Intro to Bitcoin Research

or

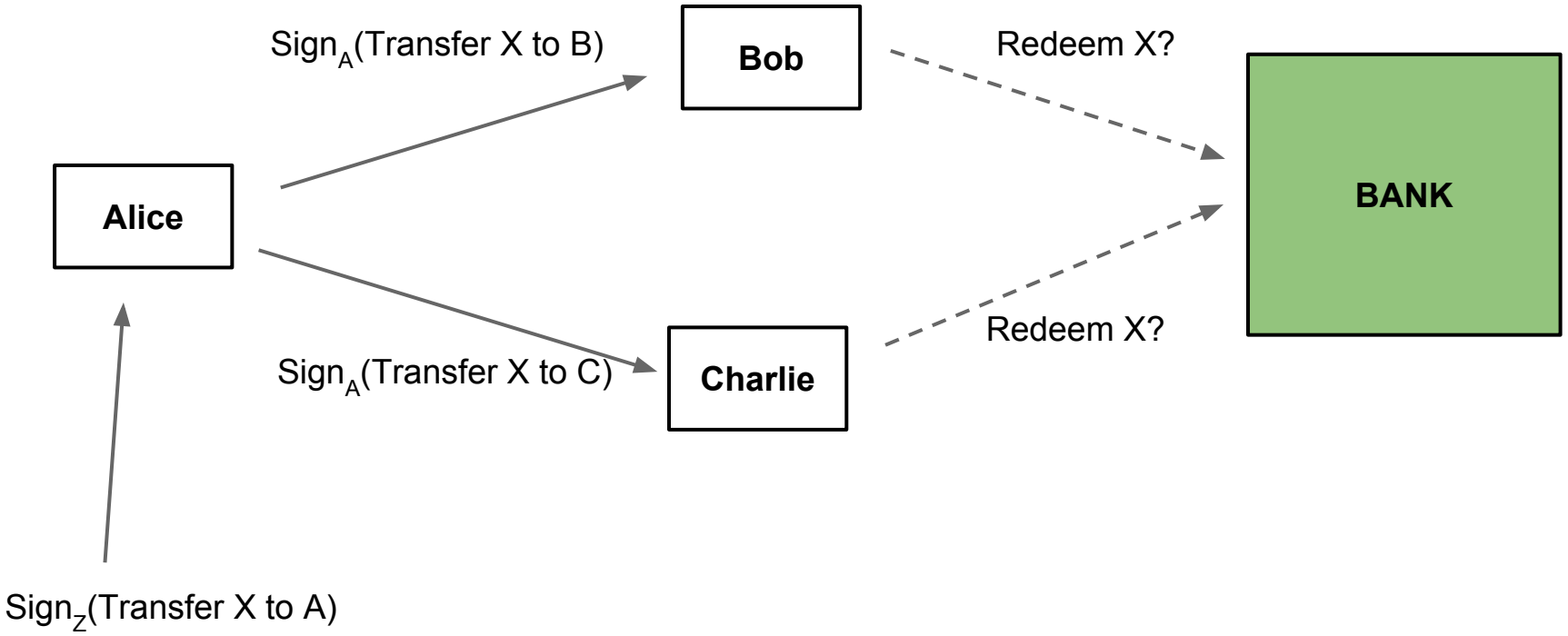
“Why Bitcoin is a full employment act for security engineers”

Joseph Bonneau
CITP, Princeton

Thanks to Andrew Miller, Arvind Narayanan, Jeremy Clark, Joshua Kroll, Ed Felten

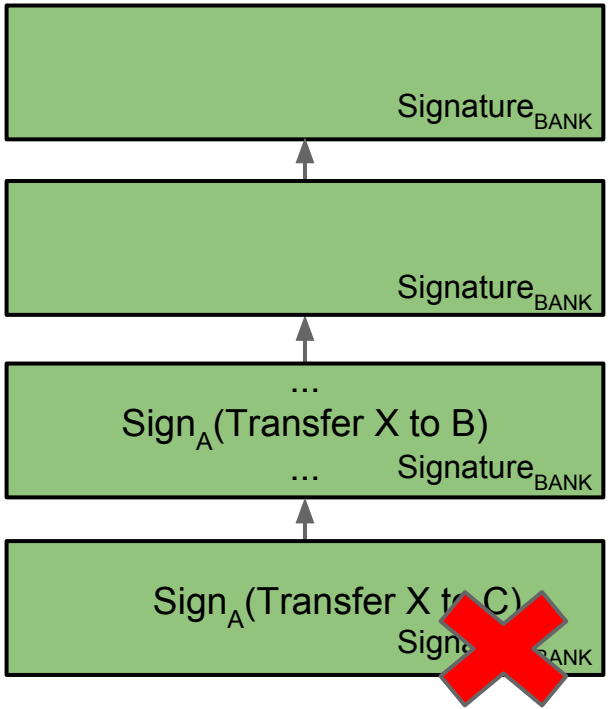
Part I: Bitcoin in 6 easy steps

Double spending: why ecash is hard

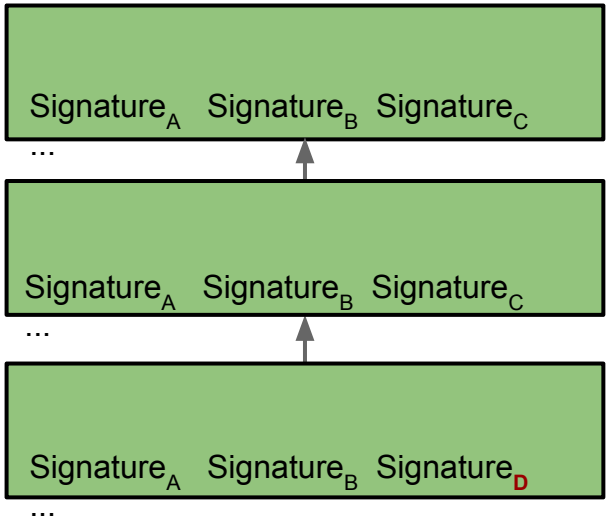


Step 1: Make the bank a global log

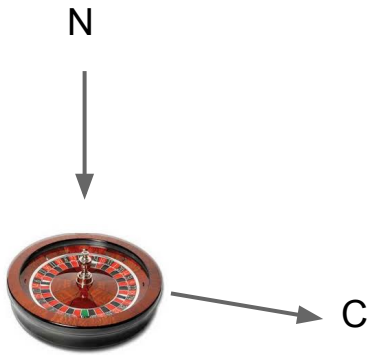
(the *block chain)*

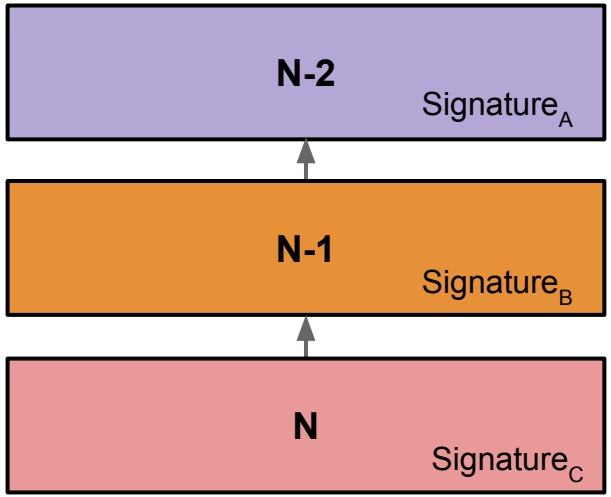


Step 2: Participants vote on blocks

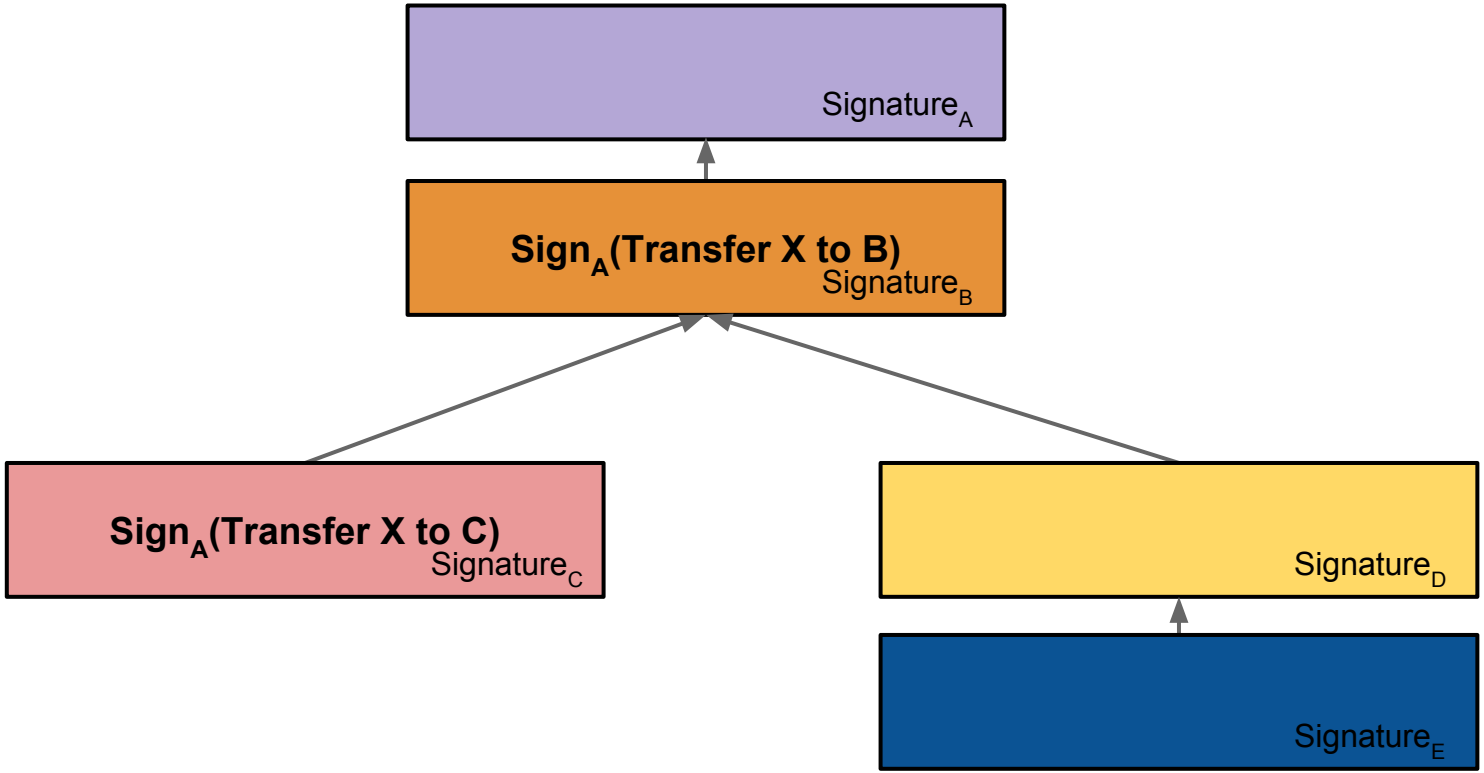


Step 3: A random user picks

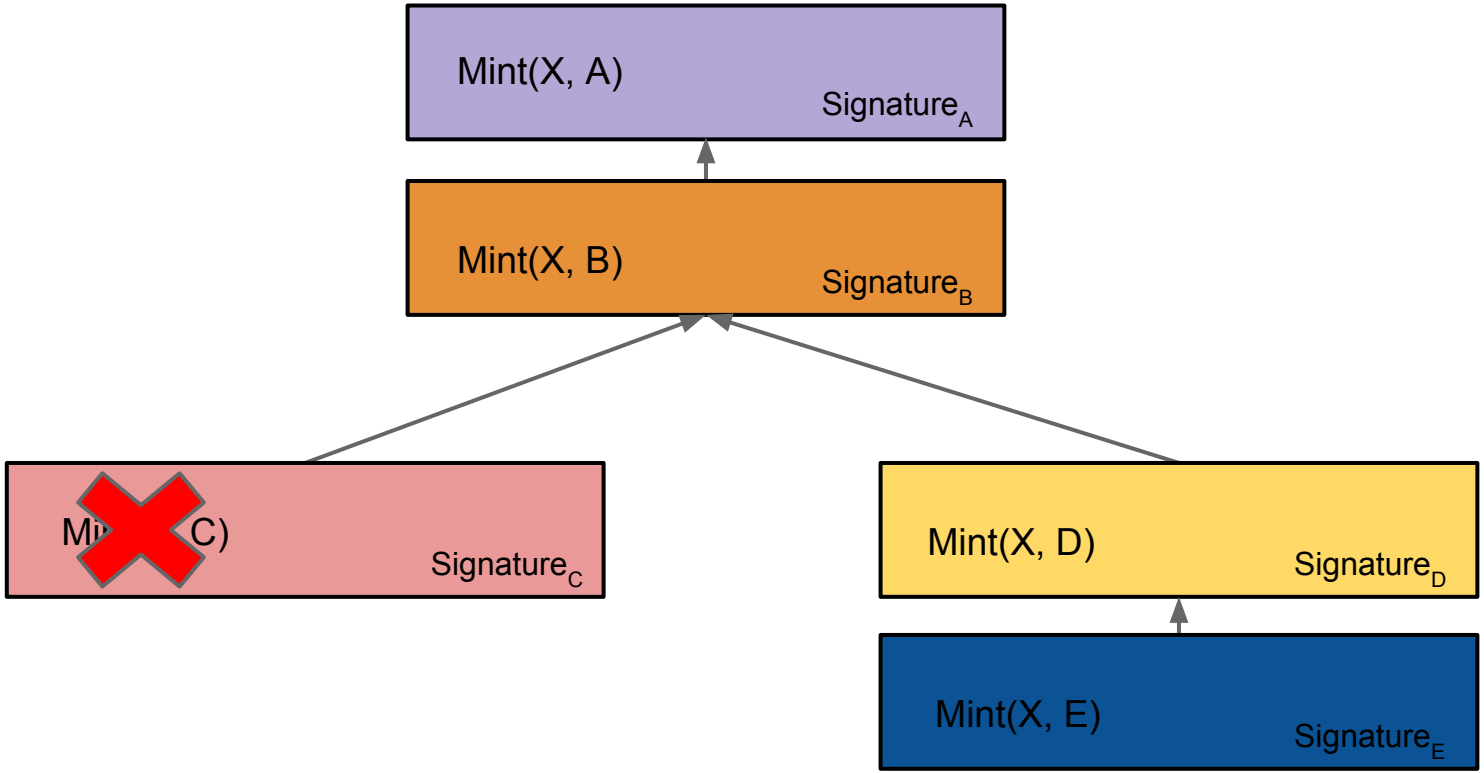




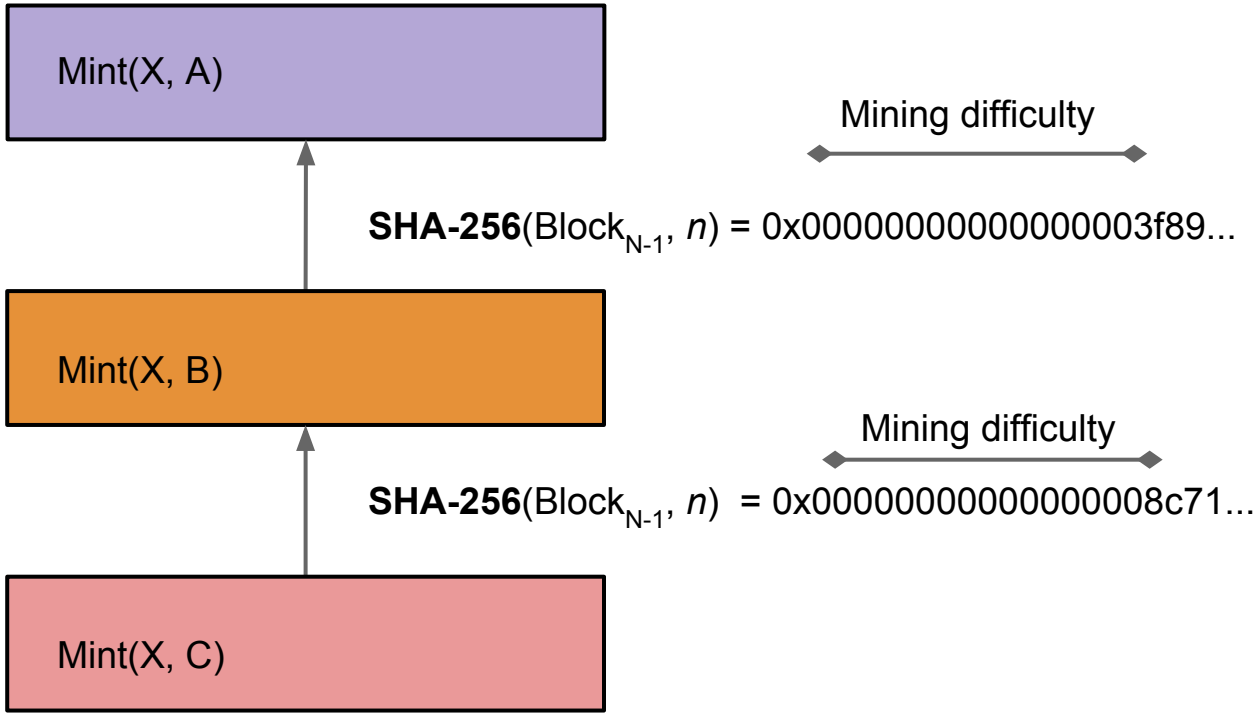
Step 4: Resolve conflicts by *forking*



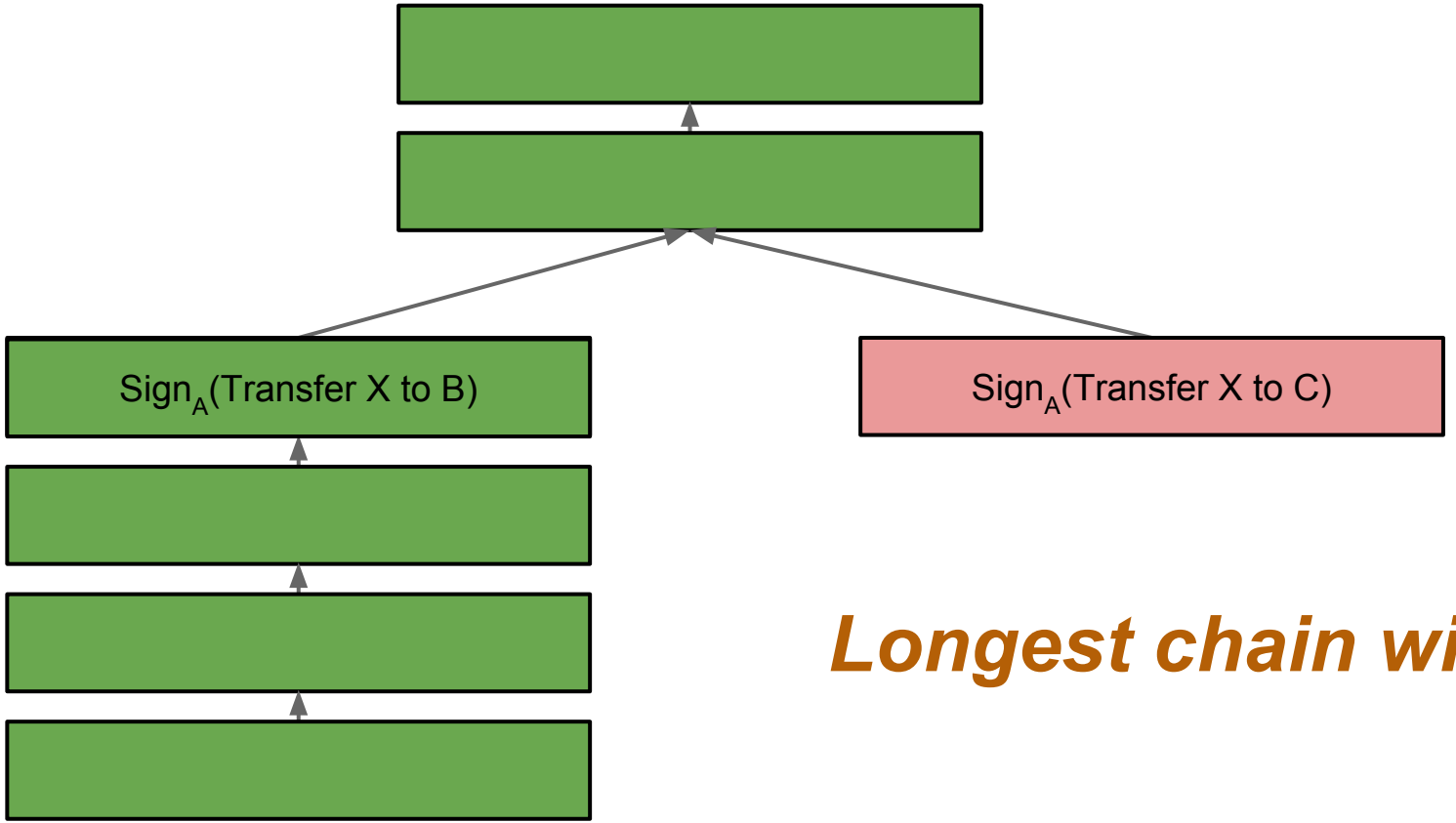
Step 5: Incentivise correct blocks



Step 6: Choose by hash power!

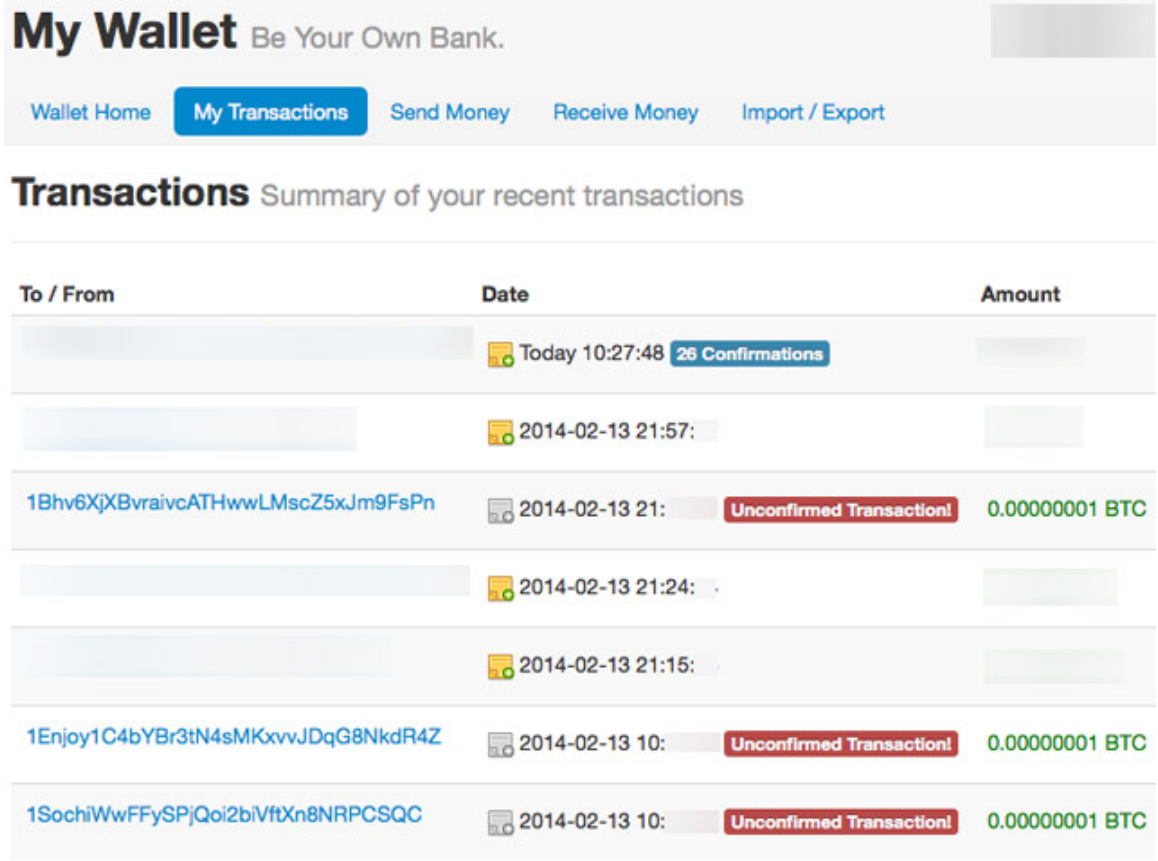


Preventing double spending

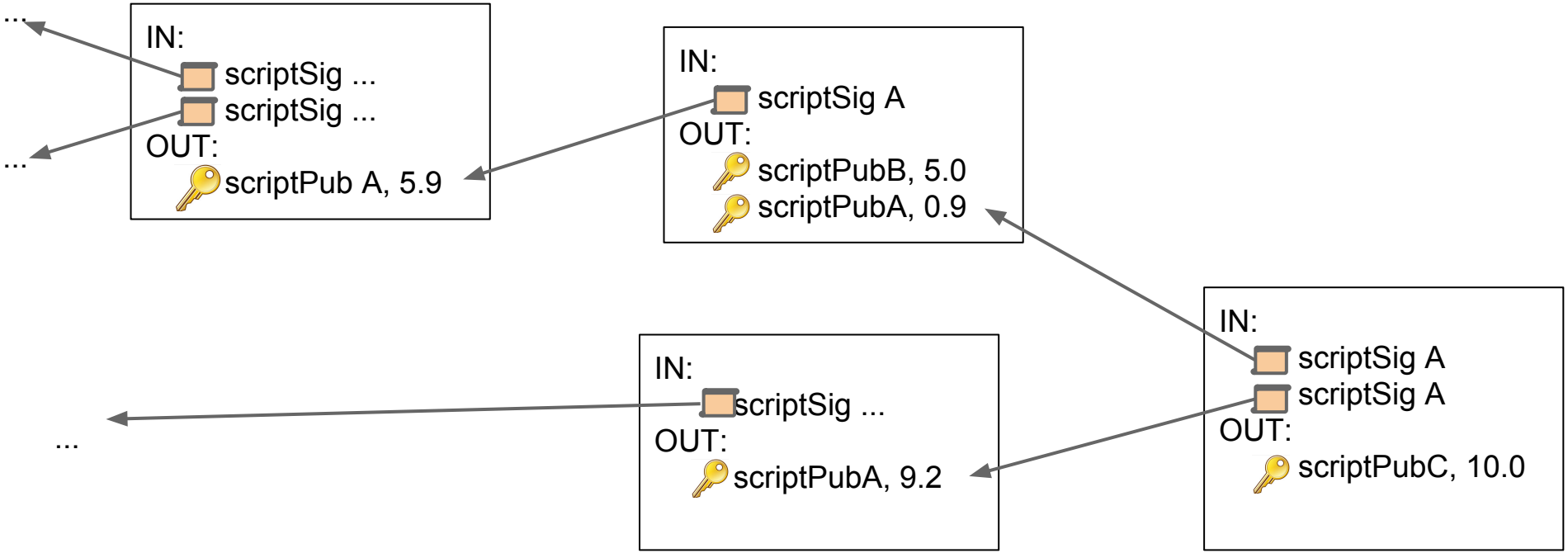


Longest chain wins

Transaction confirmation (~6 blocks)

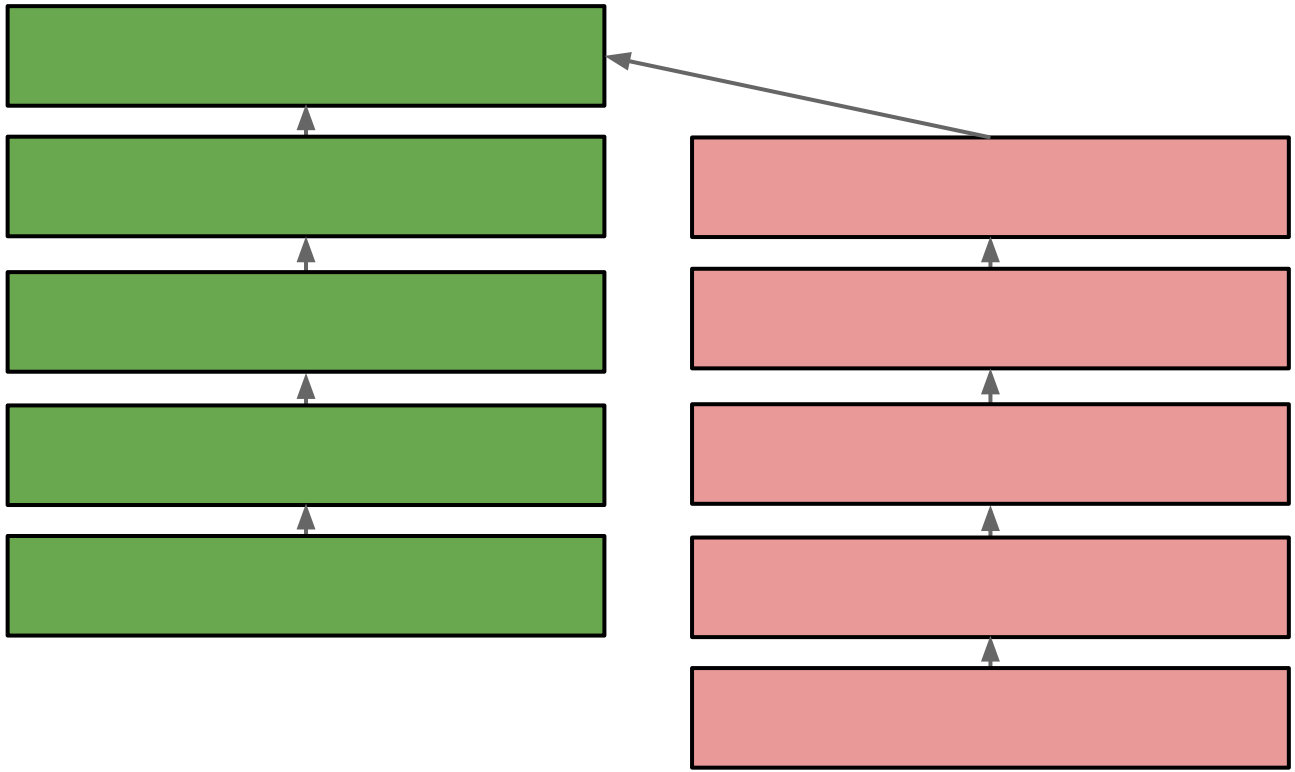


Bitcoin is *transaction-based*



Part II: Mining & Consensus

51% attacks



Goldfinger Attack?

Checkpointing

satoshi
Founder
Sr. Member

Activity: 364

Bitcoin 0.3.2 released
July 17, 2010, 09:35:51 PM

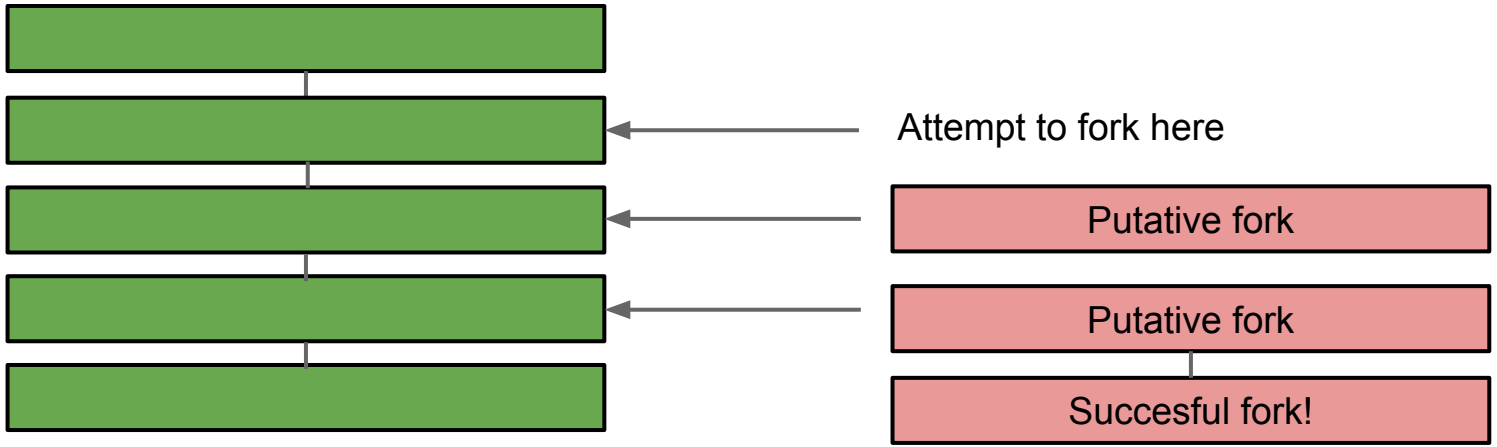
Download links available now on bitcoin.org. Everyone should upgrade to this version.

- Added a simple security safeguard that locks-in the block chain up to this point.
- Reduced addr messages to save bandwidth now that there are plenty of nodes to connect to.
- Spanish translation by milkiway.
- French translation by aidos.

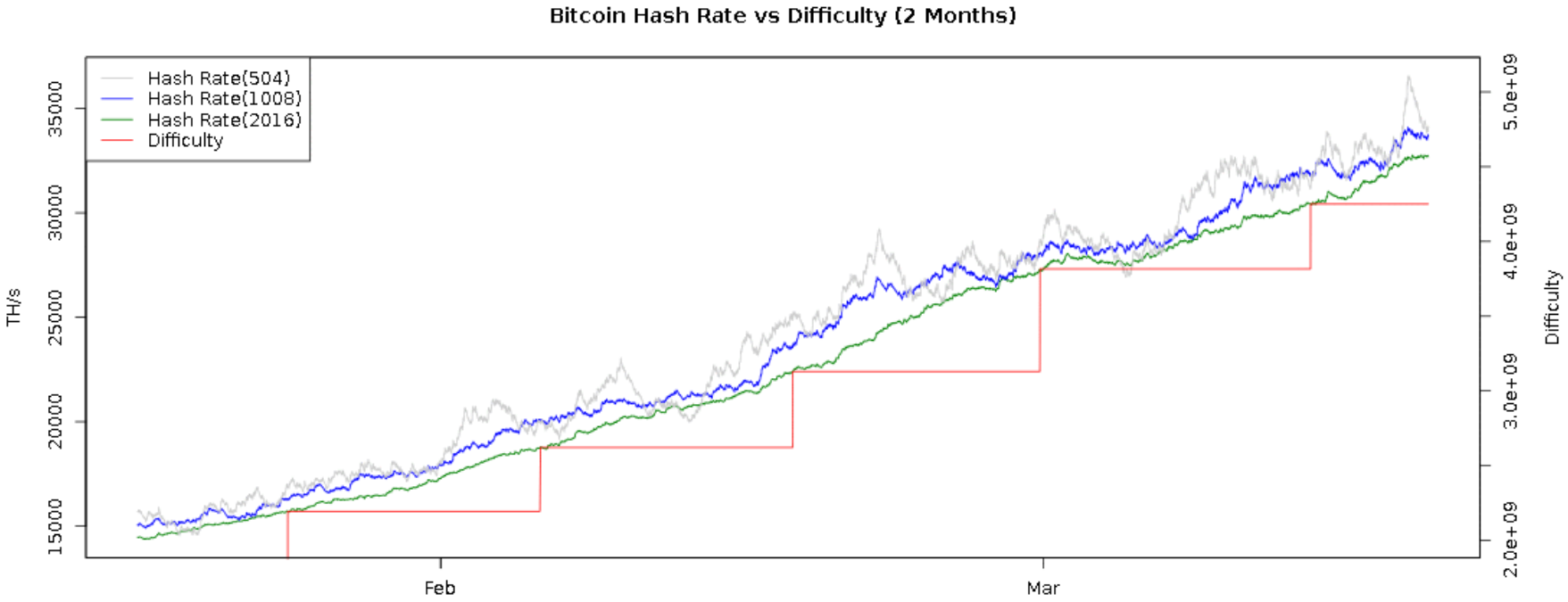
Bitcoin is *not* fully decentralized

Selfish mining

Observation: for 0.33 < *x* < 0.5, a fraction *x* of selfish miners can earn greater than a fraction *x* of rewards [Eyal, Sirer 2013]

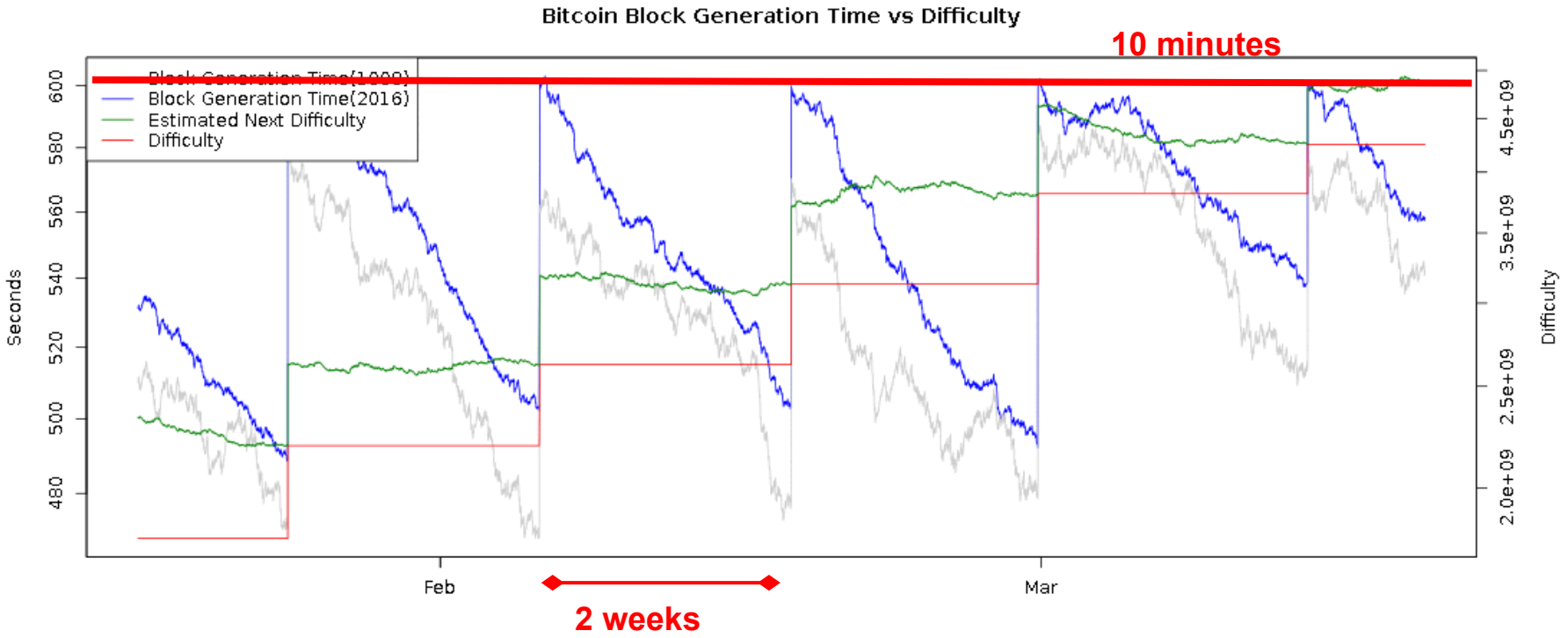


Mining difficulty



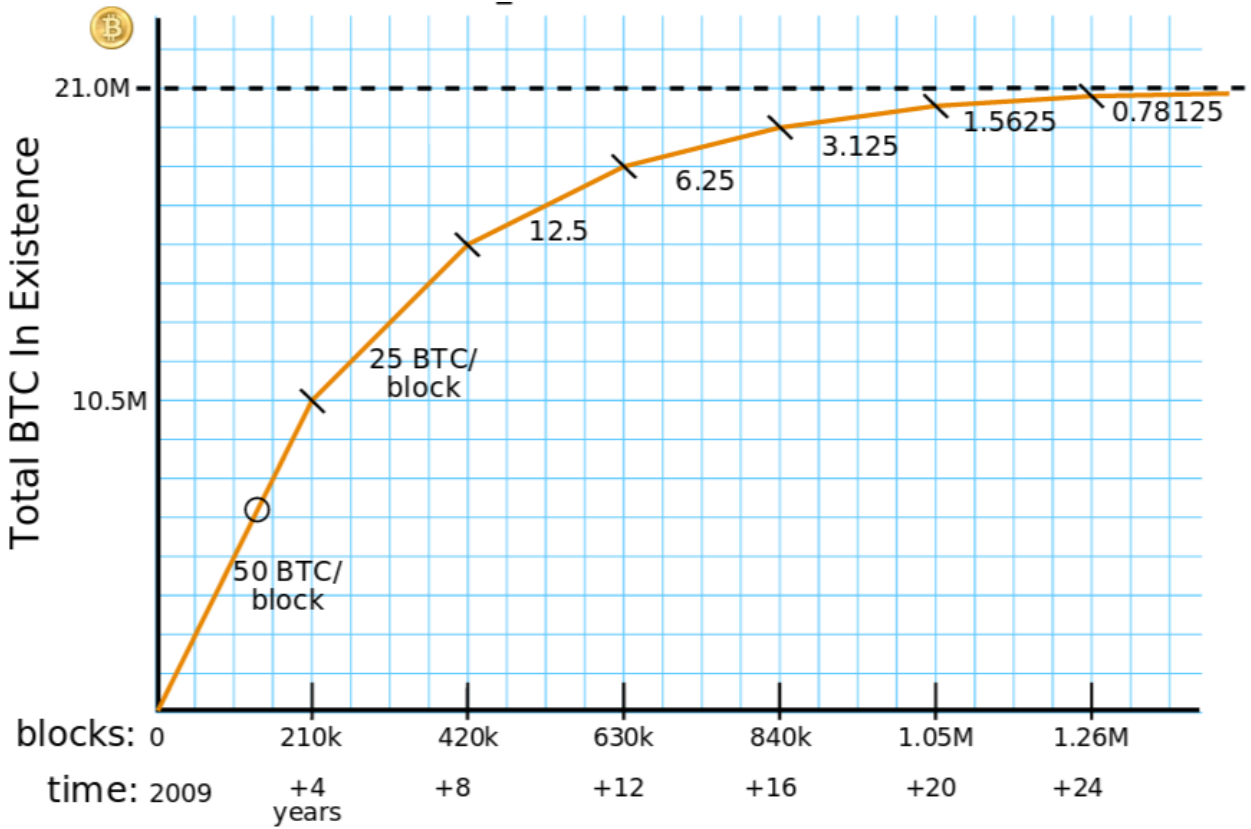
bitcoinwisdom.com

Difficulty adjustment



bitcoinwisdom.com

Mining rewards



Brian Warner

Total network capacity

- 2^{64} hashes per block (every 10 minutes!)
- 2^{75} hashes in 2013
  - In exchange for ~US$250M

Bitcoin mining hardware

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card

The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales final.

THE LEOPARD

DETAILS :

- **2,5 TH/s**
- Dimensions:
  15“ x 13.3“ x 13.7“
  (38cm x 34cm x 35cm)
- 28nm ASIC technology
- Silent Cooling
- In-built WiFi Connection (without Antenna)
- Less than 750 watt (0.3 per GH)
- 1 Year Guarantee

- $ 5.800

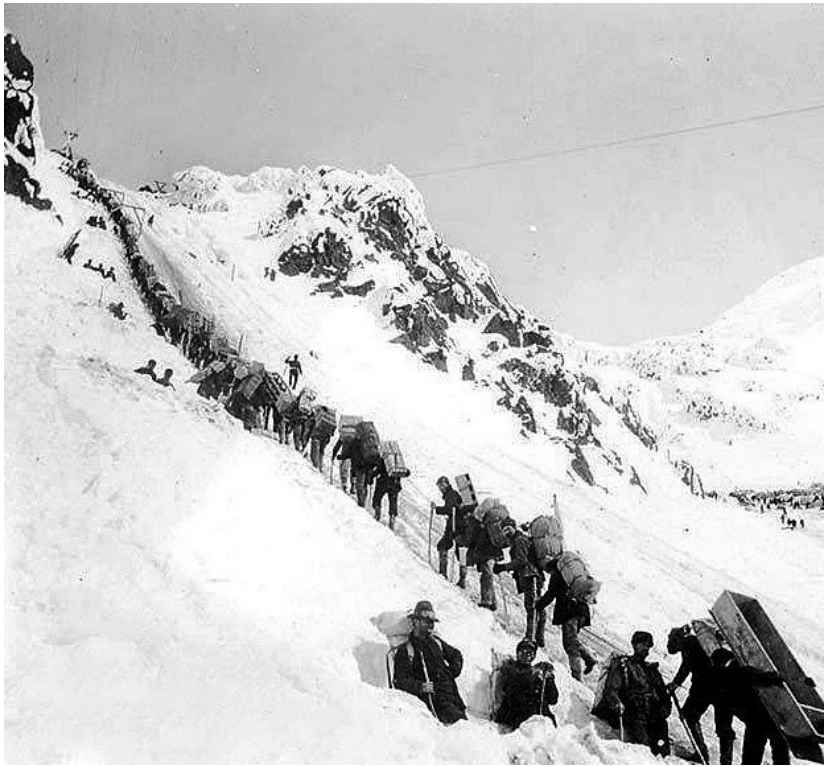
COMES WITH :

1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

SHIPPING :

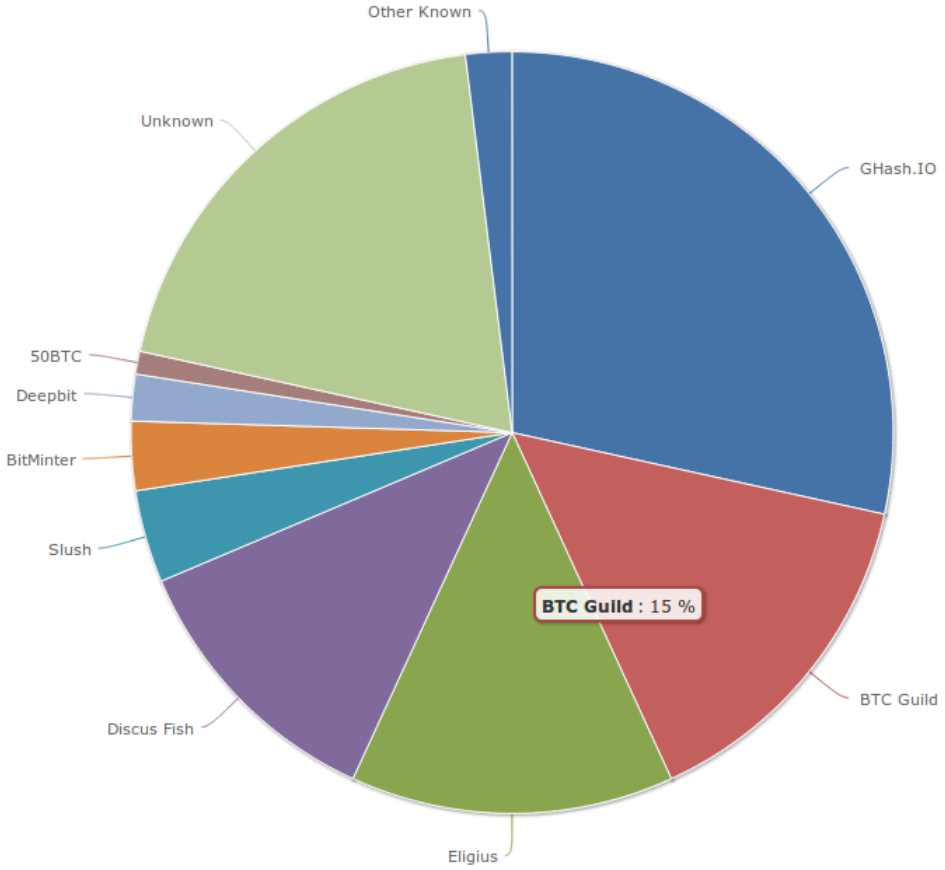
- Worldwide, Express
- Included in the price
- Available:
  100 Units: Shipping April (Week 3)

Why would anybody mine bitcoins?



Chilkoot pass,
Klondike 1898

Mining pools



Part III: Bitcoin as a currency

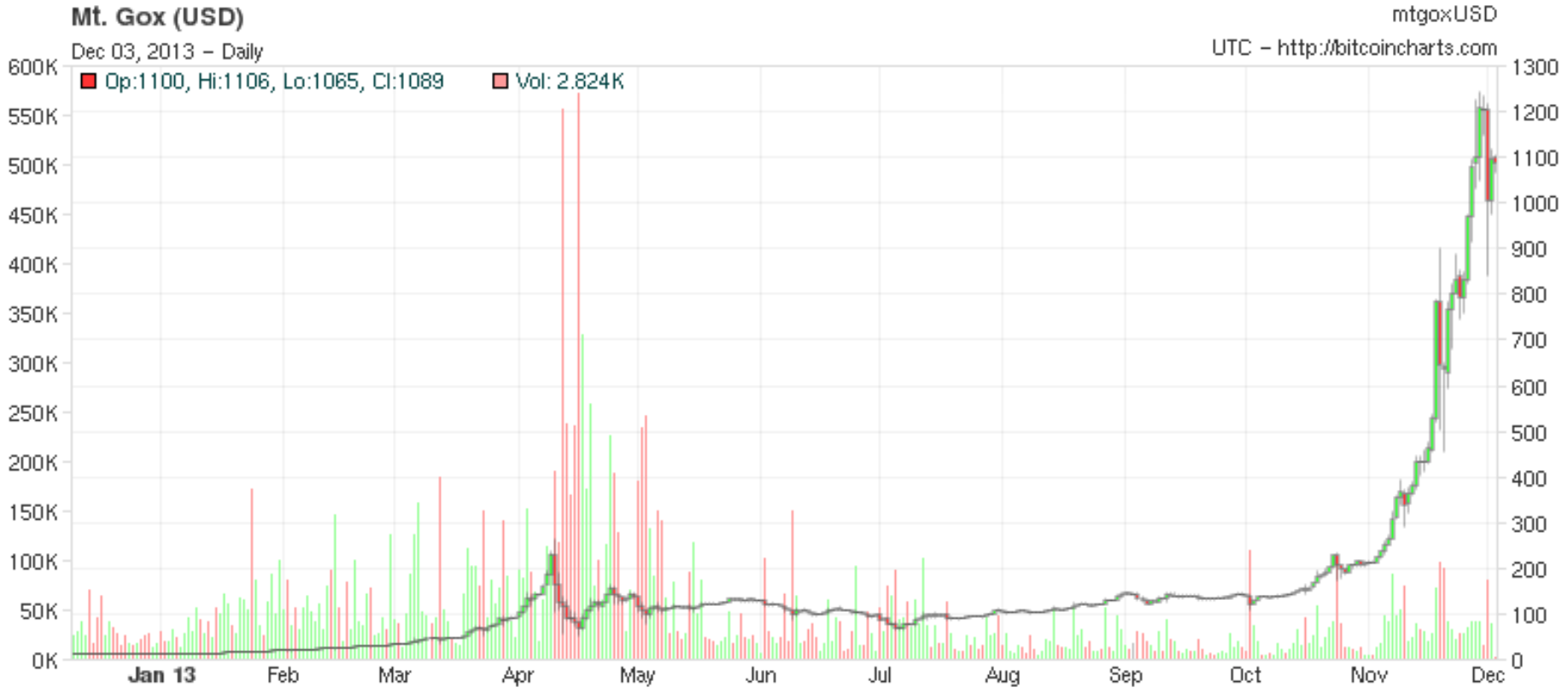
Why does Bitcoin have value?

Consensus

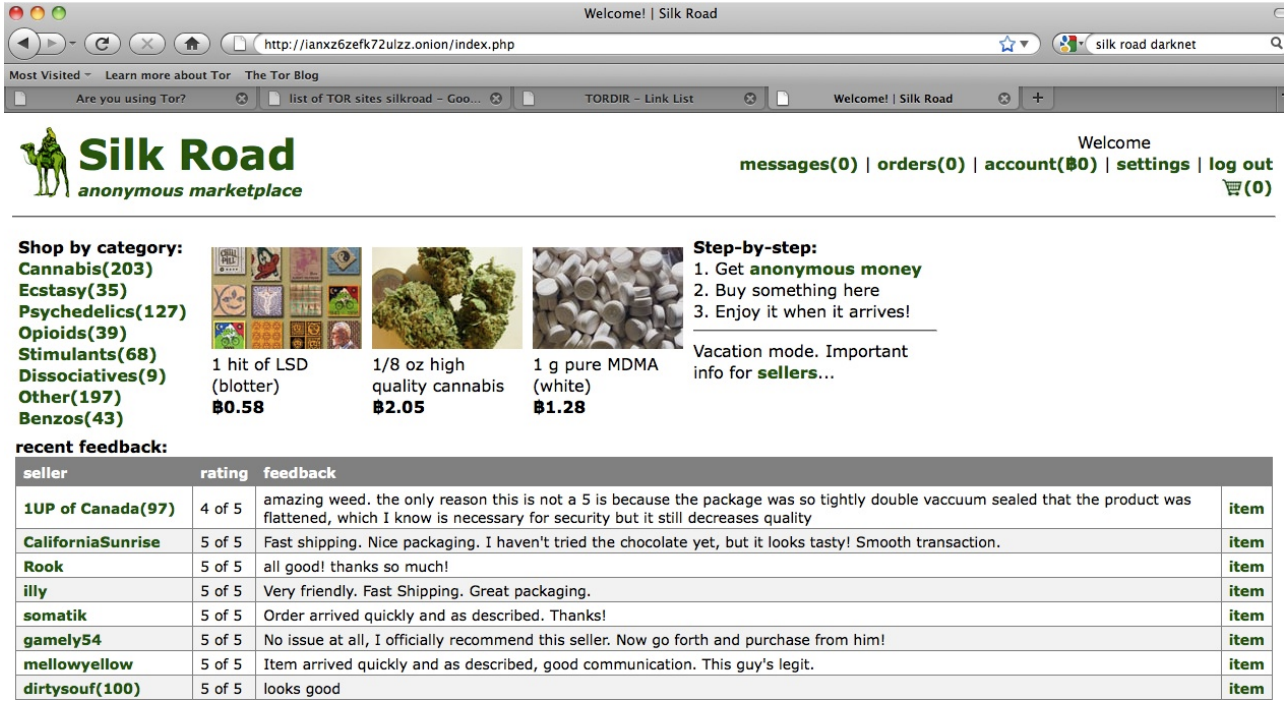
- Consensus in state (blockchain)
- Consensus in payment
- Consensus in rules

[Kroll, Felten 2013]

Price during 2013



Black Markets



Silk Road: US$14M in Revenue in 2012 [Christin 2012]

Capital controls

As Inflation Rages In Iran, Bitcoin Software Not Available

it Iran hard. The
ped up
cy exchange
ghal.com and
had rates
al's value against
cies on Tuesday.
airlines
were
into Tehran due
Iranian rial and shipping giant Maersk halted all port
calls to Iran.

12:41 pm
Feb 7, 2014 EUROPE

Central Bank Of Cyprus Does Not Like Bitcoin

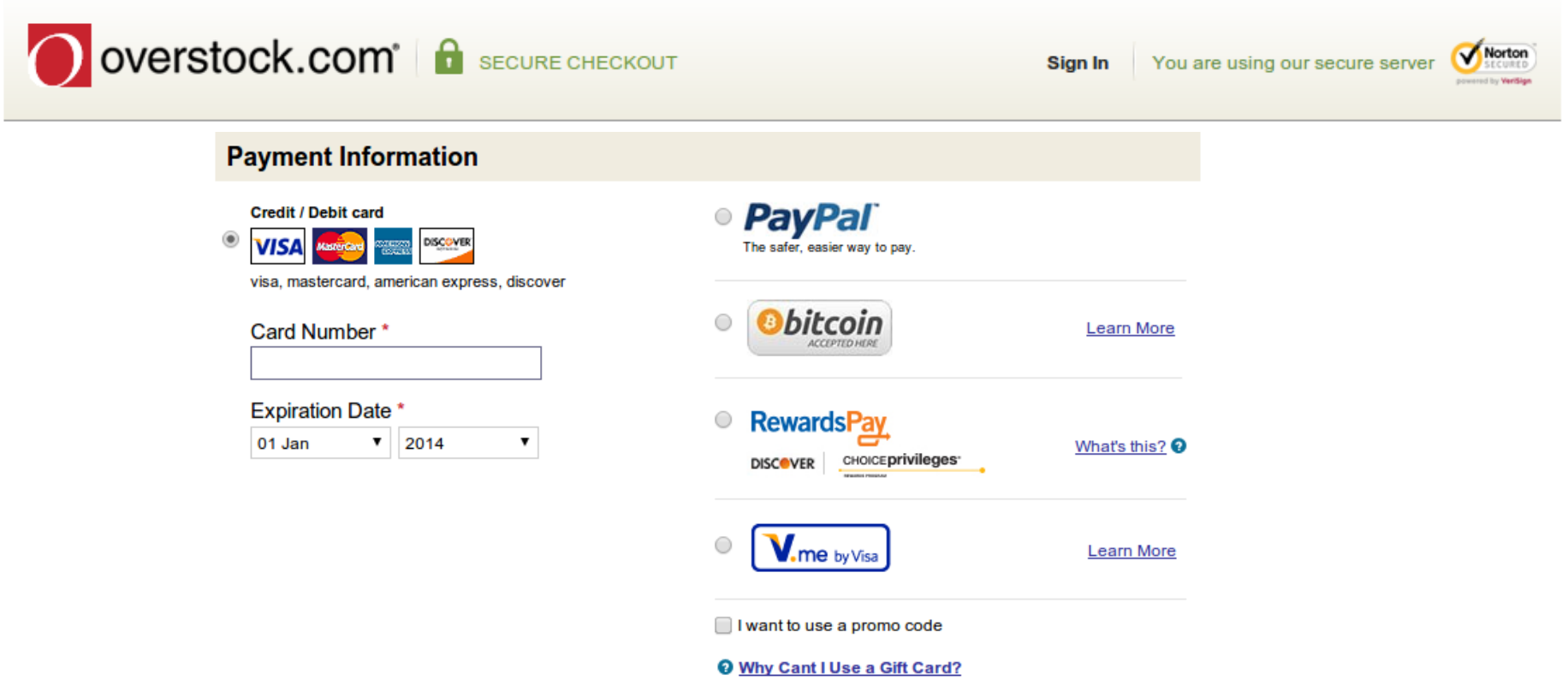
ARTICLE COMMENTS (9)

BITCOIN CYPRUS VIRTUAL CURRENCIES

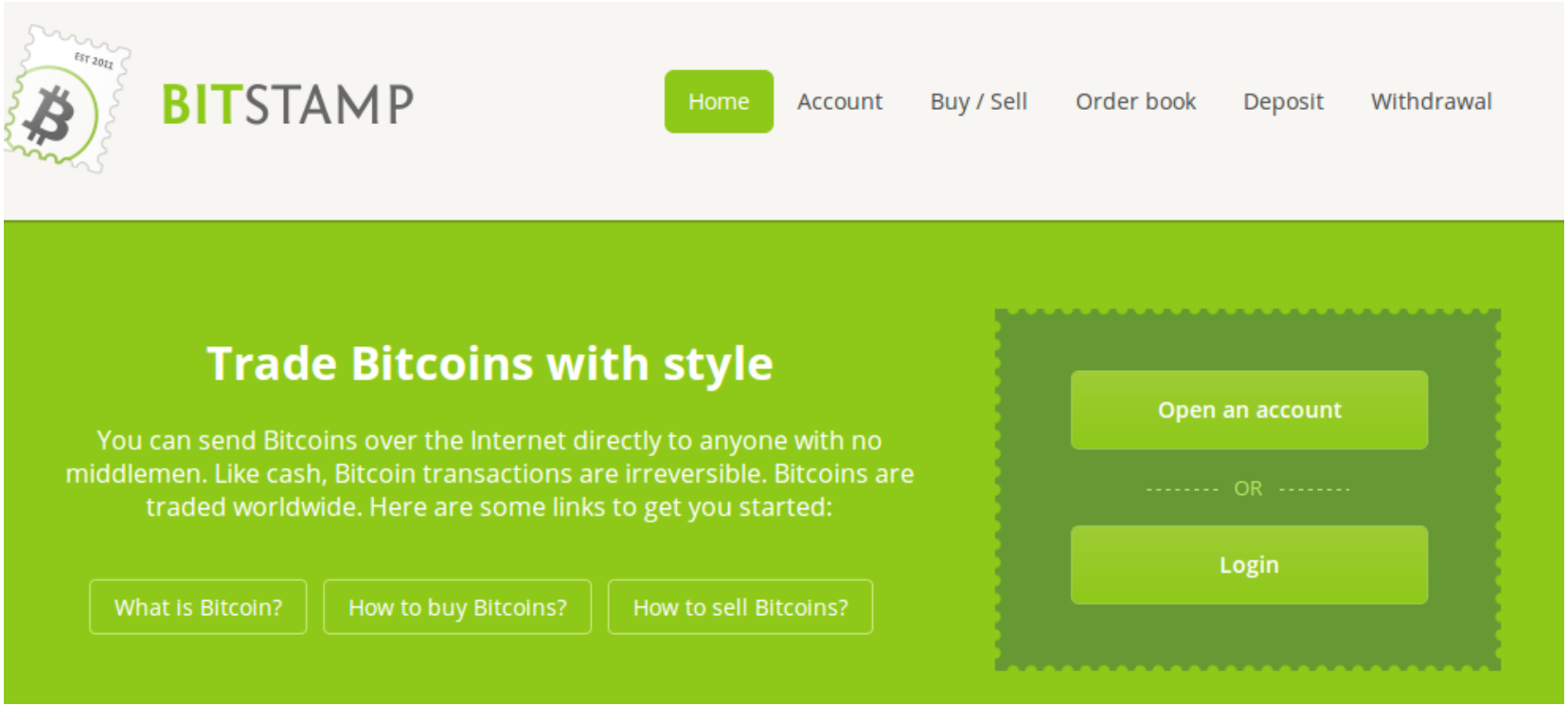
BTC China CEO Attempts To Calm The Bitcoin Market After RMB Deposit Shutdown

*Posted Dec 20, 2013 by **John Biggs** (@johnbiggs)*

E-commerce


overstock.com
SECURE CHECKOUT
Sign In
You are using our secure server
Norton SECURED
Payment Information
Credit / Debit card
VISA
MasterCard
DISCOVER
visa, mastercard, american express, discover
Card Number *
Expiration Date *
01 Jan
2014
PayPal
The safer, easier way to pay.
bitcoin ACCEPTED HERE
Learn More
RewardsPay
DISCOVER
CHOICEprivileges
What's this?
V.me by Visa
Learn More
I want to use a promo code
Why Cant I Use a Gift Card?

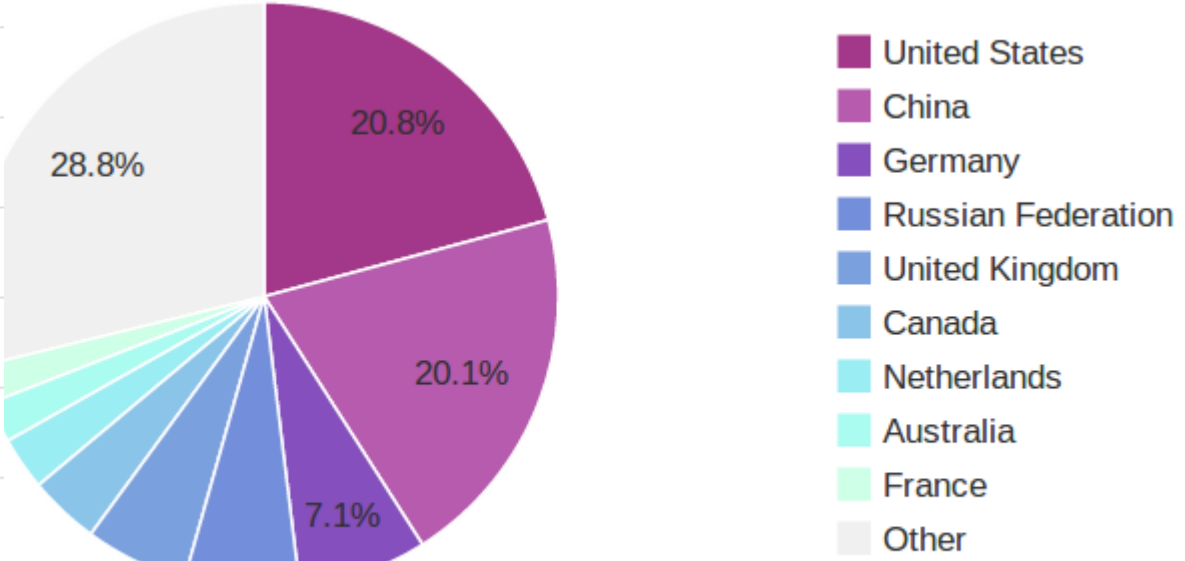
Bitcoin exchanges



Around half of all exchanges have collapsed [Moore, Christin 2012]

getaddr.bitnodes.io - 2013 Addy Yeow

1	United States	50484
2	China	48863
3	Germany	17232
4	Russian Federation	15334
5	United Kingdom	13721
6	Canada	9416
7	Netherlands	7077
8	Australia	5469
9	France	5024
10	Poland	4706



Geographic distribution of nodes (as of Dec 2013)

Questions