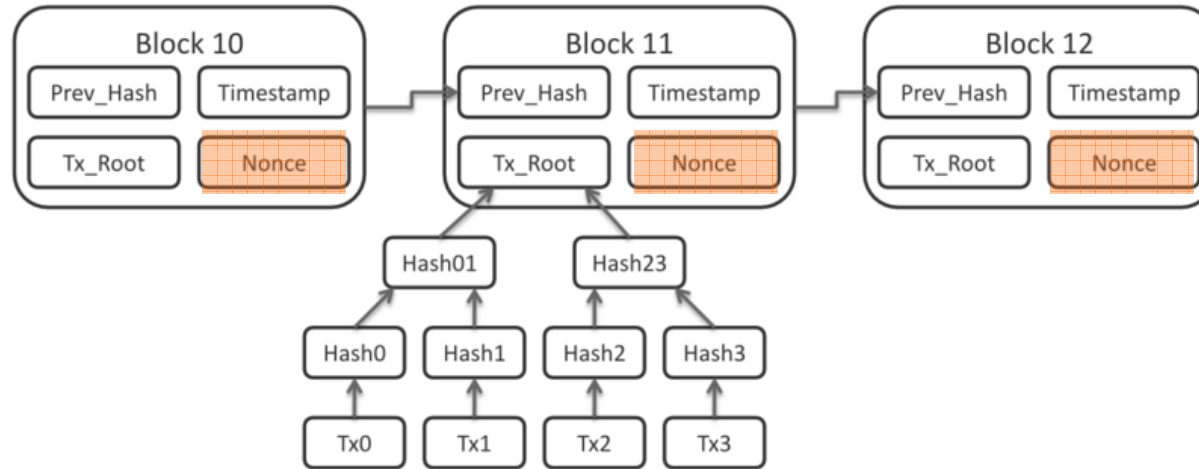
# **Blockchain governance and dispute resolution**



# Blockchain governance

- Open blockchains
  - Organic democracy
  - “Code = law”
- Private or “permissioned” blockchains

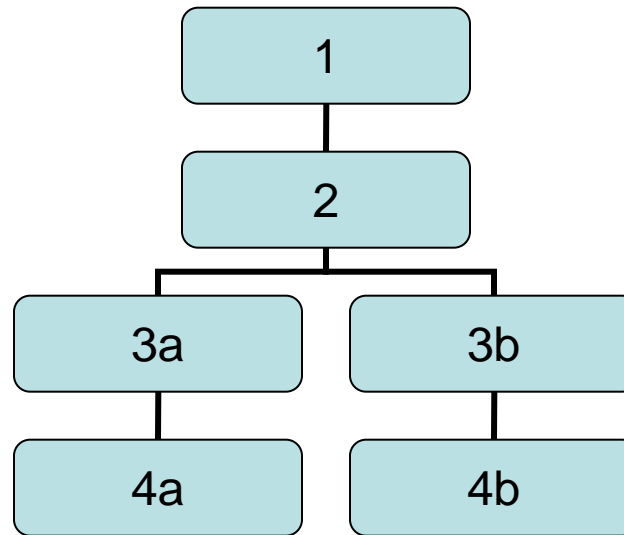
# To win a block: find a valid Nonce



- A valid “nonce” must be discovered by trial-and-error, such that the hash function for the entire block begins falls below a critical value

# Blockchain forks

**Some occur spontaneously from mining**



Assume two miners solve block 3 at exactly the same time.

Half the community adopts 3a, and the other half adopts 3b.

## **How does this get resolved?**

- Miners gravitate toward whichever chain extends itself more quickly
- How quickly does this occur? What if your transaction is in block 3a but not in block 3b?

# Wait for six blocks (one hour)?

## How many Bitcoin Confirmations are Enough?

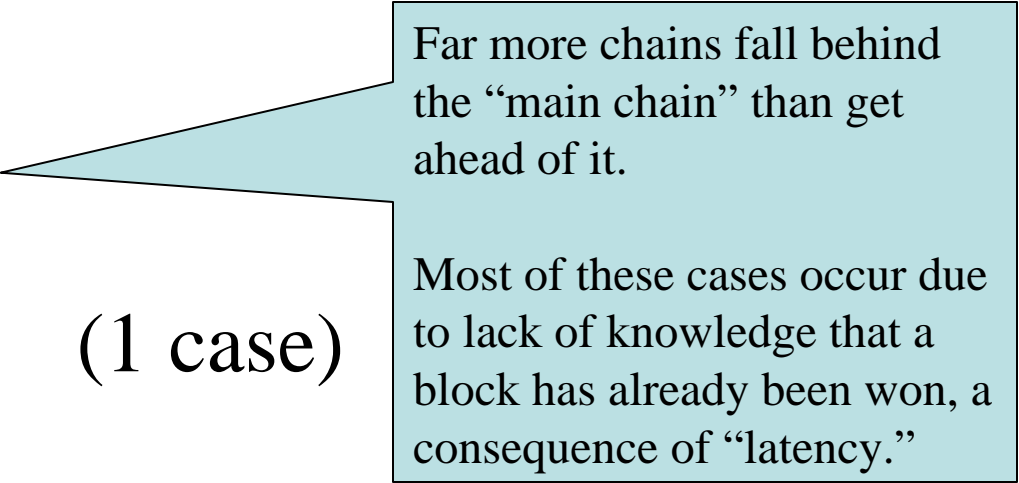
- 0 Payments with 0 confirmations can still be reversed! Wait for at least one.
- 1 One confirmation is enough for small Bitcoin payments less than \$1,000.
- 3 Enough for payments \$1,000 - \$10,000. Most exchanges require 3 confirmations for deposits.
- 6 Enough for large payments between \$10,000 - \$1,000,000. Six is standard for most transactions to be considered secure.
- 60 Suggested for large payments greater than \$1,000,000. Less is likely fine, but this is to be safe!

*Source:* <https://www.buybitcoinworldwide.com/confirmations/>

# Probability of confirmation

Most recent 10,000 blocks

- +3 100%
- +2 99.99% (1 case)
- +1 72%
- Tied 50%
- -1 40%
- -2 c. 0% (1 case)



Far more chains fall behind the “main chain” than get ahead of it.

Most of these cases occur due to lack of knowledge that a block has already been won, a consequence of “latency.”

*Source:* Saleh (2017)

# Probability of confirmation

## Most recent 10,000 blocks

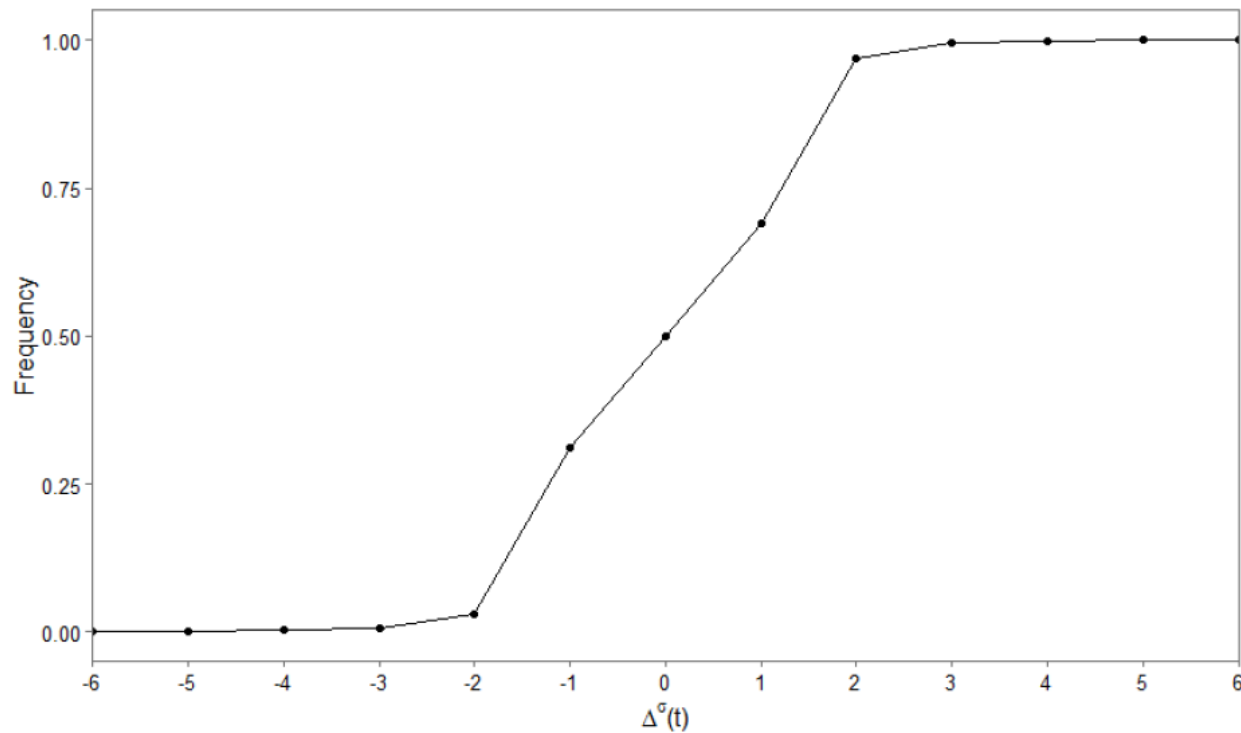


Figure 5: This figure plots the frequency with which a branch eventually becomes part of the blockchain as the difference between the two longest branches varies. The data corresponds to the Bitcoin blockchain over blocks 350,000 - 450,000 (03/30/2015 - 01/25/2017). I provide detail regarding the data-gathering process in [Appendix B](#).

*Source:* Saleh (2017)

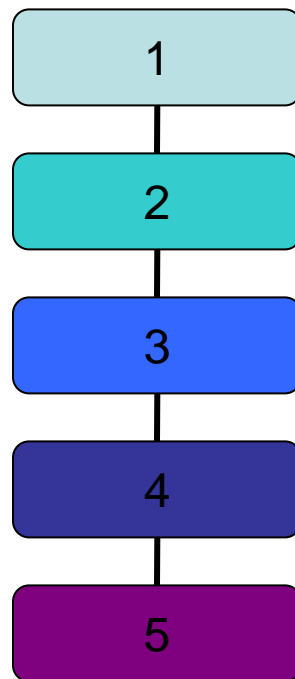


# Blockchain forks

## Some occur deliberately

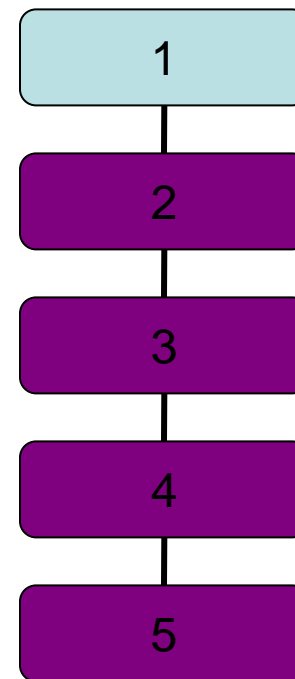
Soft:

Gradual adoption



Hard:

Mandatory adoption



# Hard and soft forks

- A *hard fork* is a software upgrade. It changes the rules for validating blocks and is not compatible with older software
  - Non-upgraded nodes will not recognize new blocks as valid
  - A hard fork is therefore mandatory
- In contrast, a *soft fork* is a software upgrade that is backward compatible.
  - Non-upgraded nodes will recognize new blocks as valid
  - A soft fork may require a minimum rate of adoption (e.g. 51%) to take effect

# Hard forks can be risky

- Bugs
  - see recent Ethereum upgrade
- Ignorant nodes
- Holdout nodes
- Dissenter nodes
  - Ethereum Classic                      2016      (15%)
  - Bitcoin Cash                              2017      (10%)
  - Bitcoin Gold                              2017      (? %)
- *These hard forks may be initiated by a minority who wish to leave the main chain*



# Bitcoin Cash hard fork

August 1, 2017

**Bitcoin has been upgraded.**

**New features are available on Bitcoin Cash.**

If you owned bitcoin on August 1<sup>st</sup>, you already have Bitcoin Cash.

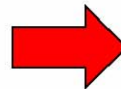
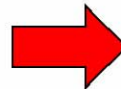
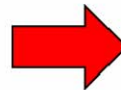
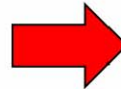


**Standard Block Size:** 1MB Maximum.

**SegWit:** Transaction signatures can be discarded from the blockchain.

**Single centralized development team** and client implementation: Bitcoin Core.

**Scaling plan:** Off-chain payment channels.



**PowerBlocks:** 8MB Maximum.

**SecureSigs:** All transaction signatures must be validated and secured on the blockchain.

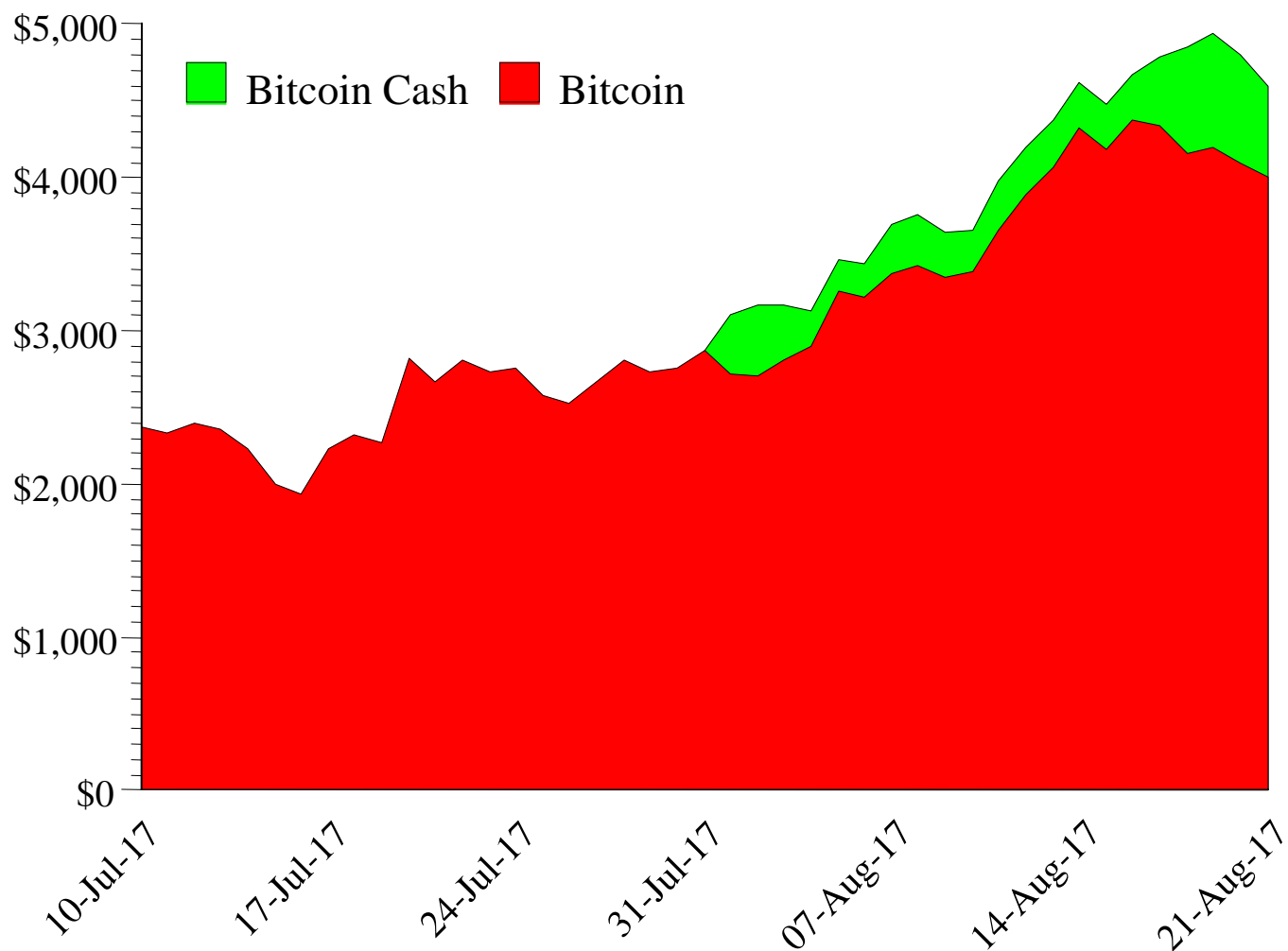
**Multiple independent development teams** and client implementations including: Bitcoin Unlimited, Bitcoin ABC, Bitcoin XT, and Bitcoin Classic.

**Scaling Plan:** On-chain transactions and market driven blocksize increases.

Find out more at: [www.bitcoincash.org](http://www.bitcoincash.org) | [www.bitcoinabc.org](http://www.bitcoinabc.org) | [www.reddit.com/r/btc](http://www.reddit.com/r/btc)

# Free money?

No apparent ex dividend effect



**Why not do this again and again?**



OCTOBER 25

# An overview of Bitcoin forks

<https://forkdrop.io/>

## What are Bitcoin forks?

A fork is where a new project starts and decides on different set of blockchain consensus rules, but decides to continue on from the Bitcoin blockchain. It decides on a block to serve as the fork point and begins generating a different block sequence that is incompatible with the Bitcoin chain. It has common ancestry with the Bitcoin blockchain, so private keys that held balances of coins before the fork block have the ability to spend those coins on the new chain and separately on the Bitcoin blockchain.

## Is this free money?

Yes, it is! A number of these coins have achieved some level of price support and these coins may be bought or sold on some cryptocurrency exchanges.

# Bitcoin forks, 2014-present

## Prices as of 20 September 2018

|                   |        |           |          |                        |        |           |        |
|-------------------|--------|-----------|----------|------------------------|--------|-----------|--------|
| CLAMs             | 300377 | 12-May-14 | \$1.96   | Bitcoin Boy            | 502233 | 02-Jan-18 |        |
|                   |        |           |          | World Bitcoin          | 503888 | 12-Jan-18 |        |
| Dalilcoin         | 350000 | 30-Mar-15 |          | BitVote                | 505050 | 19-Jan-18 |        |
| Qeditas           | 350000 | 30-Mar-15 |          | Bitcoin Smart          | 505050 | 19-Jan-18 |        |
|                   |        |           |          | Bitcoin Interest       | 505083 | 20-Jan-18 | \$1.37 |
| Bitcoin Cash      | 478558 | 01-Aug-17 | \$455.01 | Bitcoin Atom           | 505888 | 24-Jan-18 | \$0.24 |
| Bitcoin Clashic   | 478558 | 01-Aug-17 |          | Bitcoin Community      | 506066 | 25-Jan-18 |        |
| Bitcoin Coral     | 491407 | 24-Oct-17 |          | Bitcoin Pro            | 506984 | 31-Jan-18 |        |
| Bitcoin Gold      | 491407 | 24-Oct-17 | \$21.57  | Bitcoin Parallel       | 507000 | 31-Jan-18 |        |
| BitCore           | 492820 | 02-Nov-17 | \$0.45   | Bitcoin Hush           | 507089 | 01-Feb-18 |        |
| Bitcoin Diamond   | 495866 | 24-Nov-17 | \$17.87  | Bitcoin 2              | 507850 | 05-Feb-18 |        |
| Bitcoin@CBC       | 498754 | 11-Dec-17 |          | Big Bitcoin            | 508888 | 12-Feb-18 |        |
| Bitcoin Hot       | 498848 | 12-Dec-17 |          | Bitcoin Cloud          | 510048 | 20-Feb-18 |        |
| BitClassic Coin   | 498888 | 12-Dec-17 |          | Bitcoin Private        | 511346 | 28-Feb-18 | \$2.98 |
| BitcoinX          | 498888 | 12-Dec-17 | \$44.08  | Bitcoin Candy          | 512666 | 12-Jan-18 |        |
| Oil Bitcoin       | 498888 | 12-Dec-17 |          | Bitcoin Lambo          | 515350 | 27-Mar-18 |        |
| Nash              | 498888 | 12-Dec-17 | \$5.91   | ClassicBitcoin         | 516095 | 01-Apr-18 |        |
| Bitcoin Pay       | 499345 | 15-Dec-17 |          | Bitcoin Clean          | 518800 | 18-Apr-18 |        |
| Bitcoin World     | 499777 | 17-Dec-17 |          | Smart Bitcoin          | 520000 | 20-Apr-18 |        |
| Bitcoin King      | 499999 | 18-Dec-17 |          | Fox BTC                | 520419 | 30-Apr-18 |        |
| Bitcoin Stake     | 499999 | 18-Dec-17 |          | Bitcoin Reference Line | 523118 | 17-May-18 |        |
| Lightning Bitcoin | 499999 | 18-Dec-17 | \$6.26   | MicroBitcoin           | 525000 | 28-May-18 |        |
| Bitcoin Faith     | 500000 | 18-Dec-17 |          | Bitcoin Class          | 528000 | 29-Apr-18 |        |
| Bitcoin Wonder    | 500000 | 18-Dec-17 |          | Bitcoin Dao            | 531650 | 30-Jun-18 |        |
| FastBitcoin       | 501225 | 27-Dec-17 |          | BitcoinZero            | 539360 | 31-Aug-18 |        |
| Bitcoin File      | 501225 | 27-Dec-17 |          | ANONymous              | 540870 | 10-Sep-18 |        |
| Bitcoin God       | 501225 | 27-Dec-17 | \$11.06  |                        |        |           |        |
| Quantum Bitcoin   | 501368 | 28-Dec-17 |          |                        |        |           |        |
| Bitcoin Cash Plus | 501407 | 28-Dec-17 |          |                        |        |           |        |
| Segwit2X          | 501451 | 28-Dec-17 | \$0.19   |                        |        |           |        |
| Bitcoin Holocaust | 501488 | 29-Dec-17 |          |                        |        |           |        |
| Bitcoin Pizza     | 501888 | 31-Dec-17 |          |                        |        |           |        |
| Bitcoin Nano      | 501888 | 31-Dec-17 |          |                        |        |           |        |
| Bitcoin Ore       | 501949 | 31-Dec-17 |          |                        |        |           |        |

Source: <https://forkdrop.io/>



# **“Code = law”**

## **Nakamoto’s idea of consumer protection**

### **1. Introduction**

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

# Code = law?

## Why it might be a good idea

- Cost savings
  - Better designed software might lead to fewer disputes
    - Transparency
    - Better security
  - In the legacy system, everyone pays a “tax” for consumer protection
    - Often an artifact of aggressive regulation that protects the lazy or uninformed (e.g. CFPB)
    - Reduces freedom of choice
    - Prevents the market from deciding upon the optimal amount of consumer protection
- Places responsibility on parties to monitor, thereby reducing moral hazard problems
  - The current system encourages free riding
  - Gaming of the dispute resolution occurs frequently

# Code = law?

## Accidental fees to miners

- On August 28, 2013, a bitcoin user sent a 200 bitcoin fee (\$23,518) that was processed by ASICMiner
  - Solution carried out: complaints on Reddit leading to a *purported* refund
- On April 25, 2015, a BitGo user, due to a software glitch, accidentally sent 85 bitcoins (\$19,197) as a mining fee to AntPool
  - Solution carried out: complaints on Reddit leading to a refund
- On September 11, 2015, another user sent 4.6 bitcoins (worth \$1,113) as a fee to AntPool
  - Solution carried out: Bitmain, the parent company, once again returned the fee to the user
- On April 27, 2016, a user sent a 291 bitcoin fee (~ \$137,000) that was packaged by BitClub Network, a pool in the Netherlands
  - Half the fee (146 bitcoins) was later donated to The Bitcoin Foundation

Source: Tim Swanson

# Code = law?

## Breakdowns on the bitcoin blockchain

- On August 15, 2010, block 74638 contained 184.4 billion bitcoins
  - Solution: Hard fork / soft fork (depends on who you talk to)
- On March 11, 2013, an accidental fork occurred and 24 blocks (600 bitcoins) were orphaned
  - Solution: coordination on IRC via mining pools, exchanges, and developers
    - Losers: BTC Guild (which mined some of the blocks), OKPay (hit by a double-spend)

Source: Tim Swanson

**Code = law?**

**Swanson's (controversial) conclusion**

- Code is not law.
- If it were, we would not be having this discussion.