The Blockchain
and Other Definite Articles

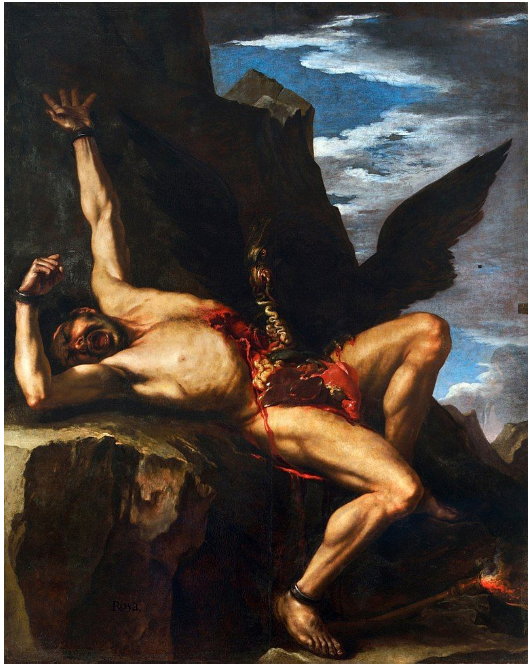
Baeo Maltinsky & Colleen McKenzie
The Median Group

The Overview

- First published as the algorithm behind Bitcoin
- Developed in 2008
  - Previous work from 1990s, e.g. "b-money"
  - Core data structures invented in 1970s (hash lists, hash trees)
- Author: Satoshi Nakamoto

Satoshi Nakamoto and the Blockchain of Secrets

- An elusive and mysterious figure brings dangerous and powerful magicks down to the mortals without betraying his true form
- Paper sent out to a chosen few contacts
- Discussion continues on the iconoclastic Cypherpunks mailing list



Artist's rendition of Satoshi Nakamoto, attempting to explain his recent absence.

The Algorithm

What it takes:

1. Cryptographic hash function
2. State update structure
3. Consensus mechanism

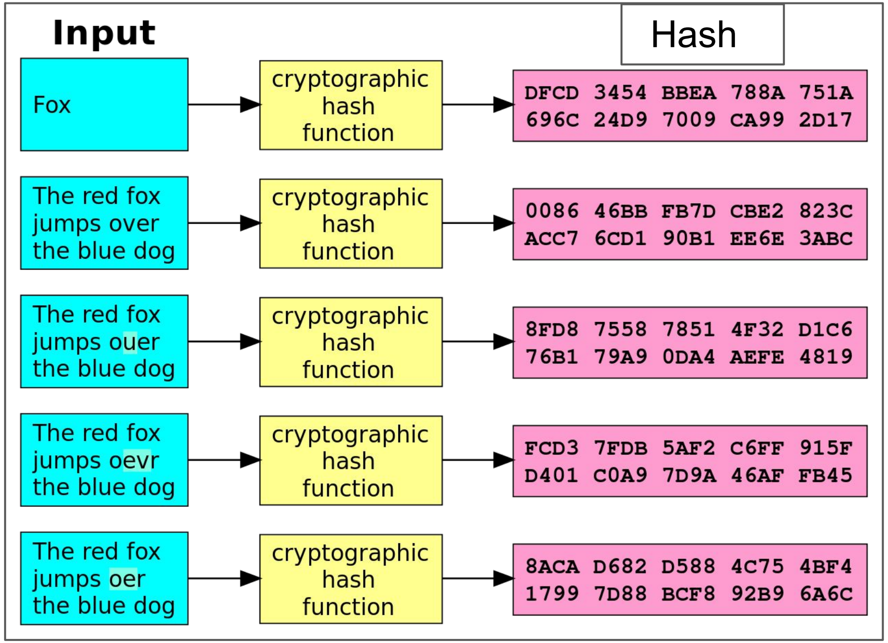
What it makes:

A single, canonical record of events which is effectively tamper-proof

The Cryptographic Hash Function

Turns a string of any length into a string of a given length.

This function should be fairly easy to compute, but very difficult to invert. That is, given the hash, one should not be able to easily recover information about the inputs.



Input

Hash

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

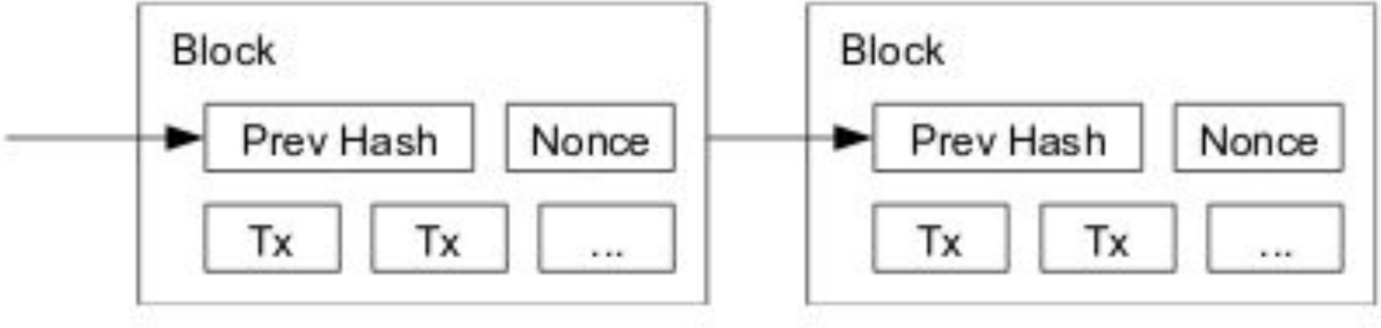
The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

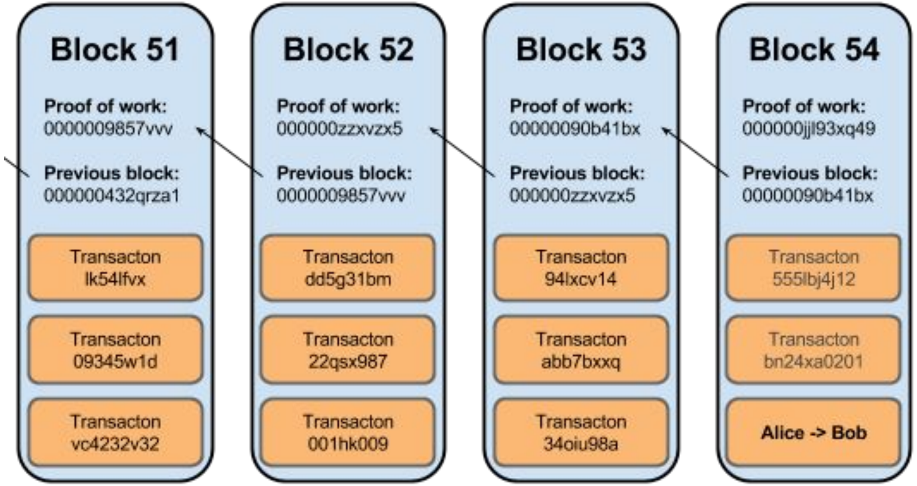
The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

The State Update Structure



The Consensus Mechanism

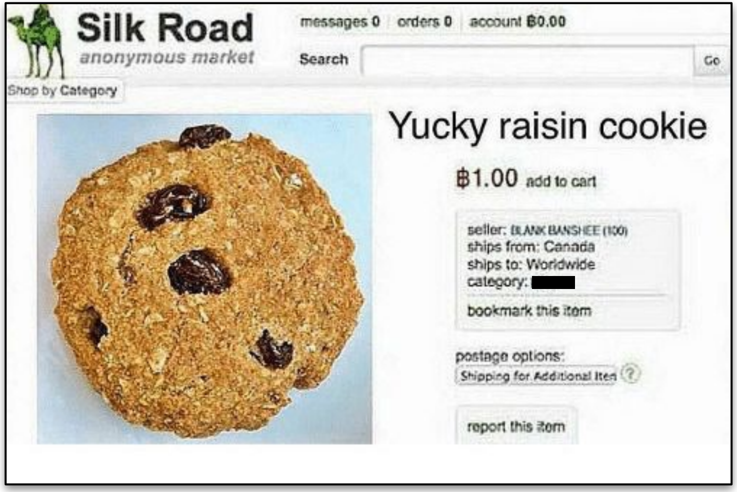
1. Transactions are broadcasted to the network as they happen
2. Miners aggregate transactions into blocks
3. The race is on!
   a. The goal: find a string that combines with the hash of the last block to make a new string that starts with a lot of zero bits.
   b. Requires randomly trying different strings because cryptographic hash functions are difficult to invert
   c. When someone finds it, they receive their reward and a new block is added.



The Cult Following

Early culture: free-market libertarian, agorist mindset, flourishing grey & black markets, e.g. The Silk Road

The Silk Road marketplace, before and after



Silk Road

anonymous market

messages 0 | orders 0 | account ฿0.00

Search

Go

Shop by Category

Yucky raisin cookie

฿1.00 add to cart

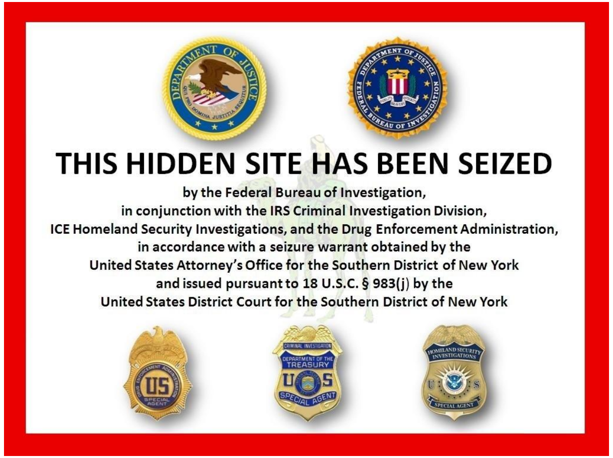
seller: BLANK BANSHEE (100)
ships from: Canada
ships to: Worldwide
category: [redacted]

bookmark this item

postage options:

Shipping for Additional Iten

report this item



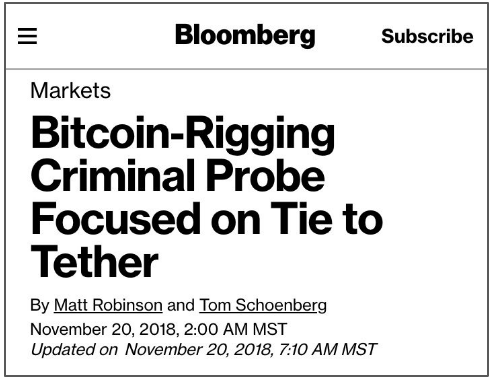
THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

The Cult Following

Current culture: enthusiastic flocking to the promise of riches with less understanding of its mechanisms

- Both subtle and obvious fraud (Tether, EOS.io)
- Healthy market for unexamined arcane scribblings

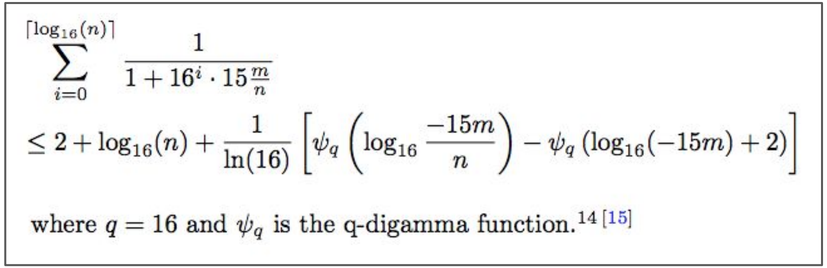


Bloomberg Subscribe

Markets

Bitcoin-Rigging Criminal Probe Focused on Tie to Tether

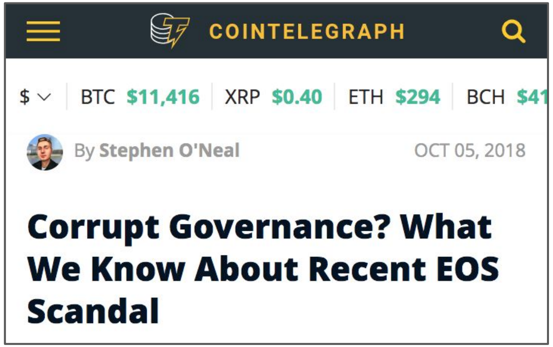
By Matt Robinson and Tom Schoenberg
November 20, 2018, 2:00 AM MST
Updated on November 20, 2018, 7:10 AM MST



$$\sum_{i=0}^{\lceil \log_{16}(n)\rceil} \frac{1}{1+16^{i}\cdot 15\frac{m}{n}} \le 2+\log_{16}(n)+\frac{1}{\ln(16)}\left[\psi_q\left(\log_{16}\frac{-15m}{n}\right)-\psi_q\left(\log_{16}(-15m)+2\right)\right]$$

where $q=16$ and ψ_q is the q-digamma function.[14] [15]

Arcane scribblings from ICTP whitepaper (2019)



COINTELEGRAPH

$ | BTC $11,416 | XRP $0.40 | ETH $294 | BCH $41

By Stephen O'Neal OCT 05, 2018

Corrupt Governance? What We Know About Recent EOS Scandal

The Cult Following

"The claw!"