



Bitcoin

Based on “Bitcoin Tutorial” presentation by
Joseph Bonneau, Princeton University

Bonneau slides marked “JB”

Bitcoin Snapshot: October 2, 2015

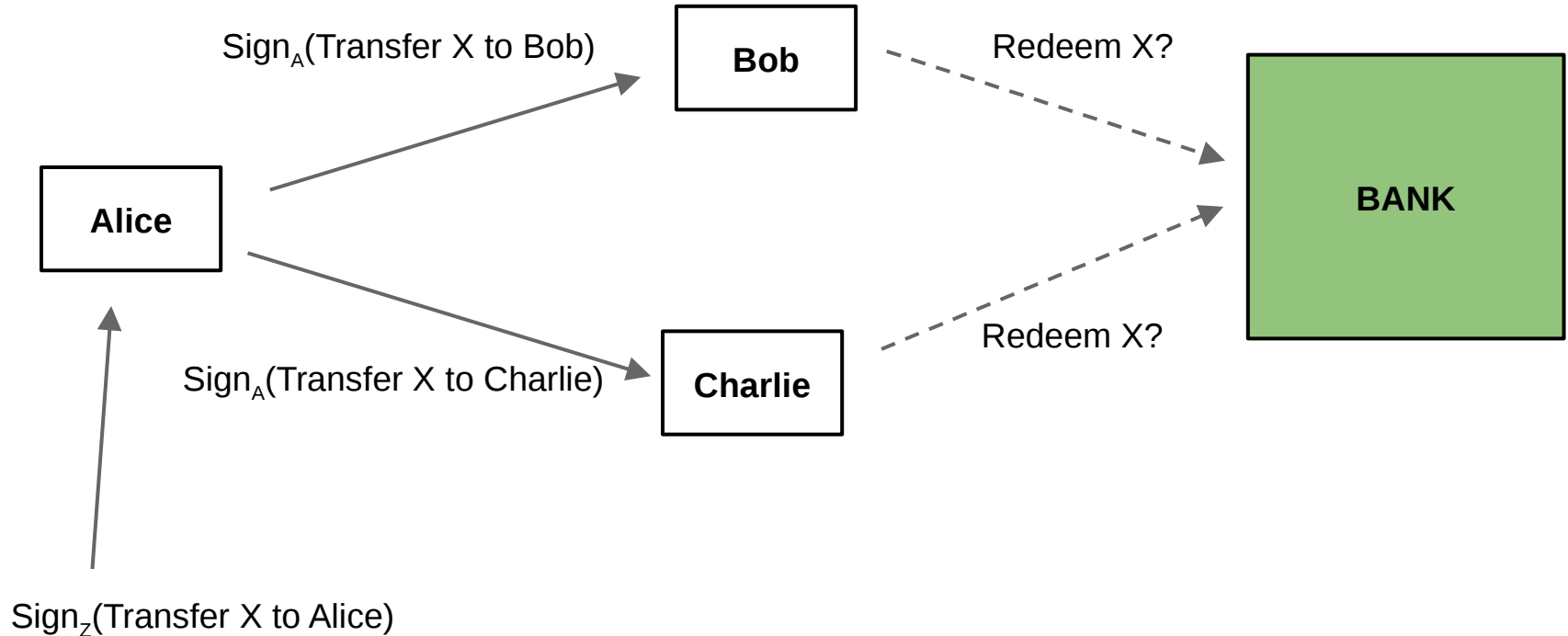
Bitcoin is a combination of several things: a currency, a payment system, and a collection of algorithms and software implementations.

The goal of bitcoin is to enable payments with low transaction costs. Bitcoin can also sometimes provide anonymity.

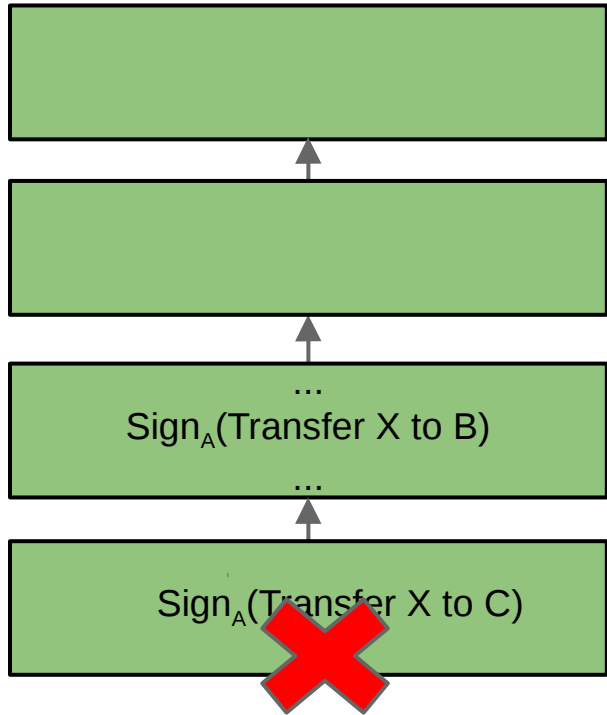
One bitcoin (BTC) is worth about \$238. (A year ago: \$394.)

Approximately 14 million bitcoins have been created (mined) to date, for a total value of approximately \$3.5 billion.

Double spending: why ecash is hard



Solution: Maintain a global public append-only log



*The block chain –
a public ledger of
all transactions.*

(In Bitcoin, the log is
extended in
increments of blocks,
each of which may
contain thousands of
transactions.)

Getting started

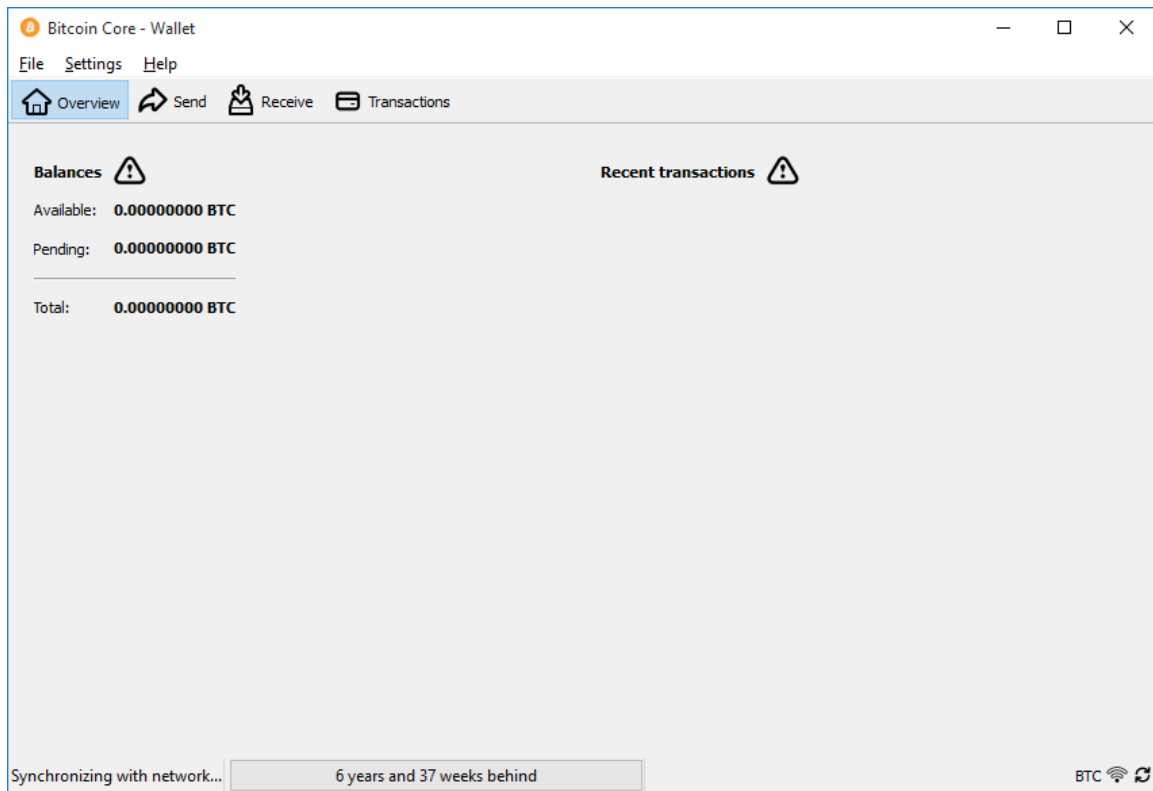
Download software to create a Bitcoin wallet (see [https://
bitcoin.org/en/choose-your-wallet](https://bitcoin.org/en/choose-your-wallet))

The wallet holds the private keys you use to prove you own specific Bitcoins.

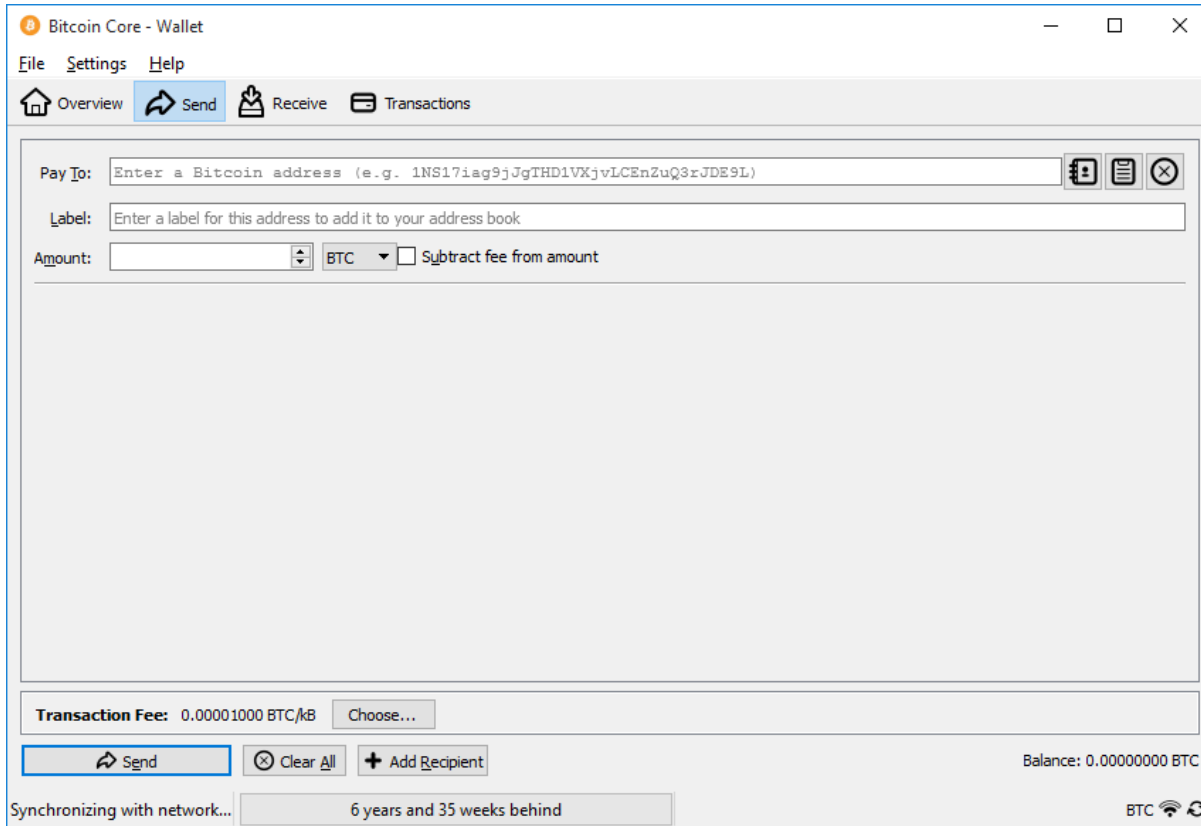
The software creates public/private key pairs for you as needed. For each pair, there is a corresponding bitcoin address, which is a 160-bit hash of the public key. Bitcoins are sent to addresses.

The wallet also contains software that allows you to send and receive bitcoins. You send bitcoins by registering your payments in the block chain, which is bitcoin's public ledger containing all transactions since the beginning of bitcoin.

Bitcoin Core (original) wallet on first start-up



Send



bmm

Spending a Bitcoin

A transaction is of the form “send these Bitcoins from address Y to address Z”

Specific Bitcoins are described as outputs of previous transactions.

The transaction is signed with the private key of address Y and broadcast, along with the public key of Y, to the payment network

A transaction might also include a transaction fee, to be described later.

Bitcoin mining

Every ten minutes, one lucky Bitcoin miner earns a reward for extending the block chain by one block.

In 2009, the reward was 50 BTC. Today it is 25 BTC. (See <https://blockchain.info/q> to issue queries about the block chain.)

Mining is the only mechanism for creating new bitcoins. The total number of Bitcoins will never exceed 21M.

The rewarded miner also receives all (optional) transaction fees in the block.

How is a new block created?

A Bitcoin miner creates a block by

- (1) Gathering a set of pending transactions, possibly prioritizing those with transaction fees
- (2) Verifying the transactions
- (3) Solving a hashing problem

On October 3, 2015, according to <https://blockchain.info/q>, average number of transactions per block is 411, current number of pending unconfirmed transactions is 2495.

How is a transaction verified?

“send these Bitcoins from address Y to address Z”

The miner first checks the signature using the public key for address Y.

- compute hash of public key for Y, which should be Y
- check signature of transaction using public key for Y

Then the miner checks the public ledger to verify that Y hasn't already sent these Bitcoins to someone else.

The Hashing Problem

To extend the blockchain, a miner creates a new block, containing:

- (1) hash of previous block
- (2) new transactions to include in the blockchain, including transactions fees
- (3) creation of reward bitcoins (e.g., 25 new BTC)
- (4) nonce

Block is valid if hash of (1)-(4) ends in enough zeroes, as determined by current difficulty. Miner has to find the right nonce by trial and error!

Difficulty chosen so that the time until the first miner wins is about ten minutes, on average.

Why use a proof of work scheme to pick the winning miner?

Why not just hold a lottery and choose a miner at random?

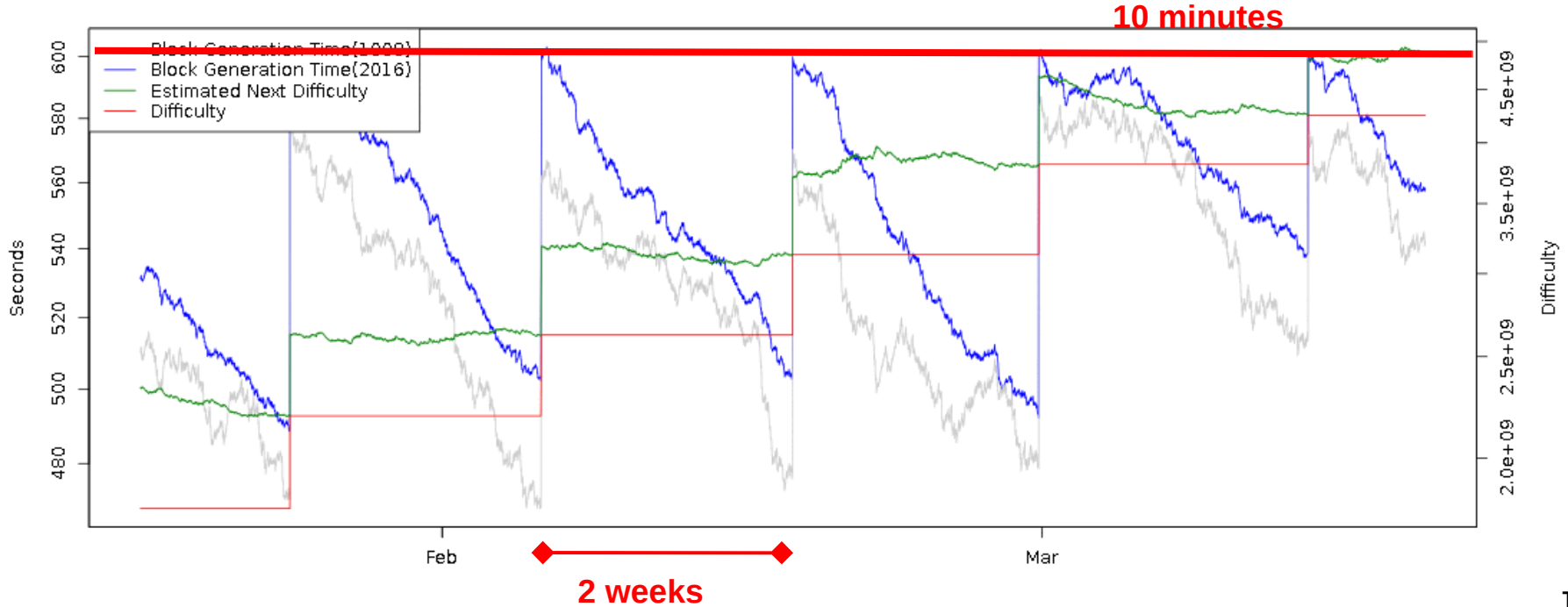
Have to solve the Sybil problem: What if one person enters the lottery many times?

The proof of work scheme makes it difficult for one party to “enter the lottery so many times” that they can take control of the block chain.

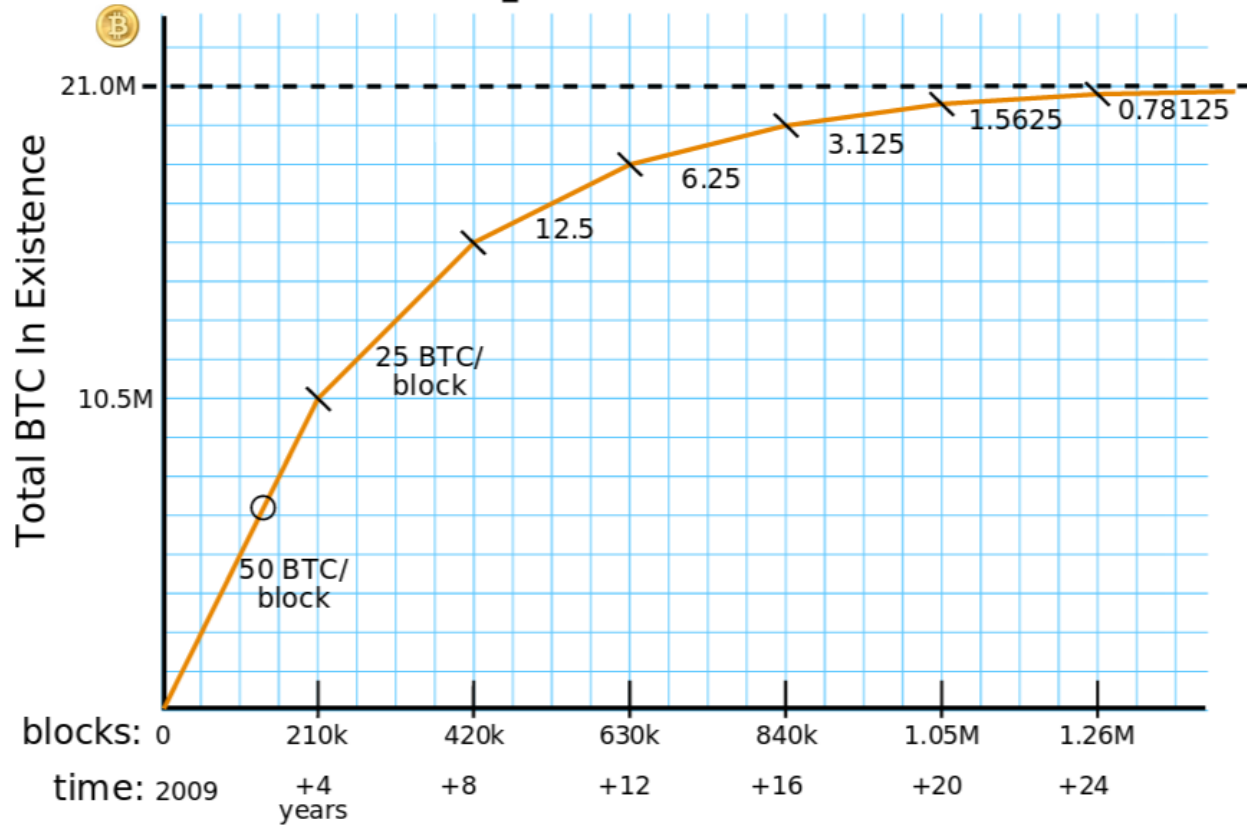
bmm

Difficulty adjustment

Bitcoin Block Generation Time vs Difficulty



Mining rewards



Courtesy:
Brian Warner

JB

Total network capacity

- **9×10^{18}** hashes per block (every 10 minutes!)
on average, based on difficulty level on
October 3, 2015
- **2^{75}** hashes in 2013
 - In exchange for **~US\$250M**
- Consuming > **100 MW**

Transaction costs

Assuming one BTC is worth \$400, reward (25 BTC) per block is \$10,000. (Transaction fees negligible today.)

Today number of transactions per second is about 2, number per block is about 1200.

Reward per transaction is about \$8.33 !!!!

Cost of electricity spent mining is probably close to reward.

Fundamental problem: 1MB limit on block size implies at most 10 transactions per second.

Transaction Confirmations

A transaction is said to have received k confirmations if it has been published in a block that has been added to the block chain, and $k-1$ more blocks have also been added.

A transaction is typically considered “confirmed” once it has 6 confirmations.

Newly minted Bitcoins are typically considered confirmed once they have received 100 confirmations.








Transaction confirmation (~6 blocks)

My Wallet Be Your Own Bank.

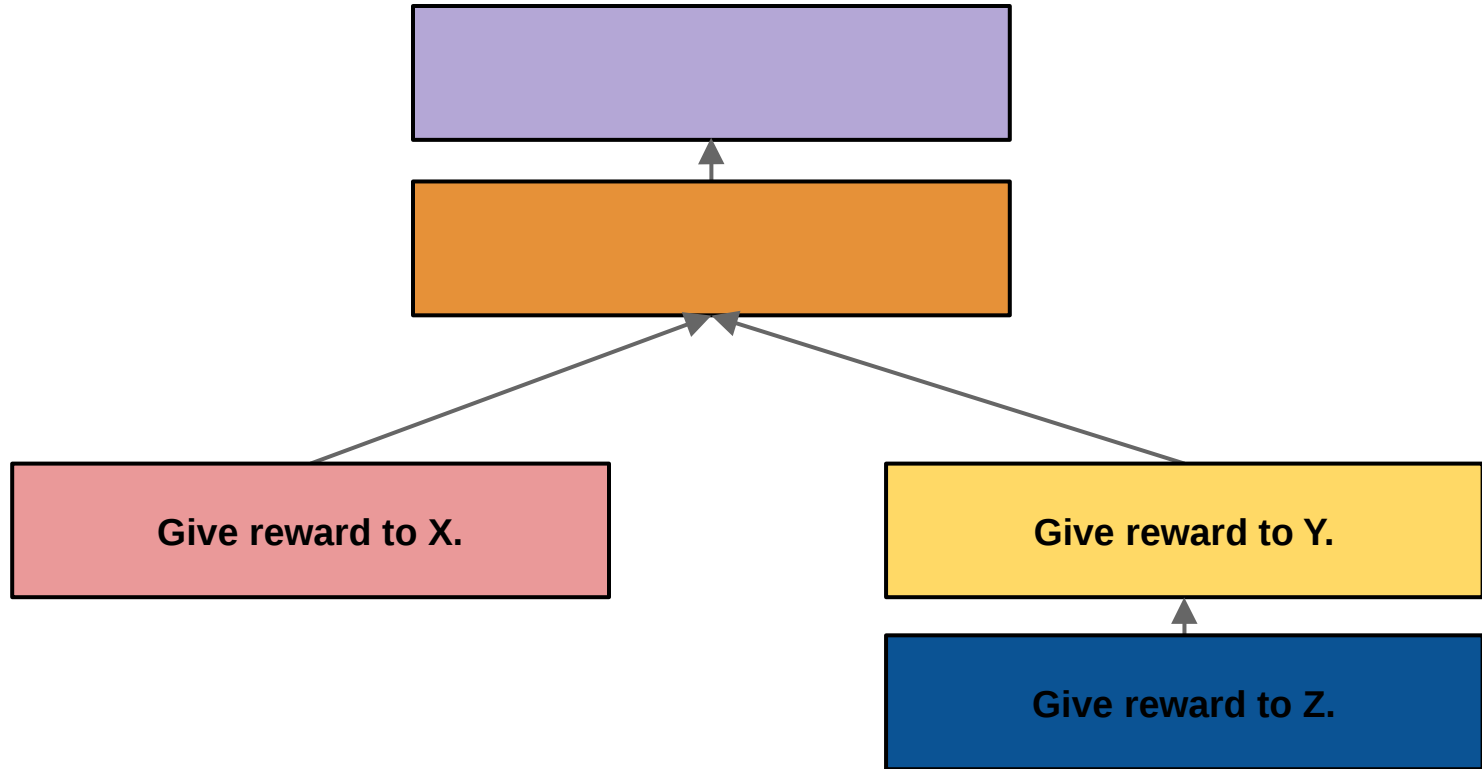
Wallet Home **My Transactions** Send Money Receive Money Import / Export

Transactions

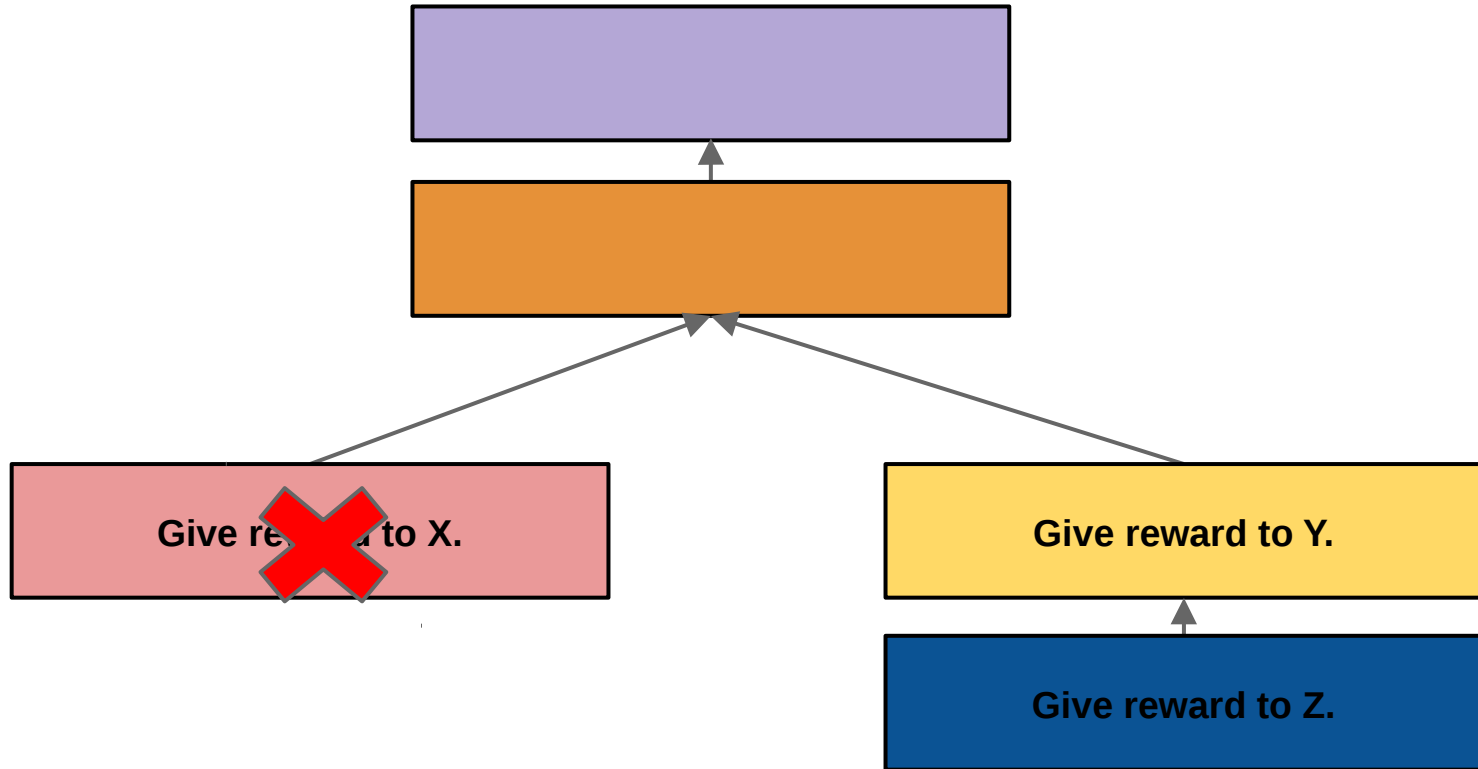
Summary of your recent transactions

To / From	Date	Amount
	 Today 10:27:48 26 Confirmations	
	 2014-02-13 21:57:	
1Bhv6XjXBvraivcATHwwLMscZ5xJm9FsPn	 2014-02-13 21: Unconfirmed Transaction!	0.00000001 BTC
	 2014-02-13 21:24:	
	 2014-02-13 21:15:	
1Enjoy1C4bYBr3tN4sMKxvJdQg8NkdR4Z	 2014-02-13 10: Unconfirmed Transaction!	0.00000001 BTC
1SochiWwFFySPjQoi2biVftXn8NRPCSQC	 2014-02-13 10: Unconfirmed Transaction!	0.00000001 BTC

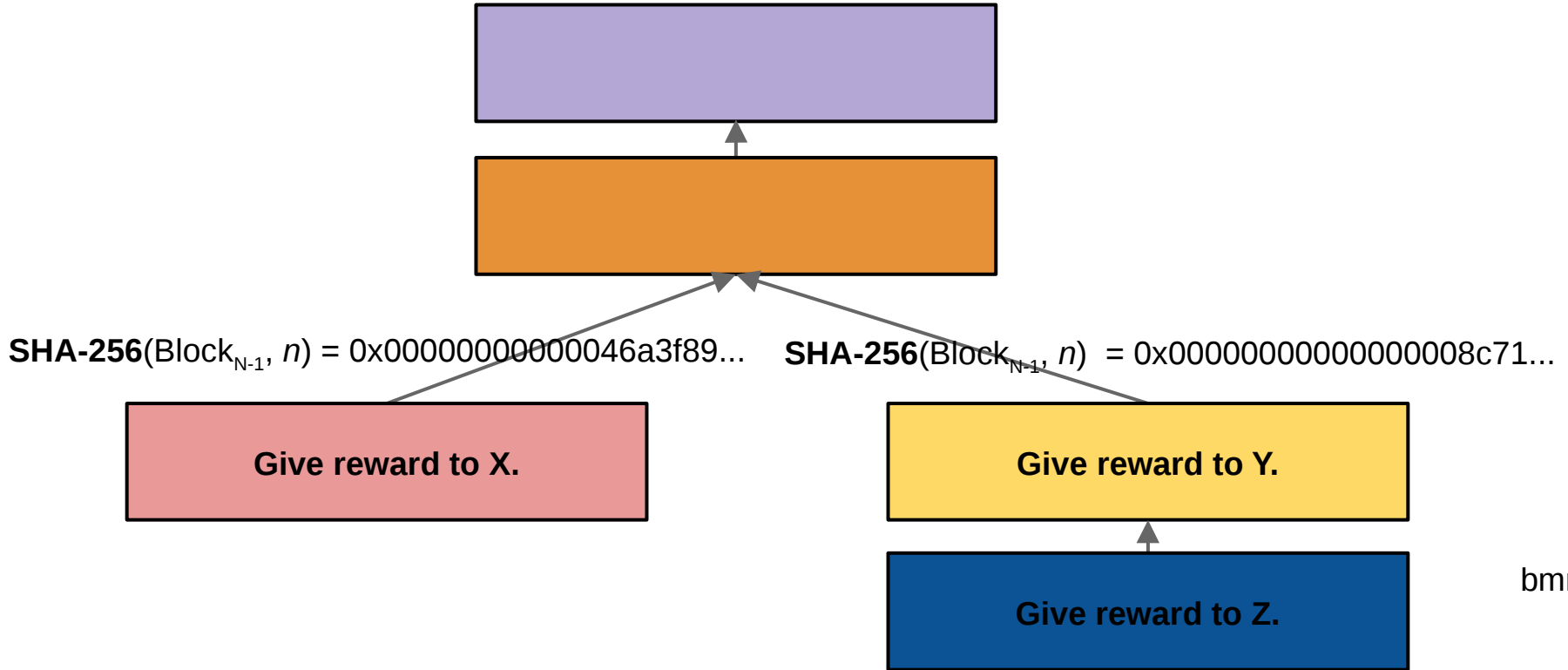
A *fork* can occur when two miners publish blocks simultaneously. Such blocks are almost always in conflict.



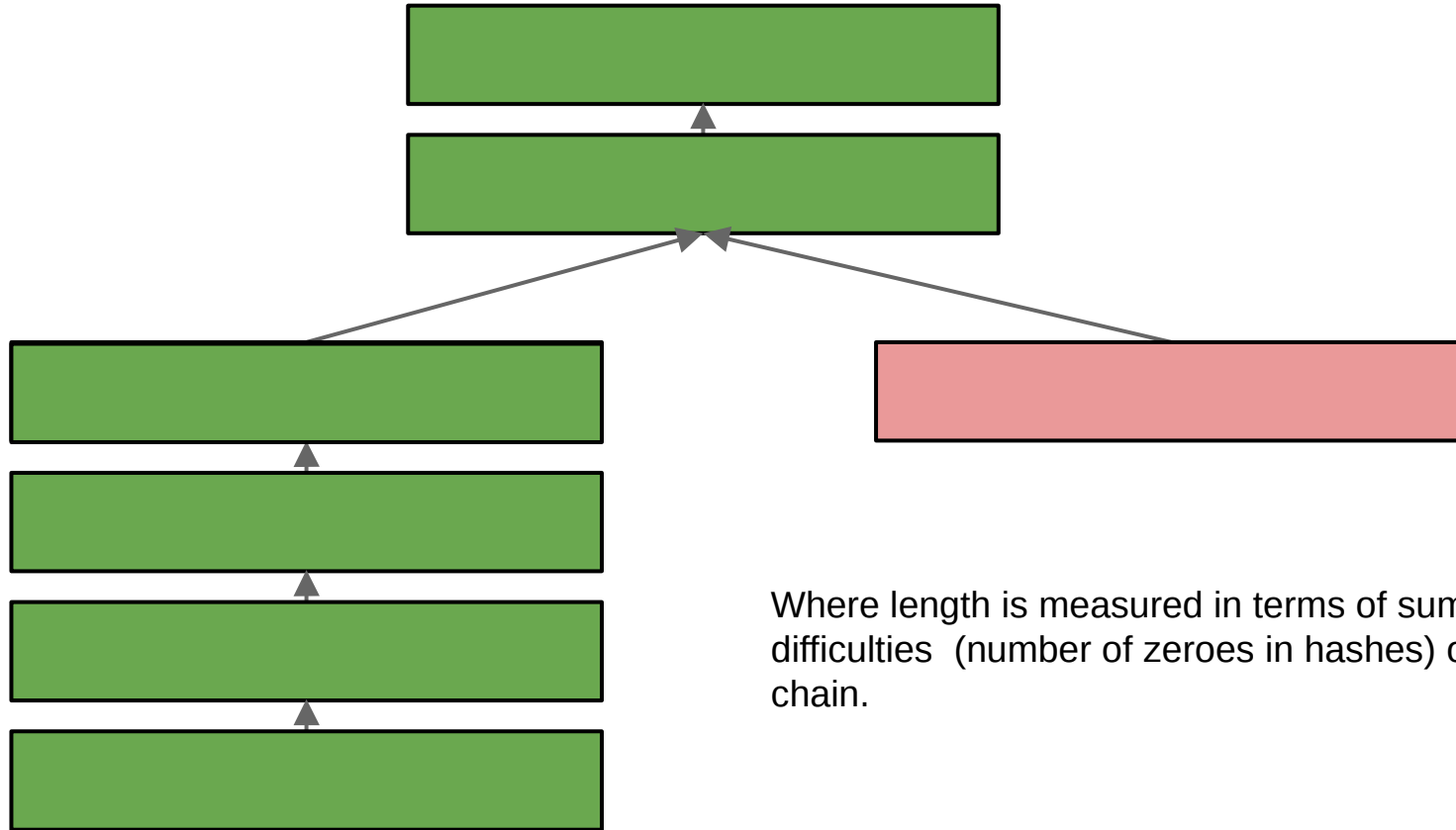
Effort spent on a fork that eventually loses is wasted.



To break ties, choose branch with greater number of zeros in hash.



More generally, longest chain wins.



Where length is measured in terms of sum of difficulties (number of zeroes in hashes) of blocks in chain.

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](#)



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 :

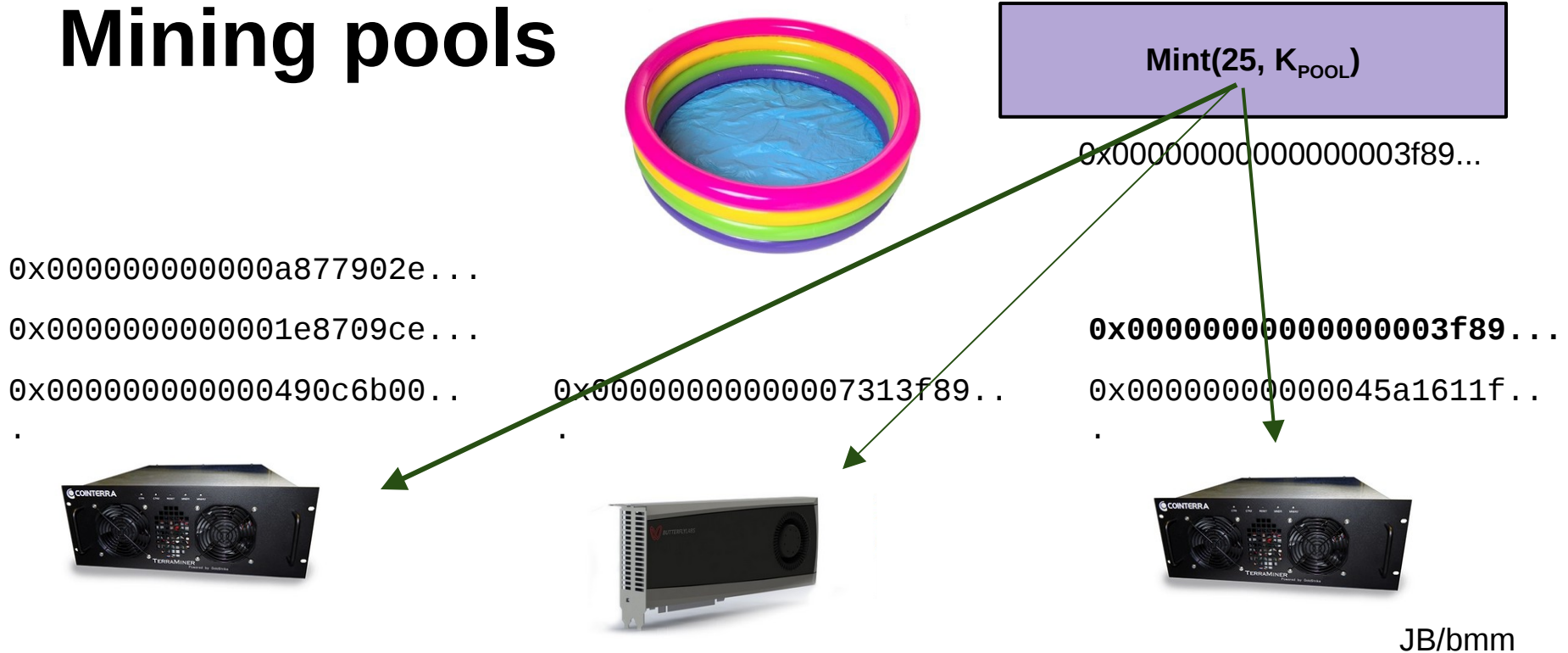
- Worldwide, Express
- Included in the price
- Available:
100 Units: Shipping April
(Week 3)



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.

JB

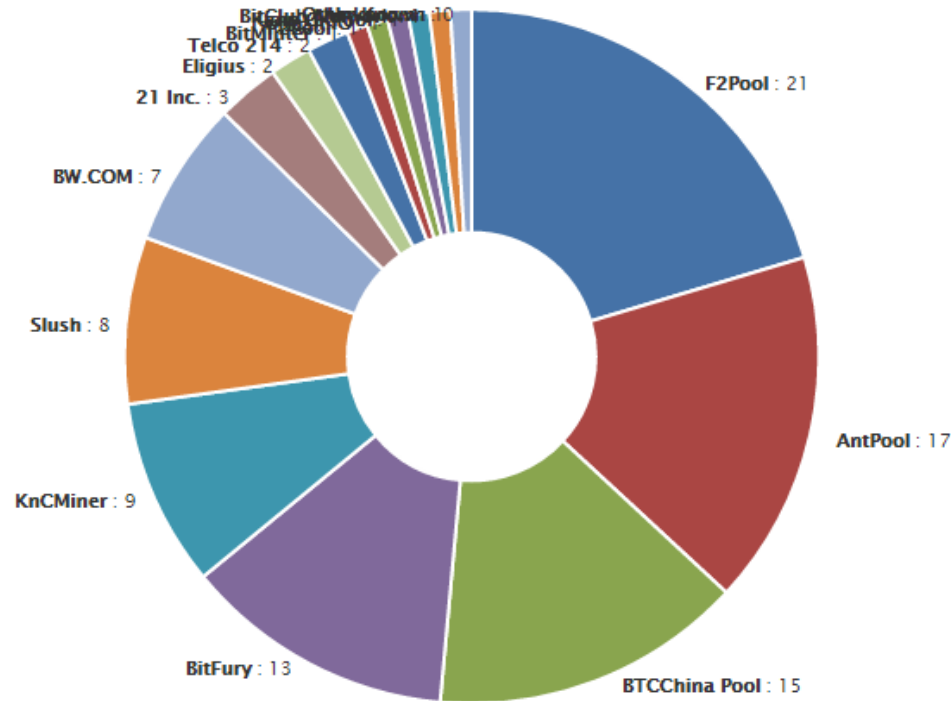
Mining pools



A miner creates a new block assigning reward and transaction fees to the pool.

Every miner “proves” to the pool how much effort has been expended by submitting the hash with largest number of zeros.

Mining pools



At times in the past, one pool, Ghash.IO had over 51% of the computing power.

51% attack: If one guild has more power than all others combined, they can extend their fork faster than any other fork, reaping all rewards and transaction fees, and choosing which transactions to confirm.

October 3, 2015

Why does Bitcoin have value?

Consensus

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

JB

The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries

Joshua Kroll, Ian Davey, Ed Felten, WEIS 2013

Price during 2013



Black Markets

The screenshot shows a web browser window with the address bar displaying `http://ianxz6zefk72ulzz.onion/index.php`. The page title is "Welcome! | Silk Road". The browser's address bar also shows "silk road darknet". The page content includes the Silk Road logo (a camel and rider) 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:

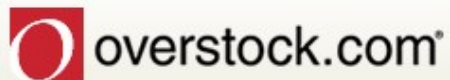
seller	rating	feedback	
1UP of Canada(97)	4 of 5	amazing weed. the only reason this is not a 5 is because the package was so tightly double vacuum sealed that the product was flattened, which I know is necessary for security but it still decreases quality	item
CaliforniaSunrise	5 of 5	Fast shipping. 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

JB

Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace

Nicolas Christin, WWW 2013

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 *

PayPal

The safer, easier way to pay.



[Learn More](#)



RewardsPay

DISCOVER CHOICEprivileges

[What's this?](#)



[Learn More](#)

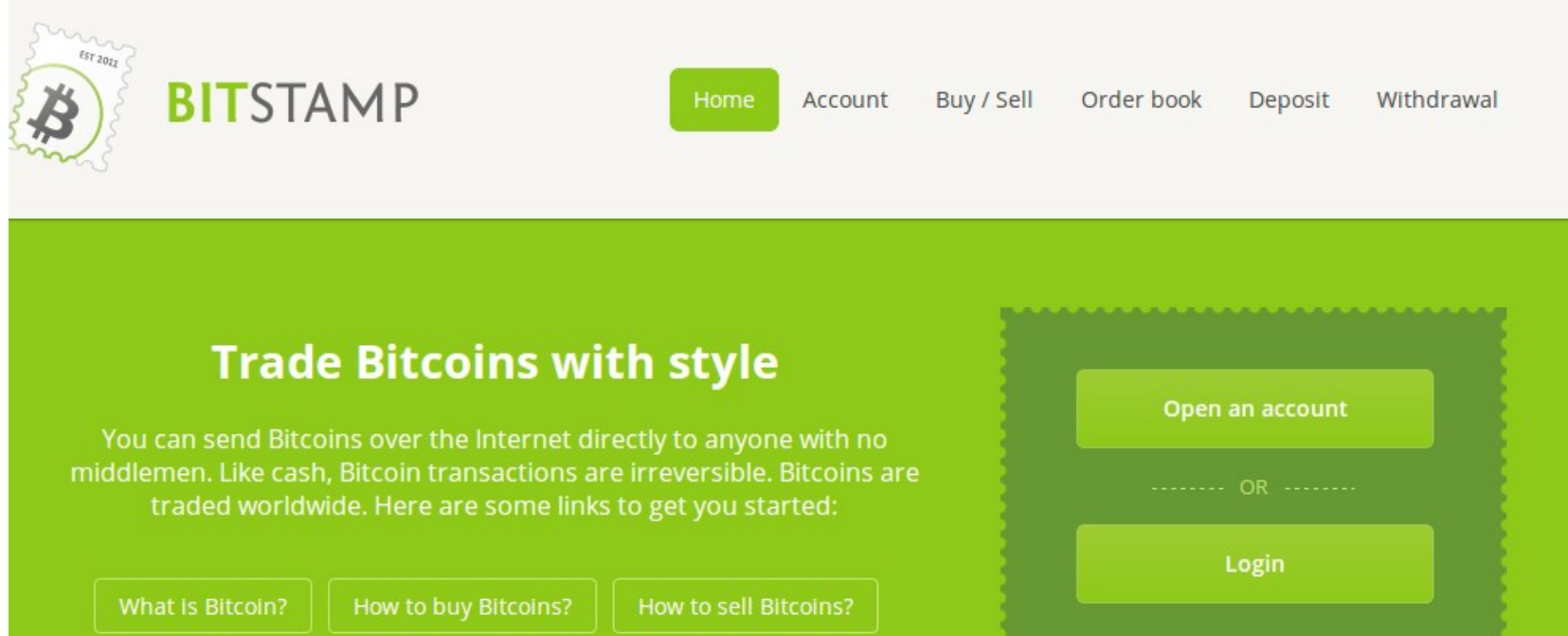


I want to use a promo code



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

Bitcoin exchanges – buy and sell bitcoin using different currencies



The image shows the homepage of Bitstamp, a Bitcoin exchange. The header features the Bitstamp logo (a Bitcoin symbol with 'EST 2012') and the name 'BITSTAMP'. Navigation links include 'Home' (highlighted in green), 'Account', 'Buy / Sell', 'Order book', 'Deposit', and 'Withdrawal'. The main content area has a green background with the heading 'Trade Bitcoins with style'. Below this, text explains that Bitcoin transactions are irreversible and provides links for 'What is Bitcoin?', 'How to buy Bitcoins?', and 'How to sell Bitcoins?'. On the right, there are buttons for 'Open an account' and 'Login', separated by 'OR'.

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](#)

JB

Beware the middleman: Empirical analysis of Bitcoin-exchange risk
Tyler Moore and Nicolas Christin, Financial Crypto 2013

Physical Bitcoin (a gimmick?)



private key is embedded in coin
and can be accessed (possibly
electronically) only by
physically breaking the coin

trust creator to destroy any
record of private key

<http://media.coindesk.com/2014/09/casascius-coins.jpg>

bmm

Anonymity?

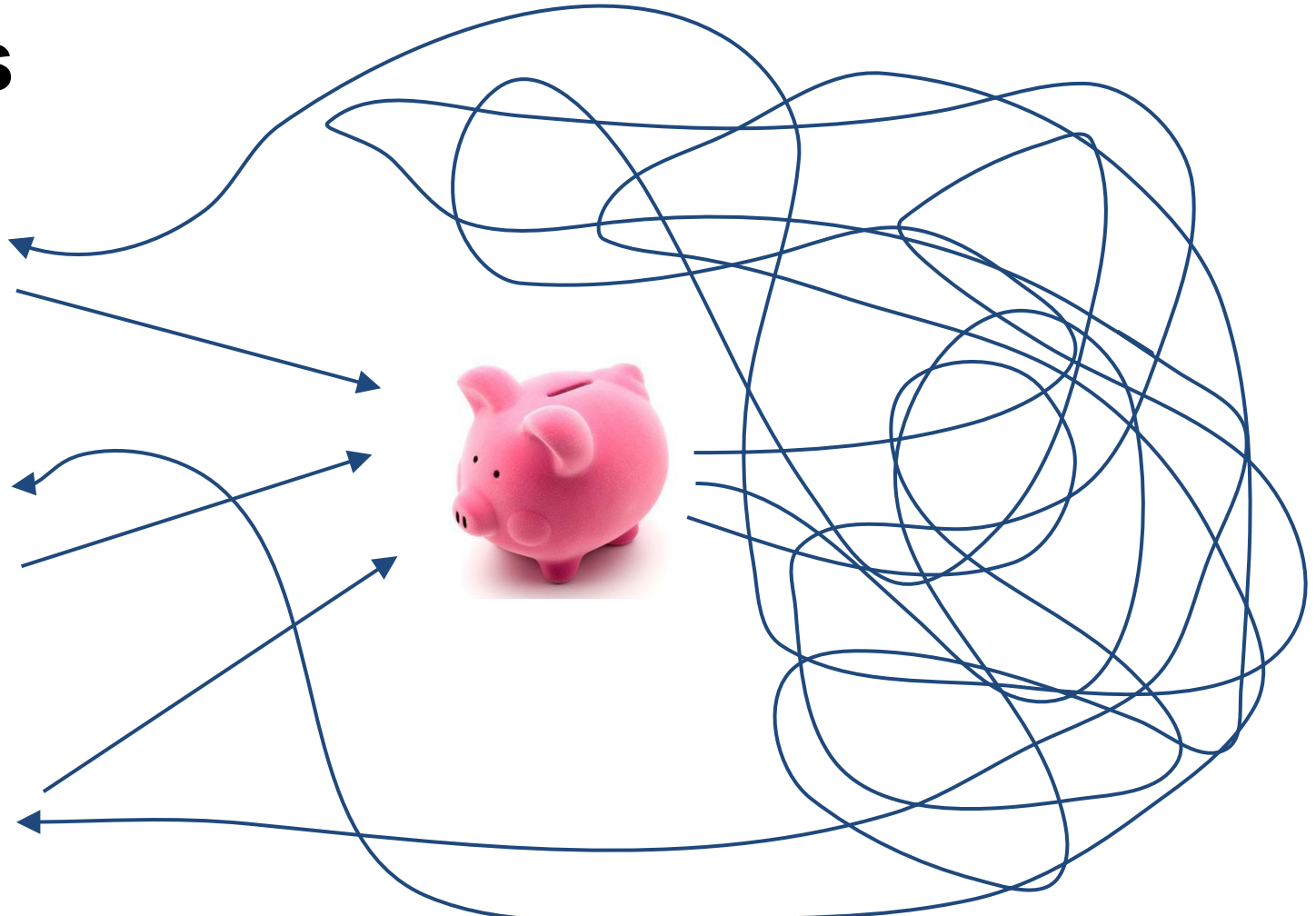
A transaction history is recorded for every Bitcoin

Key to anonymity is to avoid tying any personal information to your Bitcoin addresses

Use an address only once

Self-mined Bitcoins, using an anonymizing network to connect to the payment system, are hardest to trace

Mixes



Mixes today

Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion.

-The Bitcoin Wiki

An inquiry into money laundering tools in the Bitcoin ecosystem
Möser, Malte, Rainer Böhme, and Dominic Breuker, ECRIME 2013 JB

Bitcoin in the news

In the news

- [BitPay](#) reports a theft of 5,000 BTC and is suing its insurer for declining to pay a \$1 million settlement.
- [Mark Karpelès](#) (*pictured*) is charged with embezzling ¥321 million from [Mt. Gox](#) customers.
- [Shaun Bridges](#) pleads guilty to stealing \$820,000 from the [Silk Road](#).
- A flash crash on [Bitfinex](#) brings a low of \$162 before quickly recovering.
- [Bitcoin Core 0.11](#) is released.



Ongoing: [Block size limit controversy](#)

https://en.bitcoin.it/wiki/Main_Page