



Intro to Bitcoin Research



or

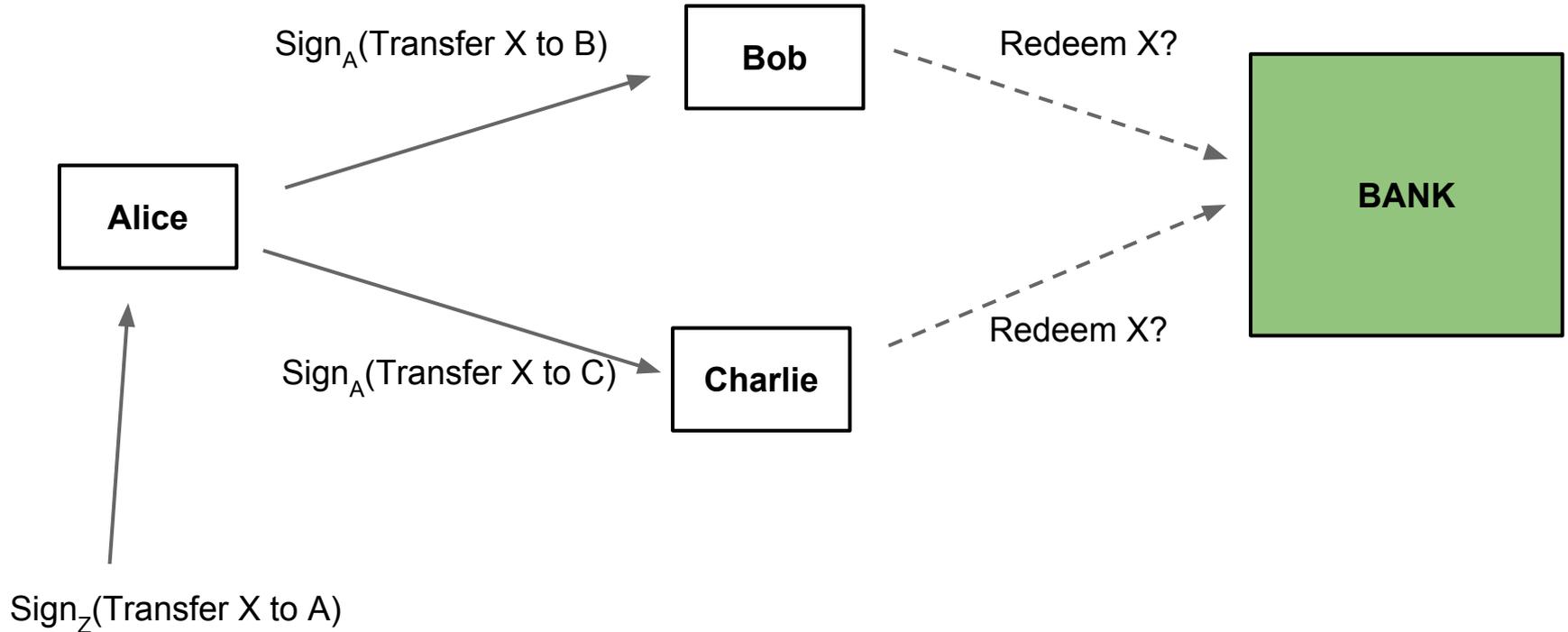
“Why Bitcoin is a full employment act for security engineers”

Joseph Bonneau
CITP, Princeton

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

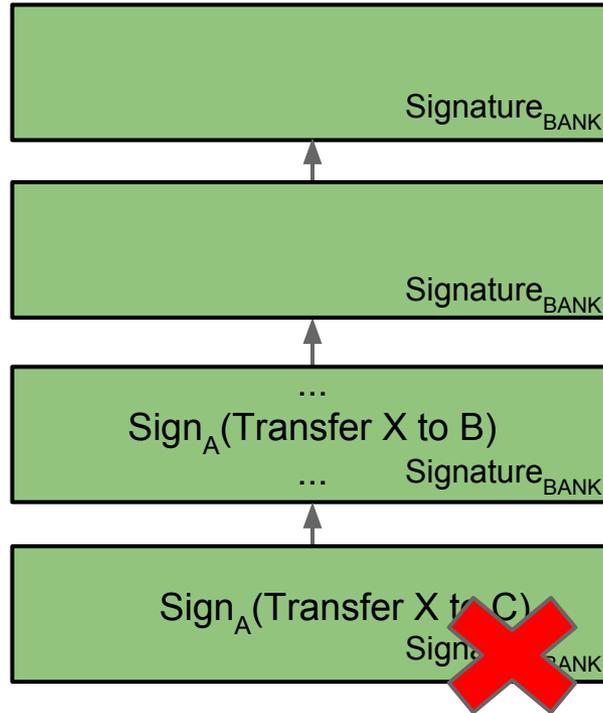
Part I: Bitcoin in 6 easy steps

Double spending: why ecash is hard

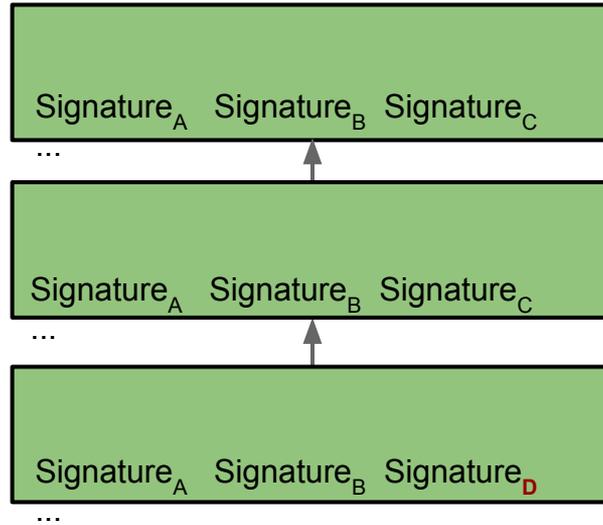


Step 1: Make the bank a global log

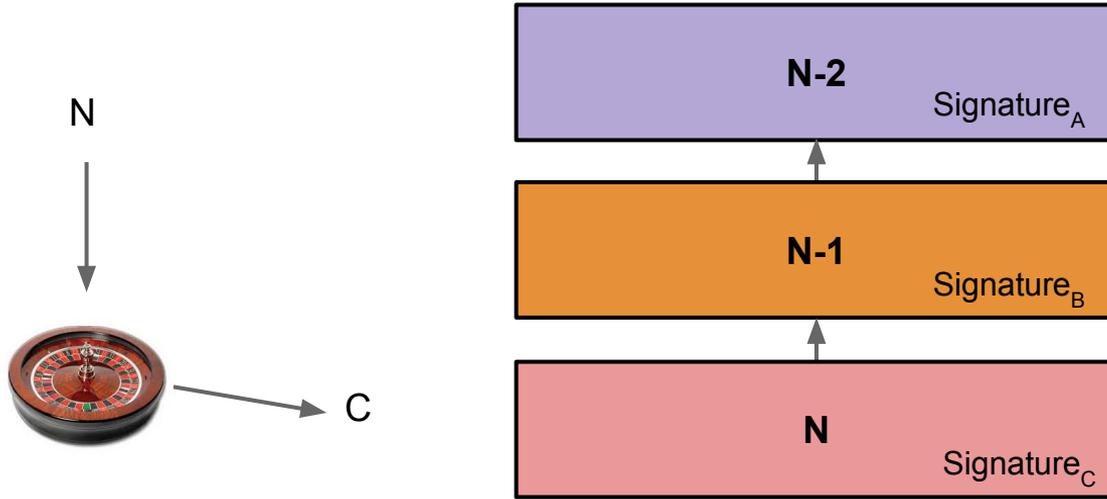
(the *block chain*)



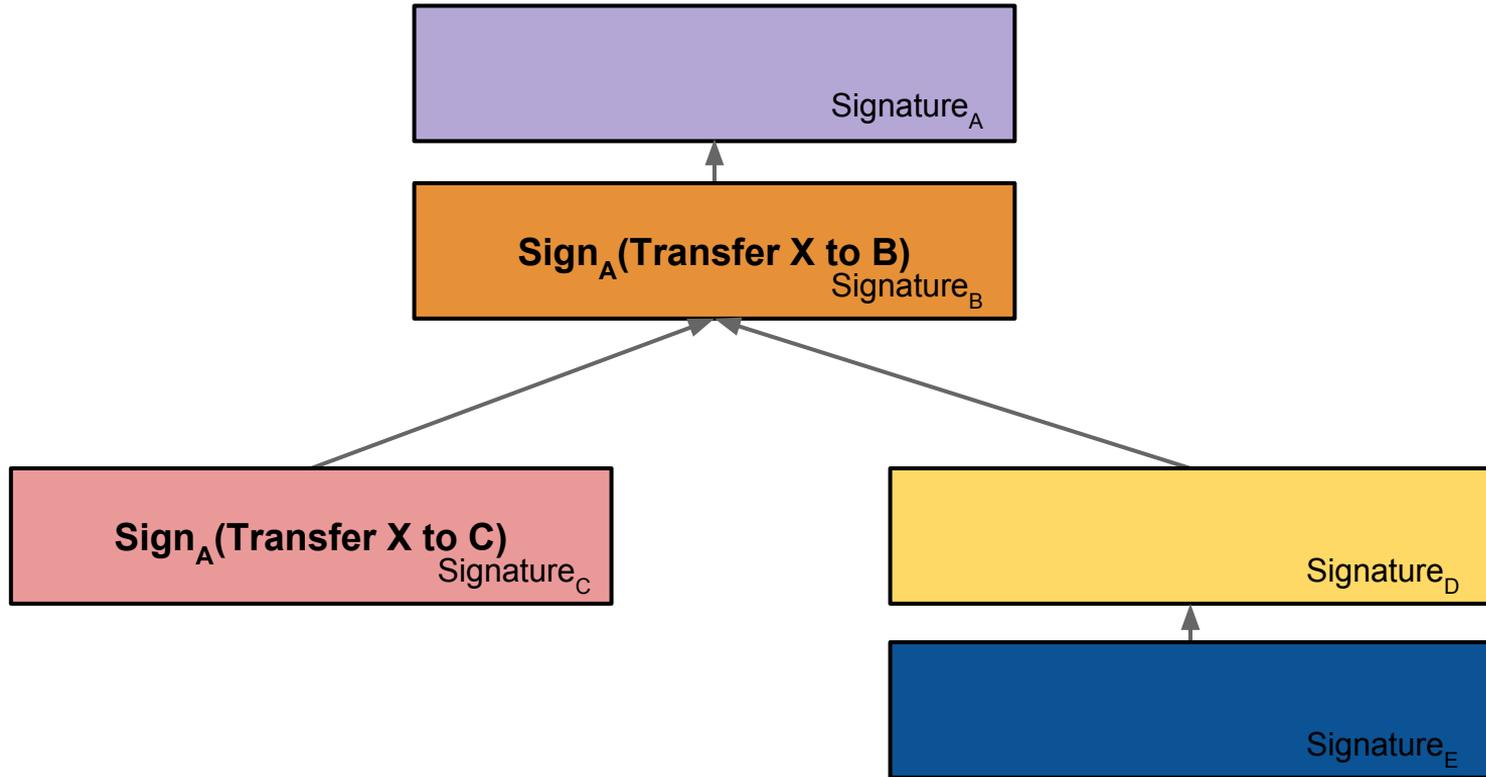
Step 2: Participants vote on blocks



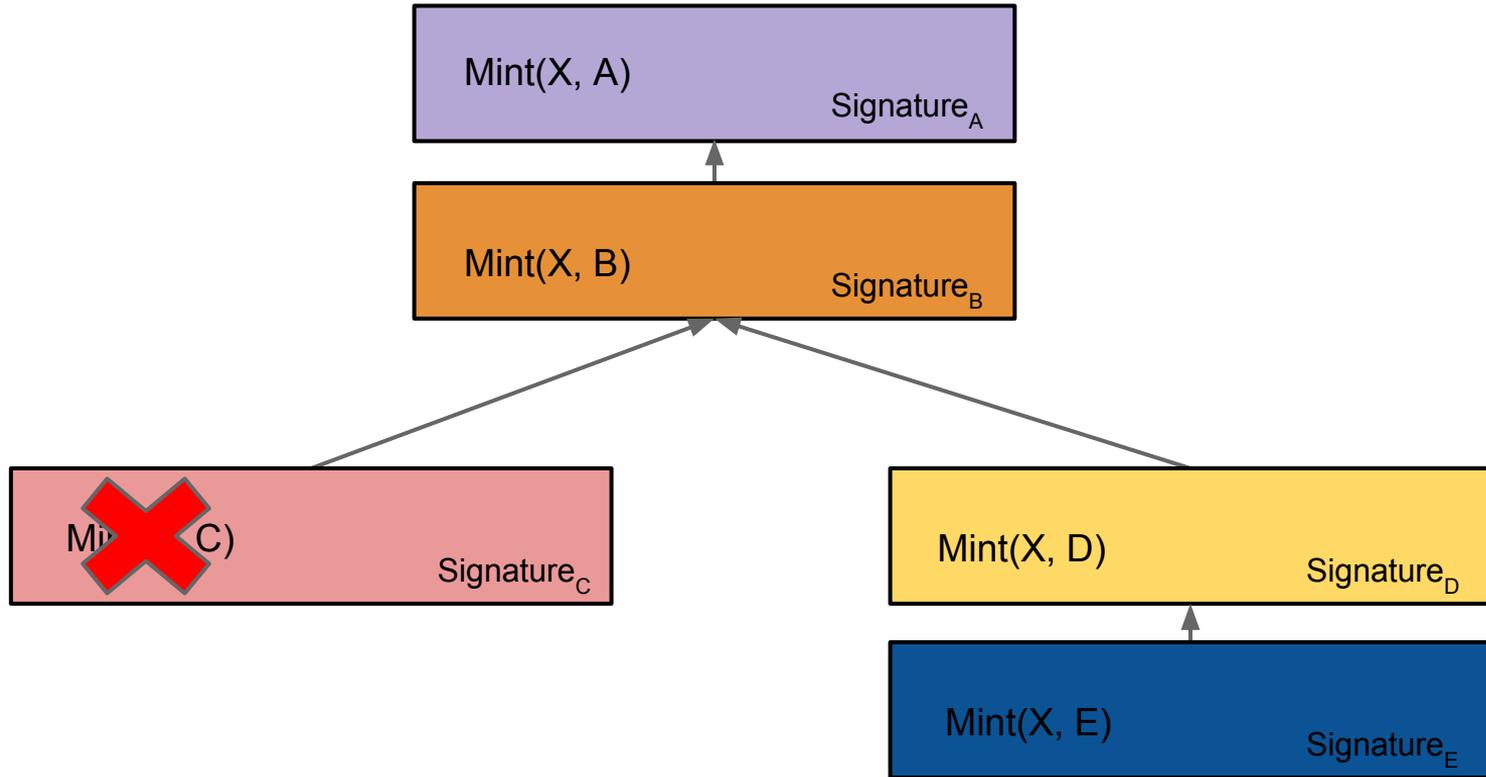
Step 3: A random user picks



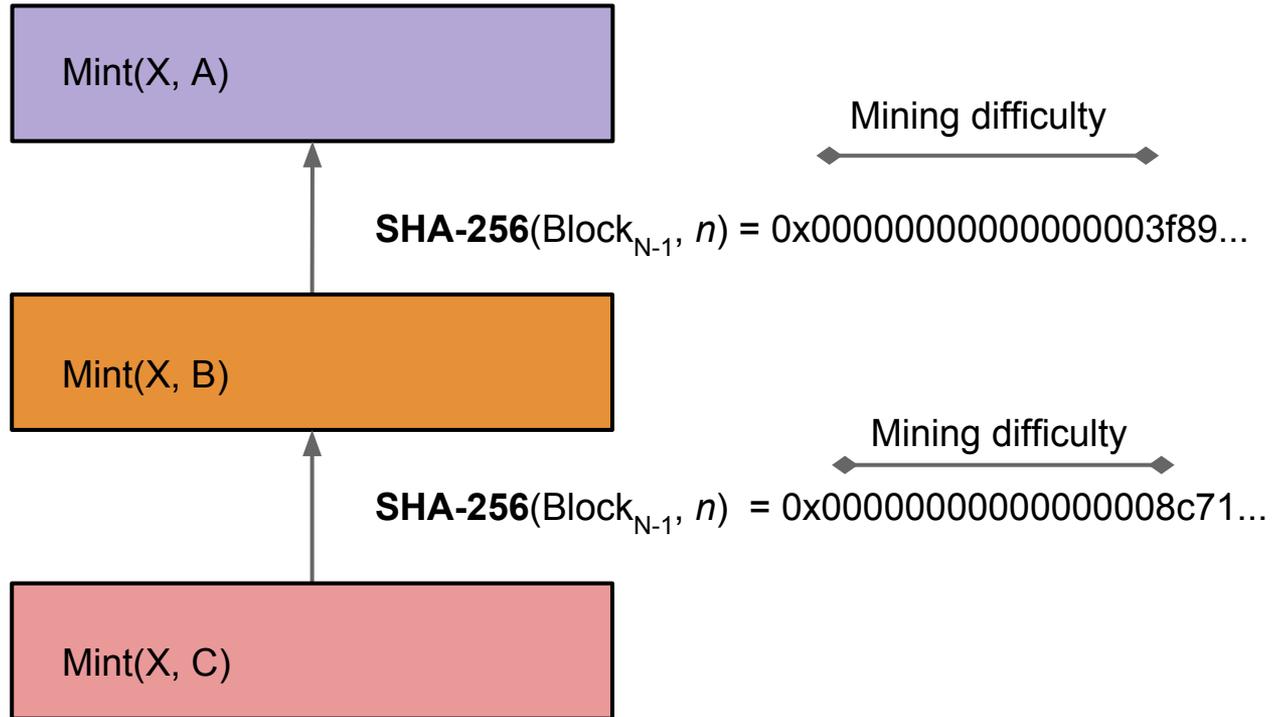
Step 4: Resolve conflicts by *forking*



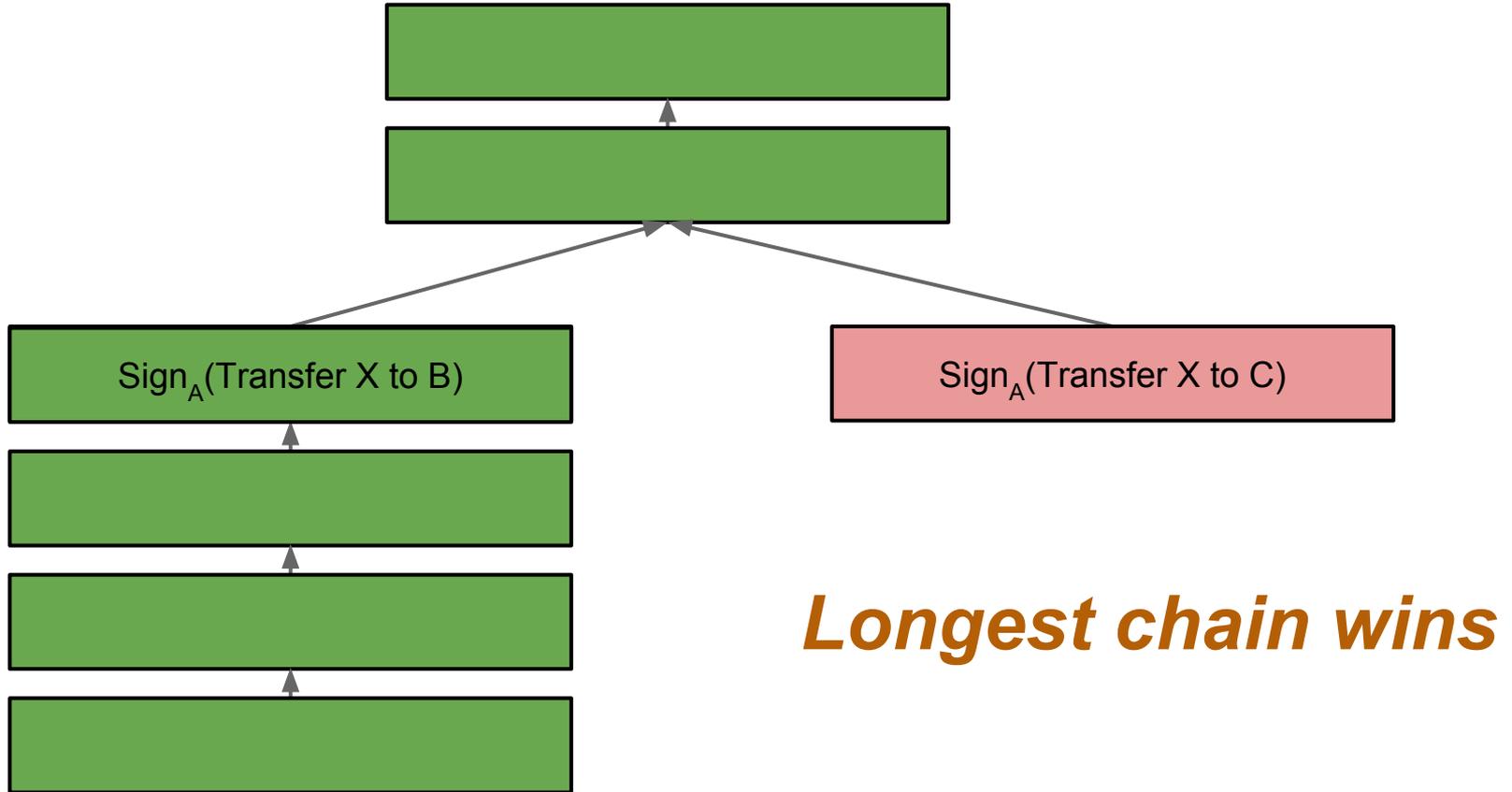
Step 5: Incentivise correct blocks



Step 6: Choose by hash power!



Preventing double spending



Transaction confirmation (~6 blocks)

My Wallet Be Your Own Bank.

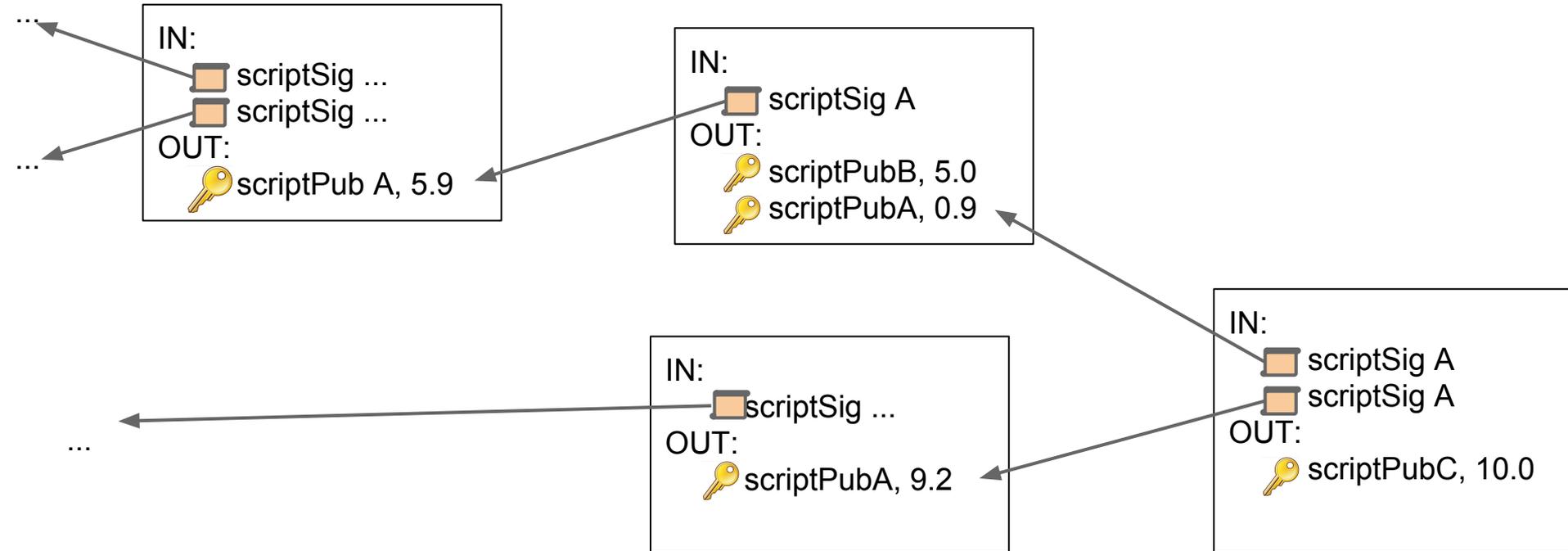
[Wallet Home](#) **My Transactions** [Send Money](#) [Receive Money](#) [Import / Export](#)

Transactions

Summary of your recent transactions

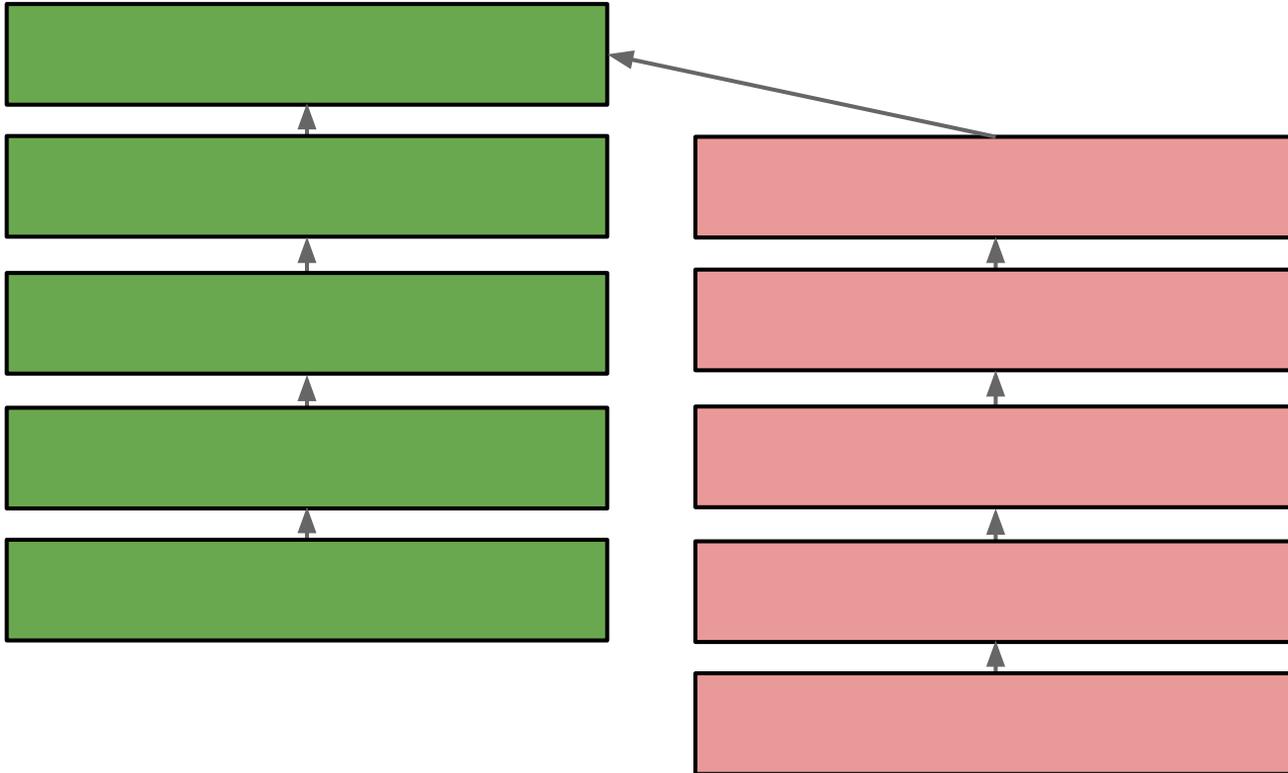
To / From	Date	Amount
[Redacted]	 Today 10:27:48 26 Confirmations	[Redacted]
[Redacted]	 2014-02-13 21:57: [Redacted]	[Redacted]
1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn	 2014-02-13 21: [Redacted] Unconfirmed Transaction!	0.00000001 BTC
[Redacted]	 2014-02-13 21:24: [Redacted]	[Redacted]
[Redacted]	 2014-02-13 21:15: [Redacted]	[Redacted]
1Enjoy1C4bYBR3tN4sMKxvJdQg8NkdR4Z	 2014-02-13 10: [Redacted] Unconfirmed Transaction!	0.00000001 BTC
1SochiWwFFySPjQoi2biVftXn8NRPCSQC	 2014-02-13 10: [Redacted] Unconfirmed Transaction!	0.00000001 BTC

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

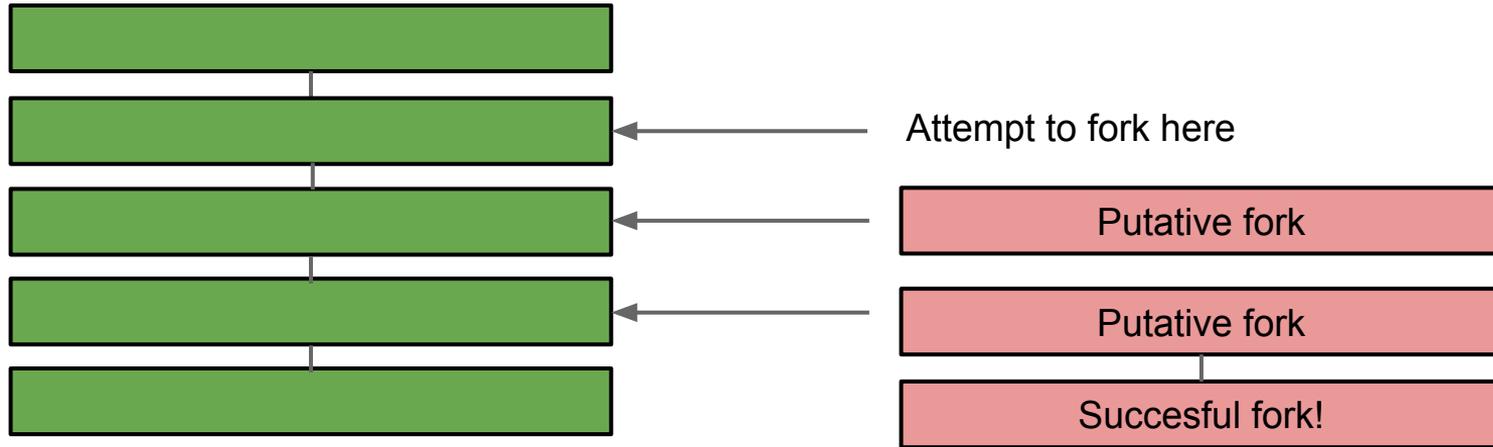
Download links available now on bitcoin.org. Everyone should upgrade to this version.

- 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

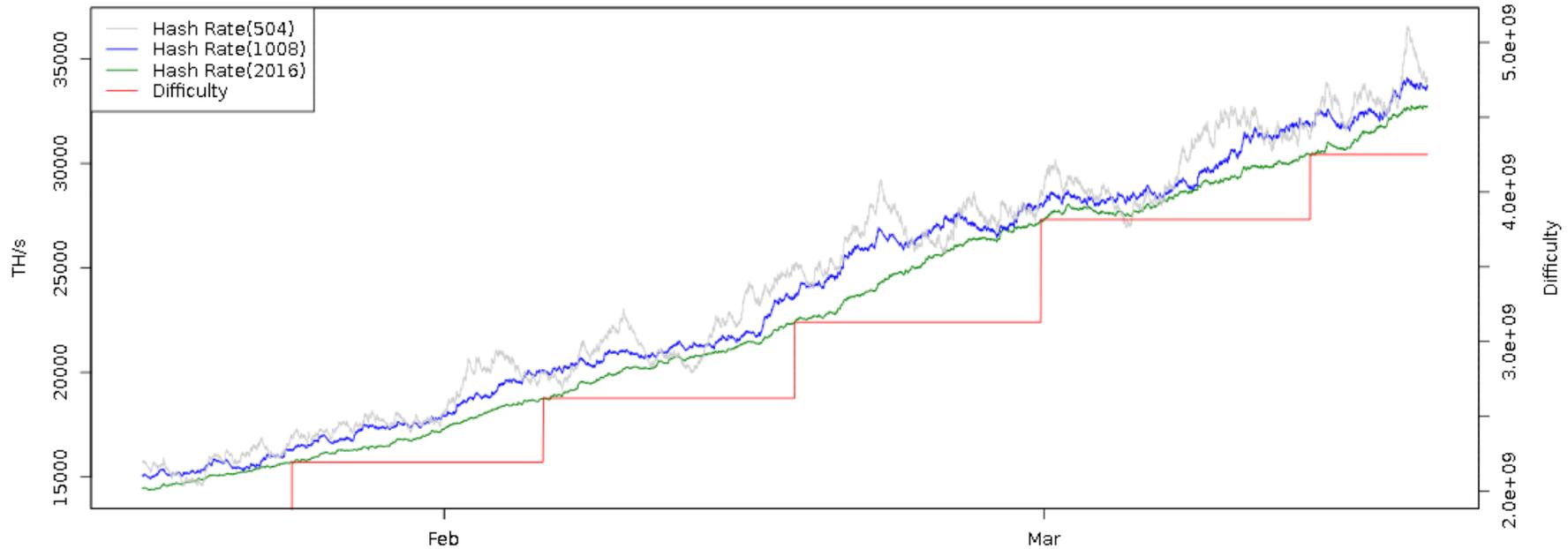
Selfish mining

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]



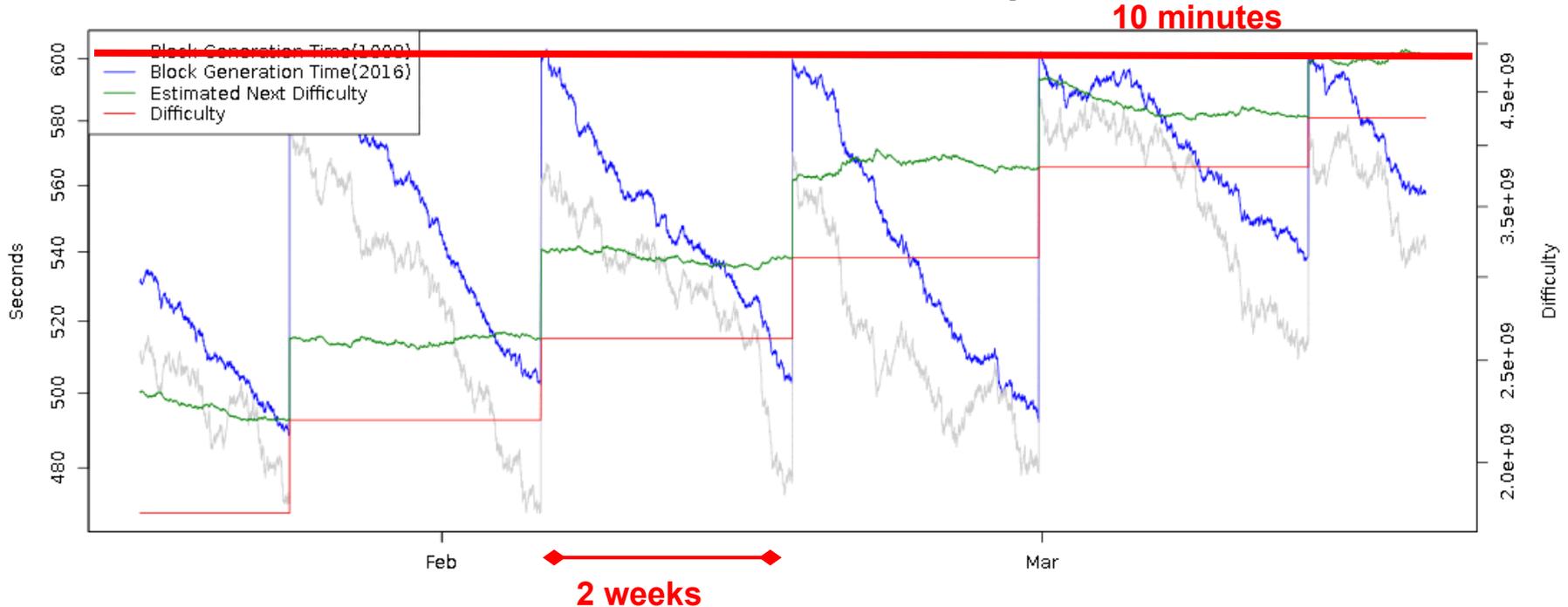
Mining difficulty

Bitcoin Hash Rate vs Difficulty (2 Months)

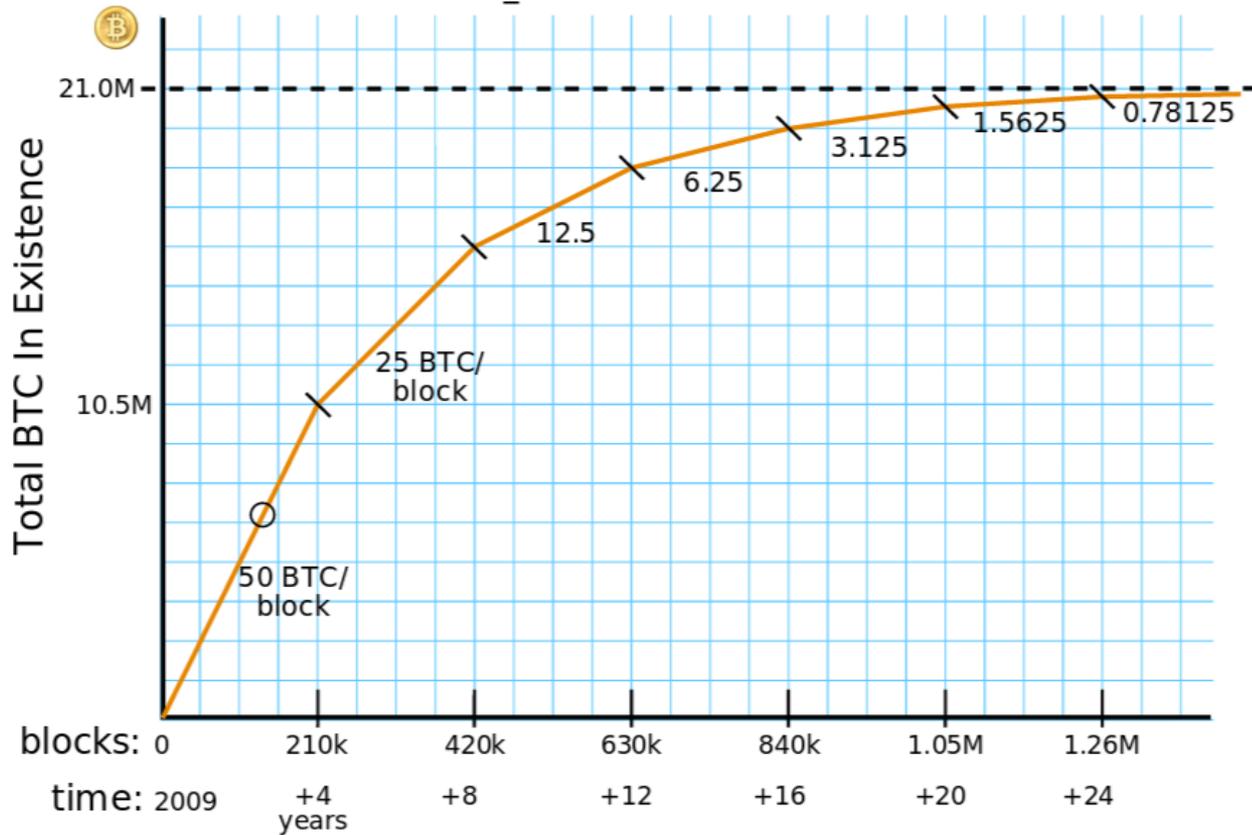


Difficulty adjustment

Bitcoin Block Generation Time vs Difficulty



Mining rewards



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:

[ADD TO CART](#)



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)



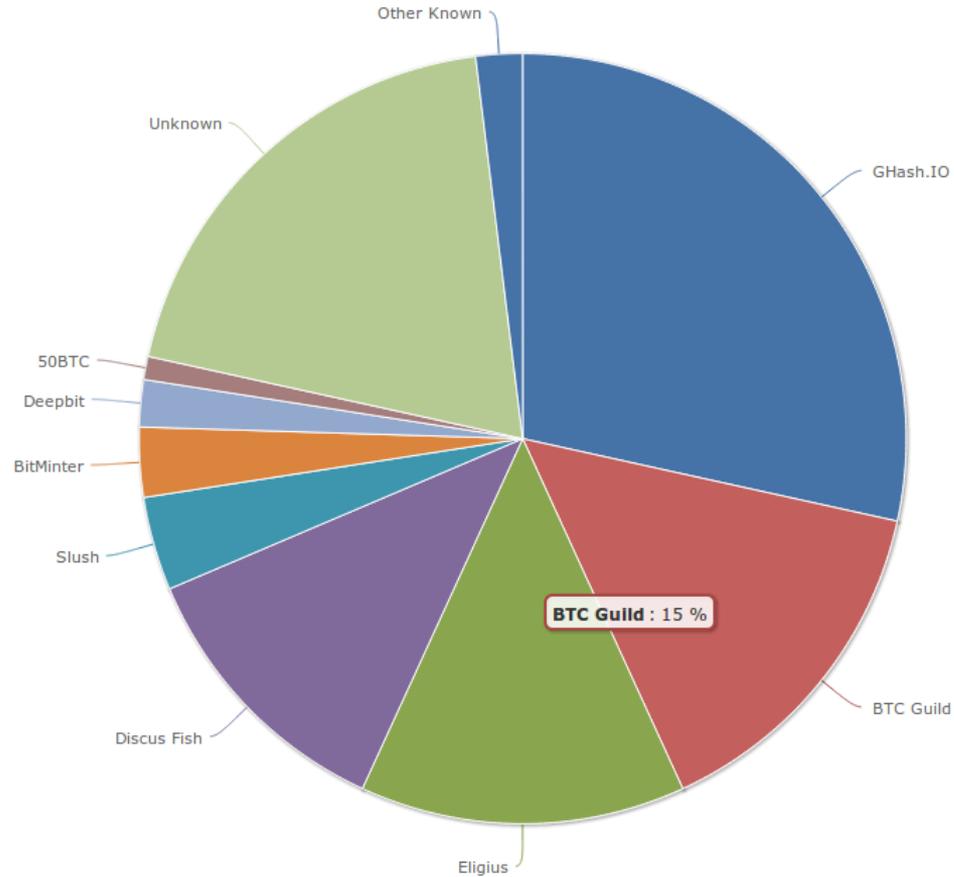
Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

Why would anybody mine bitcoins?



Chilkoot pass,
Klondike 1898

Mining pools



Part III: Bitcoin as a currency

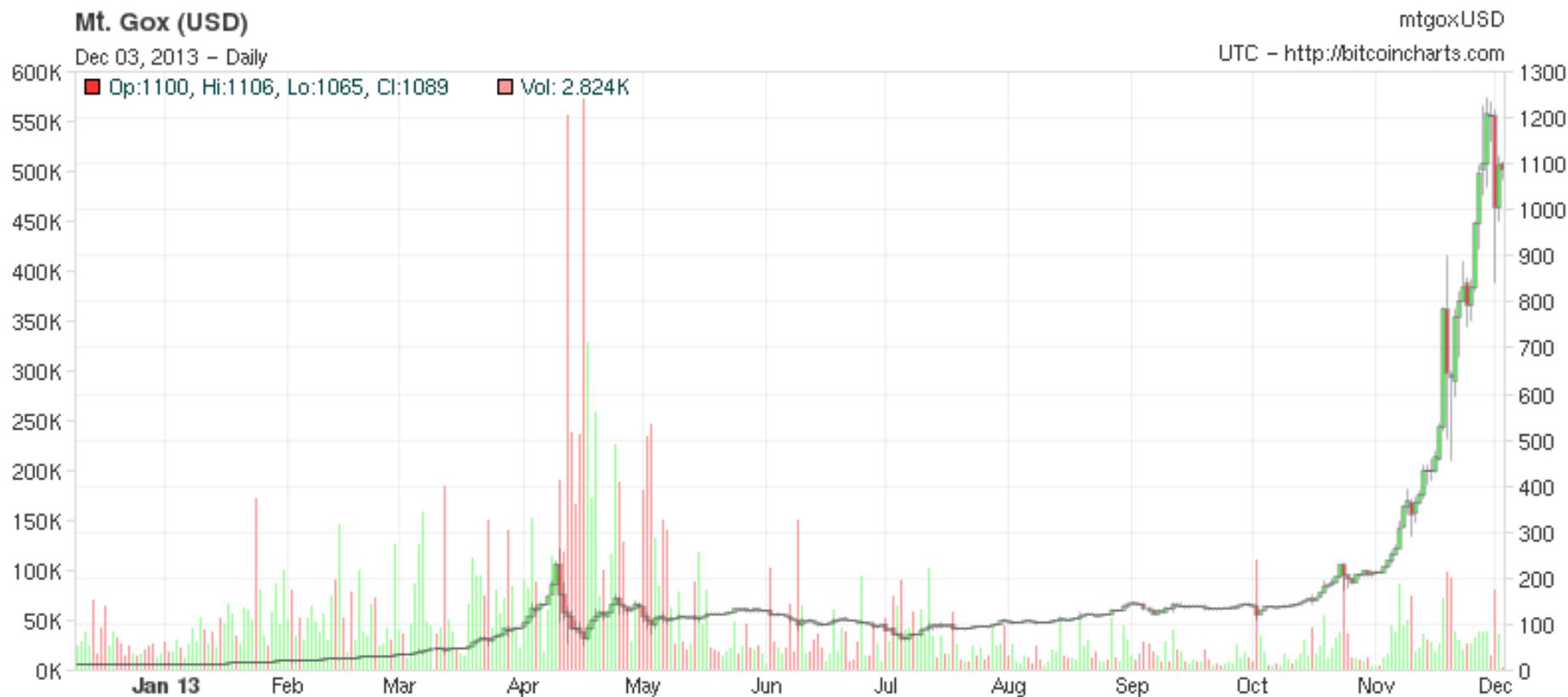
Why does Bitcoin have value?

Consensus

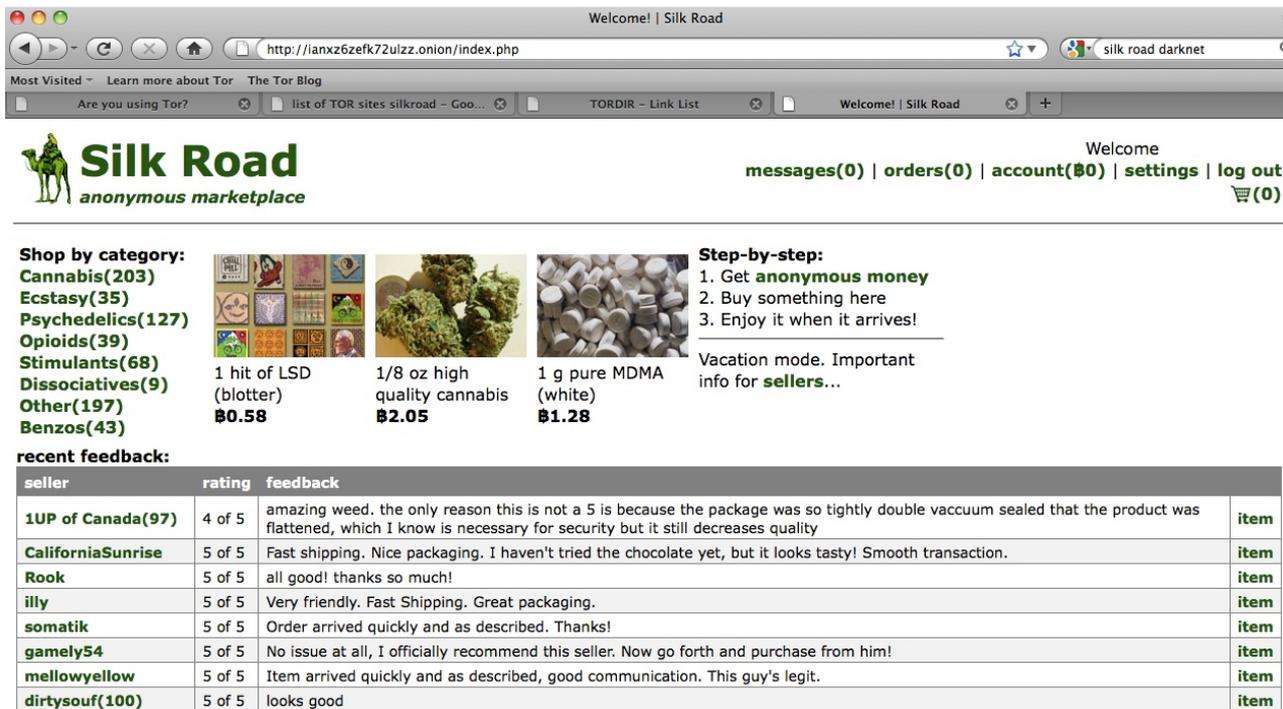
- Consensus in state (blockchain)
- Consensus in payment
- Consensus in rules

[Kroll, Felten 2013]

Price during 2013



Black Markets



The screenshot shows a web browser window with the URL `http://lanxz6zefk72ulzz.onion/index.php`. The page header includes the Silk Road logo (a camel) and the text "Silk Road anonymous marketplace". Navigation links include "messages(0)", "orders(0)", "account(\$0)", "settings", and "log out". A shopping cart icon shows "(0)".

Shop by category:

- Cannabis(203)
- Ecstasy(35)
- Psychedelics(127)
- Opioids(39)
- Stimulants(68)
- Dissociatives(9)
- Other(197)
- Benzos(43)

Step-by-step:

1. Get **anonymous money**
2. Buy something here
3. Enjoy it when it arrives!

Vacation mode. Important info for **sellers**...

recent feedback:

seller	rating	feedback	
1UP of Canada(97)	4 of 5	amazing weed. the only reason this is not a 5 is because the package was so tightly double vacuum sealed that the product was flattened, which I know is necessary for security but it still decreases quality	item
CaliforniaSunrise	5 of 5	Fast shipping. Nice packaging. I haven't tried the chocolate yet, but it looks tasty! Smooth transaction.	item
Rook	5 of 5	all good! thanks so much!	item
illy	5 of 5	Very friendly. Fast Shipping. Great packaging.	item
somatik	5 of 5	Order arrived quickly and as described. Thanks!	item
gamely54	5 of 5	No issue at all, I officially recommend this seller. Now go forth and purchase from him!	item
mellowyellow	5 of 5	Item arrived quickly and as described, good communication. This guy's legit.	item
dirtysouf(100)	5 of 5	looks good	item

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

Capital controls

As Inflation Rages In Iran, Bitcoin Software Not Available

12:41 pm
Feb 7, 2014 EUROPE

Central Bank Of Cyprus Does Not Like Bitcoin

ARTICLE

COMMENTS (9)

[BITCOIN](#) [CYPRUS](#) [VIRTUAL CURRENCIES](#)

it Iran [hard](#). The
ped up
y exchange
ghal.com and
had [rates](#)
al's value against
cies on Tuesday.
1 airlines
were
: into Tehran due
: Iranian rial and shipping giant Maersk [halted](#) all port



calls to Iran.

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

Posted Dec 20, 2013 by [John Biggs \(@johnbiggs\)](#)

E-commerce



SECURE CHECKOUT

Sign In

You are using our secure server



Payment Information

Credit / Debit card



visa, mastercard, american express, discover

Card Number *

Expiration Date *

01 Jan ▼	2014 ▼
----------	--------



PayPal

The safer, easier way to pay.



[Learn More](#)



RewardsPay

DISCOVER | CHOICEprivilegesSM

[What's this?](#) ?



[Learn More](#)

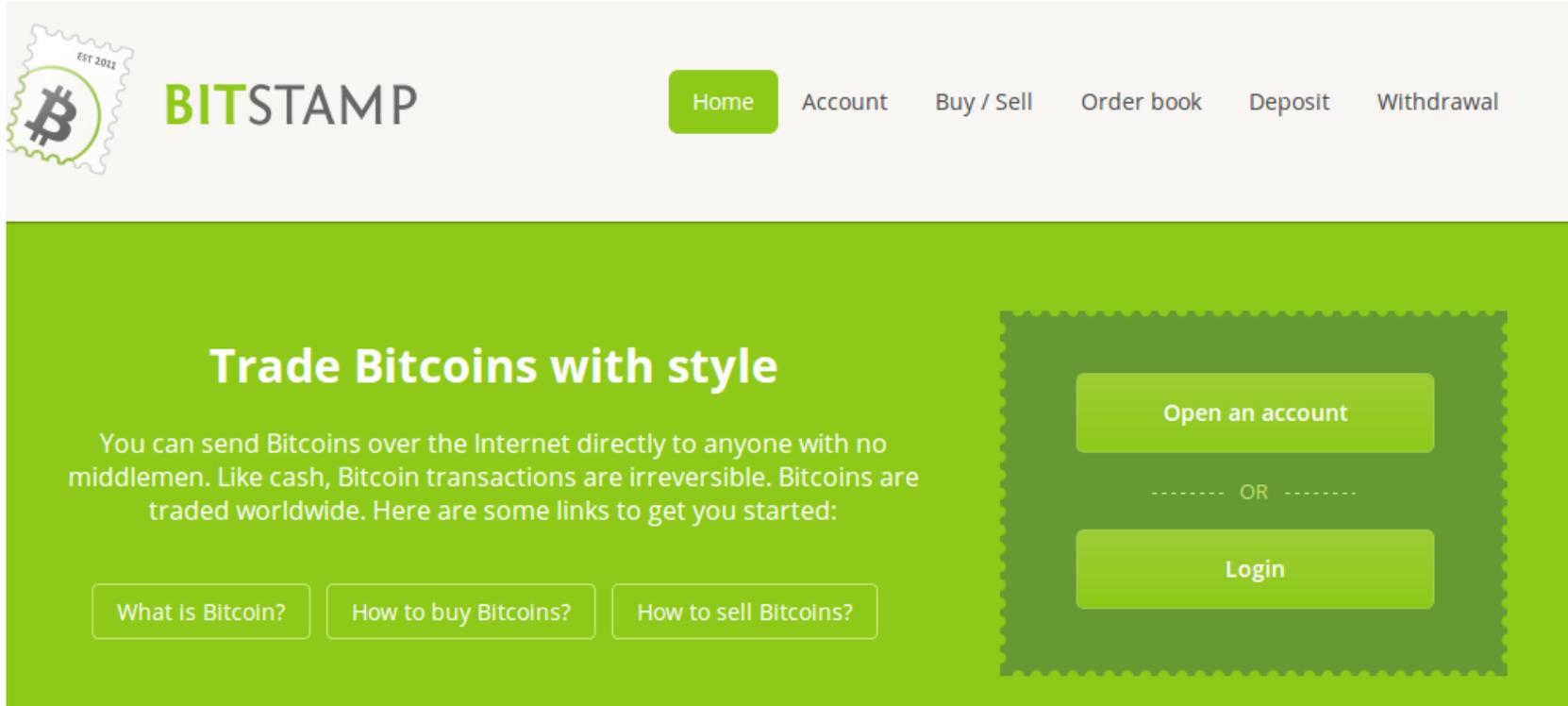


I want to use a promo code



[Why Cant I Use a Gift Card?](#)

Bitcoin exchanges



The image shows the Bitstamp website homepage. At the top left is the Bitstamp logo, which includes a Bitcoin symbol and the text 'EST 2012'. To the right of the logo is the word 'BITSTAMP' in a green and grey font. A navigation menu is located at the top right, with 'Home' highlighted in a green button, followed by 'Account', 'Buy / Sell', 'Order book', 'Deposit', and 'Withdrawal'. The main content area has a green background. On the left, the text reads 'Trade Bitcoins with style' followed by a paragraph explaining that Bitcoin transactions are irreversible and can be sent directly over the internet. Below this text are three buttons: 'What is Bitcoin?', 'How to buy Bitcoins?', and 'How to sell Bitcoins?'. On the right side of the main content area, there is a dark green box with a scalloped border containing two buttons: 'Open an account' and 'Login', with 'OR' in between.

Trade Bitcoins with style

You can send Bitcoins over the Internet directly to anyone with no middlemen. Like cash, Bitcoin transactions are irreversible. Bitcoins are traded worldwide. Here are some links to get you started:

[What is Bitcoin?](#) [How to buy Bitcoins?](#) [How to sell Bitcoins?](#)

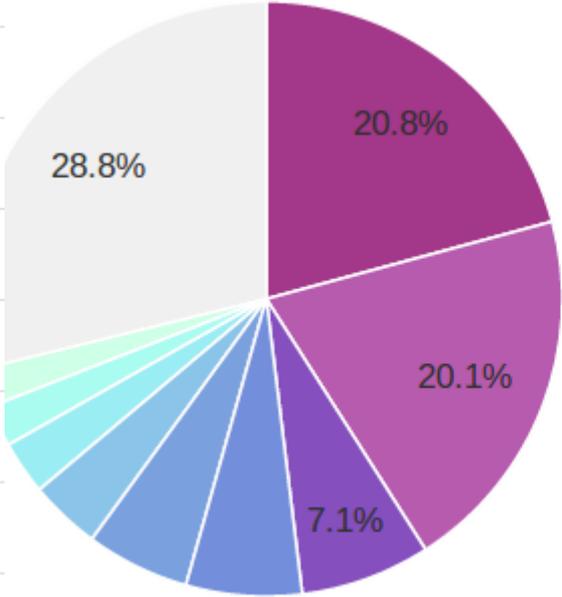
[Open an account](#)

----- OR -----

[Login](#)

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

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