Are You Ready for Bitcoin? (Is the World Ready for Bitcoin?)

Bebo White

SLAC National Accelerator Laboratory/
Stanford University

bebo@slac.stanford.edu

MacMania 17, Somewhere@Sea, June 2014

May 8th, 2014
03:20 PM ET

4 weeks ago

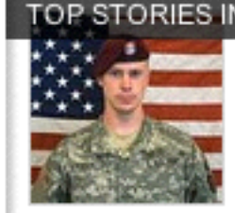
Bitcoin OK for politics, with $100 limit

Posted by
CNN's Jennifer Liberto

Washington (CNN) – The Federal Election Commission on Thursday approved the use of the alternative currency Bitcoin for political contributions with limits of $100 per donor per election cycle.

THE WALL STREET JOURNAL. | OPINION

TOP STORIES IN OPINION



1 of 12
Trading With the Taliban

2 of 12
Ted Cruz: The Democratic Assault on the...

3 of 12
Bitcoin's Futile Quest to Be a Currency

OPINION

Bitcoin's Futile Quest to Be a Currency

The IRS treats bitcoins as property, and any transaction using them triggers a taxable event.

Who owns Bitcoin?

Why?/Why Not?

MacMania 17, Somewhere@Sea, June 2014

https://www.google.com/search?q=bitcoin+sucks
~2,400,000 results

https://www.google.com/search?q=bitcoin+rocks
~52,400,000 results

What is Bitcoin?

- Designed for an “Internet Society” using Internet technologies
- Decentralized and independent of “state currencies”
- Excellent for anonymous transactions like “hard currency” (i.e., unlike credit cards)
- Excellent for E-Commerce - online exchange, no specific currency, micro payments
- Easily convertible to “state currencies”

People are using it…

- Not just for illegal activities (e.g., Silk Road)
- Some financial analysts advise portfolio diversification with BTC
- Sacramento Kings - customized jersey (.37 BTC)
- Egifter - $500 Hyatt voucher (.601 BTC)
- Lamborghini Newport Beach - pre-owned Tesla Model S (91.4 BTC)
- EVR Gastro-Lounge - Vanilla Mint Julep (0.18 BTC)

THE BITCOIN AND RASPBERRY PI POWERED POOL TABLE

http://www.coindesk.com/bitcoin-pool-table-raspberry-pi/

MacMania 17, Somewhere@Sea, June 2014

bitcoin LANDSCAPE by @ssubo

EMERGENCE CAPITAL PARTNERS

EXCHANGES / TRADING

MT.GOX · BitBox · vaurum · BTC · coinbase · LocalBitcoins.com · TRADEHILL · Coinabul · CoinLab · BITSTAMP · kraken · Bitfinex · coinsetter

WALLETS

MULTIBIT · ELECTRUM · BIPS · WalletBit · wallabit · bitcoin Wallet · Blockchain · eCoin Cashier (Cash as you need it) · mycelium · PIKAPAY

MERCHANT SERVICES

bitpay · BitMonet · BitMerch · BITS · BTC Merch · BW · BIPS · BITPagos

MINING

ASICMINER · AVALON · CLOUD HASHING · alydian · Cognitive Mining

HARDWARE

BUTTERFLYLABS · LAMASSU BITCOIN VENTURES

IDENTITY

GLIPH · VerifyBTC · BLOCKSCORE

ALTERNATIVE CURRENCIES

litecoin · PPCOIN · namecoin · OpenCoin · ripple · Terracoin · Feathercoin

OTHERS

REMITTANCES

bitcoinWireless · Buttercoin

MEDIA

CoinDesk · BITCOIN MAGAZINE · bitcoin charts

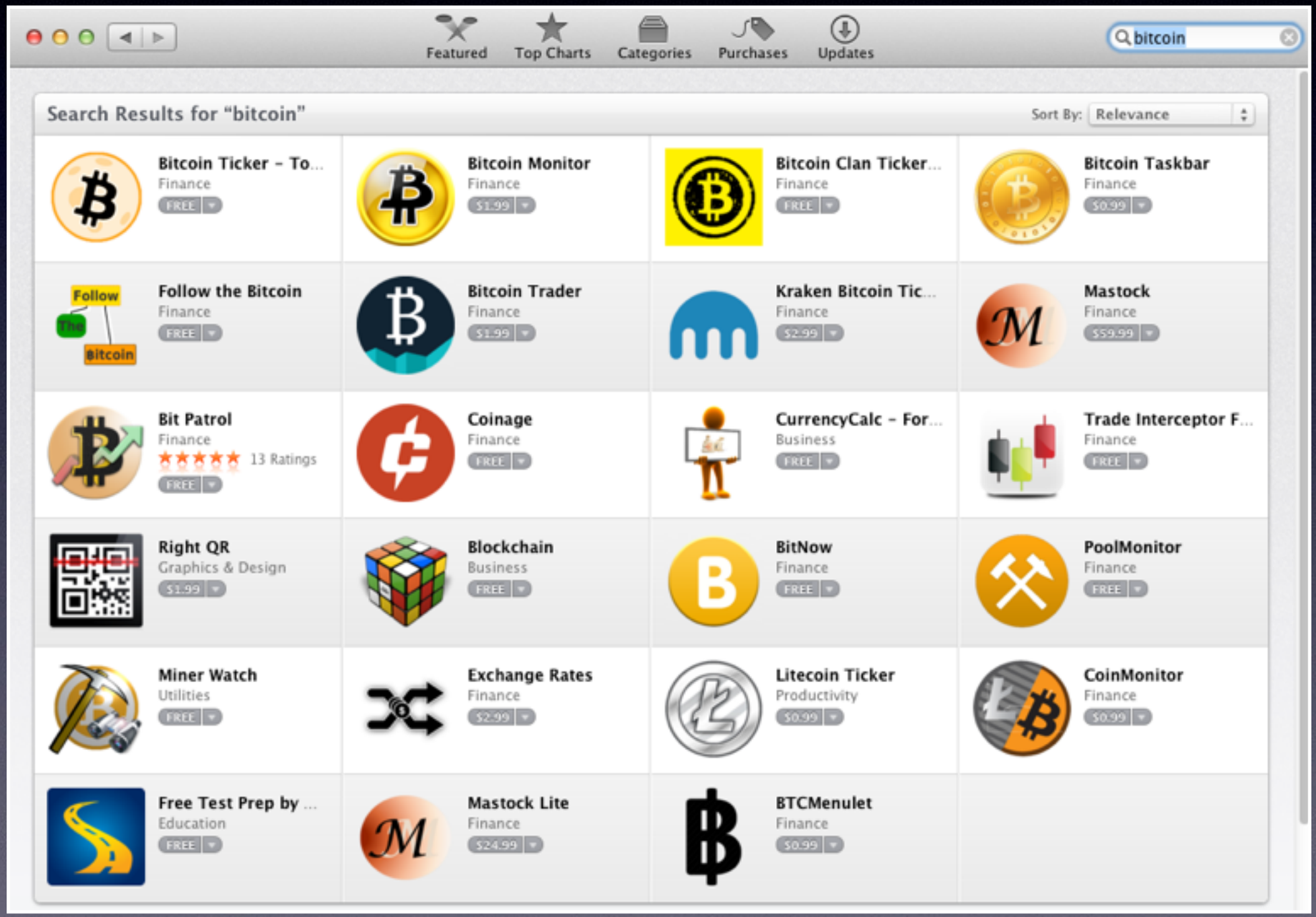
GAMING

satoshiDICE! · arbiter

INVESTORS

boost · union square ventures · WINKLEVOSS CAPITAL · ANDREESSEN HOROWITZ · FOUNDERS FUND · Google ventures · LIGHTSPEED VENTURE PARTNERS · TVP TRIBECA VENTURE PARTNERS · Ribbit Capital

Apple & Mac/iOS users must see something there…



First, a quick look at money…

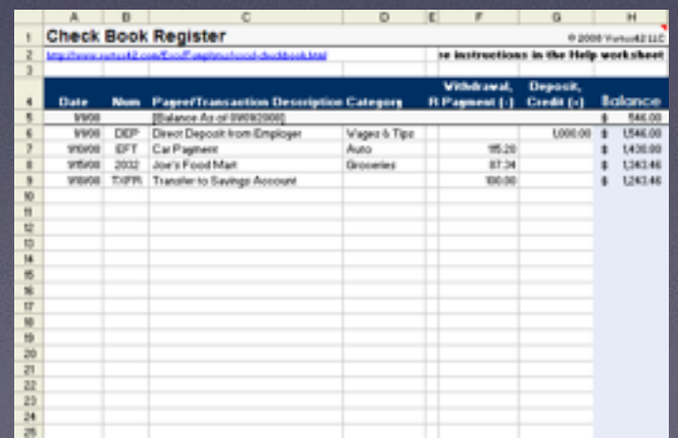
MacMania 17, Somewhere@Sea, June 2014

Token Money

- Represented by a physical object (token) such as a banknote, coin, traveler's check, etc.
- Without that token, the value is lost
- No intermediary is required for spending
- BUT - requires faith in the ISSUER, usually a government or a bank

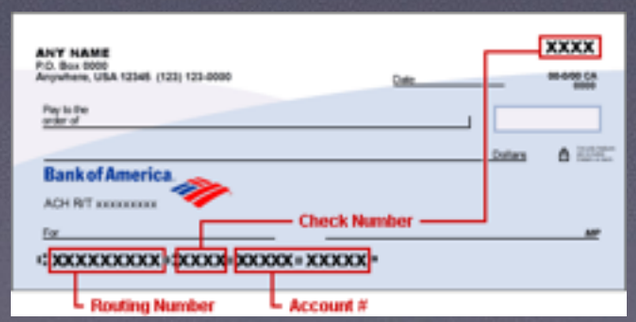
Notational Money

- Represented by a notation in a ledger, passbook or database (e.g., a bank account)
- Notational money cannot be lost
- BUT - requires an intermediary (bank or clearing house) for spending
- ALSO - requires faith in the MAINTAINER of the ledger



Hybrid Money

- Requires BOTH a token AND a ledger account (e.g., personal check, stored value or gift card)
- Can be lost AND requires faith in the ISSUER
- AND requires an intermediary (bank or clearing house) for spending



Virtual Money (?)

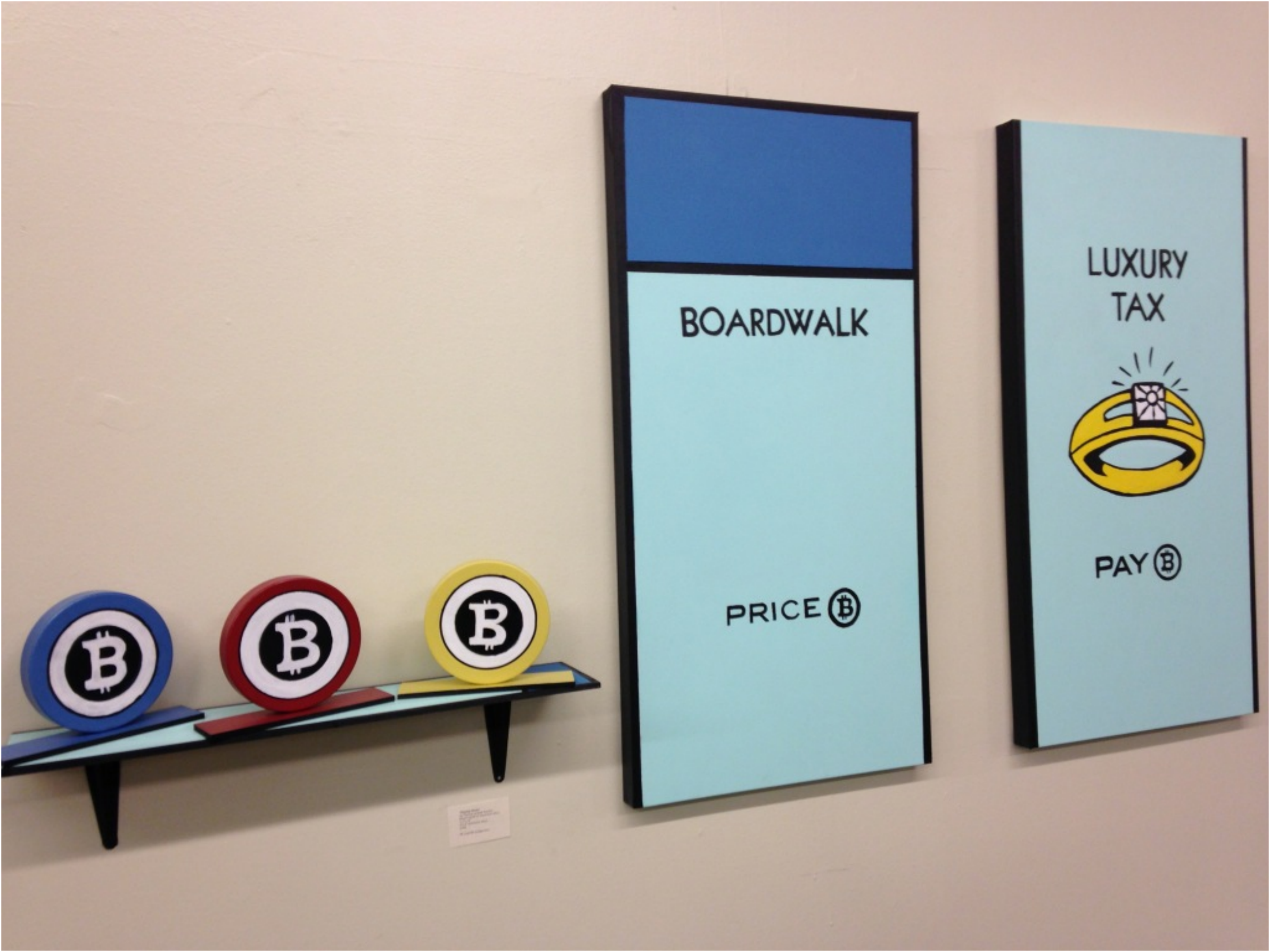
- No token
- No ledger
- No issuer, no government backing (or supervision)
- No intermediary required for spending

BUT

- Is this even possible?
- Who creates the money? Why is it money?
- Without a token or ledger, how do you know how much you have? What is its value?
- How do you know the spender is the owner?
- What prevents spending the same money twice?

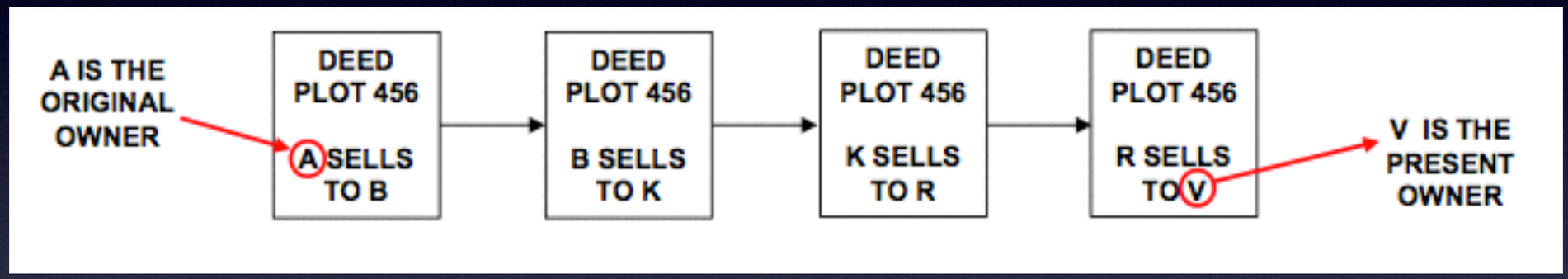
Another reason to backup…

- Your money is just a string of bytes (data) on your device
- Device failure means your money is gone
- Device intrusion means your money can be stolen


BOARDWALK
PRICE
LUXURY
TAX
PAY

Analogy: Real Estate

- Land ownership is defined by a "chain of title," a sequence of deeds leading from the original owner to the present owner

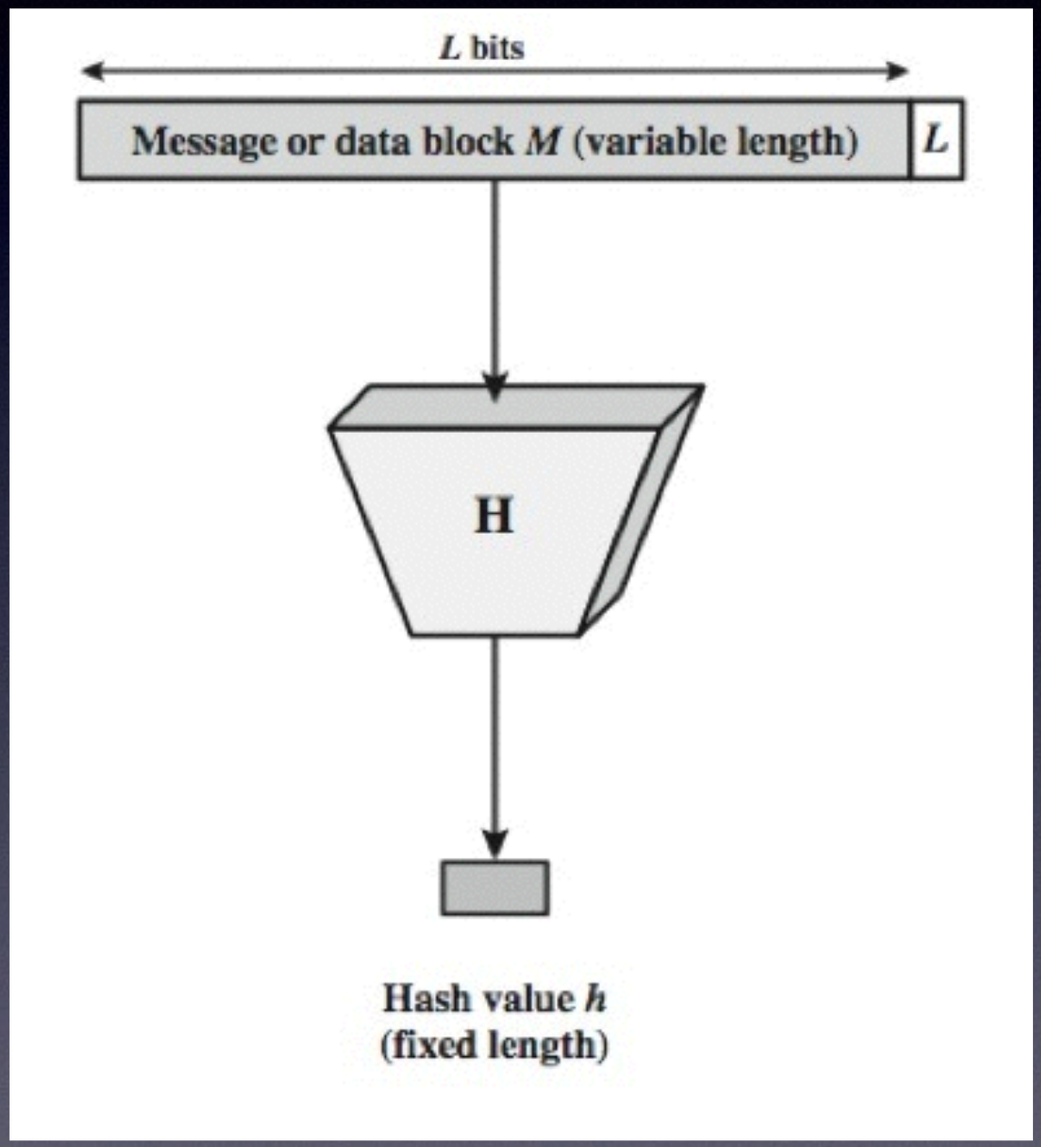


- Deeds are recorded in the Land Registry
- Ownership determined by searching the Registry
- The Land Registry is, in effect, a ledger holder
- If the Registry is altered, ownership can be lost
- Double-selling is prevented by timestamps

Distributed Registry

- Suppose we broadcast ALL deeds to thousands of nodes of a decentralized public network?
- IF the deeds are genuine AND the network members agree on the chain of title, THEN we can tell who owns a piece of property
- Ask the network and count the responses - if a majority say that someone is the owner, then they are
- There must be enough honest members that false responses cannot dominate (or they have some incentive)
- The registry is NOT under government control

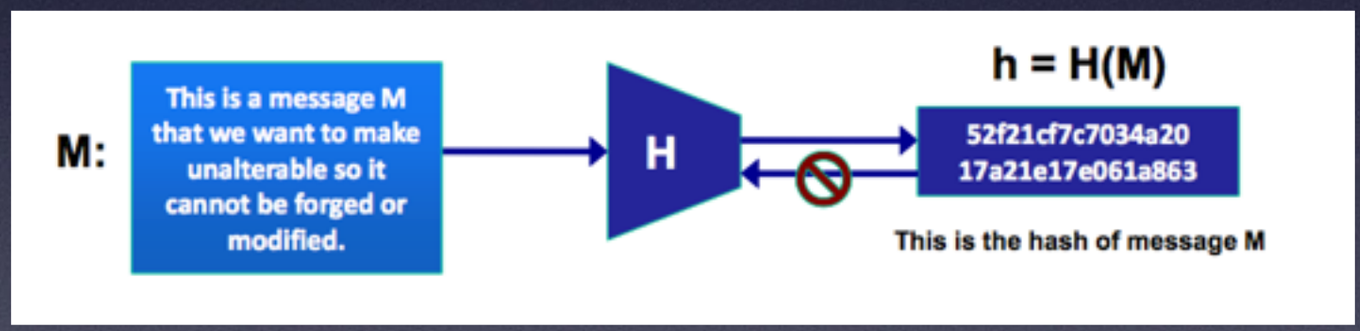
A Little Math - Hash Functions



- A "hash" is a short function of a message
- BUT: a hash is not uniquely reversible
- Many messages have the same hash
- Hash function H produces a fixed size hash of message M, usually 128-512 bits
- h = H(M)

One-Way Hash Functions

- Hashes are easy (fast) to compute but computationally difficult to invert
- Should not be able to find any message corresponding to a given hash



- Bitcoin uses a well-known published hash function SHA-256, which produces 256 bit hashes

A Little More Math/CS - Asymmetric Encryption

- Same as public-private key encryption
- Provides the security in PKI/certificates, HTTPS, secure e-mail, digital signatures, etc.
- Everyone has a public key (which they openly share) and a private key (which they protect) that are linked by very complex mathematics
- Insures end-to-end security, non-repudiation, etc.

What is Bitcoin Really?

- No physical object, not even a character string
- “A chain of digitally signed transaction records leading from the original owner to the current holder” - similar to a chain of land deeds
- The transaction records contain
  - Hashes that are difficult to find AND
  - Virtual owner IDs, called addresses
- There is NO bitcoin registry, NO centralization
- Bitcoin blockchains are broadcast to everyone; anyone can verify them

Bitcoin Protocol

- Bitcoin was invented in 2008 by an anonymous person or team named "Satoshi Nakamoto"
- The bitcoin protocol for generating and exchanging bitcoin is implemented in publicly available, open source software
- Anyone can obtain and run a bitcoin client

Bitcoin Addresses

- Bitcoin software generates bitcoin addresses of 25-44 characters for users
- Sample address: 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ
- The address is actually an elliptic curve public key; a 44 character key is as secure as a 7000-bit RSA key
- To send bitcoins, user specifies a receiving address and amount then clicks “send”
- To receive bitcoins, just tell the sender your address!
- Addresses are not registered to users. A user can have a different address for every transaction

WarpWallet

Passphrase [redacted]

Optional: your email [as a salt] bebo.white@gmail.com

Sanity check: I confirm bebo.white@gmail.com

Clear & reset

Public bitcoin address 1HDAQozS8z2FY999KjouuyBFXhPXuhPQ5f

Private key (don't share) [redacted]

Public address QR Code

Private key QR Code (Wallet Import Format)

What is WarpWallet?

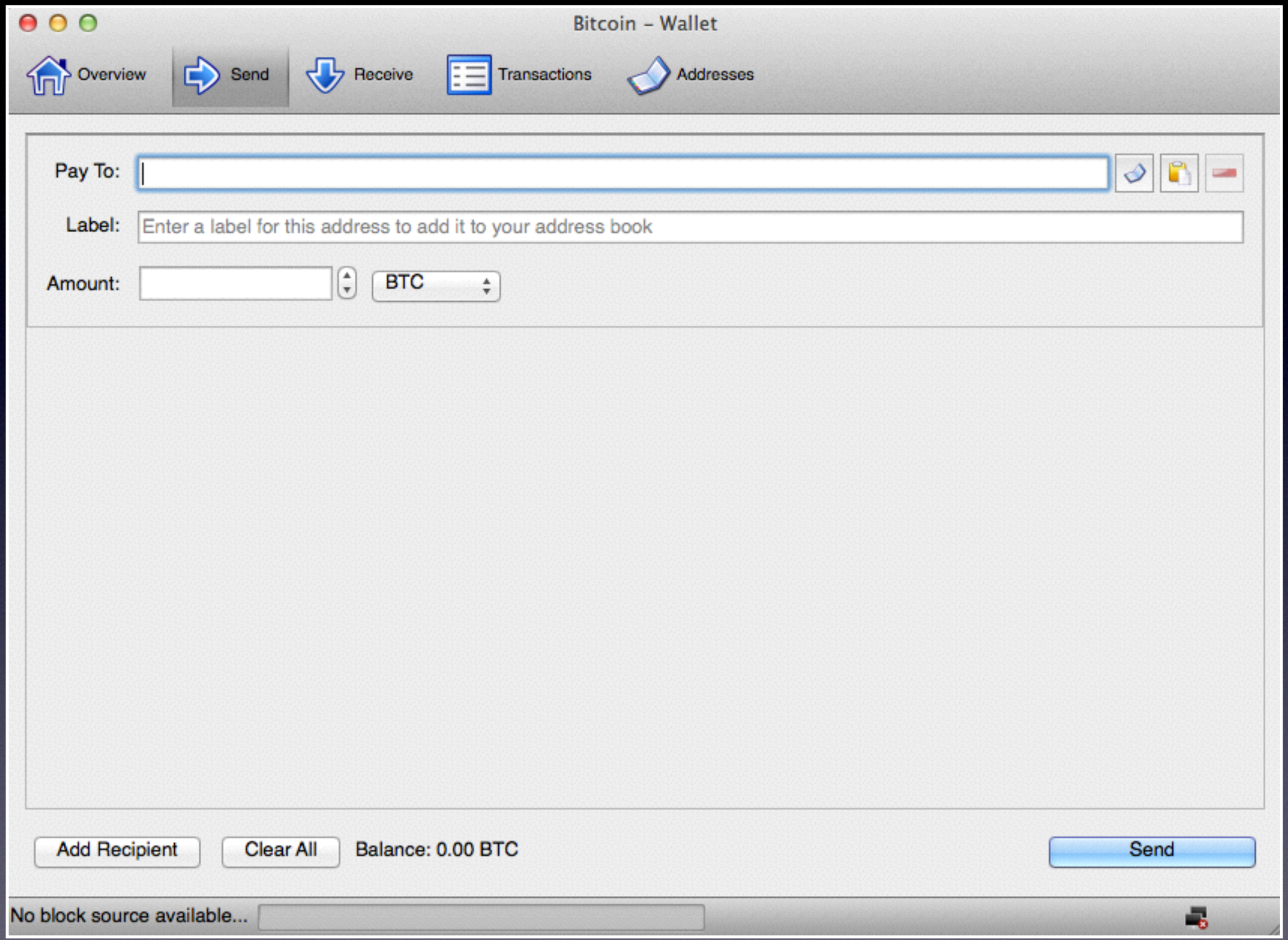
WarpWallet is a deterministic bitcoin address generator. You never have to save or store your private key anywhere. Just

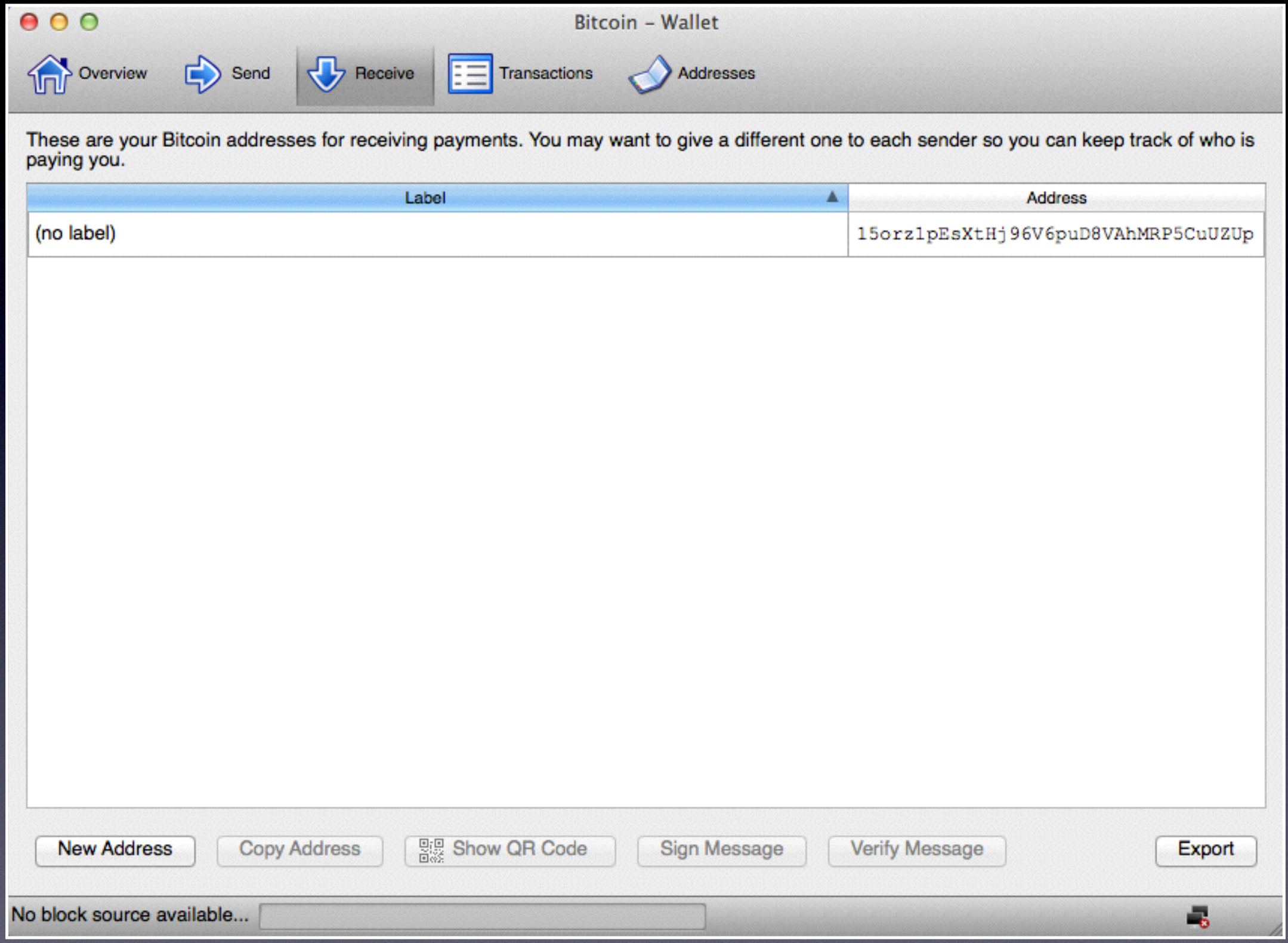
WarpWallet Challenge

The following challenges are designed to test the safety of WarpWallet, and scrypt in general. We expect the first 4 to fall quickly and hope to lose our bitcoins to nice

Authors

We are Max Krohn (https://twitter.com/maxtaco) and Chris Coyne (https://twitter.com/malgorithms), co-founders of OkCupid, SparkNotes, and


Bitcoin - Wallet
Overview
Send
Receive
Transactions
Addresses
Pay To:
Label:
Enter a label for this address to add it to your address book
Amount:
BTC
Add Recipient
Clear All
Balance: 0.00 BTC
Send
No block source available...


Bitcoin - Wallet
Overview
Send
Receive
Transactions
Addresses
These are your Bitcoin addresses for receiving payments. You may want to give a different one to each sender so you can keep track of who is paying you.
Label
Address
(no label)
15orz1pEsXtHj96V6puD8VAhMRP5CuUZUp
New Address
Copy Address
Show QR Code
Sign Message
Verify Message
Export
No block source available...

So if you want to tip me…

MacMania 17, Somewhere@Sea, June 2014

How do you get bitcoin?

- Sell something
- Salary (?)
- Use a bitcoin exchange (including bitcoin ATMs)

- Bitcoin mining

Bitcoin Mining (1/3)

- Bitcoin blockchain begins with data "mined" by using a large number of hash function computations
- "Mining" software is run on mining machines
- A "miner" tries many different (e.g., 10^15) numbers, trying to find one whose hash value is less than a given threshold (A); a "brute force" computation
- Verified success is rewarded with a number of bitcoins (N)

Bitcoin Mining (2/3)

x = blockchain
y= proposed added block
n = additional number
A = threshold value
N = miner's reward

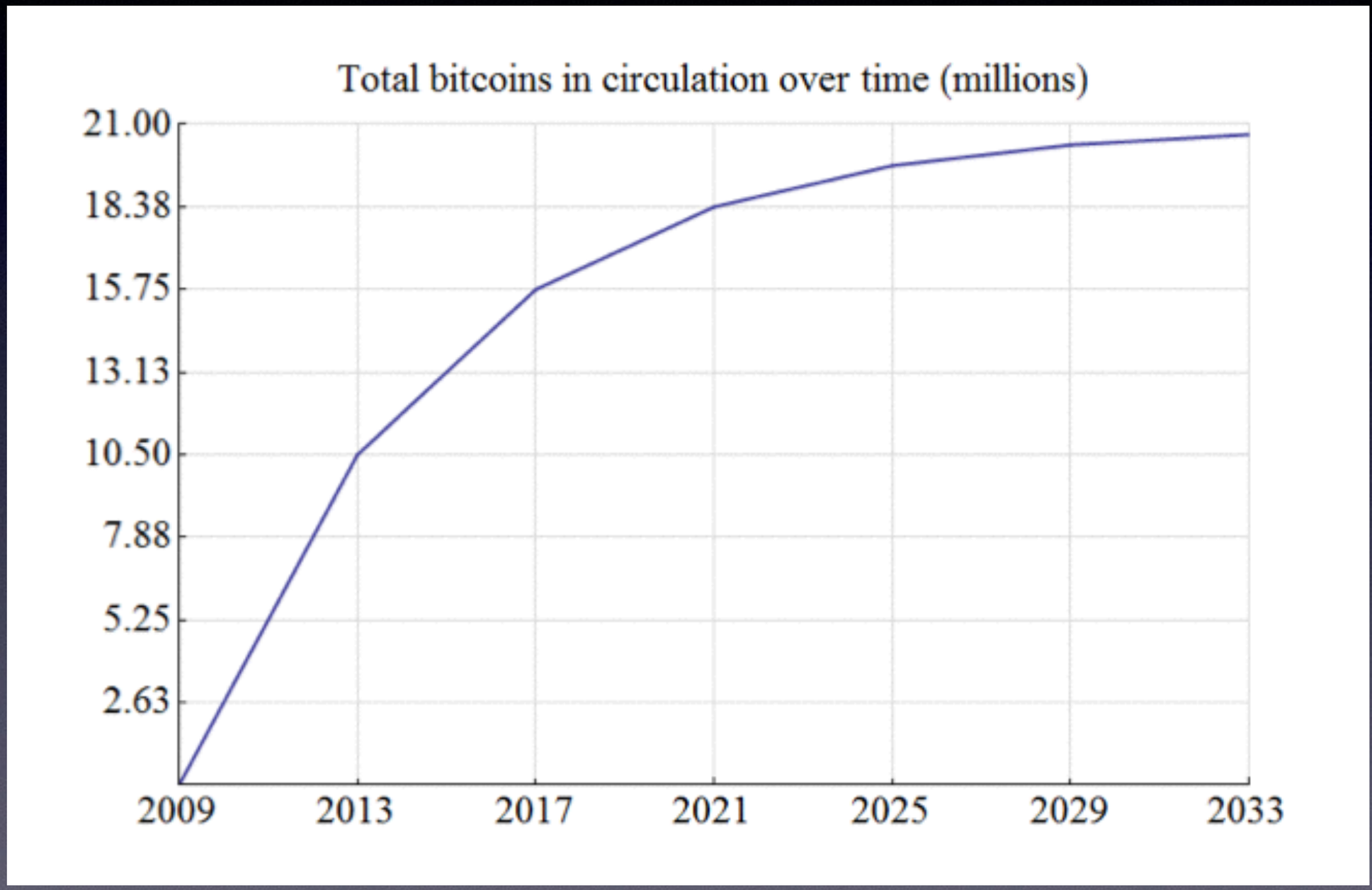
find n such that:
H(x,y,n) < A

Miner includes N BTC in "y" for themselves

Miner broadcasts solution to network for verification

N began at 50 and is halved every 210,000 blocks

Controlled Bitcoin Inflation



Bitcoin Mining (3/3)

- The threshold (A) adjusted every 2 weeks (to establish rate of 6 blocks/hour)
- Therefore, bitcoin hashes are progressively more difficult to find (i.e., finding "n" more difficult); part of finding "n" involves verifying that no bitcoin transacted in block "y" has already been spent in blockchain "x"
- There will never be more than 21 million BTC. (2*50*210,000); divisible into units as small as 1/100 millionth of a BTC

Exchange: BitStamp (USD)

Exchange: BitStamp (USD)

The New York Times By NATHANIEL POPPER and RACHEL ABRAMS FEB. 25, 2014

Apparent Theft at Mt. Gox Shakes Bitcoin World

The most prominent Bitcoin exchange appeared to be on the verge of collapse late Monday, raising questions about the future of a volatile marketplace.

On Monday night, a number of leading Bitcoin companies jointly announced that Mt. Gox, the largest exchange for most of Bitcoin's existence, was planning to file for bankruptcy after months of technological problems and what appeared to have been a major theft. A document circulating widely in the Bitcoin world said the company had lost 744,000 Bitcoins in a theft that had gone unnoticed for years. That would be about 6 percent of the 12.4 million Bitcoins in circulation.

While Mt. Gox did not respond to numerous requests for comments, and the companies issuing the statement scrambled to determine the exact situation at Mt. Gox, which is based in Japan, the news helped push the price of a single Bitcoin below $500 for the first time since November, when it began a spike that took it above $1,200.

Forbes

Alex Berezow, (http://www.forbes.com/sites/alexberezow/) Contributor

I write about science, science policy and a dash of European affairs.

FOLLOW

OP/ED (/OPINIONS) 12/24/2013 @ 8:31AM | 5,665 views

Bitcoin Meets Google Trends and Wikipedia

Comment Now Follow Comments

Bitcoin, the digital currency *du jour*, is a bit of an economic curiosity. Unlike gold, it has no intrinsic value. Unlike a currency issued by a country, its price is not affected by GDP, inflation, interest rates or any other typical macroeconomic indicator. So what gives Bitcoin value, and what is behind its incredible price volatility? Supply and demand. And since supply is already predetermined by an algorithm, demand is the biggest factor driving both its value and volatility.

Thus, understanding Bitcoin demand is central to analyzing the currency. But how exactly do you measure demand? Economist Ladislav Krištoufek from Charles University in Prague thinks he has an answer: Use Google (/companies/google/) GOOG +1.61% (/companies/google/) Trends and Wikipedia to determine how many times people search for the term "Bitcoin."

Plotting Internet searches against the value of Bitcoin, Dr. Krištoufek found a strong correlation between the two. (See figure.)

(http://b-

Is this really different from stock market, currency market, commodities market fluctuations?

MacMania 17, Somewhere@Sea, June 2014

S**t happens - Mt. Gox vs. Bernie Madoff

Willie Sutton would use bitcoin

MacMania 17, Somewhere@Sea, June 2014

Possible Vulnerabilities

- No way to reverse a transaction without the payee's cooperation
- Software bugs
- Bank robbery by hackers (e.g., Mt. Gox)
- Malware attacks against wallets
- Government attempts to control
  - Silk Road raided by FBI in October 2013
- Competing digital currencies easy to make (forks) - Auroracoin, Dogecoin, Namecoin, Primecoin, and others - imitation is flattery

The Willy Report

The Willy Report: proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin

Posted on May 25, 2014

Somewhere in December 2013, a number of traders including myself began noticing suspicious bot behavior on Mt. Gox. Basically, a random number between 10 and 20 bitcoin would be bought every 5-10 minutes, non-stop, for at least a month on end until the end of January. The bot was dubbed "Willy" at some point, which is the name I'll continue to use here. Since Willy was buying in such a recognizable pattern, I figured it would be easy to find in the Mt. Gox trading logs that were leaked about two months ago (there's a torrent of the data here). However, the logs only went as far as November 2013; luckily, I was able to detect the buying pattern in the last few days of November. Below is a compiled log of its trades on the last two days of November (from the file "2013-11_mtgox_japan.csv"):

```
29-11-2013 0:38 - UID: 817985 Type: buy Currency: USD BTC: 10.02069695 Fiat: 11011.54
29-11-2013 0:47 - UID: 817985 Type: buy Currency: USD BTC: 16.80501168 Fiat: 18256.07
29-11-2013 0:56 - UID: 817985 Type: buy Currency: USD BTC: 13.46333525 Fiat: 15078.58
29-11-2013 1:01 - UID: 817985 Type: buy Currency: USD BTC: 14.60390798 Fiat: 16324.46
29-11-2013 1:10 - UID: 817985 Type: buy Currency: USD BTC: 18.89383201 Fiat: 21909.61
29-11-2013 1:15 - UID: 817985 Type: buy Currency: USD BTC: 12.63500728 Fiat: 14339.39
29-11-2013 1:21 - UID: 817985 Type: buy Currency: USD BTC: 15.36861265 Fiat: 17395.3
29-11-2013 1:30 - UID: 817985 Type: buy Currency: USD BTC: 13.69985504 Fiat: 15469.14
29-11-2013 1:40 - UID: 817985 Type: buy Currency: USD BTC: 16.24860284 Fiat: 18411.35
29-11-2013 1:46 - UID: 817985 Type: buy Currency: USD BTC: 13.08811052 Fiat: 14901.38
29-11-2013 1:53 - UID: 817985 Type: buy Currency: USD BTC: 15.95674773 Fiat: 18116.97
29-11-2013 2:01 - UID: 817985 Type: buy Currency: USD BTC: 13.37224115 Fiat: 15224.97
29-11-2013 2:10 - UID: 817985 Type: buy Currency: USD BTC: 19.88618992 Fiat: 22699.37
29-11-2013 2:16 - UID: 817985 Type: buy Currency: USD BTC: 14.53897264 Fiat: 17228.68
29-11-2013 2:24 - UID: 817985 Type: buy Currency: USD BTC: 13.06074749 Fiat: 15496.65
29-11-2013 2:31 - UID: 817985 Type: buy Currency: USD BTC: 17.2701824 Fiat: 20845.52
29-11-2013 2:40 - UID: 817985 Type: buy Currency: USD BTC: 12.01285719 Fiat: 14394.19
```

Possible Future of Bitcoin/ Virtual Currencies (Social)

- For the world's unbanked, there is no choice
- For small businesses, freelancers and startups in developing nations, there is no choice
- When you have choice, it is hard to imagine those without
- New generation growing up with instant expectations, who are or will be disillusioned by huge economic bailouts
- From stones to precious metals to paper to bytes

Possible Future of Bitcoin/Virtual Currencies (Economic/Political)

- A future with digital currencies and decentralized stores is guaranteed - people trust math over people
- National adoption of decentralized currencies would bring political transparency and economic neutrality
- Developing nations seeking to curb corruption and break free of economic dependence on other countries could see potential in these technologies

Summary - the 5 Pillars of Bitcoin

- Currency - send units of value, convertible, divisible
- Commodity - scarcity stores wealth, market fluctuates with speculation
- Brand - marketing message, community and sharing knowledge
- Protocol - decentralized trust on the block chain
- Technology - services and solutions implemented and integrated

I own bitcoin - why not you?

MacMania 17, Somewhere@Sea, June 2014

Thank You!
Questions? Comments?
Want slide copies?

bebo@slac.stanford.edu

MacMania 17, Somewhere@Sea, June 2014