Rambus

Cryptography Research

From Gold to Bitcoin

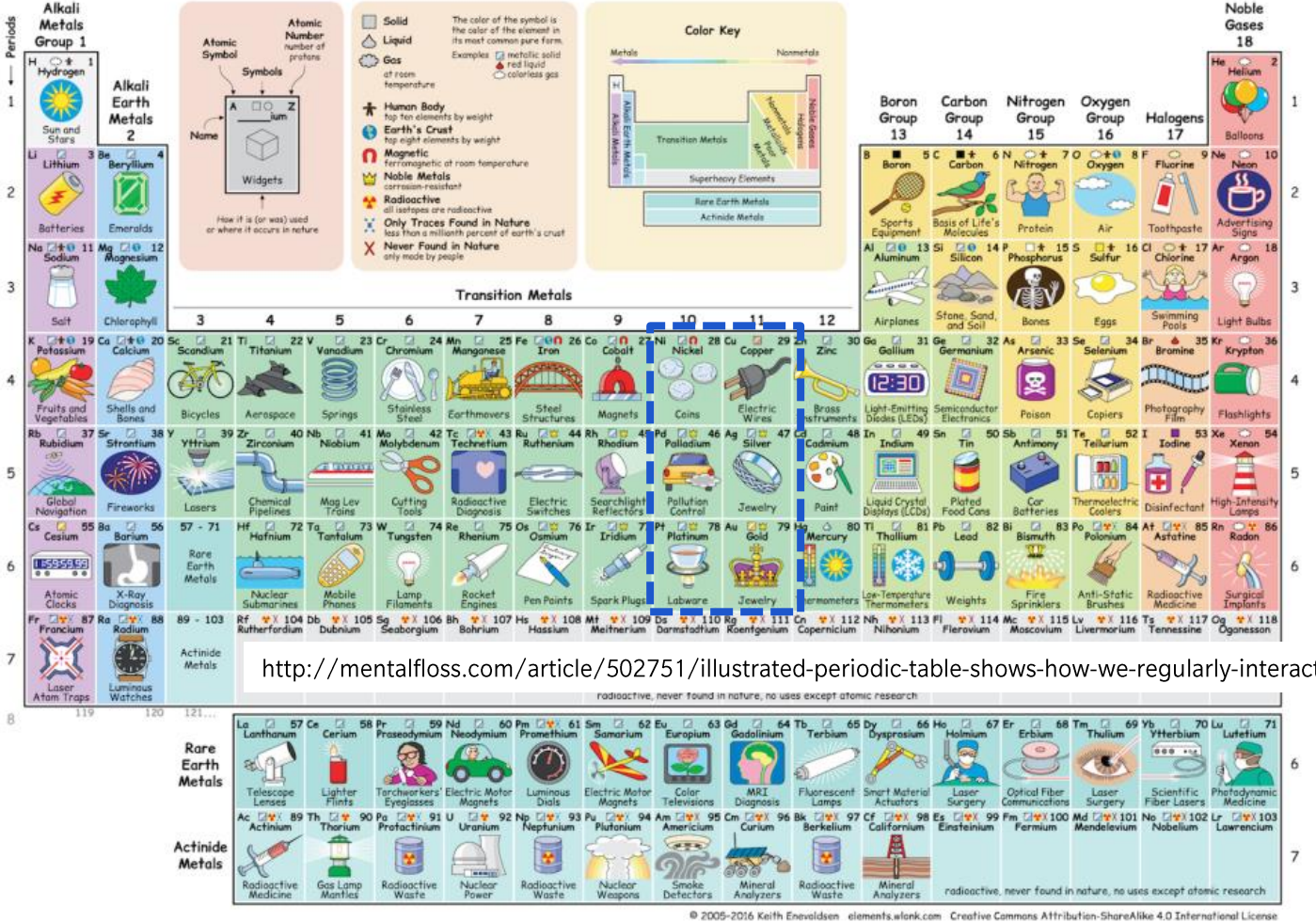
12-Aug-2017

Why is Gold Gold?

Where does it come from?

What’s so special about it?

The Periodic Table of the Elements, in Pictures



http://mentalfloss.com/article/502751/illustrated-periodic-table-shows-how-we-regularly-interact-each-element

Chemistry!

- Rare! Thank you dead stars.

  (But not impossible. Goodbye, Osmium.)
  (And not dangerous. Farewell, Lithium.)

- Provable.

- From 118 down to 7:

  Nickel, Copper, Rhodium, Palladium, Silver, Platinum and Gold

http://www.npr.org/sections/money/2011/02/07/131363098/the-tuesday-podcast-why-gold

Gold is Money.

What else is Money?

What Makes Money?

Money is a matter of functions four:
a medium, a measure, a standard, a store.

1. **Medium**: can buy stuff with it?
2. **Measure**: how valuable is that thing?
3. **Standard**: how much do you owe me?
4. **Store**: piggy bank

Two most well-known types of money

1. Currency
2. Credit Cards

Credit Card Security

Credit Card Security

4147
(4*2) + 1 + (4*2) + 7 = 24

1803
(1*2) + 8 + (0*2) + 3 = 13

9220
(9*2) + 2 + (2*2) + 0 = 15

520?
(5*2) + 2 + (0*2) + ? = 3

"Luhn Algorithm"

24 + 13 + 15 + 3 = 55

55 + ? = 60

Adding is nice. But what's harder?

Cryptographers don't add. Cryptographers **hash**.

Example hash values

0 = 12345

2 = 34512

13 = 51234

132 = 23451

120 combinations

What if I gave you an output?

- What “input” gives me 31245?

Hashes are very easy and very hard

Hashes are very easy in one direction…

… and almost impossible in the other.

- Five cards: 120 combinations (7 digit codes)
  - One card for everyone on Earth? (33 digit codes)
  - One card for every atom in the universe? (80 digit codes)

Bitcoin and the Blockchain

- The blockchain is a ledger.
- A bitcoin is an entry on that ledger.

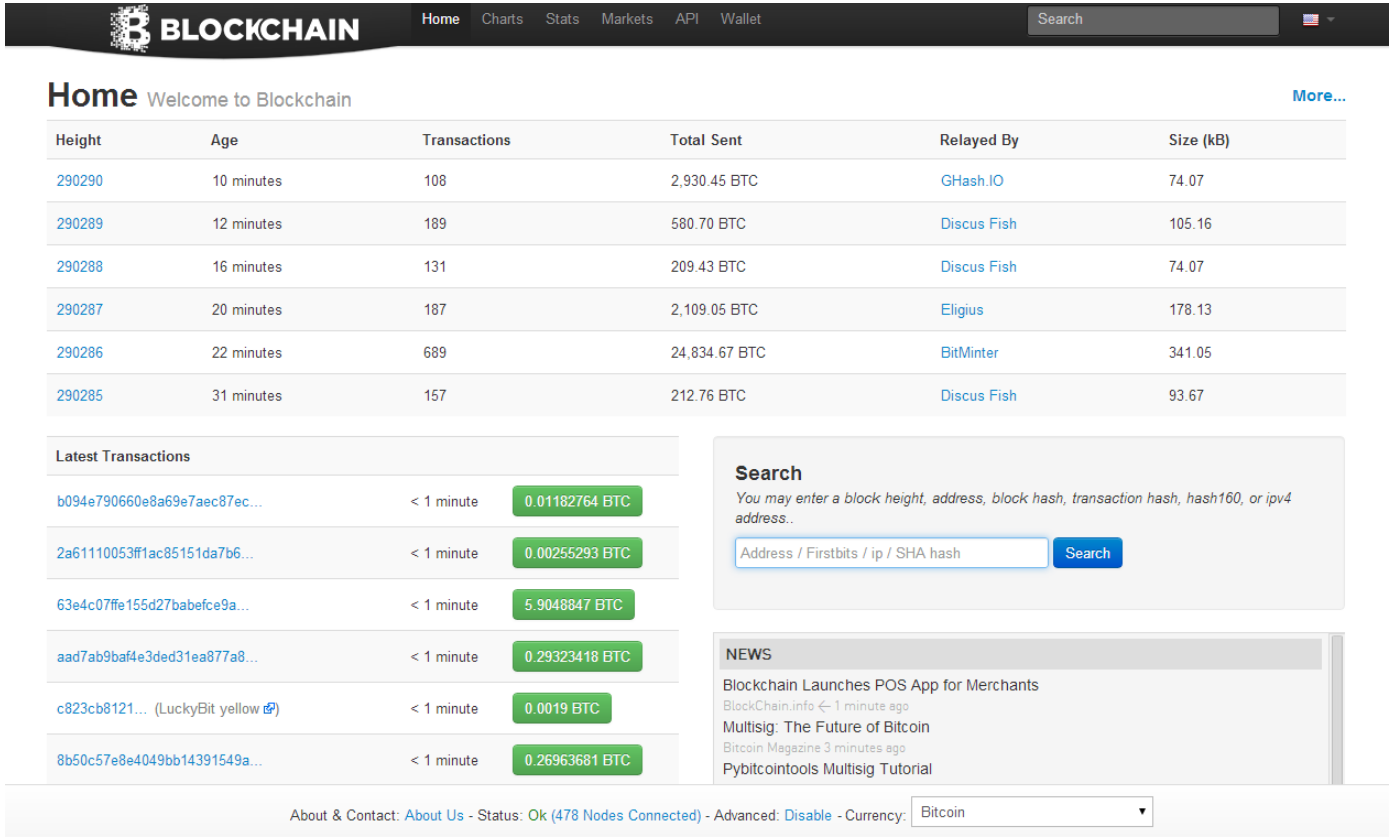
Pretty much.

Uses 256 digit codes.

Let’s Make a Ledger!

Blockchain live!

www.BlockChain.Info



Backup

How It Works

Imagine a Ledger:

From	To	Amount	When
Alice	Bob	50	3 Jan 09
Bob	Charles	25	4 Jan 09
Charles	Alice	10	5 Jan 09
…	…	…	…

A Bitcoin is nothing more than an entry on this ledger.

- The Bitcoin ledger is called the Blockchain

The Blockchain

The Blockchain is a long serialized file:

https://blockchain.info/block-height/0

From	To	$	When
--	S.N.	50	3 Jan 09

Block 0

From	To	$	When
S.N.	Alice	50	4 Jan 09
Alice	Bob	25	5 Jan 09
Bob	Charles	15	6 Jan 09

Block 1

• • •

Divisible down to 10^{-8}

From	To	$	When
Alice	Zippy	0.1	12 Mar 14
Zippy	Scott	0.8	12 Mar 14
Scott	Trixie	0.5	12 Mar 14

Block 291,000

- Each Block in the Chain references the one before it
- A new Block is created every ~10 minutes
- A Transaction isn't official until it's part of a Block ★

The End. Useful Resources:

- BlockChain info:
  http://www.BlockChain.info
- Bitcoin Wiki:
  https://en.bitcoin.it/wiki/Main_Page
- Good intro to transactions:
  http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/
- Bitcoin Commodity Exchange
  https://cex.io/