RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

The complete

Bitcoin Thief Tutorial

SESSION ID: HTA-R02

Uri Rivner
Head of Cyber Strategy
BioCatch

Etay Maor
PMM Cyber
Trusteer, an IBM Company

The first few things you should know about Bitcoin…

Most people think of Bitcoin in terms of a crazy digital currency whose dollar value has been soaring in recent months.

The only question they have is: should I buy some?

Let me show you a totally different perspective.

The first few things you should know about Bitcoin…

Bitcoin is a **payment scheme** for transferring money:

- To **anyone in the world**
- In their **own currency**
- **Instantly**
- with virtually **no commission**.

Example: a $50 money transfer to my pal in Hong Kong

The first few things you should know about Bitcoin…

Using Paypal : Owning Paypal

=

Using Bitcoin : Owning Bitcoin

$20

$1000

The first few things you should know about Bitcoin…

Bitcoin works exactly the same whether it's worth like this:

Or like this:

Bar of Gold

Bar of Soap

*You don't trade in Bitcoins. You trade in **bits** of Bitcoin. Minimal trade value = Satoshi = 0.00000001 Bitcoin*

Remind me…
What *is* Bitcoin?

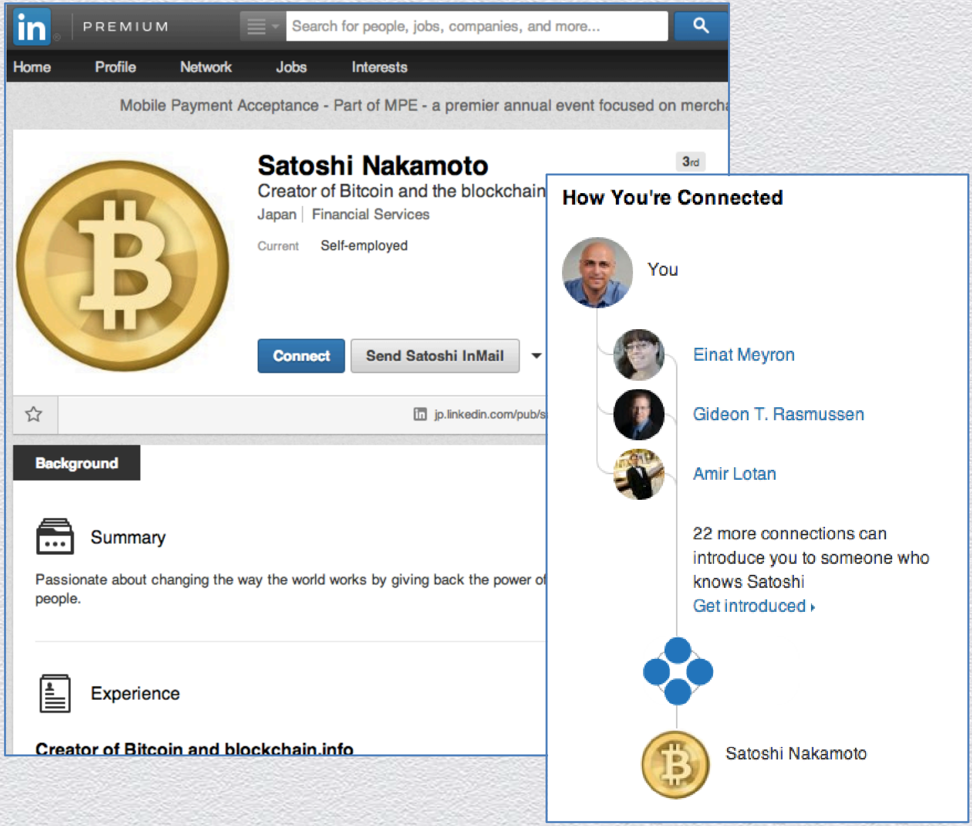
Crypto Currency

Vires in Numeris

12m / 21m

Cryptography Mailing List, 2008

Satoshi Nakamoto



Mobile Payment Acceptance - Part of MPE - a premier annual event focused on mercha

Satoshi Nakamoto

3rd

Creator of Bitcoin and the blockchain

Japan | Financial Services

Current Self-employed

Summary

Passionate about changing the way the world works by giving back the power of people.

Experience

Creator of Bitcoin and blockchain.info

How You're Connected

You

Einat Meyron

Gideon T. Rasmussen

Amir Lotan

22 more connections can introduce you to someone who knows Satoshi

Get introduced ▸

Satoshi Nakamoto

Owning a Bitcoin

A bitcoin is just a string of zeroes and ones. So, to steal a Bitcoin, all you need is just to copy them.

Hah! You fell for that one, didn’t you?

The ownership and trade of Bitcoin is one of the most amazing aspects about the protocol. The more you learn about how it’s done, the more you’d think it’s beautiful. As a fraudster you might not care about that, but you should definitely understand the principal of ownership and trade. And no, don’t look for strings of zeroes and ones that you can copy. It’s a bit more complicated than that. Don’t worry, you CAN steal Bitcoins, but it’s not a simple matter of copy and paste.

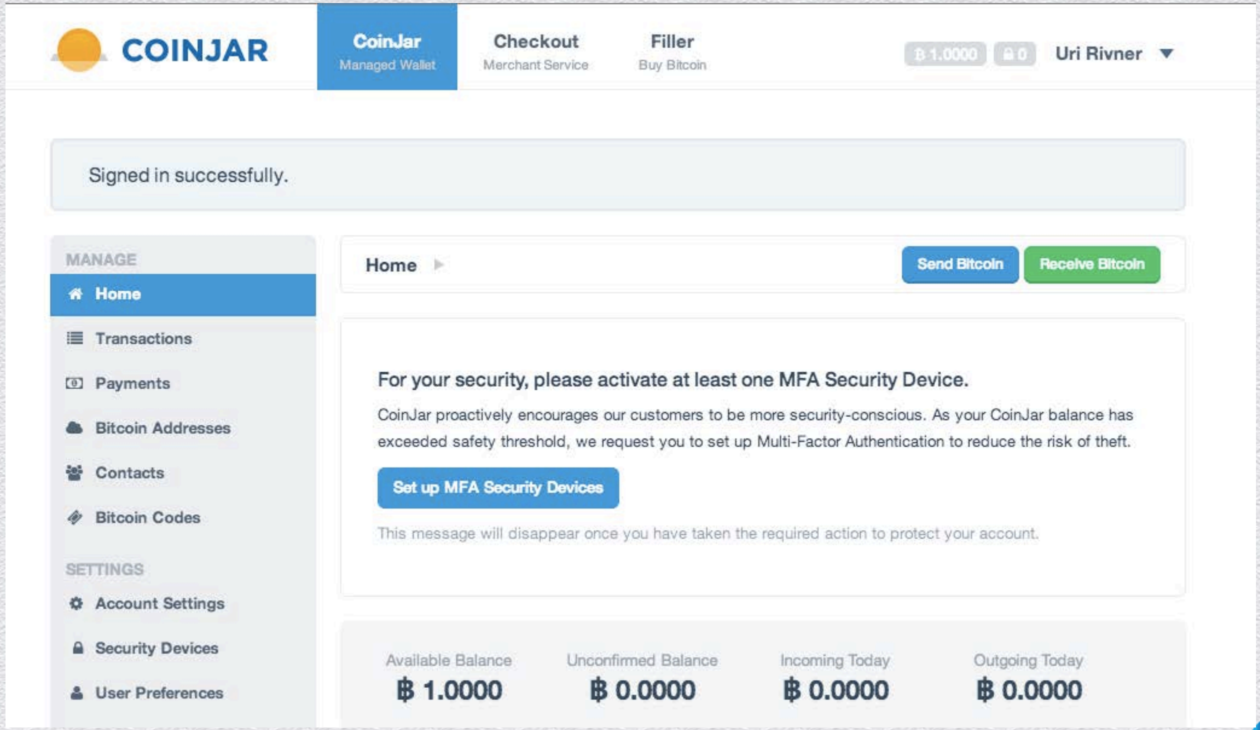
Step #1: Get a Wallet. It’s free!

In order to own bitcoins, you need a wallet. You have two choices: either

- **Download a Bitcoin wallet** (might take you a while; currently the download is around 15 GB). Or,
- Subscribe to an **eWallet service**.

Once you have a wallet, you also get your Bitcoin address. It’s free and you can get multiple ones. Here’s mine:
1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG
Essentially it’s your public key.
You don’t have to hide it. The private keys – hell ya!

Lets see a Wallet in action



Signed in successfully.

For your security, please activate at least one MFA Security Device.

CoinJar proactively encourages our customers to be more security-conscious. As your CoinJar balance has exceeded safety threshold, we request you to set up Multi-Factor Authentication to reduce the risk of theft.

Set up MFA Security Devices

This message will disappear once you have taken the required action to protect your account.

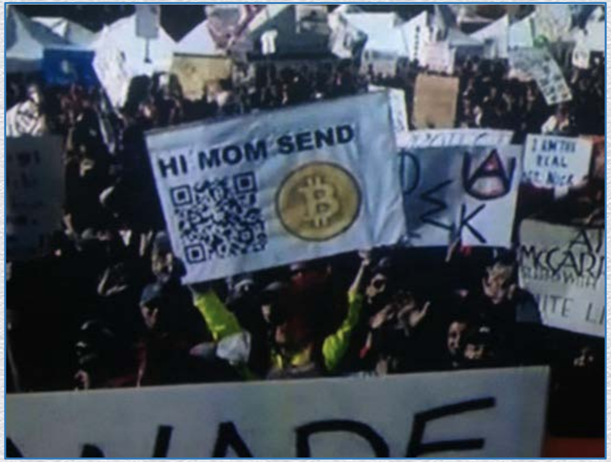
Available Balance	Unconfirmed Balance	Incoming Today	Outgoing Today
฿ 1.0000	฿ 0.0000	฿ 0.0000	฿ 0.0000

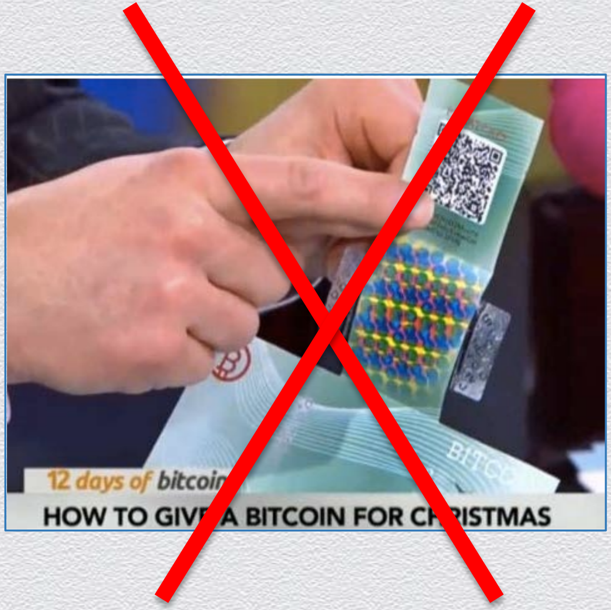
Step #2: Getting Bitcoins!

What’s the best way to fill your wallet with Bitcoins?

A. Directly buy Bitcoins from another user
B. Use a local or global Bitcoin exchange
C. Mine bitcoins (more on this later)
D. Steal some bitcoins!

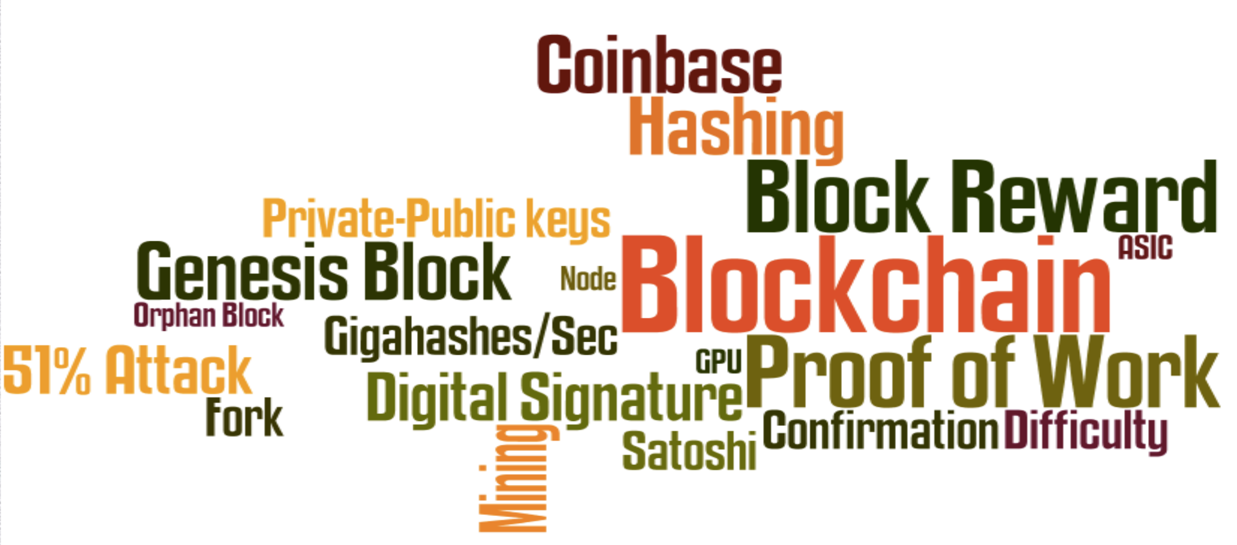
Careful with that QR Code!!





OK – I now own Bitcoins. How can I *transact*?

Ah. Transacting in Bitcoin is the most fascinating aspect of the crypto currency. There are SO many moving parts!



Validation is Key (pun intended)

The Bitcoin protocol makes sure that when I send you any Bitcoins, they really were in my possession – i.e. my digital wallet – to begin with, and that I haven't spent them already. Otherwise I can send the same Bitcoin to several people, and get away with it.

Had Bitcoin been a stock…

But it's not. So - Who validates Bitcoin transactions?

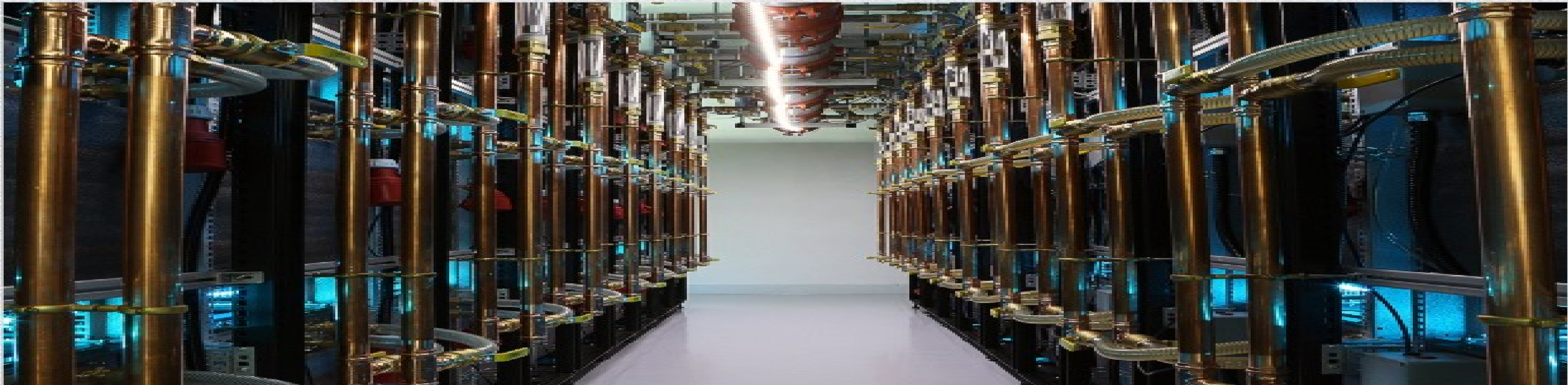
- The Secret Bitcoin Society (Nobel Laureates? Famous cryptographers? The Pope?)
- We all are (and that's the beauty of it)

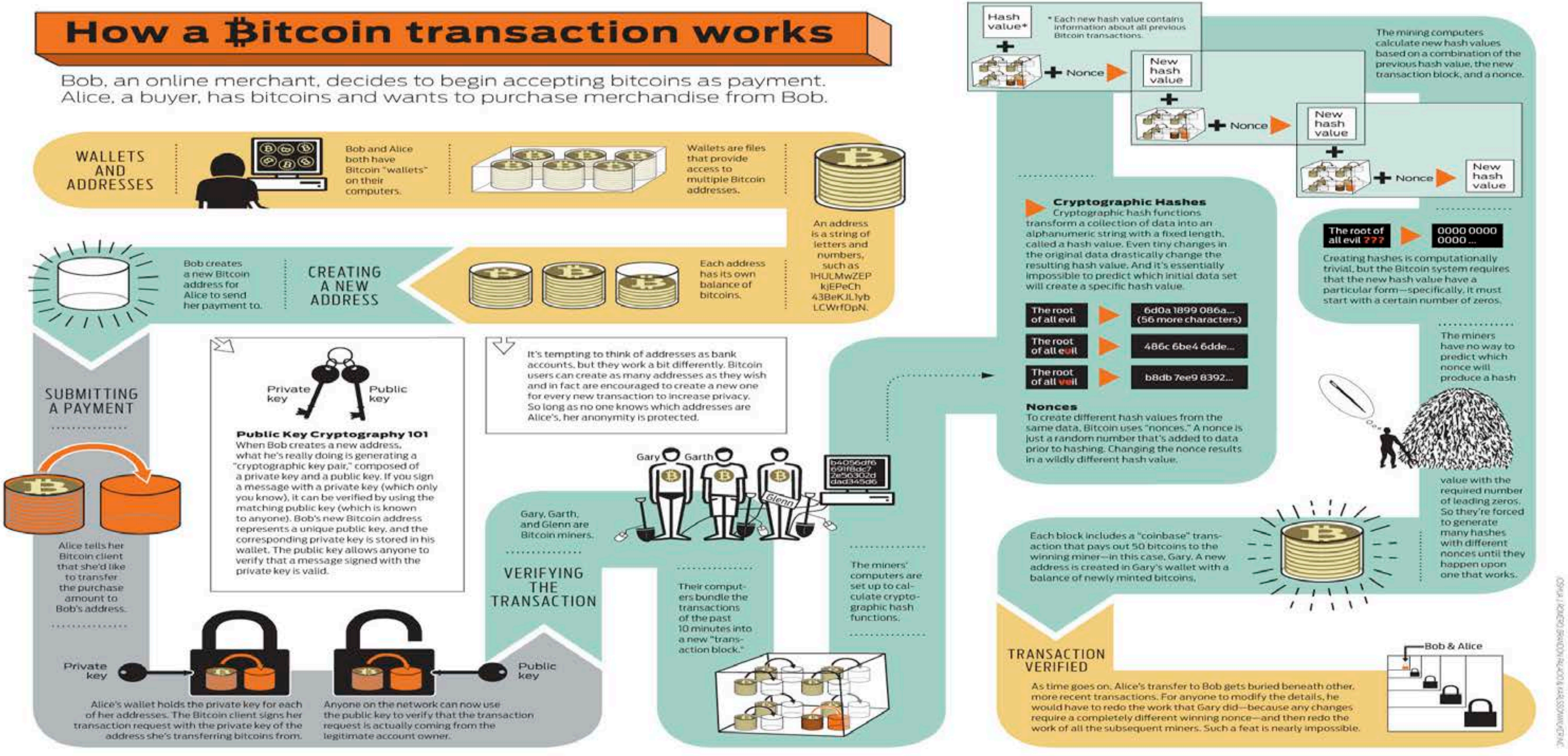
Validation by the Masses

Based on Proof of Work principal:

- Make it difficult, but –
- Reward those who go through the trouble

There's another name for it. Bitcoin Mining.





How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfOpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Private key

Public key

Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

Private key

Public key

Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

The miners' computers are set up to calculate cryptographic hash functions.

Hash value*

* Each new hash value contains information about all previous Bitcoin transactions.

The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all euil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

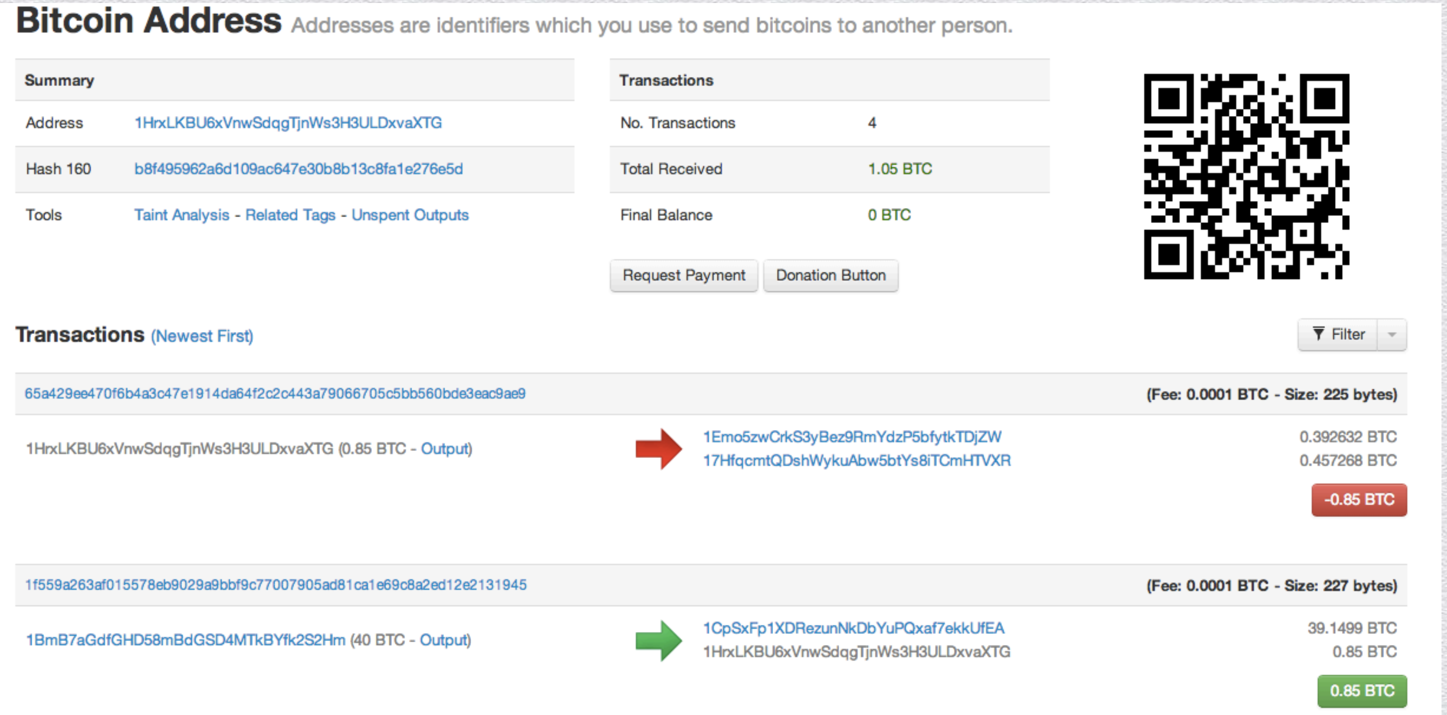
Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

This is an abstract. For advanced users who want a clear, easy to follow article on the subject, search for **"how-the-bitcoin-protocol-actually-works" by Michael Neilsen**

Follow the yellow brick blockchain



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG
Hash 160	b8f495962a6d109ac647e30b8b13c8fa1e276e5d
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	4
Total Received	1.05 BTC
Final Balance	0 BTC

Transactions (Newest First)

65a429ee470f6b4a3c47e1914da64f2c2c443a79066705c5bb560bde3eac9ae9 **(Fee: 0.0001 BTC - Size: 225 bytes)**

1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG (0.85 BTC - Output) → 1Emo5zwCrkS3yBez9RmYdzP5bfytkTDjZW 0.392632 BTC
17HfqcmtQDshWykuAbw5btYs8iTCmHTVXR 0.457268 BTC

-0.85 BTC

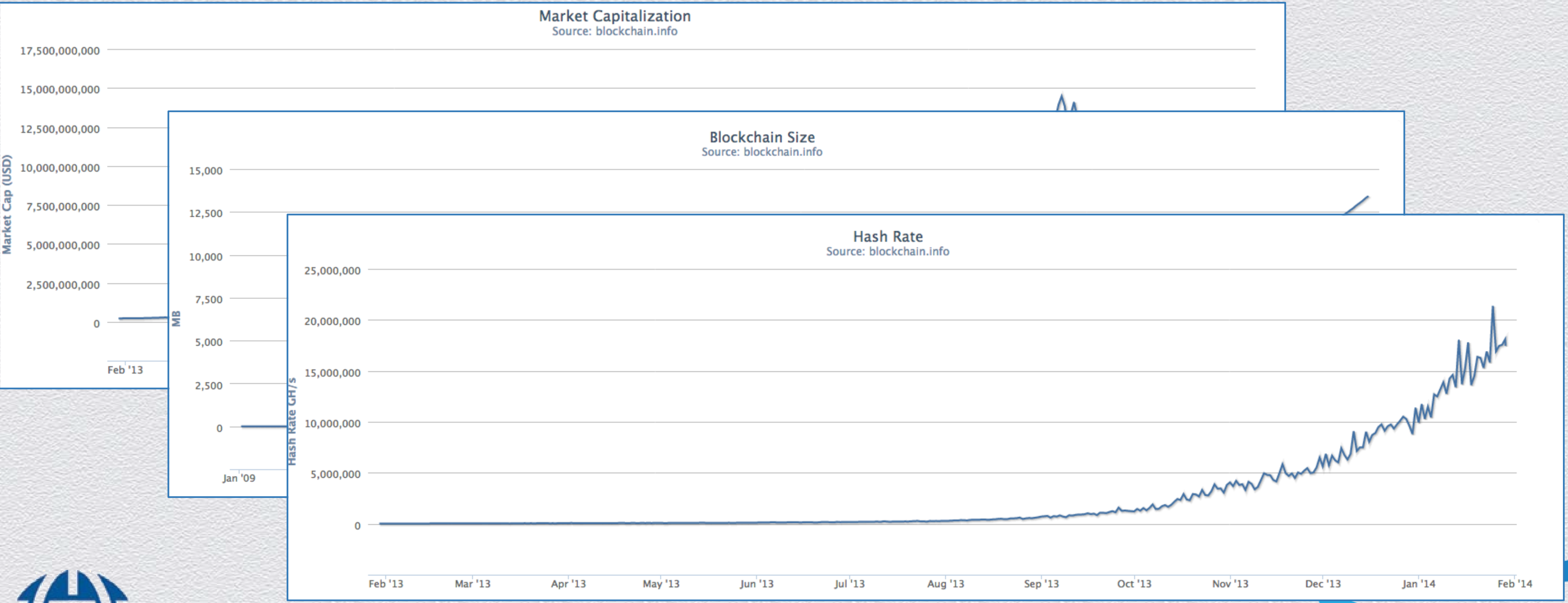
1f559a263af015578eb9029a9bbf9c77007905ad81ca1e69c8a2ed12e2131945 **(Fee: 0.0001 BTC - Size: 227 bytes)**

1BmB7aGdfGHD58mBdGSD4MTkBYfk2S2Hm (40 BTC - Output) → 1CpSxFp1XDRezunNkDbYuPQxaf7ekkUfEA 39.1499 BTC
1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG 0.85 BTC

0.85 BTC

1HrxLKBU6xVnwSdqgTjnWs3H3ULDxvaXTG

Bitcoin Charts



Market Capitalization
Source: blockchain.info

Blockchain Size
Source: blockchain.info

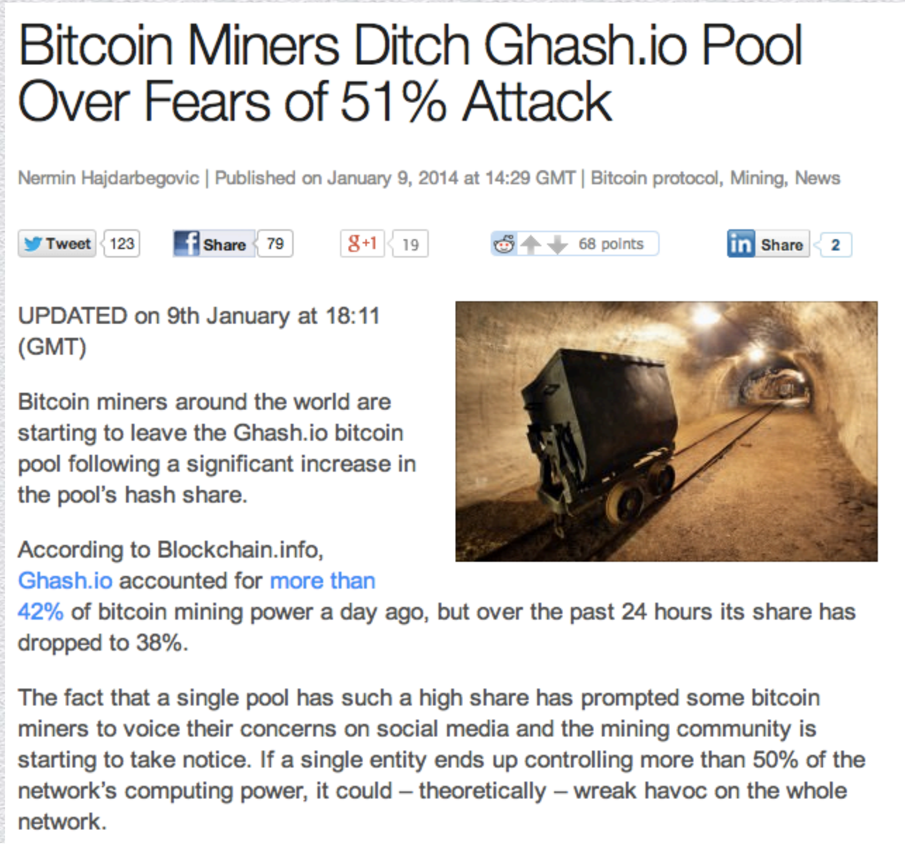
Hash Rate
Source: blockchain.info

Bitcoin: Top B2C Opportunities

- Trojan trigger lists – with popular Bitcoin exchanges
- Phishing for Bitcoin credentials
- RATs for direct wallet access
- Rogue Bitcoin apps
- Using botnets to mine bitcoin: small change…
  - Regular PC with i5 core: 10 MH/S
  - Mid-sized botnet: 5,000 PCs => 50 GH/S => $280/month

Bitcoin: Top B2B Opportunities

- Bitcoin exchanges: sitting ducks!
- Bitcoin mining operations!!
- 51% Attack!!!
- NSA!!!!



Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack

Nermin Hajdarbegovic | Published on January 9, 2014 at 14:29 GMT | Bitcoin protocol, Mining, News

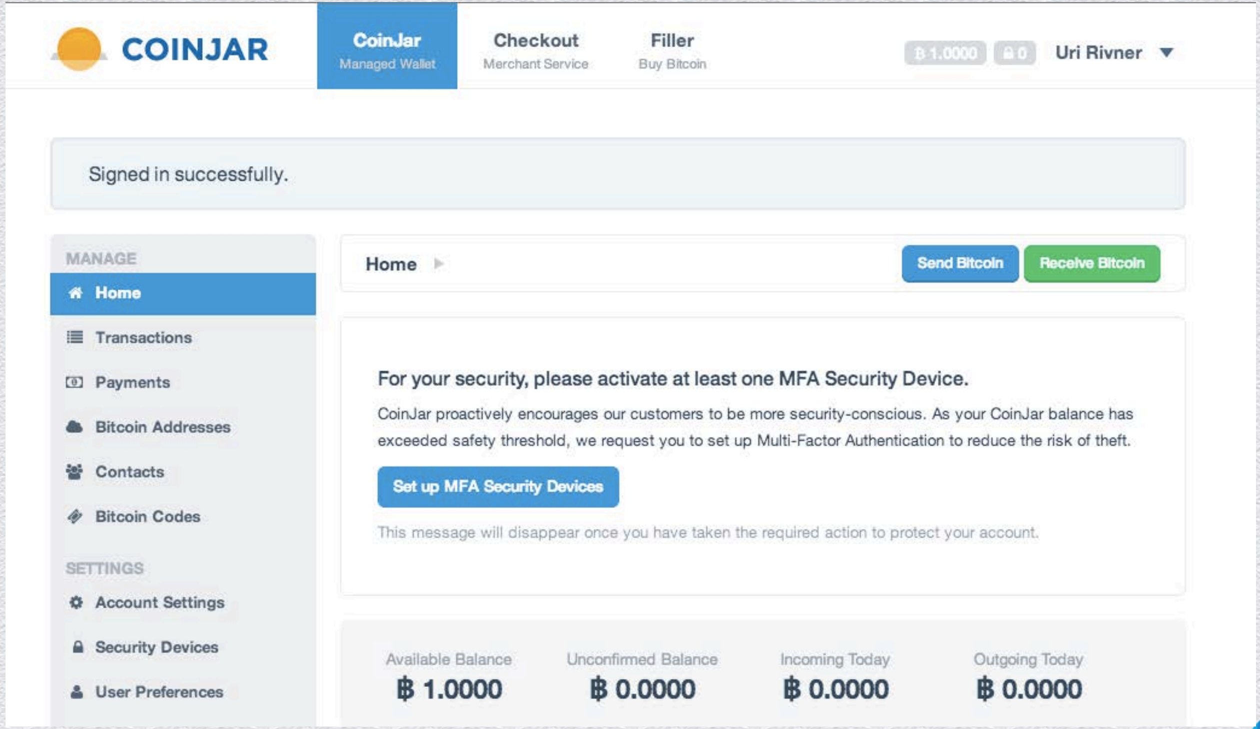
UPDATED on 9th January at 18:11 (GMT)

Bitcoin miners around the world are starting to leave the Ghash.io bitcoin pool following a significant increase in the pool's hash share.

According to Blockchain.info, Ghash.io accounted for more than 42% of bitcoin mining power a day ago, but over the past 24 hours its share has dropped to 38%.

The fact that a single pool has such a high share has prompted some bitcoin miners to voice their concerns on social media and the mining community is starting to take notice. If a single entity ends up controlling more than 50% of the network's computing power, it could – theoretically – wreak havoc on the whole network.

A few more interesting things



Signed in successfully.

For your security, please activate at least one MFA Security Device.

CoinJar proactively encourages our customers to be more security-conscious. As your CoinJar balance has exceeded safety threshold, we request you to set up Multi-Factor Authentication to reduce the risk of theft.

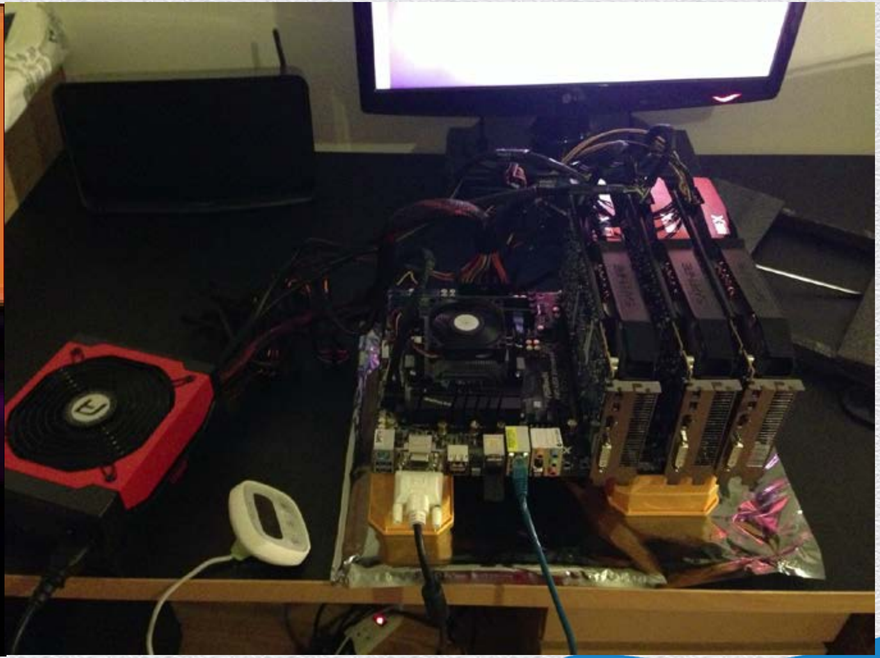
This message will disappear once you have taken the required action to protect your account.

Available Balance	Unconfirmed Balance	Incoming Today	Outgoing Today
฿ 1.0000	฿ 0.0000	฿ 0.0000	฿ 0.0000

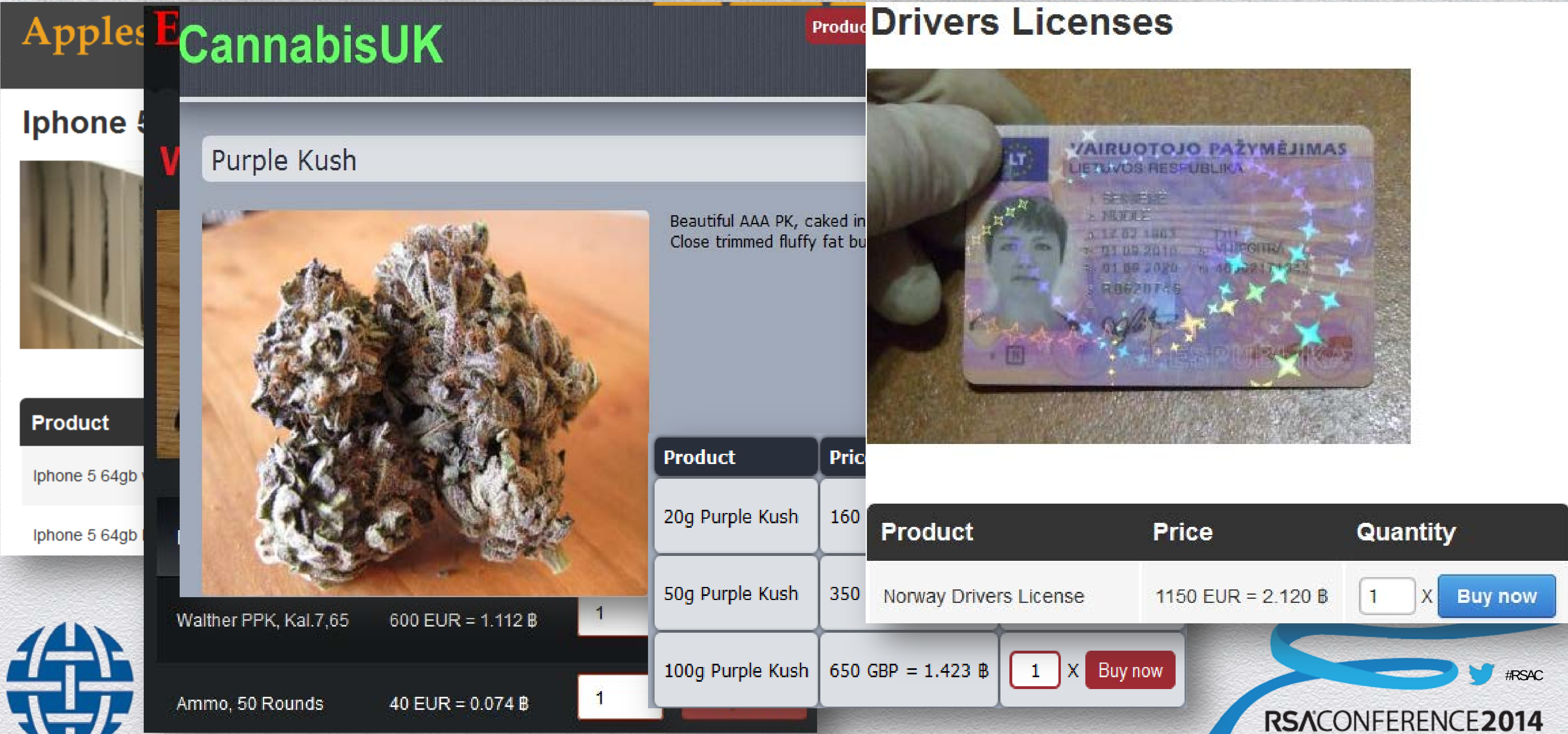
The Cybercriminal’s Dilemma

A Target?

An infrastructure and facilitator?



Facilitator for Shady Deals



Apples

Iphone 5

Product
Iphone 5 64gb
Iphone 5 64gb

Walther PPK, Kal.7,65	600 EUR = 1.112 ฿	1
Ammo, 50 Rounds	40 EUR = 0.074 ฿	1

CannabisUK

Purple Kush

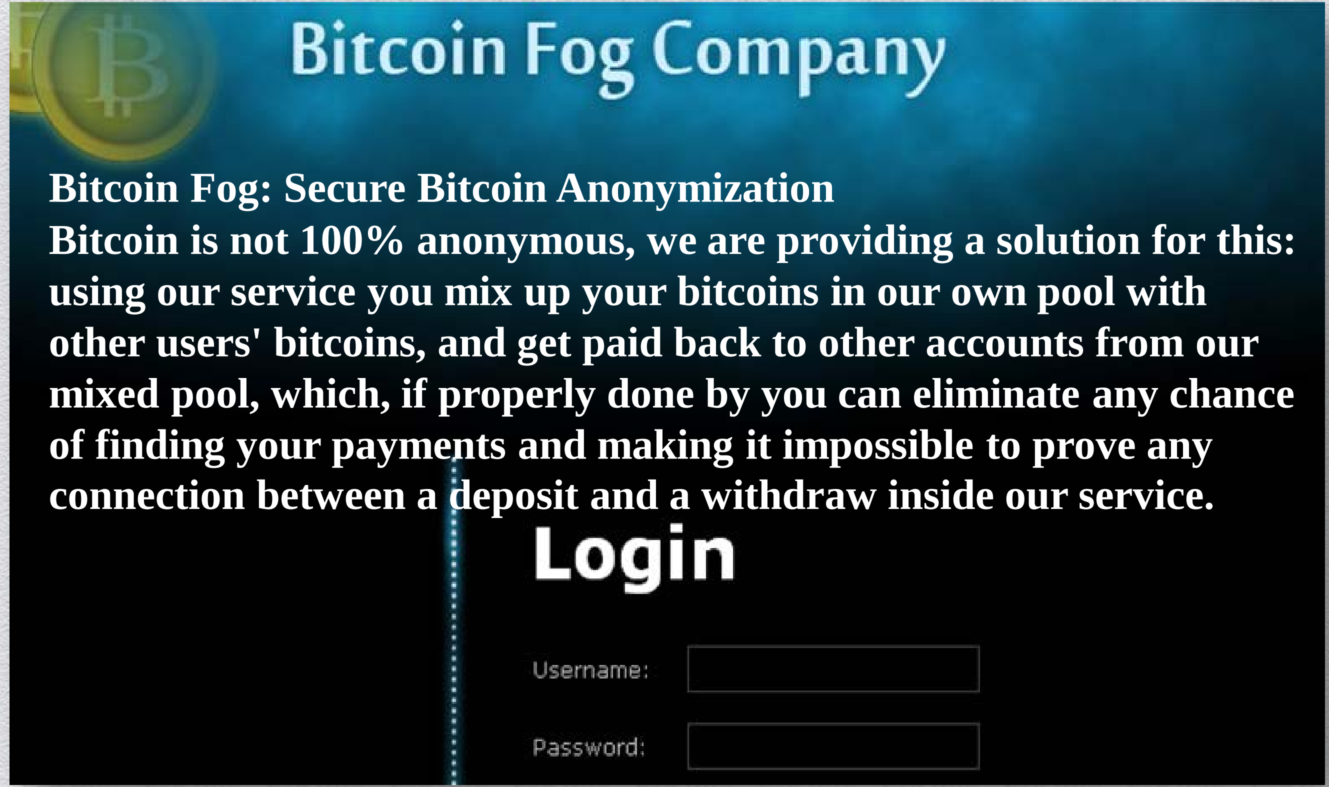
Beautiful AAA PK, caked in
Close trimmed fluffy fat bu

Product	Pric		
20g Purple Kush	160		
50g Purple Kush	350		
100g Purple Kush	650 GBP = 1.423 ฿	1 X	Buy now

Drivers Licenses

Product	Price	Quantity	
Norway Drivers License	1150 EUR = 2.120 ฿	1 X	Buy now

Is Bitcoin Truly Anonymous?



Bitcoin Fog Company

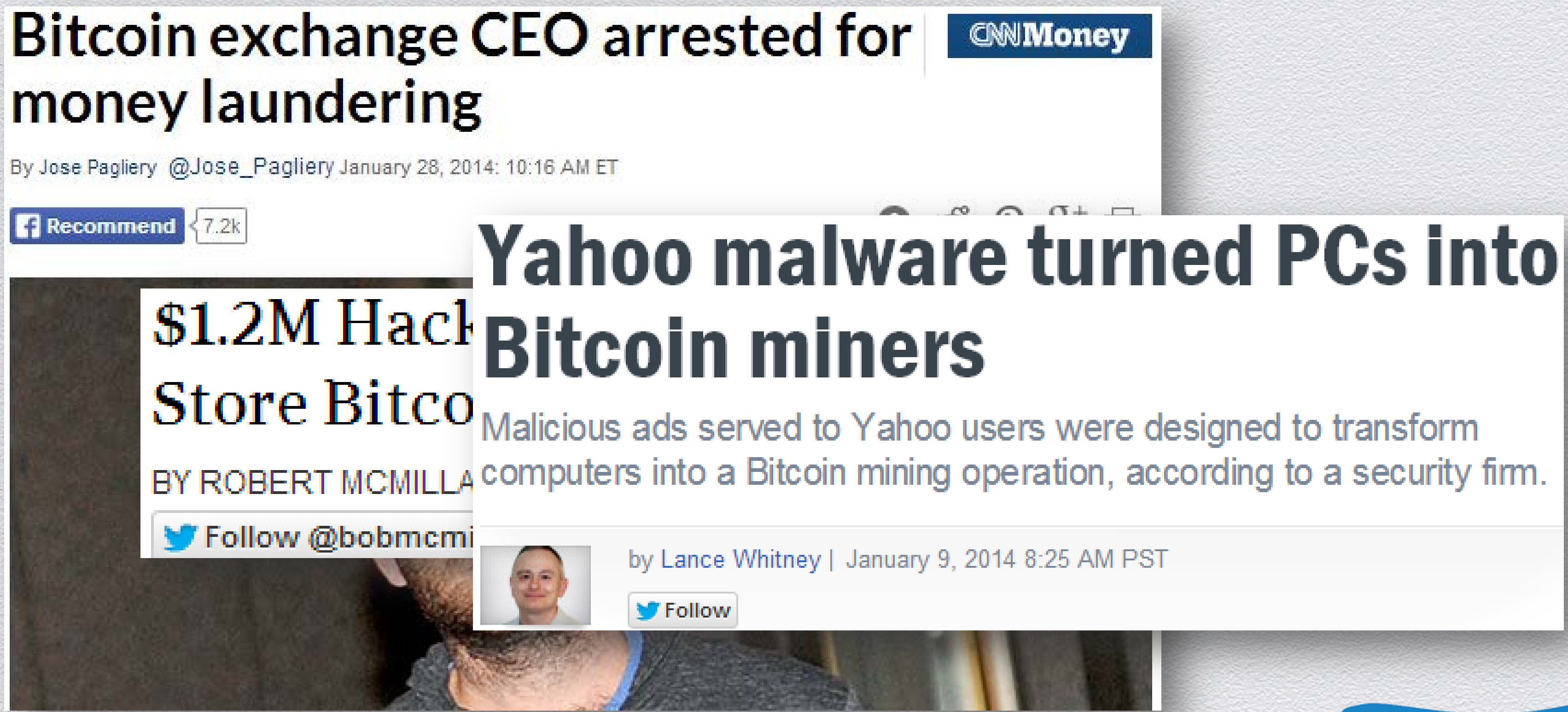
Bitcoin Fog: Secure Bitcoin Anonymization

Bitcoin is not 100% anonymous, we are providing a solution for this: using our service you mix up your bitcoins in our own pool with other users' bitcoins, and get paid back to other accounts from our mixed pool, which, if properly done by you can eliminate any chance of finding your payments and making it impossible to prove any connection between a deposit and a withdraw inside our service.

Criminal Discussions

- What people care about:
  - Discussions around crypto currency
  - Extra fogging
  - Conversation rate
  - Currency volatility

Explaining the News



Bitcoin exchange CEO arrested for money laundering

By Jose Pagliery @Jose_Pagliery January 28, 2014: 10:16 AM ET

$1.2M Hack
Store Bitco

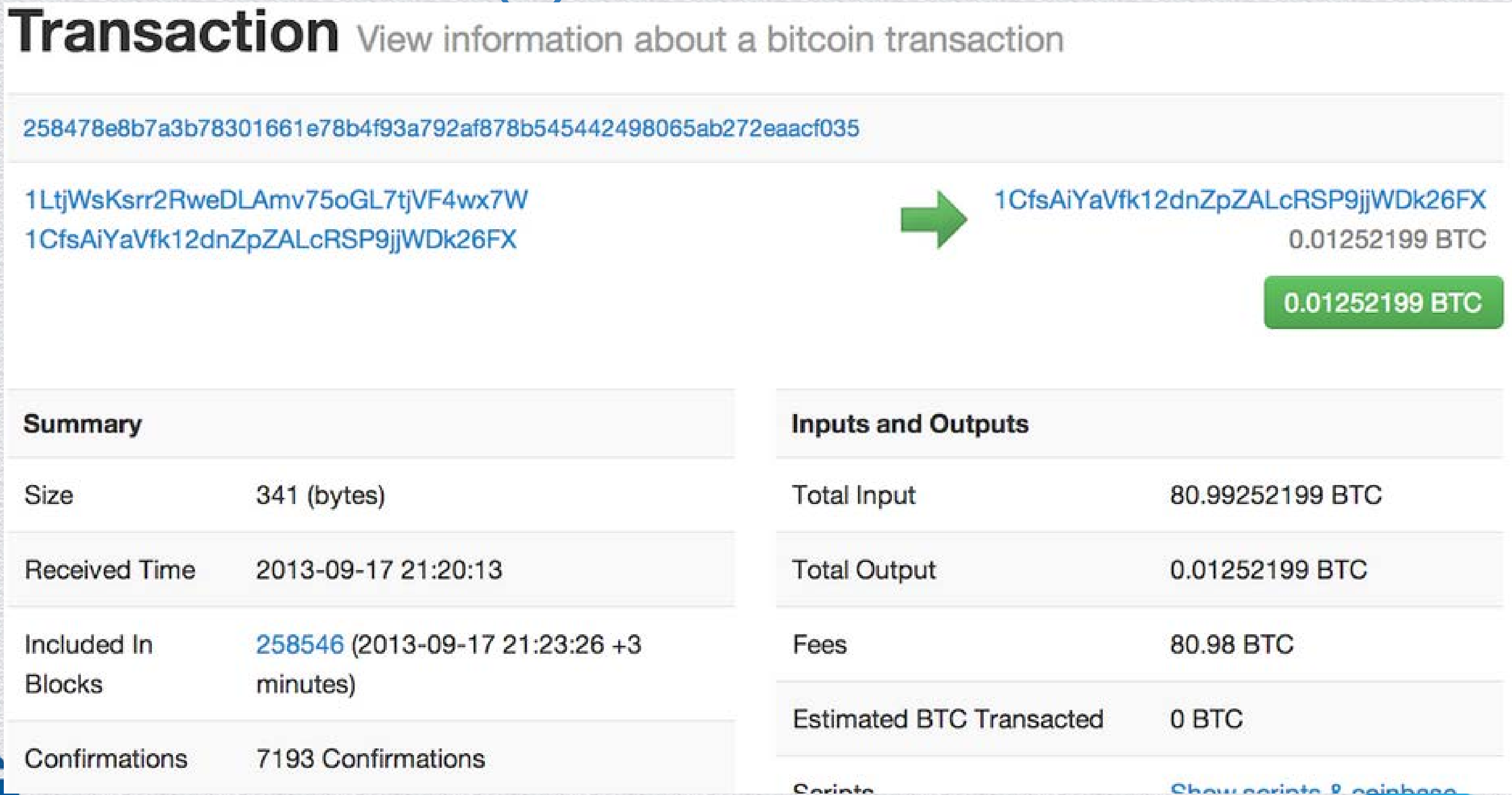
BY ROBERT MCMILLA

Yahoo malware turned PCs into Bitcoin miners

Malicious ads served to Yahoo users were designed to transform computers into a Bitcoin mining operation, according to a security firm.

by Lance Whitney | January 9, 2014 8:25 AM PST

Bitcoin Mistakes (?)



Transaction View information about a bitcoin transaction

258478e8b7a3b78301661e78b4f93a792af878b545442498065ab272eaacf035

1LtjWsKsrr2RweDLAmv75oGL7tjVF4wx7W
1CfsAiYaVfk12dnZpZALcRSP9jjWDk26FX

→ 1CfsAiYaVfk12dnZpZALcRSP9jjWDk26FX
0.01252199 BTC

0.01252199 BTC

Summary	
Size	341 (bytes)
Received Time	2013-09-17 21:20:13
Included In Blocks	258546 (2013-09-17 21:23:26 +3 minutes)
Confirmations	7193 Confirmations

Inputs and Outputs	
Total Input	80.99252199 BTC
Total Output	0.01252199 BTC
Fees	80.98 BTC
Estimated BTC Transacted	0 BTC
Scripts	Show scripts & coinbase

And now… for the LIVE DEMONSTRATION!!!

- This section includes a 20-min demonstration:
  - Logging into Bitcoin exchange account
  - Trojan configuration for the exchange
  - Credentials theft from infected device
  - Unauthorized entry and transferring Bitcoins to fraudster address
  - Confirmation in the blockchain
  - Removing traces

Summary: what have we learned?

- Bitcoin is a New Frontier:
  - Huge opportunity for Phishing and Trojan attacks
  - Exchanges are sitting ducks – hit them first!
  - Don’t bother with Bitcoin botnets
  - eWallets more lucrative than PC wallets
  - Try it at home – it’s fun!

QUESTIONS?

Etay.Maor@Trusteer.com
Uri.Rivner@BioCatch.com

Best use LinkedIn !