Bitcoin Security

陳君明 Jimmy Chen

jmchen@chroot.org

林志宏 Chris Lin

meconin@gmail.com

InfoKeyVault Technology

August 19, 2014

Agenda

- Introduction to Bitcoin
- Security of Bitcoin
- Hardware Wallet

Agenda

- Introduction to Bitcoin
  - Expanding Economy
  - Birth of Bitcoin
  - Cryptographic Primitives
  - Bitcoin Protocol
- Security of Bitcoin
- Hardware Wallet

Bitcoin recognized by Germany as 'private money'

Matt Clinch | @mattclinch81
Monday, 19 Aug 2013 | 10:25 AM ET

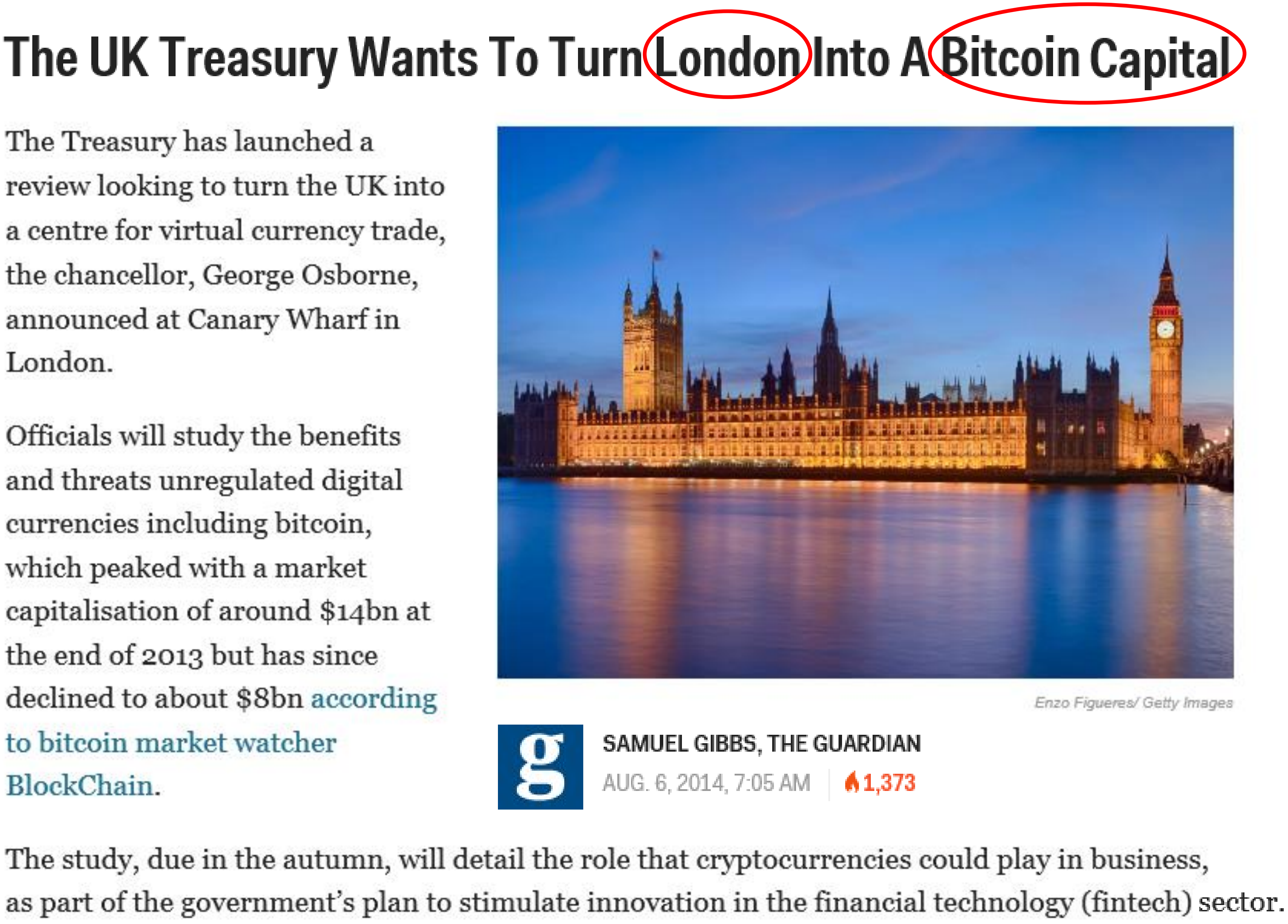
Tomohiro Ohsumi | Bloomberg | Getty Images

exactly one year ago

Virtual currency bitcoin has been recognized by the German Finance Ministry as a "unit of account", meaning it is can be used for tax and trading purposes in the country.

"We should have competition in the production of money. I have long been a proponent of Friedrich August von Hayek scheme to denationalize money. Bitcoins are a first step in this direction,"said Frank Schaeffler, a member of the German parliament's Finance Committee, who has pushed for legal classification of bitcoins.

http://www.cnbc.com/id/100971898



The UK Treasury Wants To Turn London Into A Bitcoin Capital

The Treasury has launched a review looking to turn the UK into a centre for virtual currency trade, the chancellor, George Osborne, announced at Canary Wharf in London.

Officials will study the benefits and threats unregulated digital currencies including bitcoin, which peaked with a market capitalisation of around $14bn at the end of 2013 but has since declined to about $8bn according to bitcoin market watcher BlockChain.

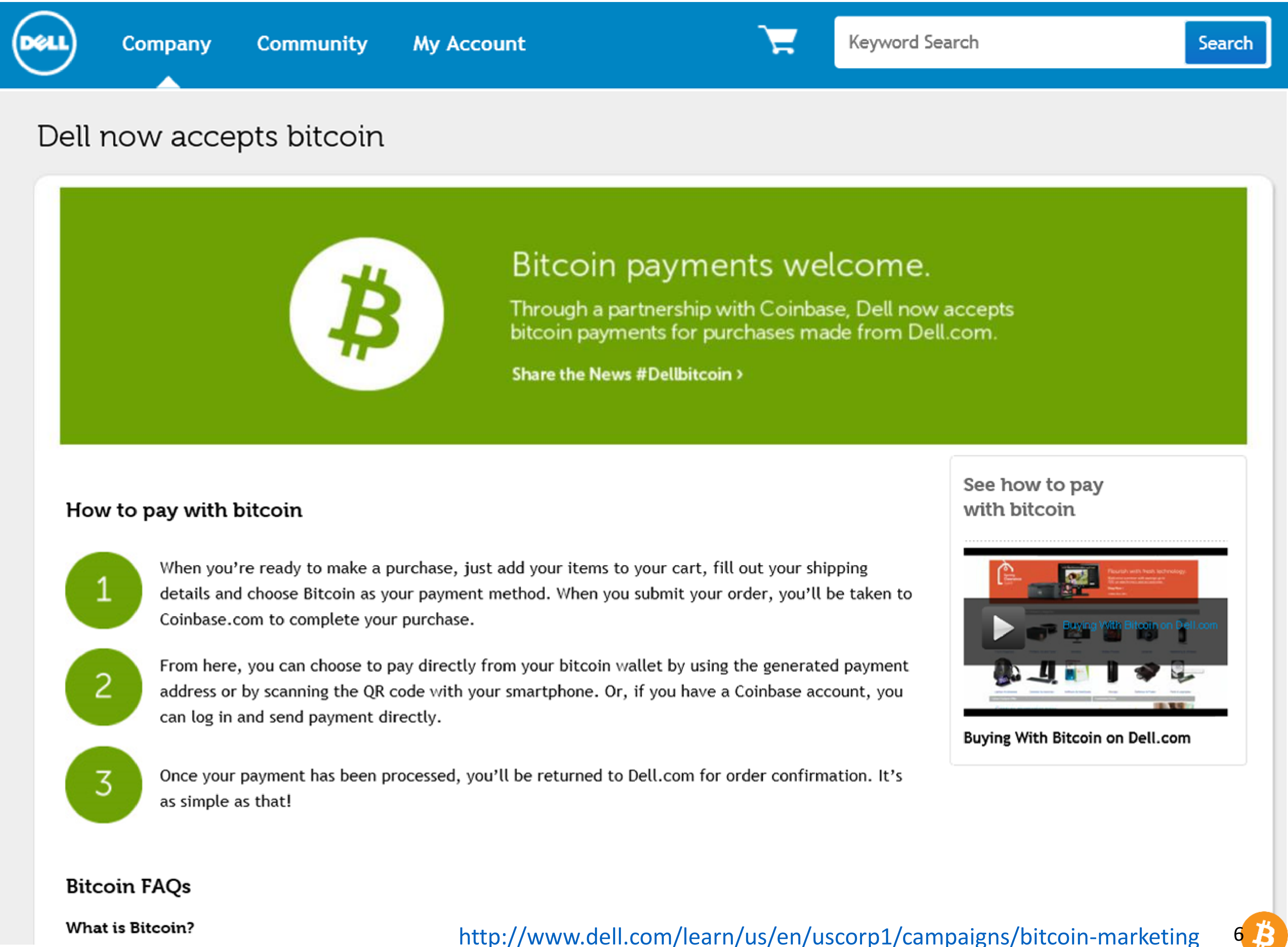
Enzo Figueres/ Getty Images

SAMUEL GIBBS, THE GUARDIAN

AUG. 6, 2014, 7:05 AM | 1,373

The study, due in the autumn, will detail the role that cryptocurrencies could play in business, as part of the government's plan to stimulate innovation in the financial technology (fintech) sector.

http://www.businessinsider.com/the-uk-treasury-wants-to-turn-london-into-a-bitcoin-capital-2014-8



Dell now accepts bitcoin

Bitcoin payments welcome.

Through a partnership with Coinbase, Dell now accepts bitcoin payments for purchases made from Dell.com.

Share the News #Dellbitcoin ›

How to pay with bitcoin

1 When you're ready to make a purchase, just add your items to your cart, fill out your shipping details and choose Bitcoin as your payment method. When you submit your order, you'll be taken to Coinbase.com to complete your purchase.

2 From here, you can choose to pay directly from your bitcoin wallet by using the generated payment address or by scanning the QR code with your smartphone. Or, if you have a Coinbase account, you can log in and send payment directly.

3 Once your payment has been processed, you'll be returned to Dell.com for order confirmation. It's as simple as that!

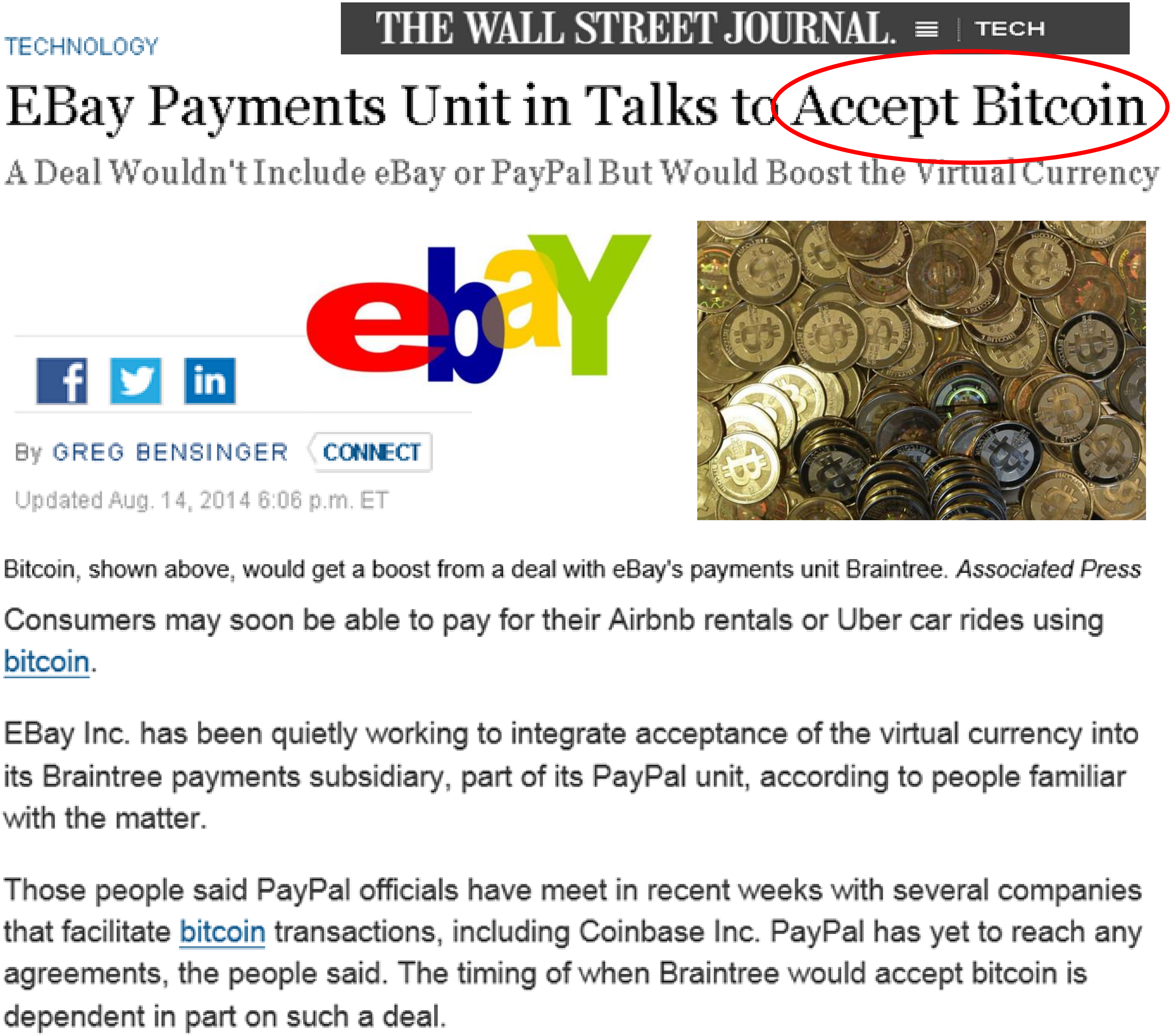
See how to pay with bitcoin

Buying With Bitcoin on Dell.com

Bitcoin FAQs

What is Bitcoin?

http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing



TECHNOLOGY

THE WALL STREET JOURNAL. ≡ | TECH

EBay Payments Unit in Talks to Accept Bitcoin

A Deal Wouldn't Include eBay or PayPal But Would Boost the Virtual Currency

By GREG BENSINGER CONNECT

Updated Aug. 14, 2014 6:06 p.m. ET

Bitcoin, shown above, would get a boost from a deal with eBay's payments unit Braintree. *Associated Press*

Consumers may soon be able to pay for their Airbnb rentals or Uber car rides using bitcoin.

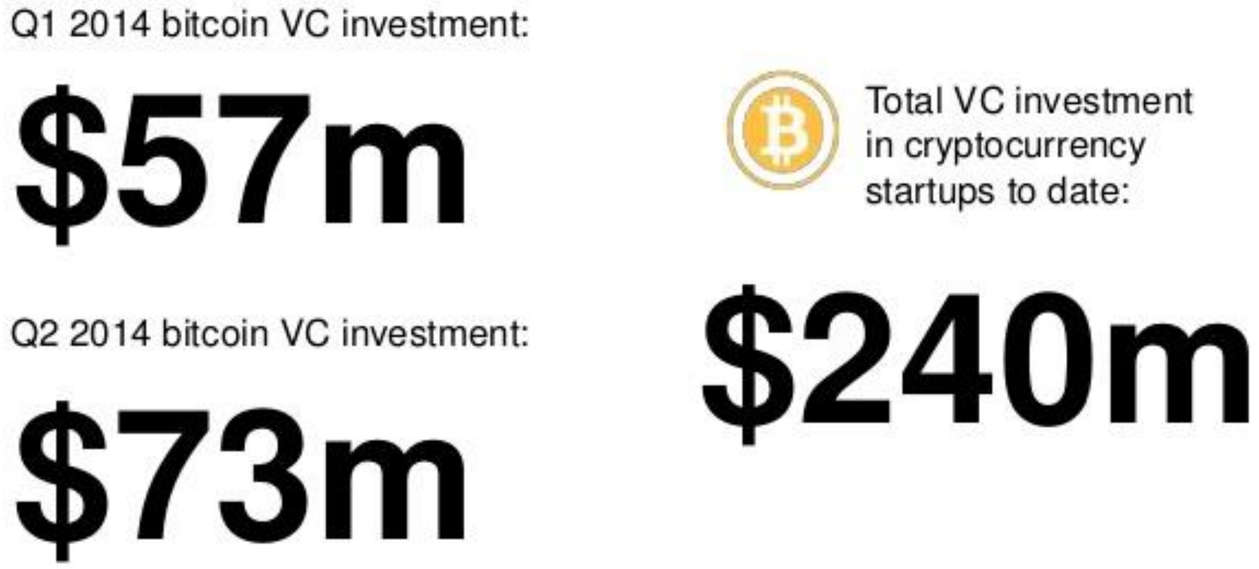
EBay Inc. has been quietly working to integrate acceptance of the virtual currency into its Braintree payments subsidiary, part of its PayPal unit, according to people familiar with the matter.

Those people said PayPal officials have meet in recent weeks with several companies that facilitate bitcoin transactions, including Coinbase Inc. PayPal has yet to reach any agreements, the people said. The timing of when Braintree would accept bitcoin is dependent in part on such a deal.

http://online.wsj.com/articles/ebay-payment-unit-in-talks-to-accept-bitcoin-1408052917

Venture Capital Investment

VC Investment up to December 2013:	US$ 110 millions
VC Investment from January to June 2014:	US$ 130 millions



Q1 2014 bitcoin VC investment:

$57m

Q2 2014 bitcoin VC investment:

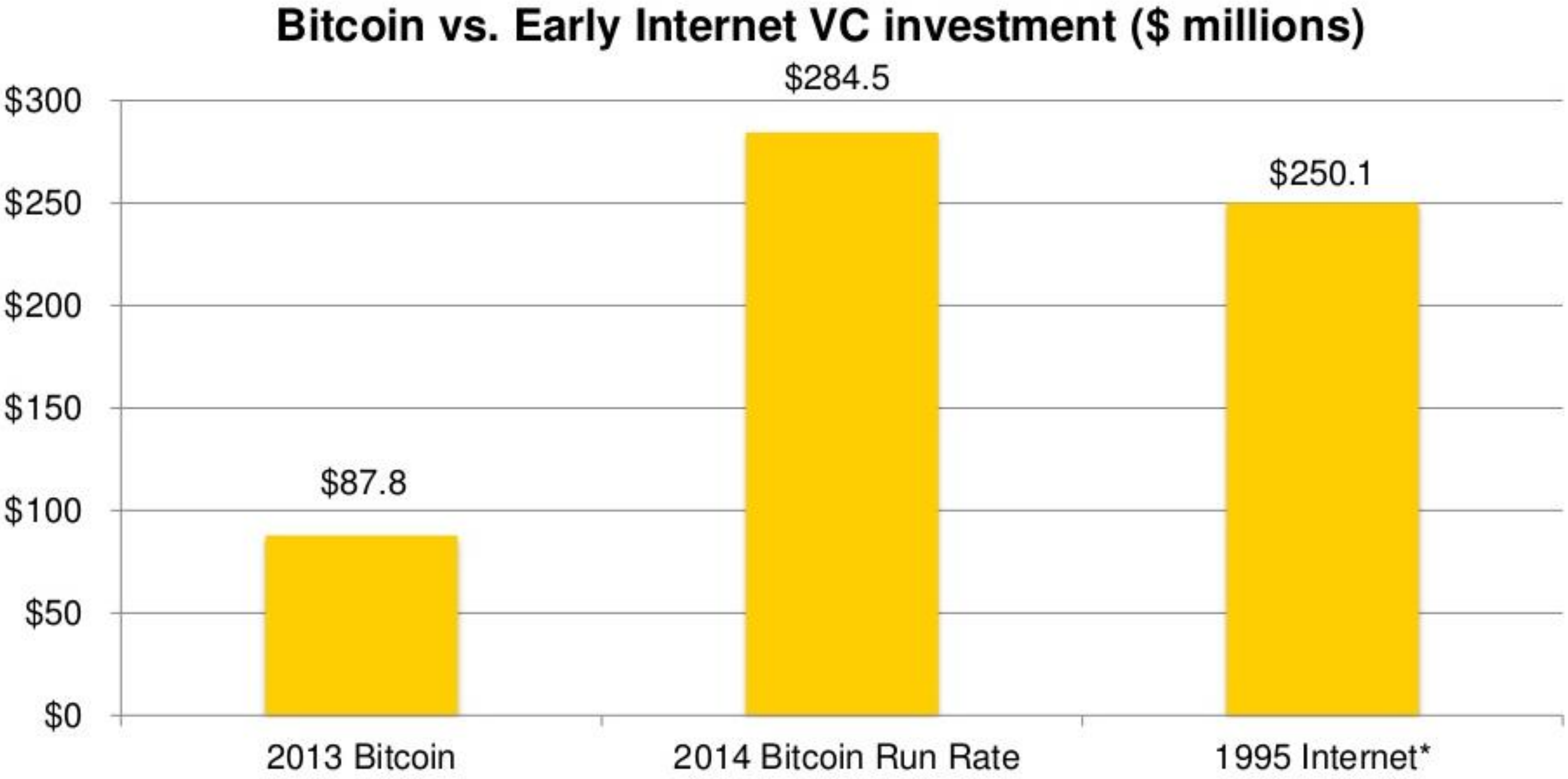
$73m

Total VC investment in cryptocurrency startups to date:

$240m

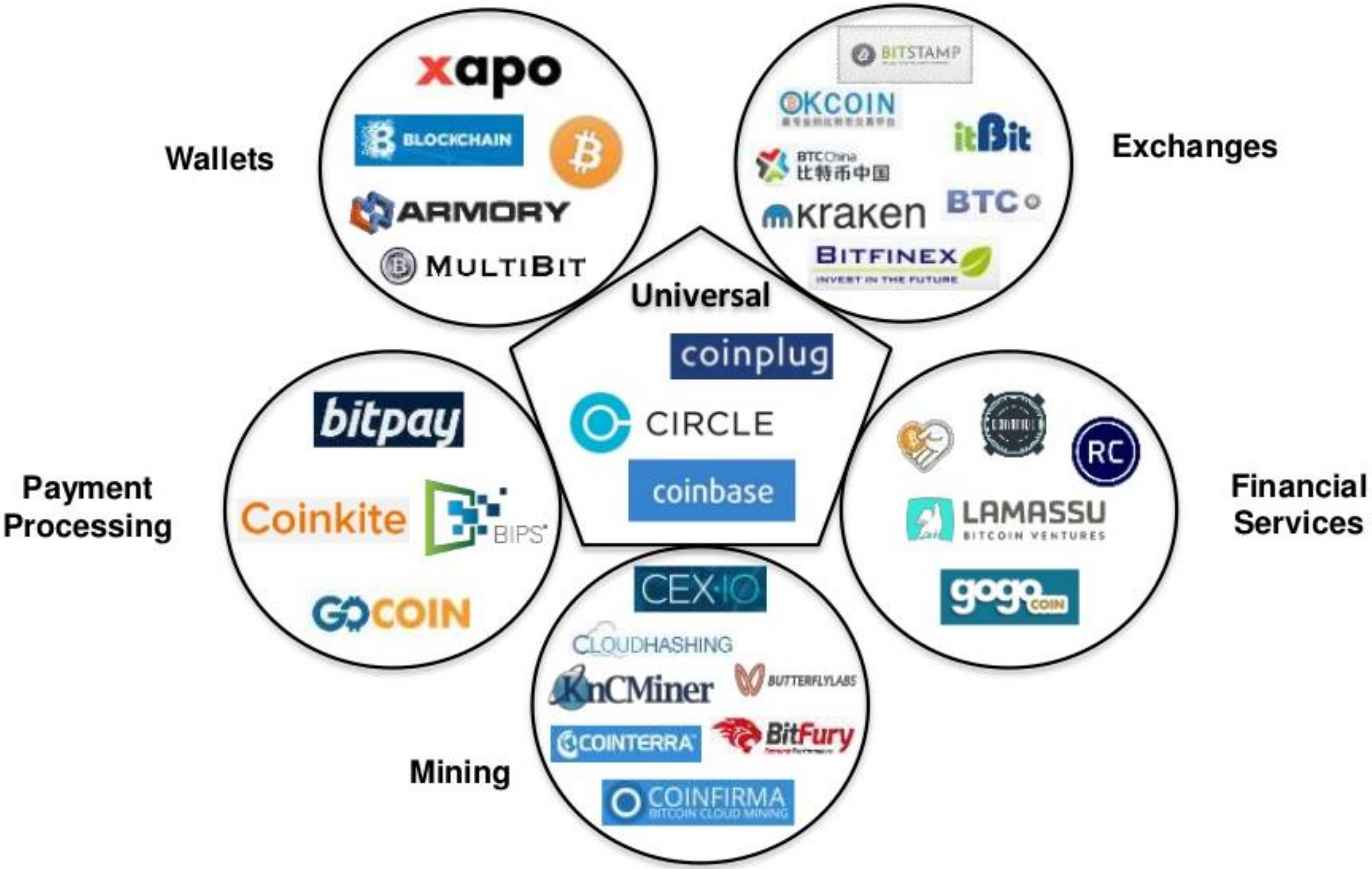
http://www.coindesk.com/state-of-bitcoin-q2-2014-report-expanding-bitcoin-economy
http://www.coindesk.com/bitcoin-venture-capital

2014 VC Investment in Bitcoin Overtakes VC Early-Stage Internet Investments



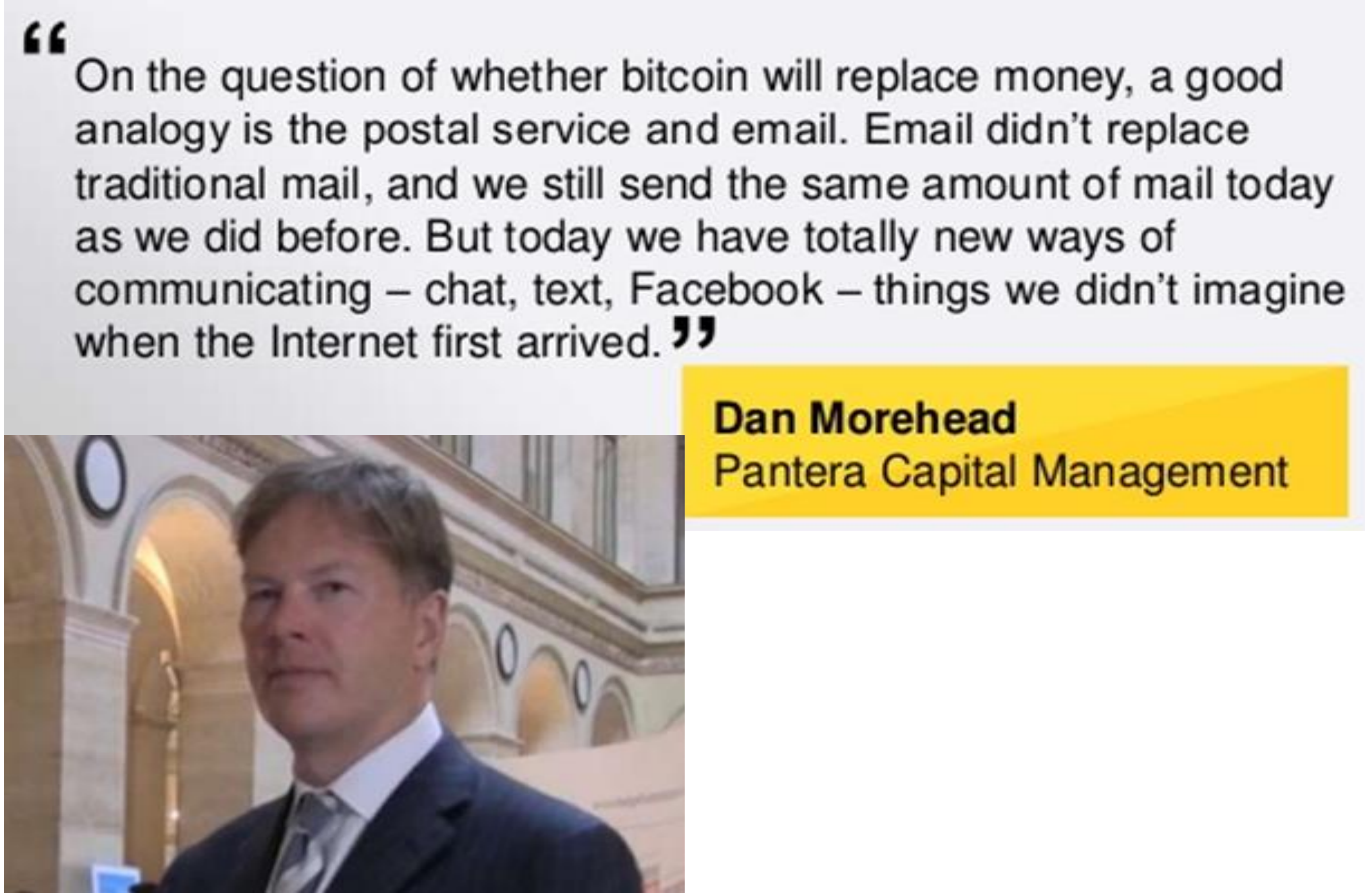
http://www.coindesk.com/state-of-bitcoin-q2-2014-report-expanding-bitcoin-economy

Startup Ecosystem: 6 Classifications



http://www.coindesk.com/state-of-bitcoin-q2-2014-report-expanding-bitcoin-economy

Investor View on Bitcoin



“On the question of whether bitcoin will replace money, a good analogy is the postal service and email. Email didn’t replace traditional mail, and we still send the same amount of mail today as we did before. But today we have totally new ways of communicating – chat, text, Facebook – things we didn’t imagine when the Internet first arrived.”

Dan Morehead
Pantera Capital Management

http://www.coindesk.com/state-of-bitcoin-q2-2014-report-expanding-bitcoin-economy

Worldwide Conferences & Events

Date	Conference/Event	Location
July 3-4	Bitcoin Finance 2014	Dublin, Ireland
July 9-10	Inside Bitcoins	Melbourne, Australia
July 19-20	North American Bitcoins Conference	Chicago, Illinois, US
July 23-24	Coin Congress	San Francisco, California, US
July 24-25	Cryptocon Sydney	Sydney, Australia
July 28-29	Inside Bitcoins	Tel Aviv, Israel
July 29	American Banker Digital Currencies Conference	New York, US
Aug 9	Bitcoin and Cryptocurrencies: Prospects for Development in Russia	St. Petersburg, Russia
Aug 15-16	Cryptolina	Raleigh, North Carolina, US
Aug 22	Toronto Bitcoin Hackathon 2014	Toronto, ON
Aug 23	Scottish Bitcoin Conference	Edinburgh, UK
Aug 25 - Sep 1	Camp Bitcoin at Burning Man	Black Rock City, Nevada, US
Sep 1-2	World Bitcoin Forum	Bonn, Germany
Sep 3-5	Bitcoinference Summer 2014	Amsterdam, Netherlands
Sep 11-12	APEX Digital Currency Partnerships	San Francisco, California, US
Sep 11-12	Bitcoin Central & Eastern European Conference	Ljubljana, Slovenia
Sep 15-16	Inside Bitcoins London	London, England
Sep 17-18	Crypto Valley Summit	Isle of Man, British Isles
Sep 17-19	Digital Currency Summit	Andorra la Vella, Andorra
Sep 19-20	Bitcoin Expo China 2014	Shanghai, China
Sep 26	Bitcoin Conference Kiev 2014	Kiev, Ukraine
Sep 28-29	Seattle Bitcoin Summit	Seattle, US
Oct 10-11	Hashers United	Las Vegas, US
Oct 16-17	Bitcoin to Business Congress	Brussels, Belgium
Nov 2-6	Bitcoin World at Money2020	Las Vegas, US
Nov 18-19	Payments Indonesia	Jakarta, Indonesia
Nov 24-25	Cryptocon Singapore	Singapore
Nov 29-30	Bitcoin South	Queenstown, New Zealand
Dec 5-7	Dubai Bitcoin Conference	Dubai, UAE

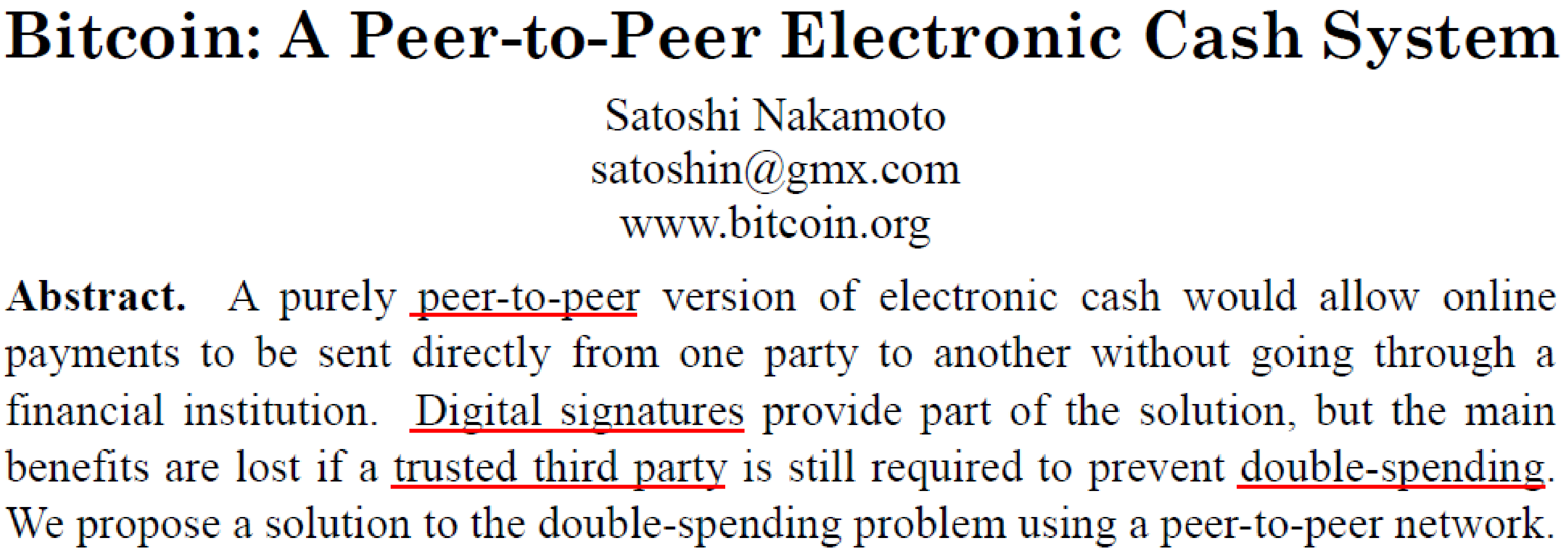
Information up to August 15

https://bitcoin.org/en/events http://www.coindesk.com/bitcoin-events

https://bitcoinfoundation.org/forum/index.php?/topic/810-upcoming-bitcoin-conferences-and-events

Birth of Bitcoin

- Described by Satoshi Nakamoto (中本聰) in 2008
- Introduced as open-source software on the evening of January 3, 2009



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

http://bitcoin.org/bitcoin.pdf

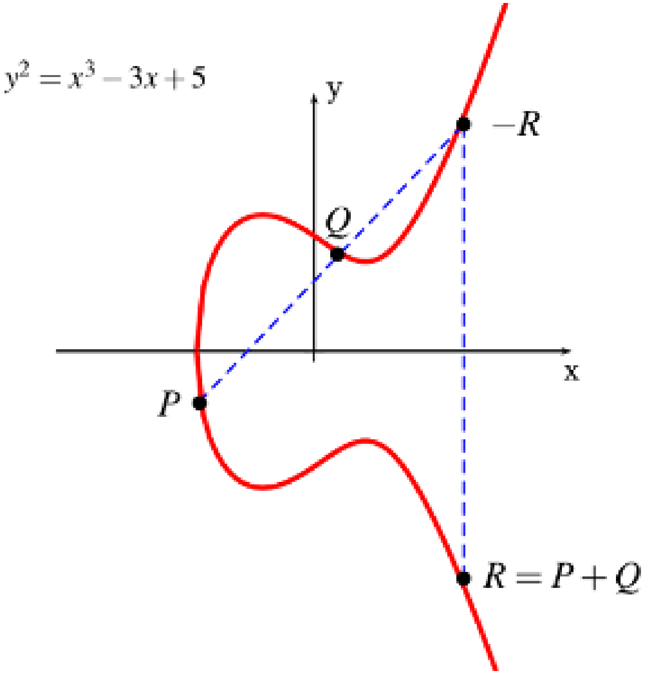
Excellent Tutorial for Beginners

- **How the Bitcoin protocol actually works**
  - Published by Michael Nielsen on December 6, 2013
  - http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works
  - "This is the best explanation of the Bitcoin protocol that I have read" by Bruce Schneier https://www.schneier.com/blog/archives/2013/12/bitcoin_explana.html
- "To understand the post, you need to be comfortable with **public key cryptography**, and with the closely related idea of **digital signatures**. I'll also assume you're familiar with **cryptographic hashing**."
- "In the world of atoms we achieve security with devices such as locks, safes, signatures, and bank vaults. In the world of bits we achieve this kind of security with cryptography. And that's why **Bitcoin is at heart a cryptographic protocol**."

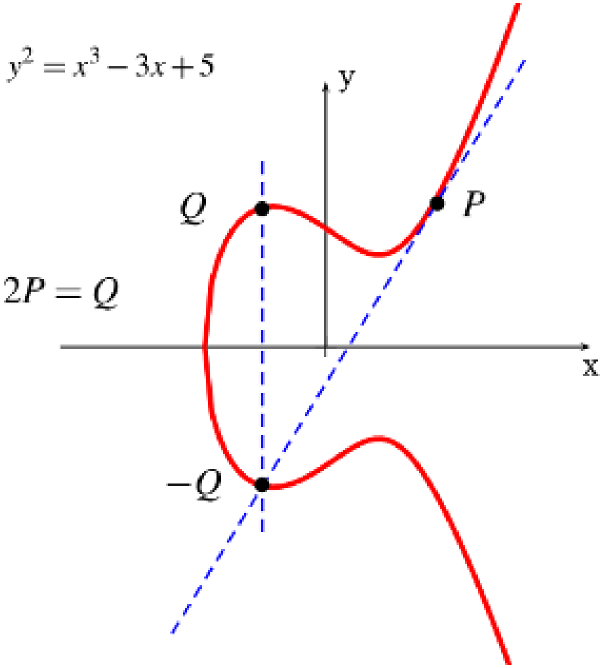
Elliptic Curves 橢圓曲線

- The rich and deep theory of Elliptic Curves has been studied by mathematicians over 150 years

Elliptic Curve over ***R***: $y^2 = x^3 + ax + b$



Point Addition



Point Doubling

Image Courtesy: http://www.embedded.com/design/safety-and-security/4396040/An-Introduction-to-Elliptic-Curve-Cryptography

Elliptic Curves over Prime Fields

Addition:

$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$

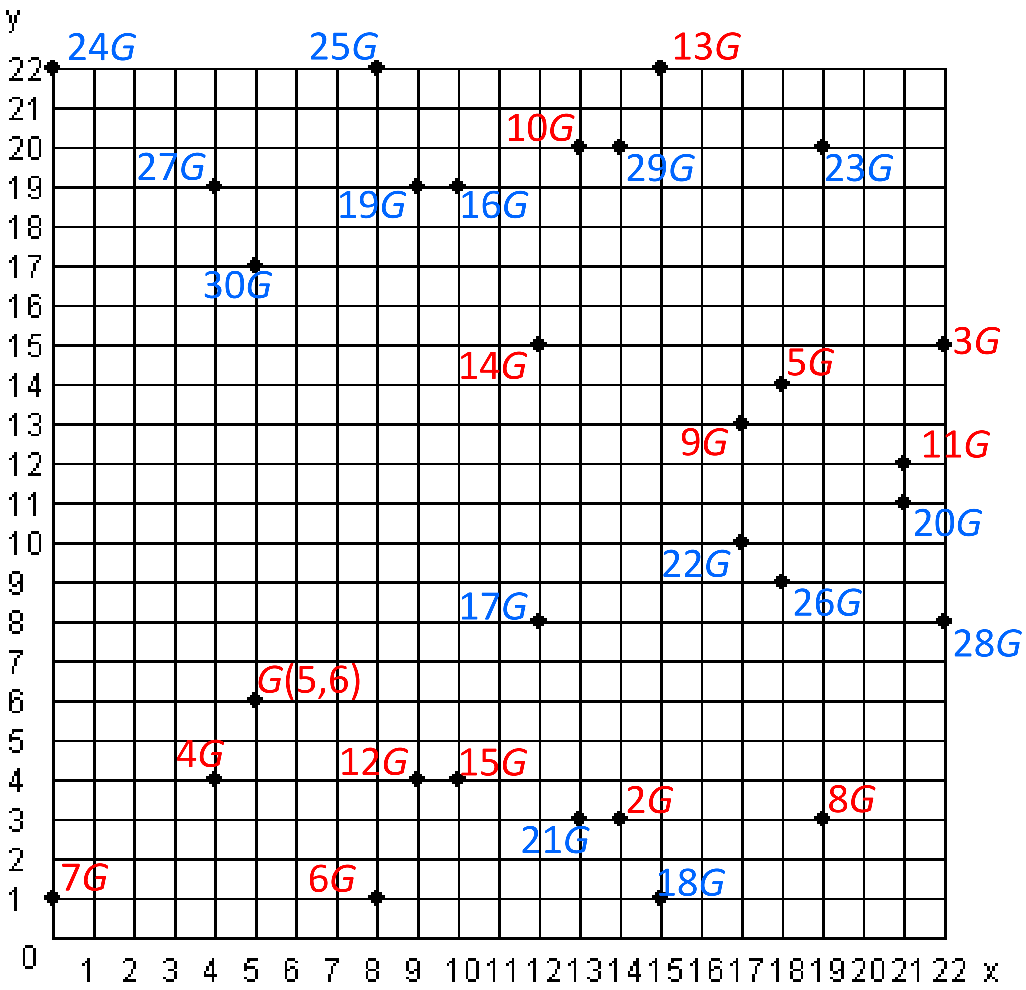
Doubling:

$(x_3, y_3) = [2]\,(x_1, y_1)$

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \text{ mod } p \quad \text{(addition)} \\[2ex] \dfrac{3x_1^2 + a}{2y_1} \text{ mod } p \quad \text{(doubling)} \end{cases}$$

$$x_3 = s^2 - x_1 - x_2 \quad \text{mod } p$$

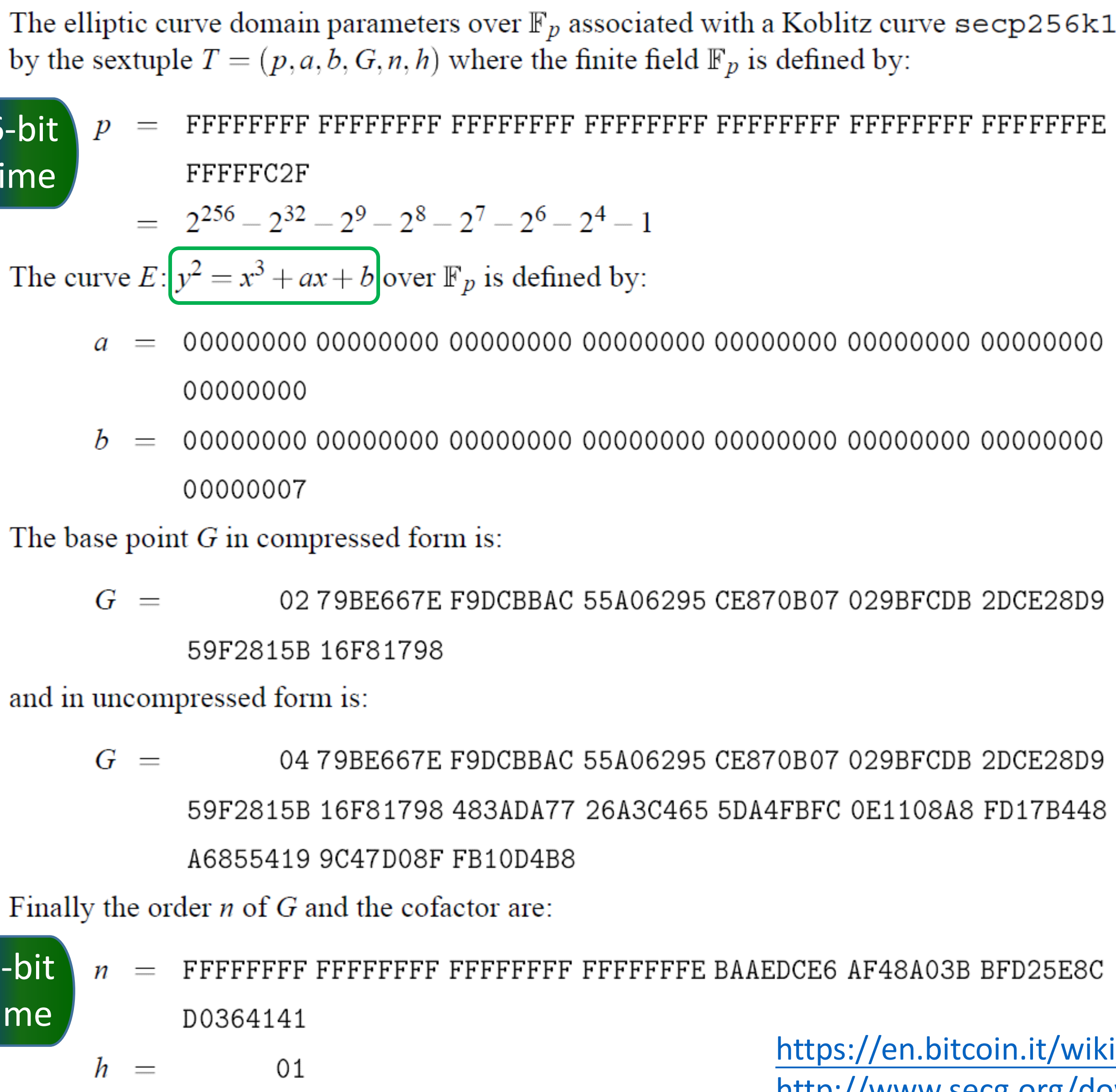
$$y_3 = s(x_1 - x_3) - y_1 \quad \text{mod } p$$



$y^2 = x^3 + 5x + 1$ over F_{23}

30 solutions

The Elliptic Curve in Bitcoin for ECDSA



The elliptic curve domain parameters over $\mathbb{F}_p$ associated with a Koblitz curve `secp256k1` are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field $\mathbb{F}_p$ is defined by:

256-bit prime

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

$= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$

The curve E: $\boxed{y^2 = x^3 + ax + b}$ over $\mathbb{F}_p$ is defined by:

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point G in compressed form is:

G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

and in uncompressed form is:

G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order n of G and the cofactor are:

256-bit prime

n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

h = 01

ECDSA : Elliptic Curve Digital Signature Algorithm

https://en.bitcoin.it/wiki/Secp256k1
http://www.secg.org/download/aid-784/sec2-v2.pdf

Key Pairs for Digital Signatures

- The base point *G* is fixed on the given Elliptic Curve
- *P* = [*m*] *G*
    - Given *m*, it is **easy and fast** to find the point *P*
        - Using "double and add" for scalar multiplication
    - Given *P*, it is **extremely hard** to find the integer *m*
        - Elliptic Curve Discrete Logarithm Problem (橢圓曲線離散對數問題)
    - A randomly generated integer *m* is a **private key** for ECDSA
        - A private key is used to sign Bitcoin transactions
    - The point *P* is the **public key** corresponding to *m*
        - A public key is used by other nodes to verify Bitcoin transactions
        - **A Bitcoin address is the hash value of a public key *P***

Hash Functions 雜湊函數

- **Definition** H is a function with **one-way property** if given any y, it is *computationally infeasible* to find any value x in the domain of H such that $H(x) = y$
- **Definition** H is a **cryptographic hash function** if
  - Input : bit strings of arbitrary length
  - Output H : bit strings of fixed length
    - "hash values" or "hash codes"
  - H has one-way property
- **Definition** H is **collision free** if it is *computationally infeasible* to find $x' \neq x$ such that $H(x') = H(x)$

SHA-256

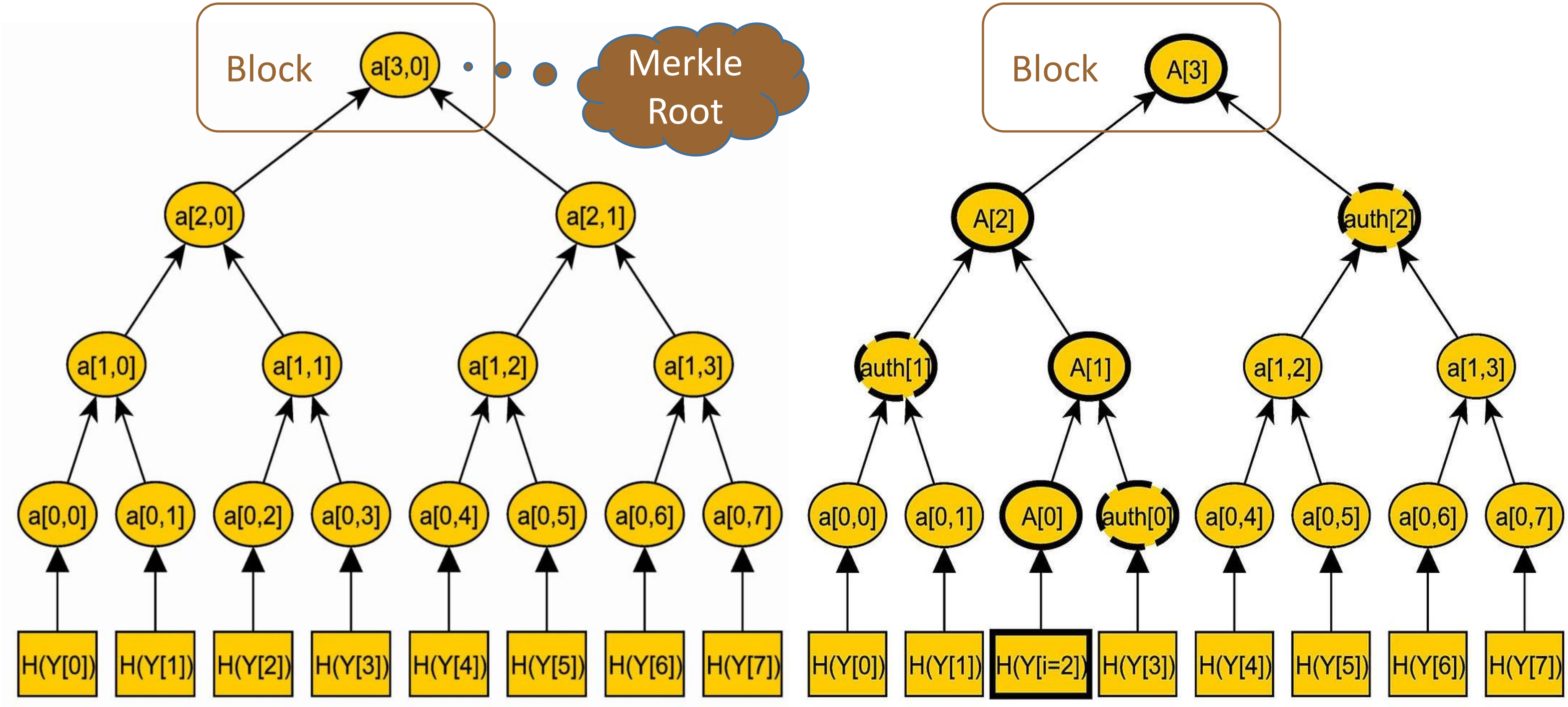
- SHA stands for Secure Hash Algorithm
- SHA-2 is a set of cryptographic hash functions designed by the U.S. National Security Agency (NSA) and published in 2001 by NIST as a U.S. Federal Information Processing Standard (FIPS)

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Word size (bits)	Rounds	Bitwise operations	Collisions found	Example Performance (MiB/s)
SHA-1		160	160	512	$2^{64} - 1$	32	80	and, or, xor, rot	Theoretical attack (2^{61})	192
SHA-2	SHA-224	224	256	512	$2^{64} - 1$	32	64	and, or, xor, shr, rot	None	139
	SHA-256	256								
	SHA-384	384	512	1024	$2^{128} - 1$	64	80	and, or, xor, shr, rot	None	154
	SHA-512	512								
	SHA-512/224	224								
	SHA-512/256	256								

http://en.wikipedia.org/wiki/SHA-2

Merkle Tree / Hash Tree

SHA-256: Hash Function in Bitcoin


Block

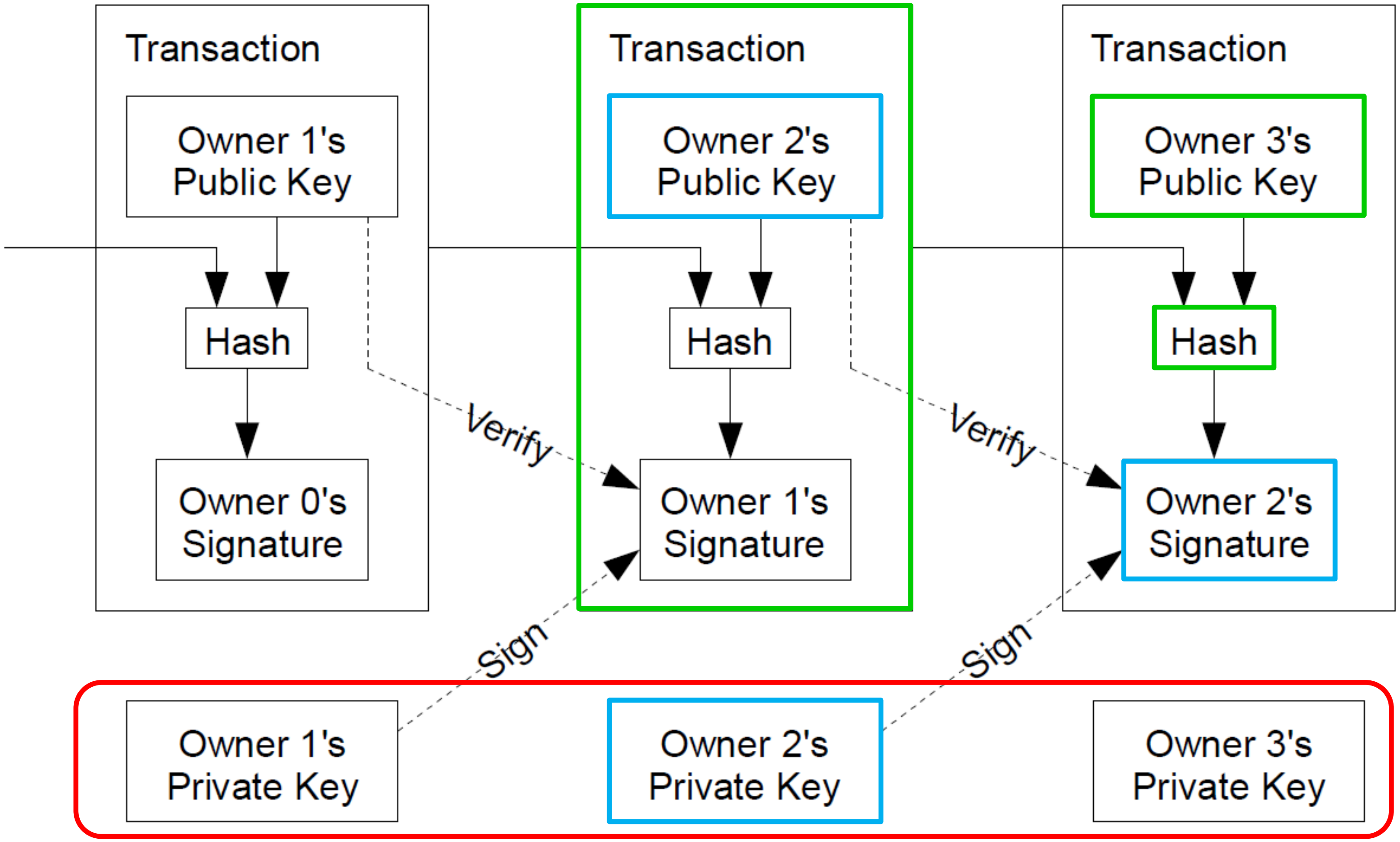
Merkle Root

Block

http://commons.wikimedia.org/wiki/File:MerkleTree1.jpg

http://commons.wikimedia.org/wiki/File:MerkleTree2.jpg

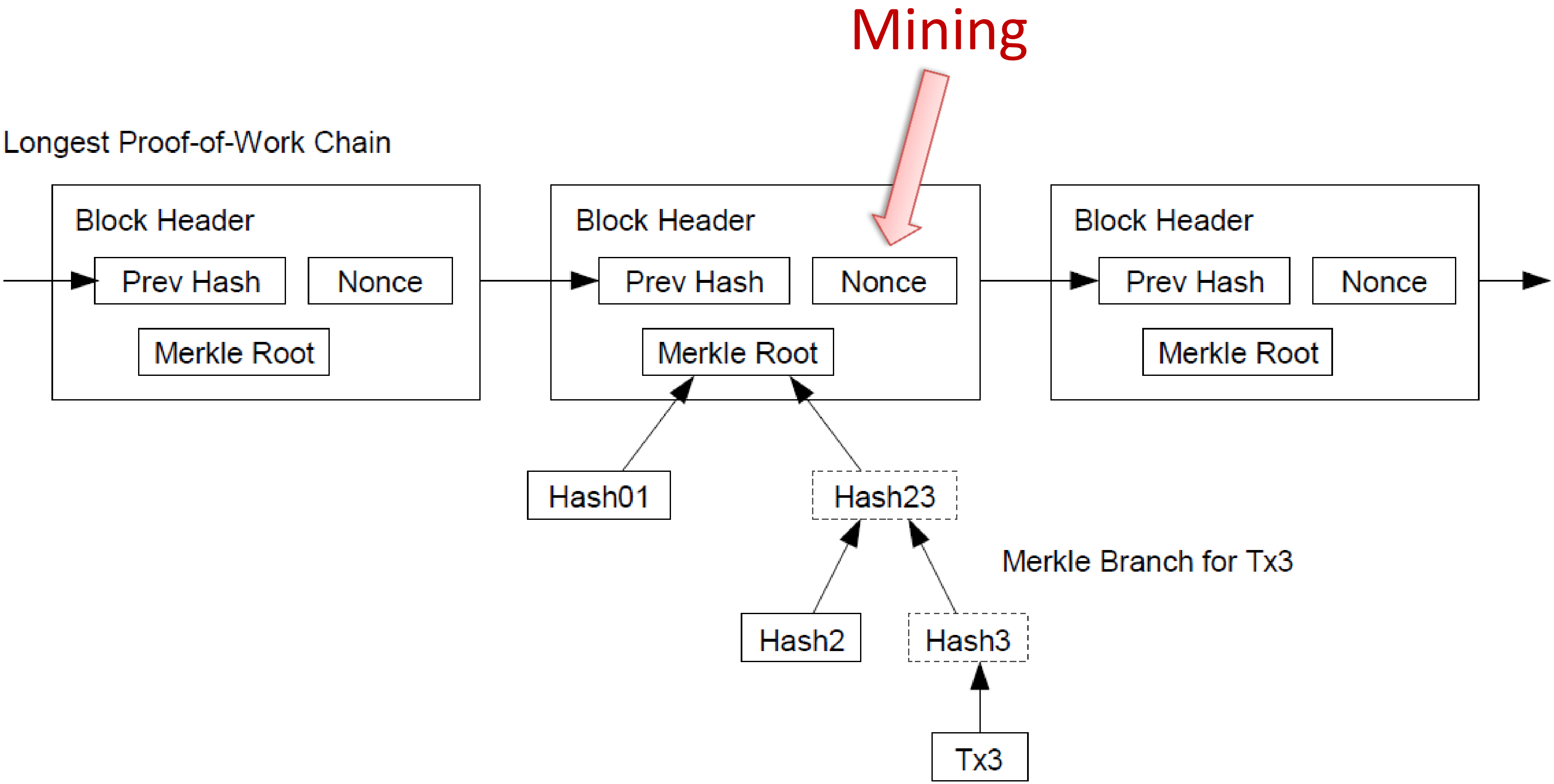
Transactions



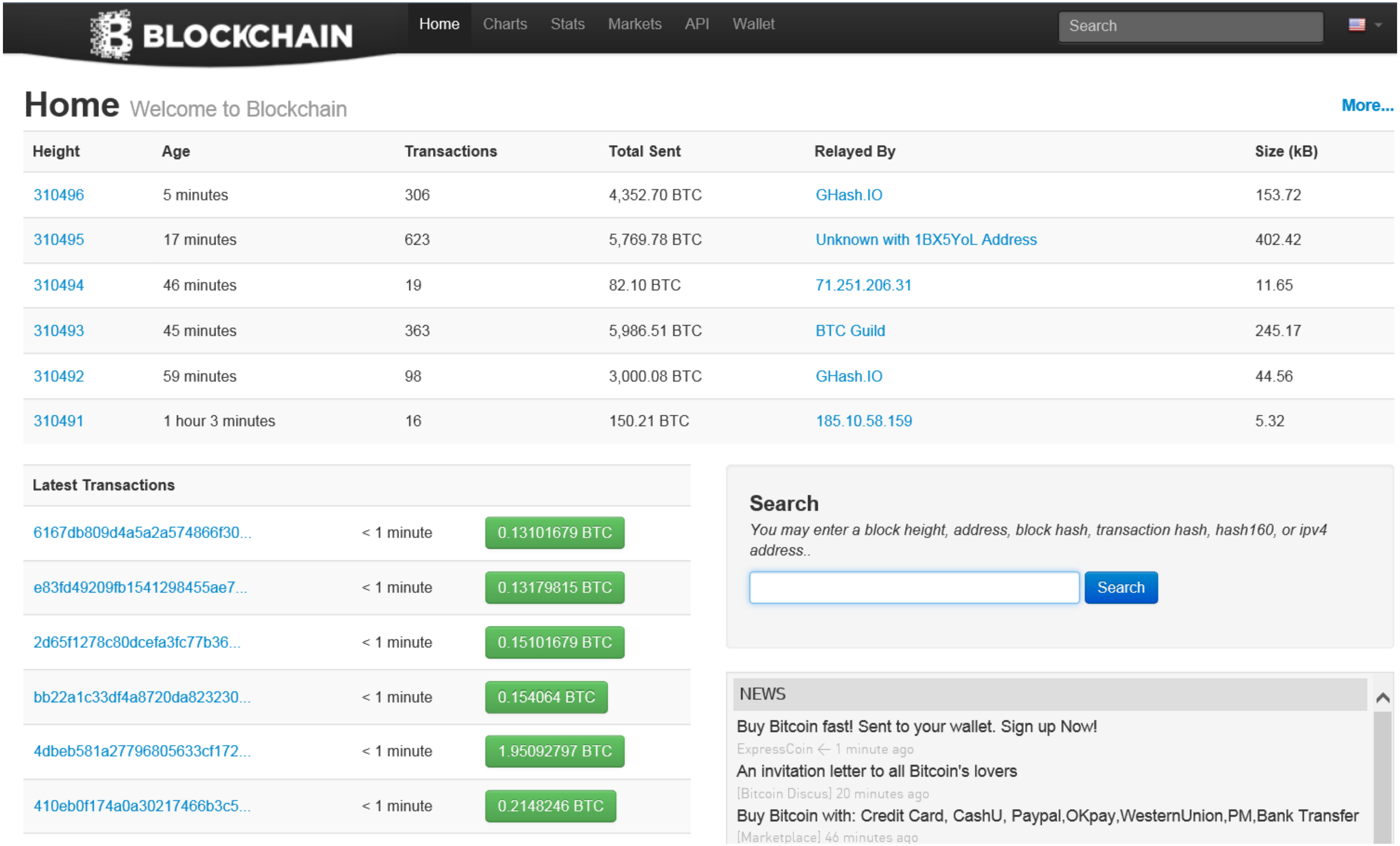
Must be protected very well!!!

http://bitcoin.org/bitcoin.pdf

Block Chain



http://bitcoin.org/bitcoin.pdf



Home Welcome to Blockchain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
310496	5 minutes	306	4,352.70 BTC	GHash.IO	153.72
310495	17 minutes	623	5,769.78 BTC	Unknown with 1BX5YoL Address	402.42
310494	46 minutes	19	82.10 BTC	71.251.206.31	11.65
310493	45 minutes	363	5,986.51 BTC	BTC Guild	245.17
310492	59 minutes	98	3,000.08 BTC	GHash.IO	44.56
310491	1 hour 3 minutes	16	150.21 BTC	185.10.58.159	5.32

Latest Transactions		
6167db809d4a5a2a574866f30...	< 1 minute	0.13101679 BTC
e83fd49209fb1541298455ae7...	< 1 minute	0.13179815 BTC
2d65f1278c80dcefa3fc77b36...	< 1 minute	0.15101679 BTC
bb22a1c33df4a8720da823230...	< 1 minute	0.154064 BTC
4dbeb581a27796805633cf172...	< 1 minute	1.95092797 BTC
410eb0f174a0a30217466b3c5...	< 1 minute	0.2148246 BTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address..

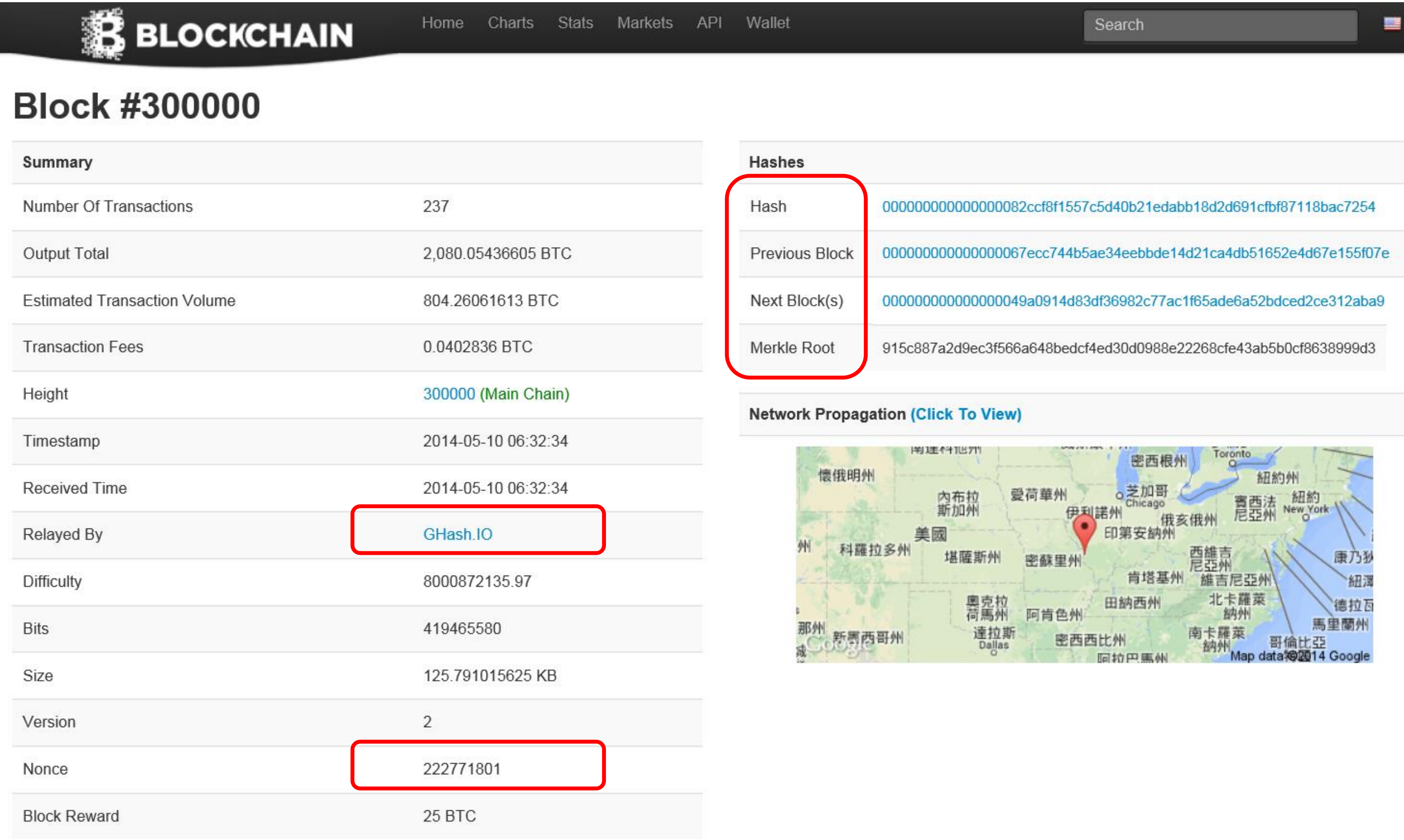
NEWS

Buy Bitcoin fast! Sent to your wallet. Sign up Now!
ExpressCoin ← 1 minute ago

An invitation letter to all Bitcoin's lovers
[Bitcoin Discus] 20 minutes ago

Buy Bitcoin with: Credit Card, CashU, Paypal,OKpay,WesternUnion,PM,Bank Transfer
[Marketplace] 46 minutes ago

https://blockchain.info

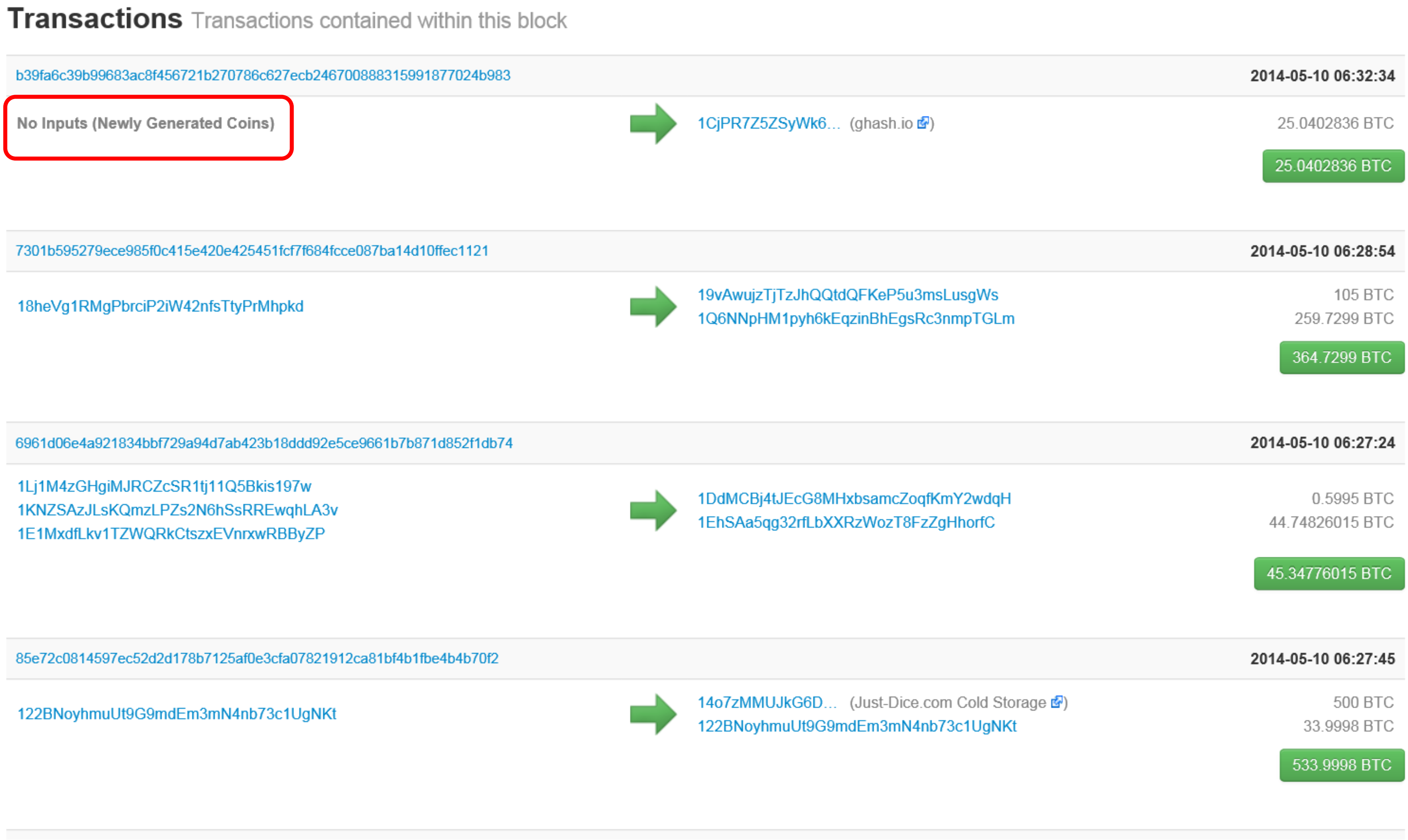


Block #300000

Summary	
Number Of Transactions	237
Output Total	2,080.05436605 BTC
Estimated Transaction Volume	804.26061613 BTC
Transaction Fees	0.0402836 BTC
Height	300000 (Main Chain)
Timestamp	2014-05-10 06:32:34
Received Time	2014-05-10 06:32:34
Relayed By	GHash.IO
Difficulty	8000872135.97
Bits	419465580
Size	125.791015625 KB
Version	2
Nonce	222771801
Block Reward	25 BTC

Hashes	
Hash	000000000000000082ccf8f1557c5d40b21edabb18d2d691cfbf87118bac7254
Previous Block	000000000000000067ecc744b5ae34eebbde14d21ca4db51652e4d67e155f07e
Next Block(s)	000000000000000049a0914d83df36982c77ac1f65ade6a52bdced2ce312aba9
Merkle Root	915c887a2d9ec3f566a648bedcf4ed30d0988e22268cfe43ab5b0cf8638999d3

Network Propagation (Click To View)



Transactions Transactions contained within this block

b39fa6c39b99683ac8f456721b270786c627ecb246700888315991877024b983 — 2014-05-10 06:32:34

No Inputs (Newly Generated Coins) → 1CjPR7Z5ZSyWk6... (ghash.io) 25.0402836 BTC

25.0402836 BTC

7301b595279ece985f0c415e420e425451fcf7f684fcce087ba14d10ffec1121 — 2014-05-10 06:28:54

18heVg1RMgPbrciP2iW42nfsTtyPrMhpkd → 19vAwujzTjTzJhQQtdQFKeP5u3msLusgWs 105 BTC
1Q6NNpHM1pyh6kEqzinBhEgsRc3nmpTGLm 259.7299 BTC

364.7299 BTC

6961d06e4a921834bbf729a94d7ab423b18ddd92e5ce9661b7b871d852f1db74 — 2014-05-10 06:27:24

1Lj1M4zGHgiMJRCZcSR1tj11Q5Bkis197w
1KNZSAzJLsKQmzLPZs2N6hSsRREwqhLA3v
1E1MxdfLkv1TZWQRkCtszxEVnrxwRBByZP
→ 1DdMCBj4tJEcG8MHxbsamcZoqfKmY2wdqH 0.5995 BTC
1EhSAa5qg32rfLbXXRzWozT8FzZgHhorfC 44.74826015 BTC

45.34776015 BTC

85e72c0814597ec52d2d178b7125af0e3cfa07821912ca81bf4b1fbe4b4b70f2 — 2014-05-10 06:27:45

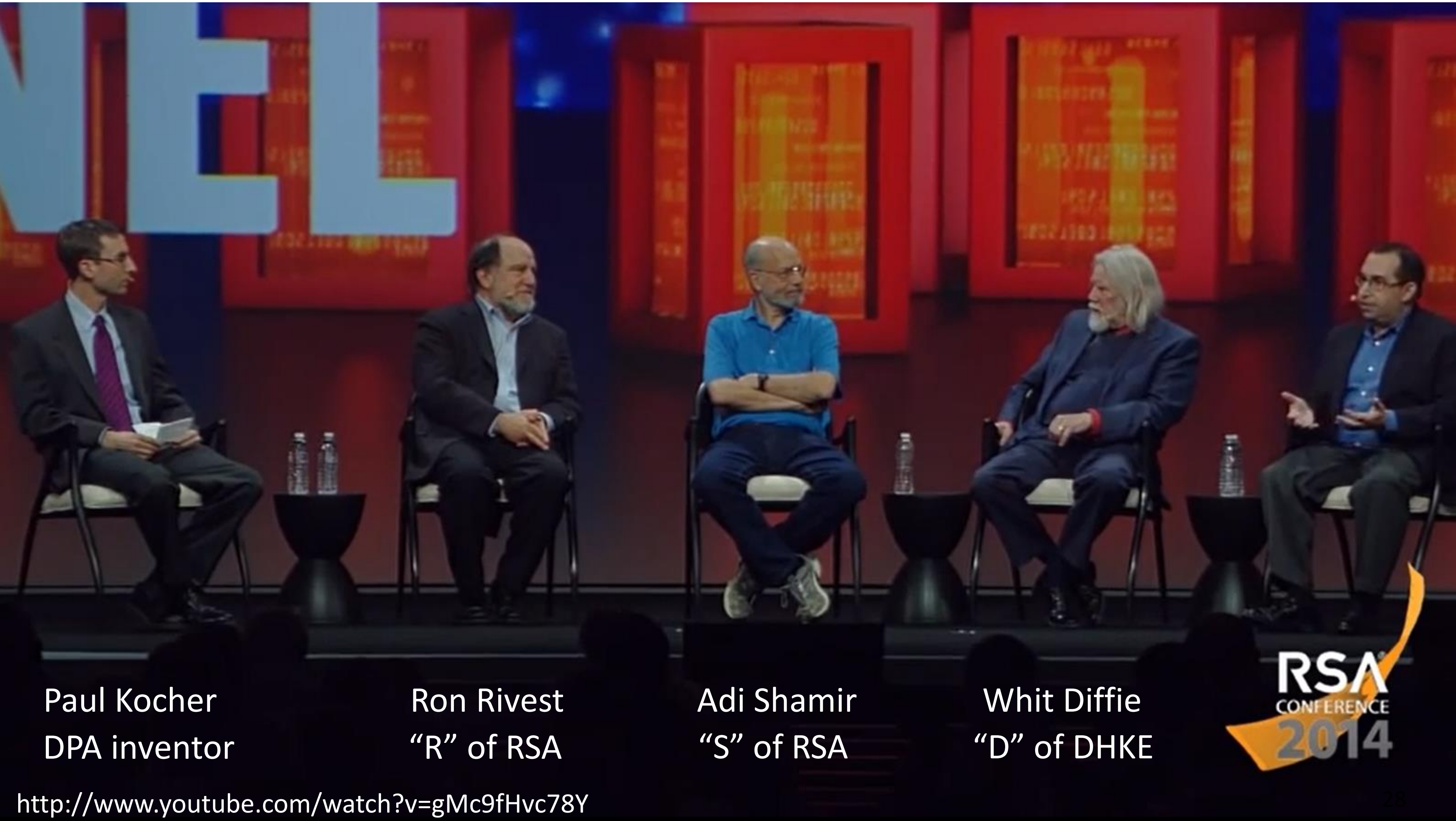
122BNoyhmuUt9G9mdEm3mN4nb73c1UgNKt → 14o7zMMUJkG6D... (Just-Dice.com Cold Storage) 500 BTC
122BNoyhmuUt9G9mdEm3mN4nb73c1UgNKt 33.9998 BTC

533.9998 BTC

Agenda

- Introduction to Bitcoin
- Security of Bitcoin
  - Strength of Crypto Primitives (ECDSA & SHA)
  - Random Number Generators
  - Side Channel Attacks
  - Transaction Malleability & Mt. Gox’ Bankruptcy
  - 51% Attack & Doomsday
  - … etc.
- Hardware Wallet

Comments from Crypto Legends



Paul Kocher
DPA inventor

Ron Rivest
“R” of RSA

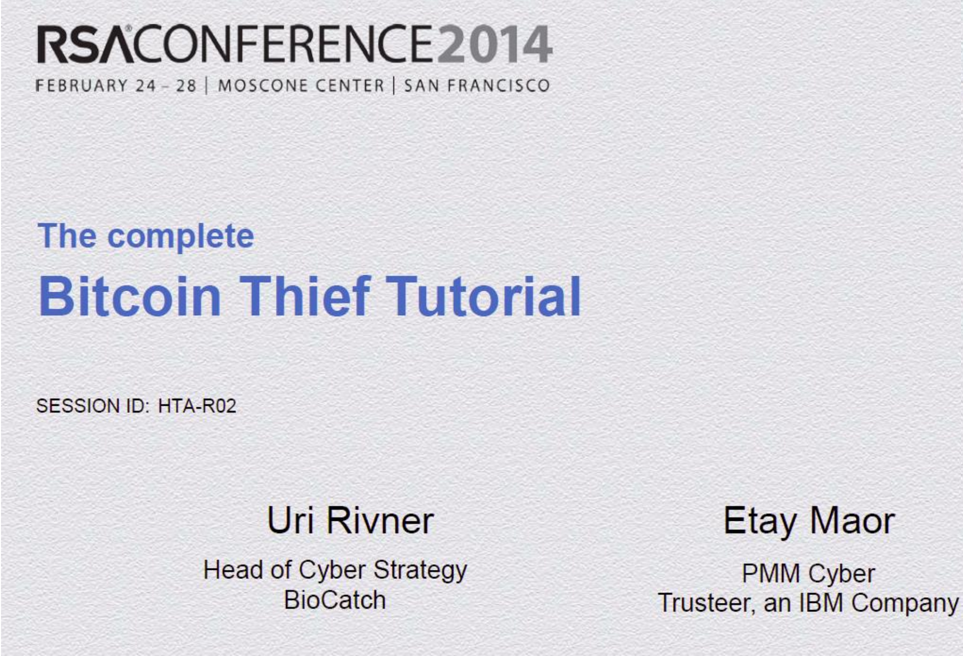
Adi Shamir
“S” of RSA

Whit Diffie
“D” of DHKE

http://www.youtube.com/watch?v=gMc9fHvc78Y

Cryptographers' Panel at RSA Conference 2014 [February 24-28]

- Adi Shamir (R **S** A)
  - "It was supposed to be a decentralized system, which no one would be in control of. It turns out that there were a few organizations which, a few exchanges which dominated the market. Almost nobody can mine Bitcoins at the moment. So if you want to make any money out of the mining operation, you have to buy these very very expensive ASICs. And therefore again, it's highly centralized."
  - "If you think about how many cases are reported, in which Bitcoins are stolen from computers – from electronic wallets kept in your computer – it shows that the currency on the Internet cannot be kept on the Internet, which I find very ironic."
- Whit Diffie (**Diffie**-Hellman Key Exchange)
  - "I thought indeed in its original vision as a totally decentralized thing, that was tremendously exciting. I mean we've been trying, we've been chasing, […] decentralized, anonymous, this, that, and the other electronic banking; now for about three decades. So this struck me as a big leap forward in that direction. And Bitcoin […] needn't be perfect as a design, there are related designs that attempt to debug it. The kind of centralization you're talking about is very hard to eliminate in anything."
- [See Appendix for complete script]



RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

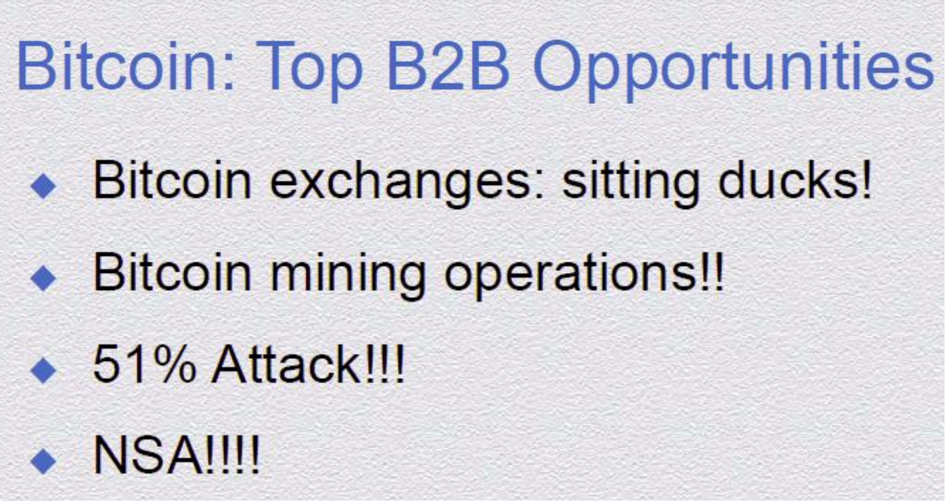
The complete

Bitcoin Thief Tutorial

SESSION ID: HTA-R02

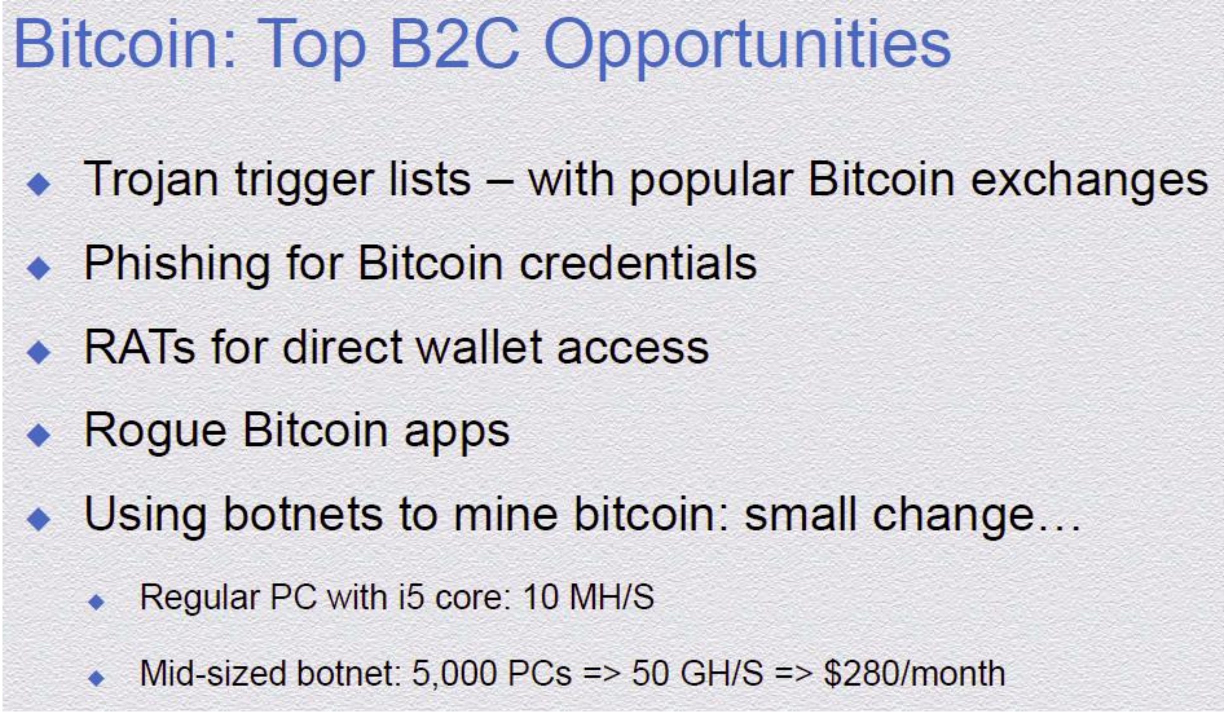
Uri Rivner
Head of Cyber Strategy
BioCatch

Etay Maor
PMM Cyber
Trusteer, an IBM Company



Bitcoin: Top B2B Opportunities

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

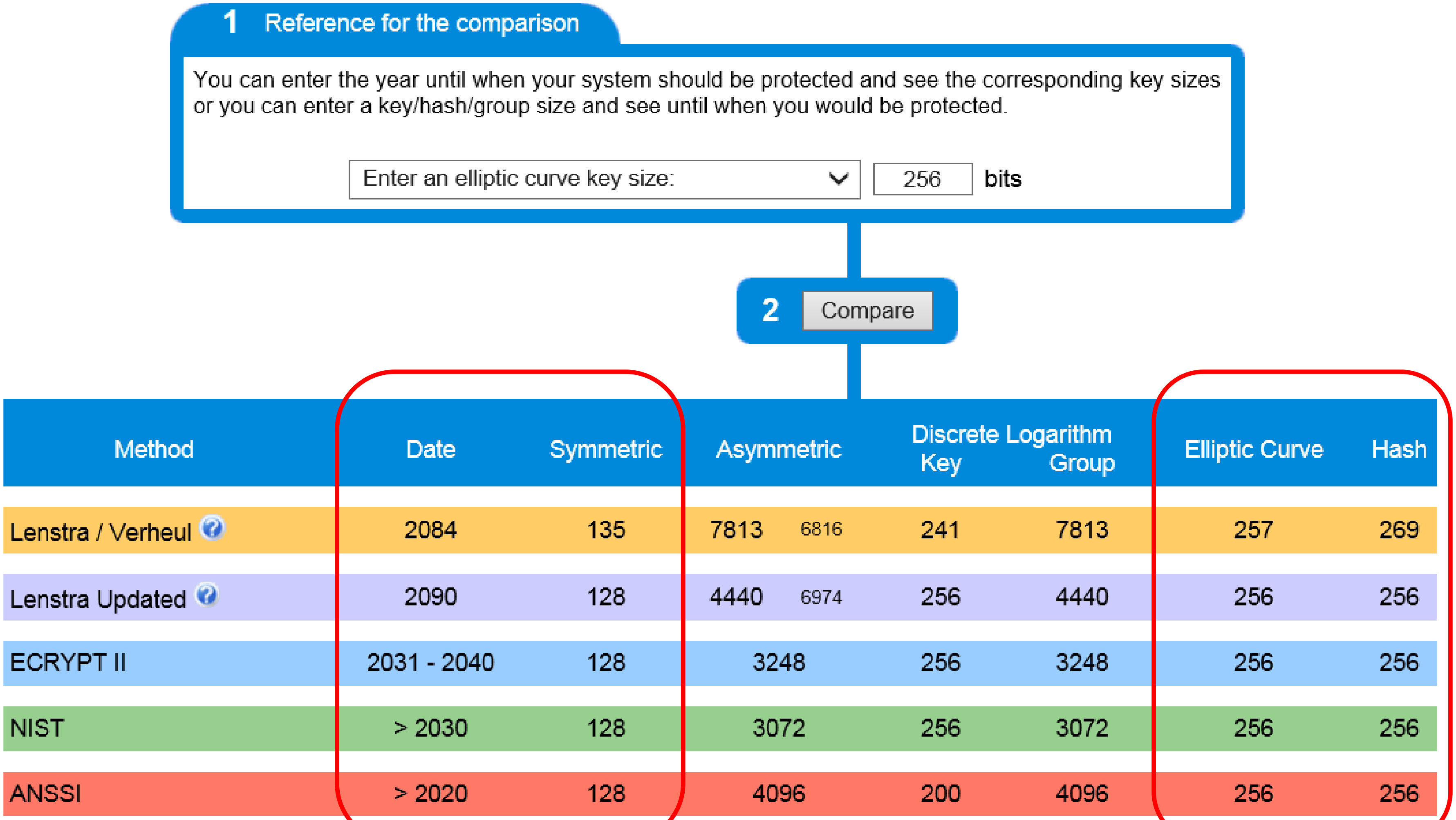


Bitcoin: Top B2C Opportunities

- 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

http://www.rsaconference.com/events/us14/agenda/sessions/973/bitcoin-is-here-how-to-become-a-successful-bitcoin

Security Level: 128 Bits (Complexity 2^{128})



1 Reference for the comparison

You can enter the year until when your system should be protected and see the corresponding key sizes or you can enter a key/hash/group size and see until when you would be protected.

Enter an elliptic curve key size: 256 bits

2 Compare

Method	Date	Symmetric	Asymmetric		Discrete Logarithm		Elliptic Curve	Hash
					Key	Group		
Lenstra / Verheul	2084	135	7813	6816	241	7813	257	269
Lenstra Updated	2090	128	4440	6974	256	4440	256	256
ECRYPT II	2031 - 2040	128	3248		256	3248	256	256
NIST	> 2030	128	3072		256	3072	256	256
ANSSI	> 2020	128	4096		200	4096	256	256

http://www.keylength.com

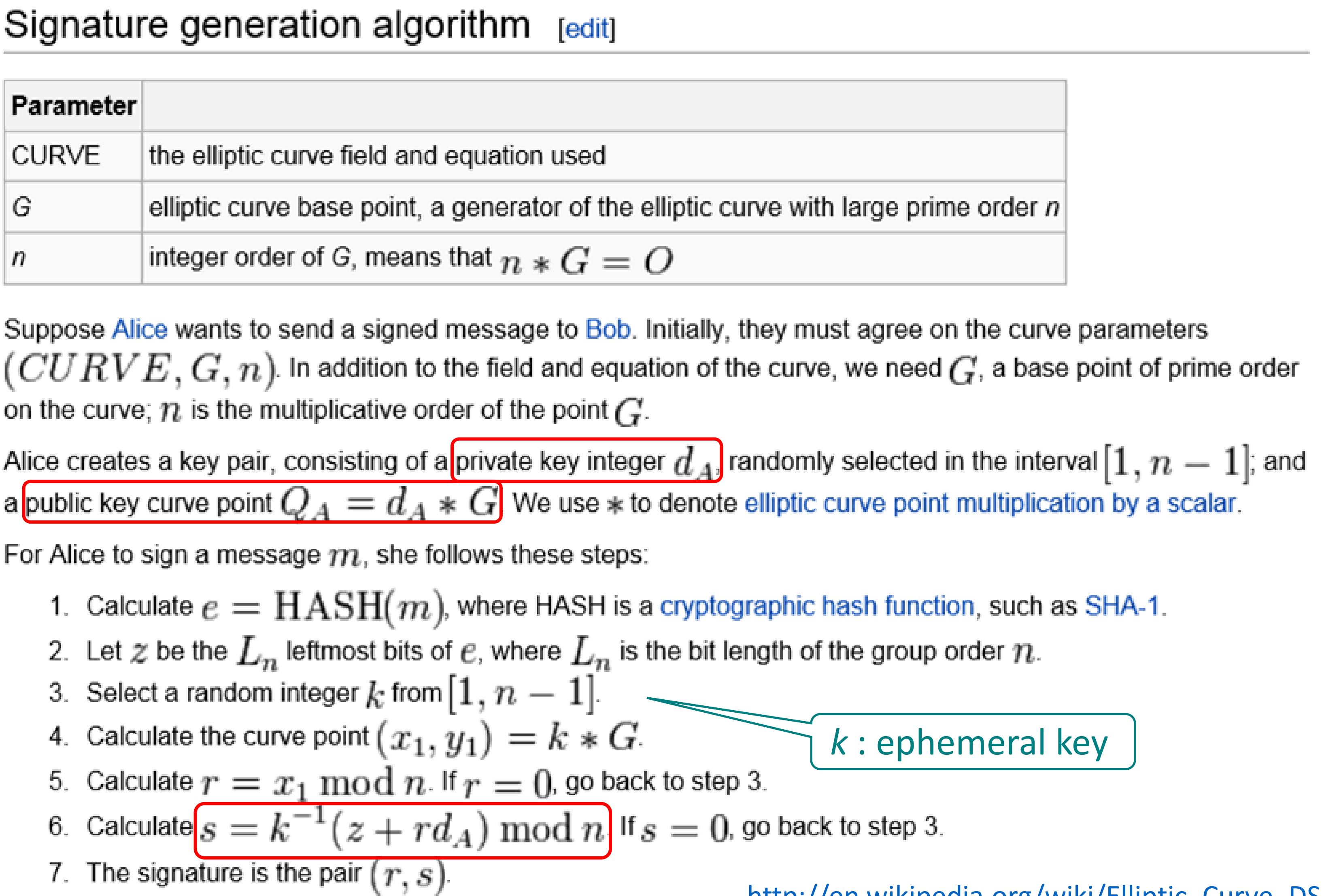
NSA Suite B Cryptography

Algorithm	Function	Specification	Parameters
ECDSA	Digital Signature	FIPS Pub 186-4	**Curve P-256 for SECRET** Curve P-384 for TOP SECRET
SHA	Hashing	FIPS Pub 180-4	**SHA-256 for SECRET** SHA-384 for TOP SECRET

http://www.nsa.gov/ia/programs/suiteb_cryptography

- The strength of Bitcoin crypto primitives is equivalent to that for protecting classified information of the USA government up to the SECRET level
- Almost all the possible problems of Bitcoin come from its **implementations**, though the Bitcoin protocol looks perfect and its cryptography is strong enough

Signing of ECDSA



Signature generation algorithm [edit]

Parameter	
CURVE	the elliptic curve field and equation used
G	elliptic curve base point, a generator of the elliptic curve with large prime order *n*
n	integer order of G, means that $n * G = O$

Suppose Alice wants to send a signed message to Bob. Initially, they must agree on the curve parameters $(CURVE, G, n)$. In addition to the field and equation of the curve, we need G, a base point of prime order on the curve; n is the multiplicative order of the point G.

Alice creates a key pair, consisting of a $\boxed{\text{private key integer } d_A}$, randomly selected in the interval $[1, n-1]$; and a $\boxed{\text{public key curve point } Q_A = d_A * G}$. We use $*$ to denote elliptic curve point multiplication by a scalar.

For Alice to sign a message m, she follows these steps:

1. Calculate $e = \mathrm{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-1.
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Select a random integer k from $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = k * G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3.
6. Calculate $\boxed{s = k^{-1}(z + r d_A) \bmod n}$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s).

k : ephemeral key

http://en.wikipedia.org/wiki/Elliptic_Curve_DSA

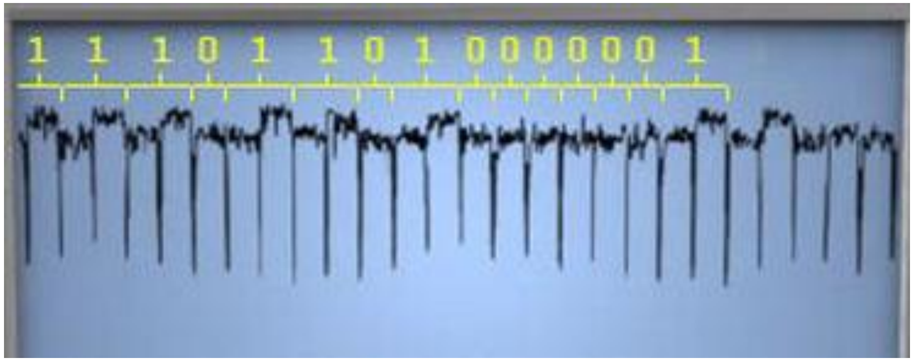
Random Number Generators (RNG)

- With DSA/ECDSA, the **entropy**, **secrecy**, and **uniqueness** of the **random ephemeral key *k*** is critical
  - Violating any one of the above three requirements can reveal the entire private key to an attacker
  - Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA/ECDSA
- [December 2010] The ECDSA private key used by **Sony** to sign software for the **PlayStation 3** game console was recovered, because Sony implemented *k* as static instead of random
- [August 2013] Bugs in some implementations of the Java class *SecureRandom* sometimes generated collisions in *k*, allowing in stealing **bitcoins** from the containing wallet on **Android app**
- This issue can be prevented by deriving *k* deterministically from the **private key** and the **message hash**, as described by **RFC 6979**

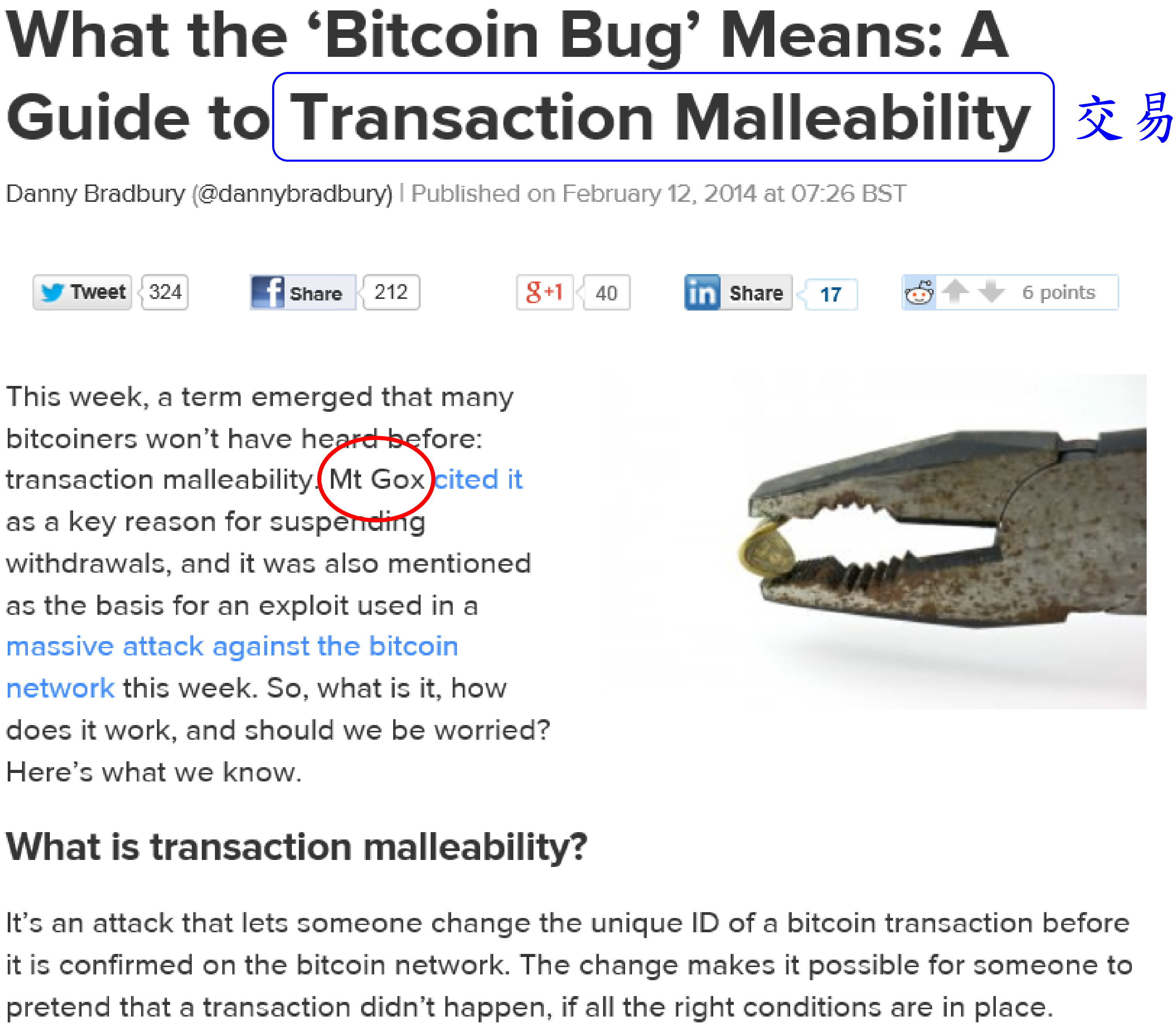
http://en.wikipedia.org/wiki/Digital_Signature_Algorithm http://en.wikipedia.org/wiki/Elliptic_Curve_DSA

Side Channel Attacks (SCA)

- A side channel attack is based on information gained from the physical implementation of a cryptosystem
  - e.g., timing information, power consumption, electromagnetic leaks, or even sound
- "Almost every smart card you buy today is going to have countermeasures to Simple Power Analysis (SPA) and Differential Power Analysis (DPA)," said Benjamin Jun, vice president of technology at Cryptography Research, Inc. (CRI); however, some newer implementations of Elliptic Curve Cryptosystems (ECC) "do in fact leak information."



http://www.cnet.com/news/workshop-exposes-deficiencies-of-electronic-encryption



What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability

交易延展

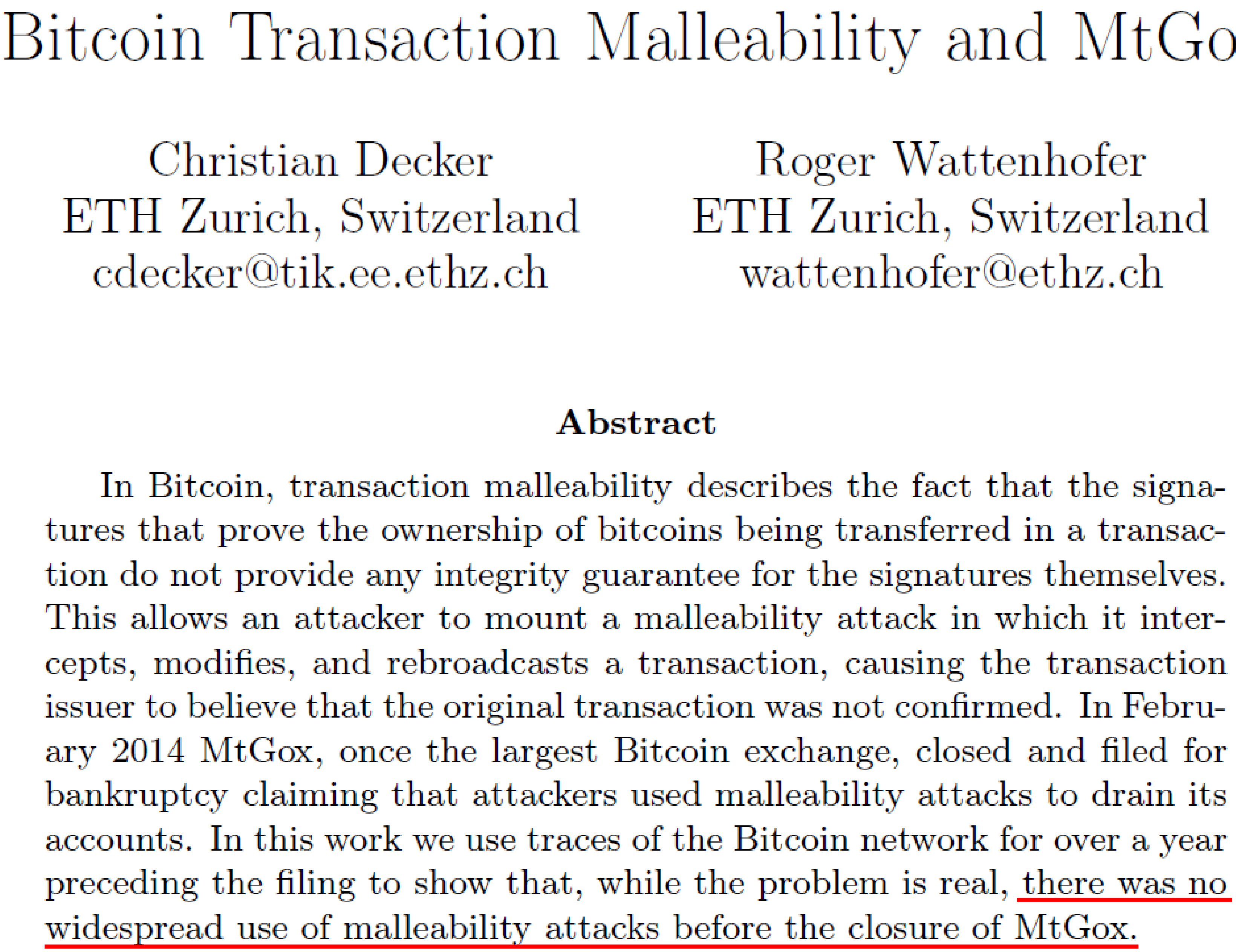
Danny Bradbury (@dannybradbury) | Published on February 12, 2014 at 07:26 BST

This week, a term emerged that many bitcoiners won't have heard before: transaction malleability. Mt Gox cited it as a key reason for suspending withdrawals, and it was also mentioned as the basis for an exploit used in a massive attack against the bitcoin network this week. So, what is it, how does it work, and should we be worried? Here's what we know.

What is transaction malleability?

It's an attack that lets someone change the unique ID of a bitcoin transaction before it is confirmed on the bitcoin network. The change makes it possible for someone to pretend that a transaction didn't happen, if all the right conditions are in place.

http://www.coindesk.com/bitcoin-bug-guide-transaction-malleability



Bitcoin Transaction Malleability and MtGox

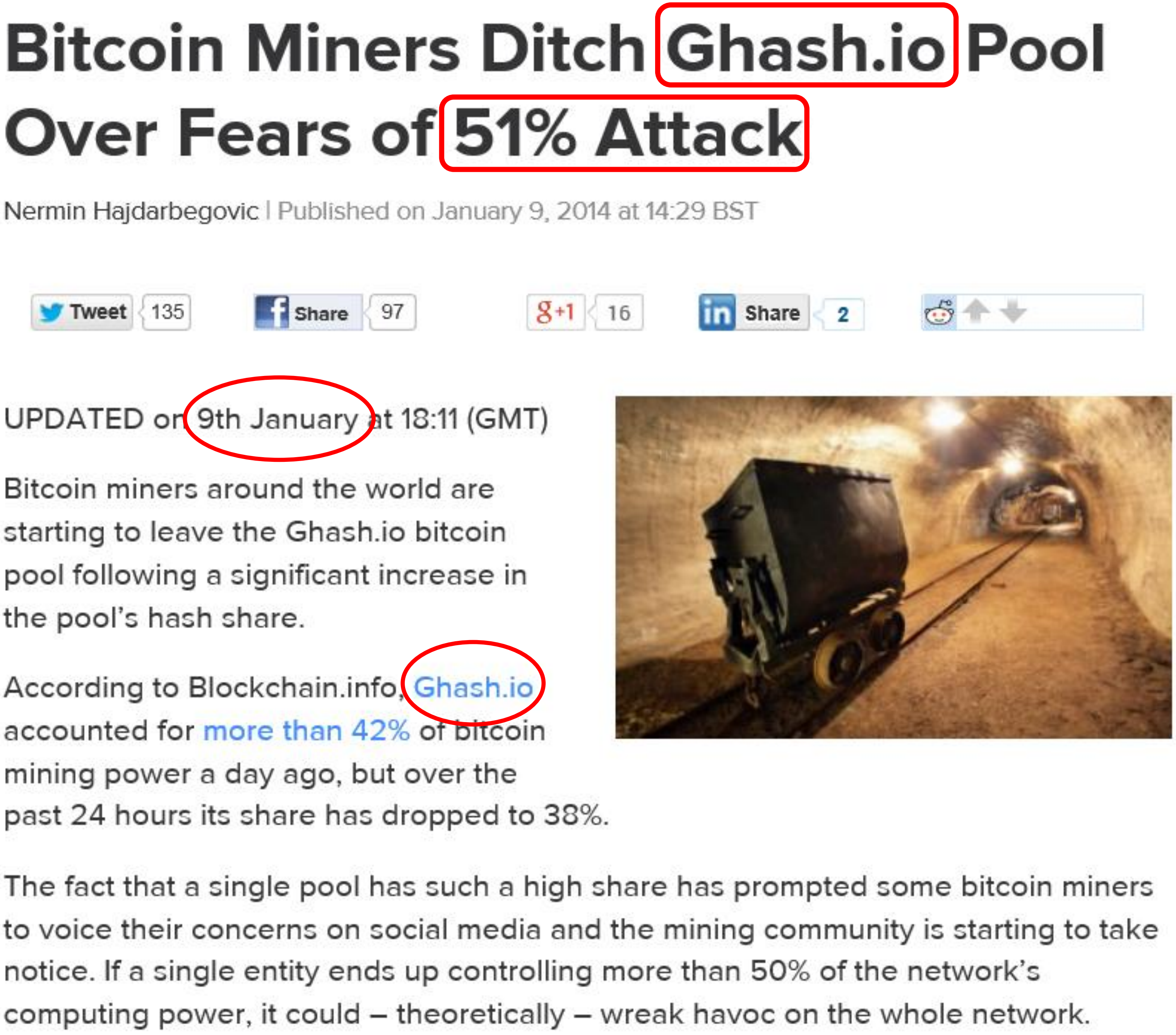
Christian Decker
ETH Zurich, Switzerland
cdecker@tik.ee.ethz.ch

Roger Wattenhofer
ETH Zurich, Switzerland
wattenhofer@ethz.ch

Abstract

In Bitcoin, transaction malleability describes the fact that the signatures that prove the ownership of bitcoins being transferred in a transaction do not provide any integrity guarantee for the signatures themselves. This allows an attacker to mount a malleability attack in which it intercepts, modifies, and rebroadcasts a transaction, causing the transaction issuer to believe that the original transaction was not confirmed. In February 2014 MtGox, once the largest Bitcoin exchange, closed and filed for bankruptcy claiming that attackers used malleability attacks to drain its accounts. In this work we use traces of the Bitcoin network for over a year preceding the filing to show that, while the problem is real, there was no widespread use of malleability attacks before the closure of MtGox.

http://arxiv.org/pdf/1403.6676v1.pdf



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

Nermin Hajdarbegovic | Published on January 9, 2014 at 14:29 BST

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.

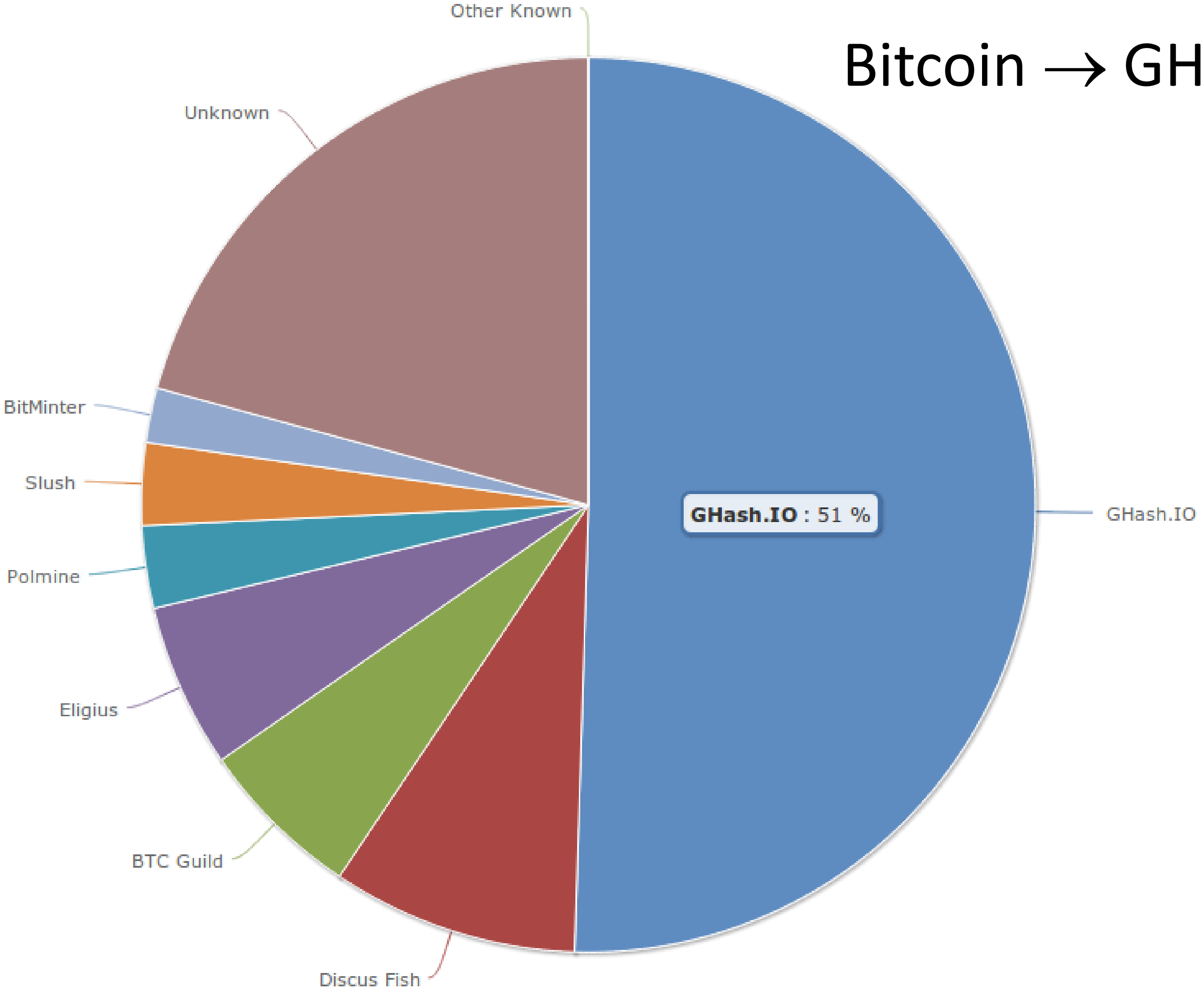
According to Blockchain.info, Ghash.io accounted for more than 42% of bitcoin mining power a day ago, but over the past 24 hours its share has dropped to 38%.

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.

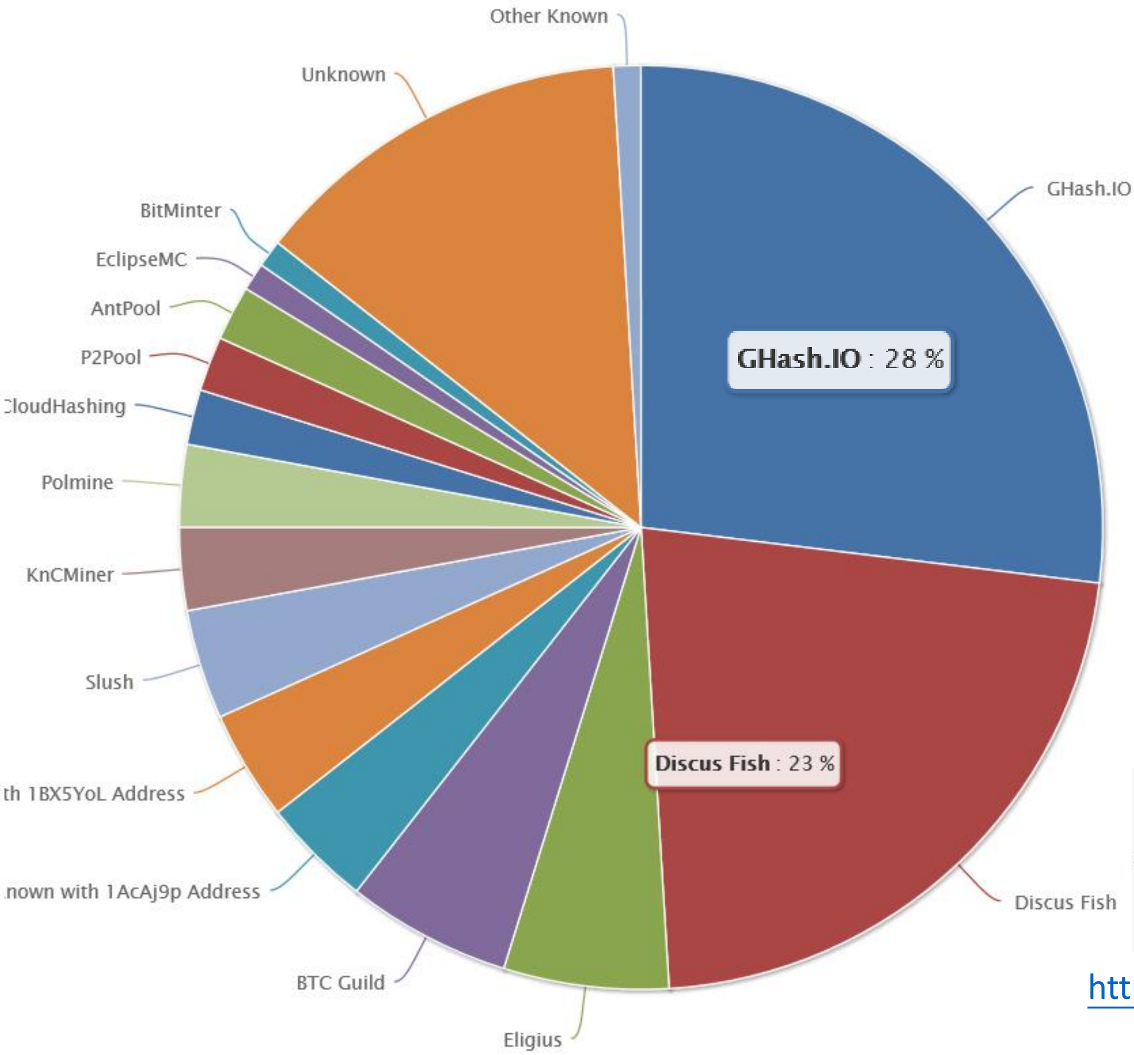
http://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack

Bitcoin's "Doomsday"? (June 14, 2014)

Bitcoin → GHashcoin?

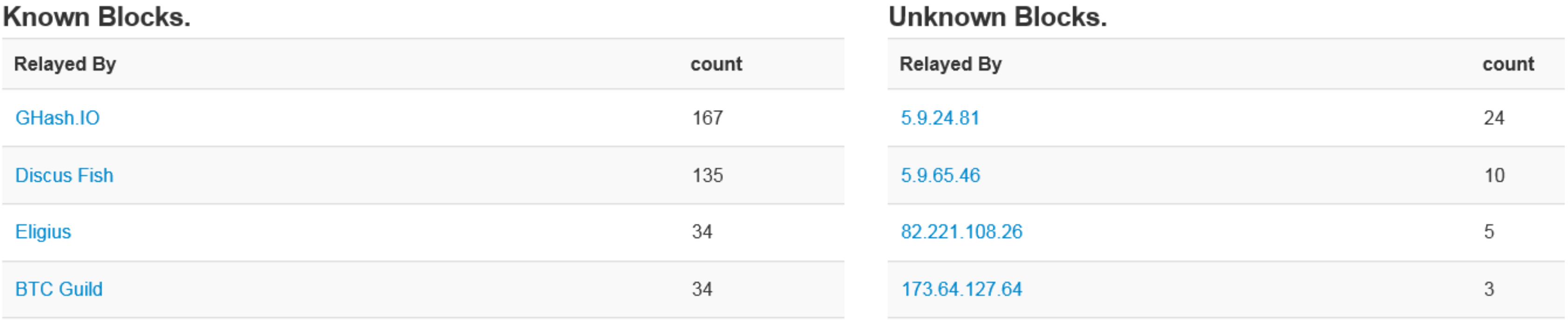


http://news.list-online.com/prices-fall-as-bitcoin-confronts-doomsday-scenario-business-insider



August 17, 2014

https://blockchain.info/pools?timespan=4days



Known Blocks.

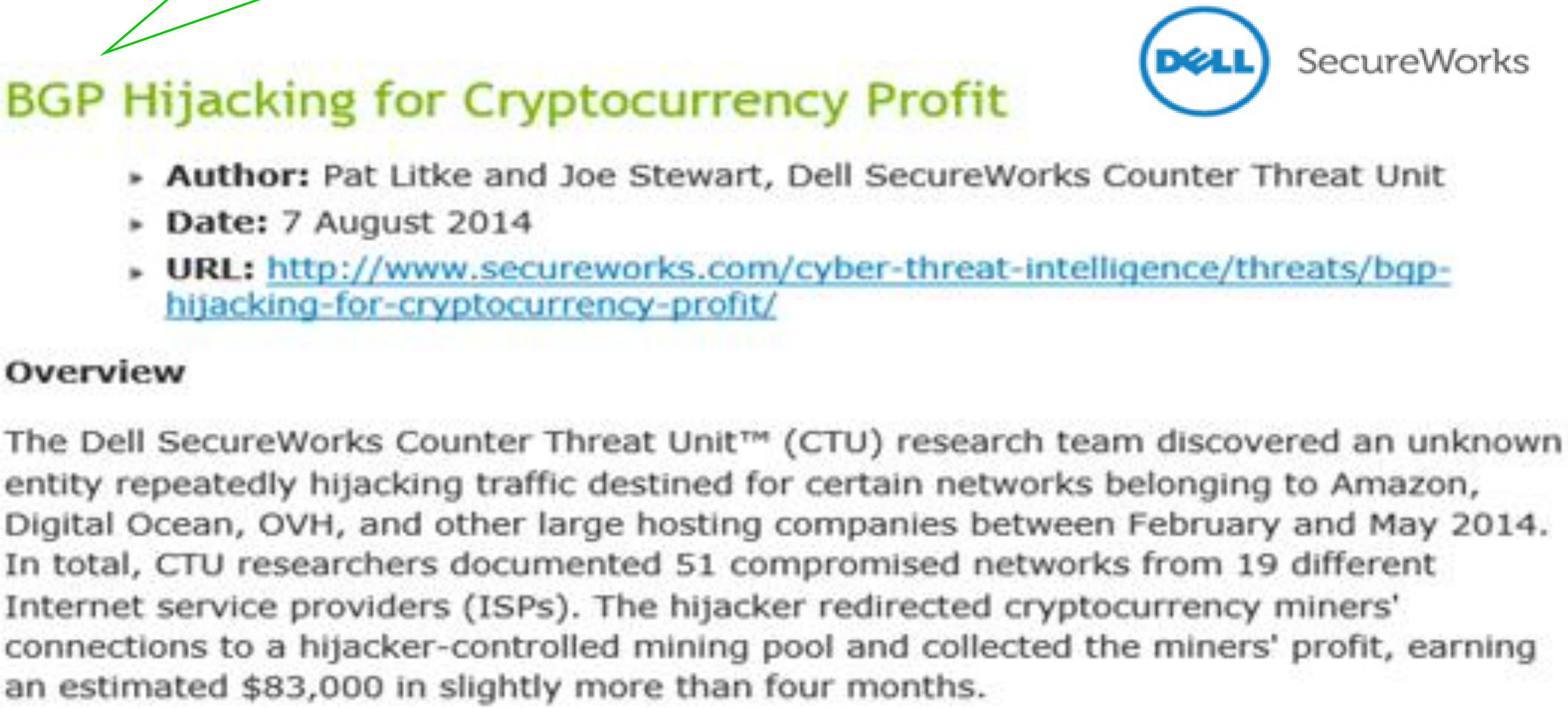
Relayed By	count
GHash.IO	167
Discus Fish	135
Eligius	34
BTC Guild	34

Unknown Blocks.

Relayed By	count
5.9.24.81	24
5.9.65.46	10
82.221.108.26	5
173.64.127.64	3

Internet Traffic Hijacking

Border Gateway Protocol



DELL SecureWorks

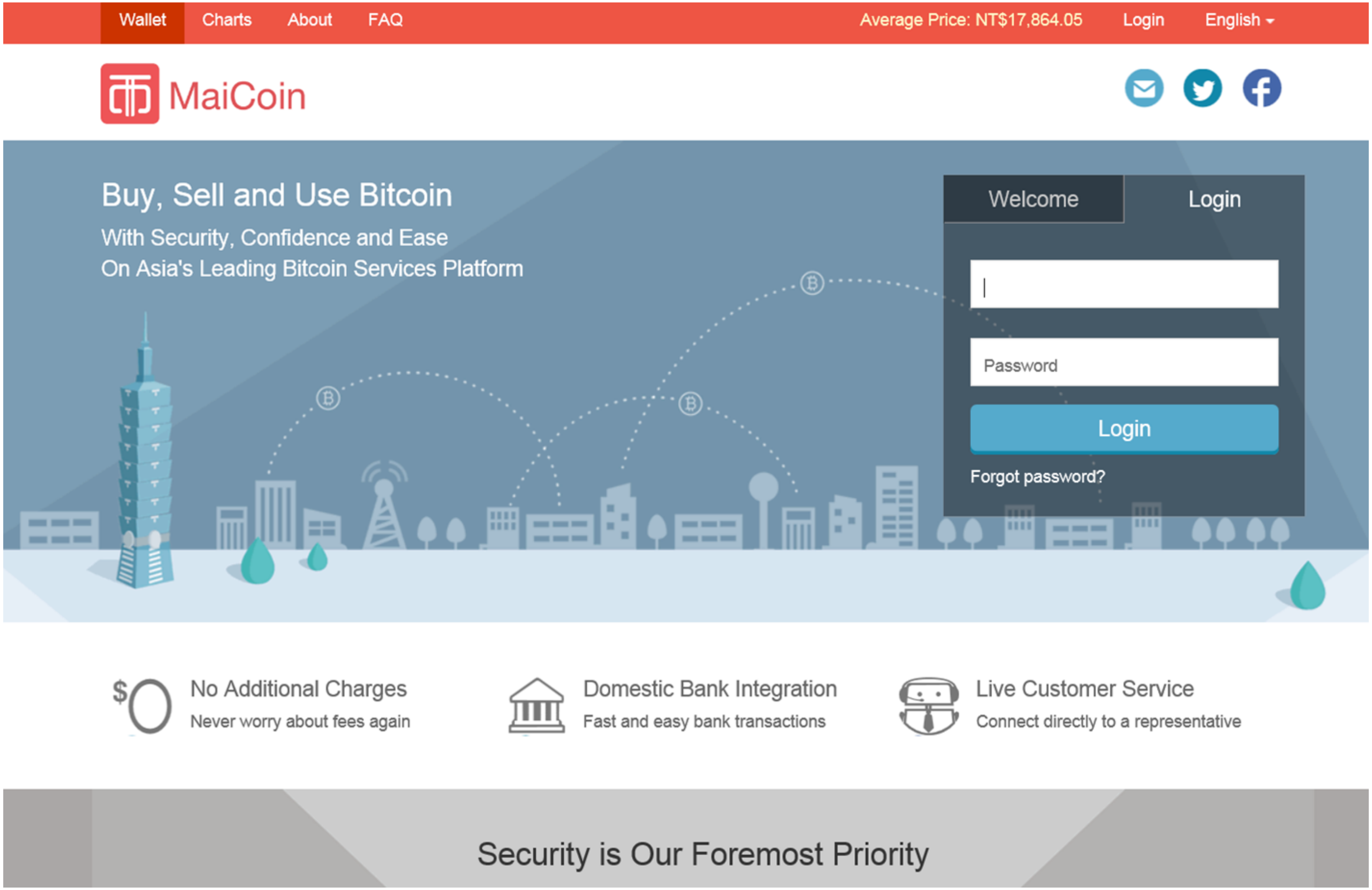
BGP Hijacking for Cryptocurrency Profit

- **Author:** Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit
- **Date:** 7 August 2014
- **URL:** http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/

Overview

The Dell SecureWorks Counter Threat Unit™ (CTU) research team discovered an unknown entity repeatedly hijacking traffic destined for certain networks belonging to Amazon, Digital Ocean, OVH, and other large hosting companies between February and May 2014. In total, CTU researchers documented 51 compromised networks from 19 different Internet service providers (ISPs). The hijacker redirected cryptocurrency miners' connections to a hijacker-controlled mining pool and collected the miners' profit, earning an estimated $83,000 in slightly more than four months.

Security of Exchange Platform



Buy, Sell and Use Bitcoin

With Security, Confidence and Ease
On Asia's Leading Bitcoin Services Platform

No Additional Charges
Never worry about fees again

Domestic Bank Integration
Fast and easy bank transactions

Live Customer Service
Connect directly to a representative

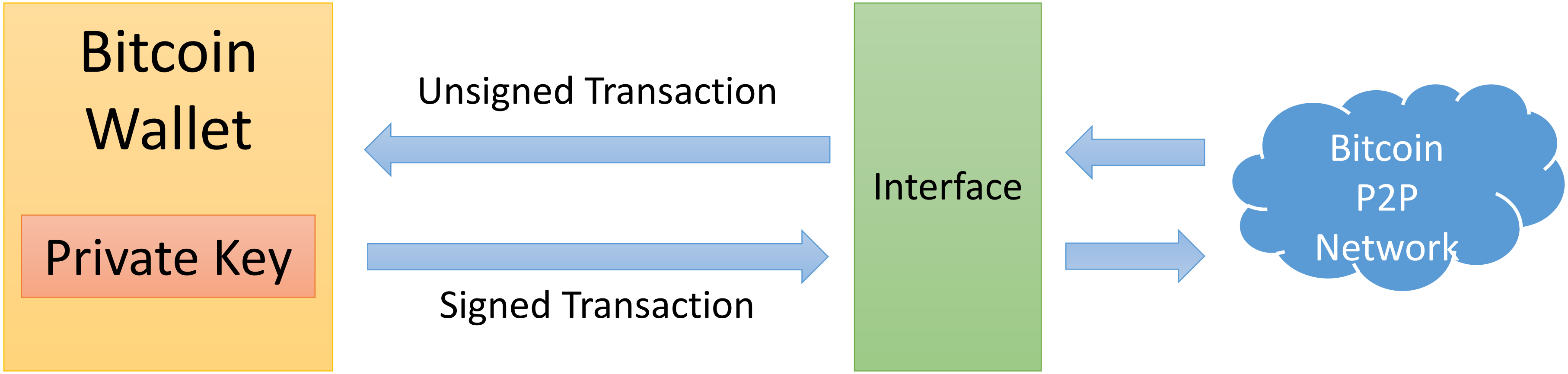
Security is Our Foremost Priority

https://www.maicoin.com

Agenda

- Introduction to Bitcoin
- Security of Bitcoin
- Hardware Wallet
  - What is Bitcoin Wallet?
  - How to Secure Bitcoin Wallets?
  - Introduction to Hardware Wallets
  - Scenario of Using the Proposed Hardware Wallet
  - Demo of the Proposed Hardware Wallet

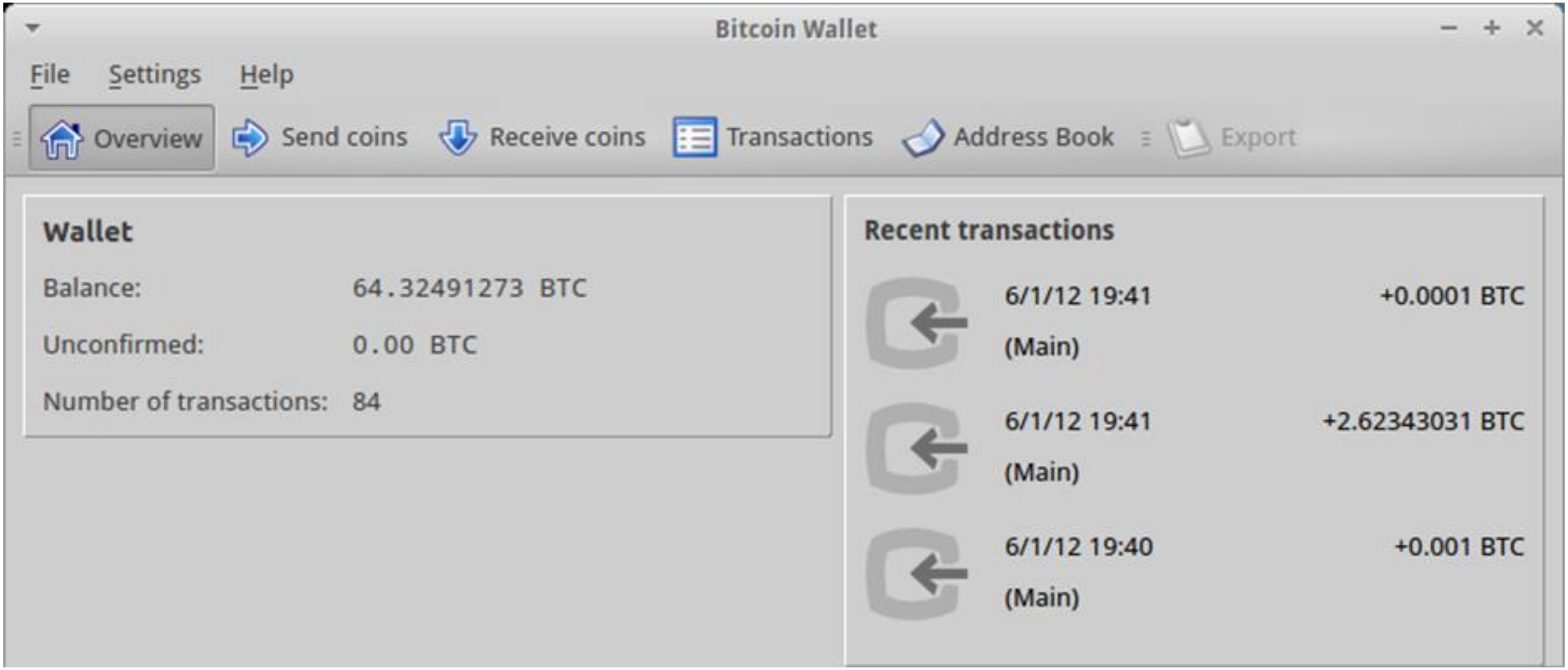
Using a Bitcoin Wallet



What is Bitcoin Wallet?

- A set of Bitcoin *private keys* & associated *addresses*
  - It can transfer Bitcoin to receivers
  - It can receive Bitcoin from somebody else
  - It can show the balance
- Hot Storage
  - Software Wallet
  - Web Wallet
- Cold Storage
  - Paper Wallet
  - Hardware Wallet

Software Wallet
(PC Program / Mobile App)



Wallet

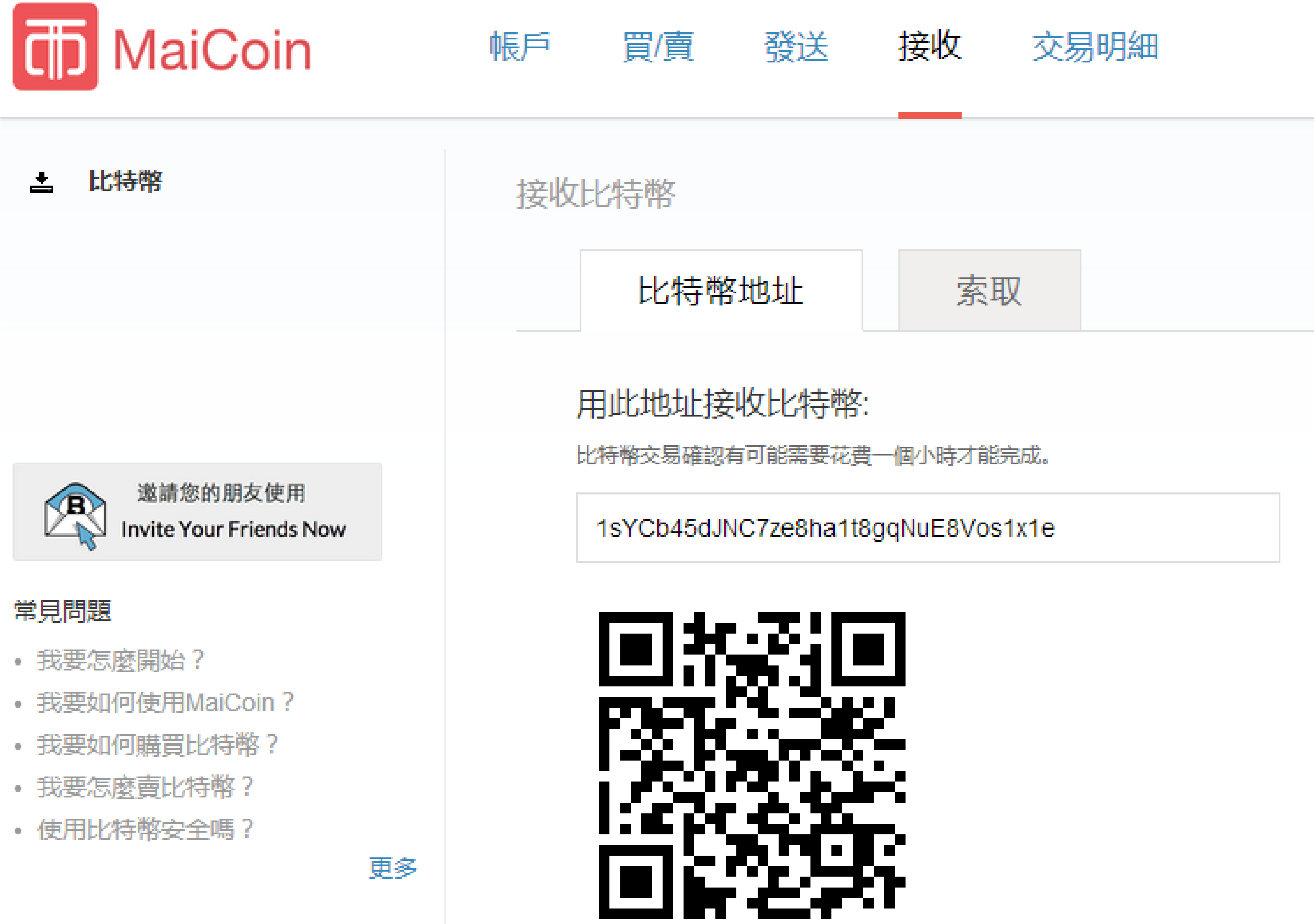
Balance:	64.32491273 BTC
Unconfirmed:	0.00 BTC
Number of transactions:	84

Recent transactions

6/1/12 19:41 (Main)	+0.0001 BTC
6/1/12 19:41 (Main)	+2.62343031 BTC
6/1/12 19:40 (Main)	+0.001 BTC

The screenshot of Bitcoin Core – https://bitcoin.org/en/download

Web Wallet



MaiCoin

帳戶 買/賣 發送 接收 交易明細

比特幣

接收比特幣

比特幣地址 索取

用此地址接收比特幣:

比特幣交易確認有可能需要花費一個小時才能完成。

1sYCb45dJNC7ze8ha1t8gqNuE8Vos1x1e

邀請您的朋友使用
Invite Your Friends Now

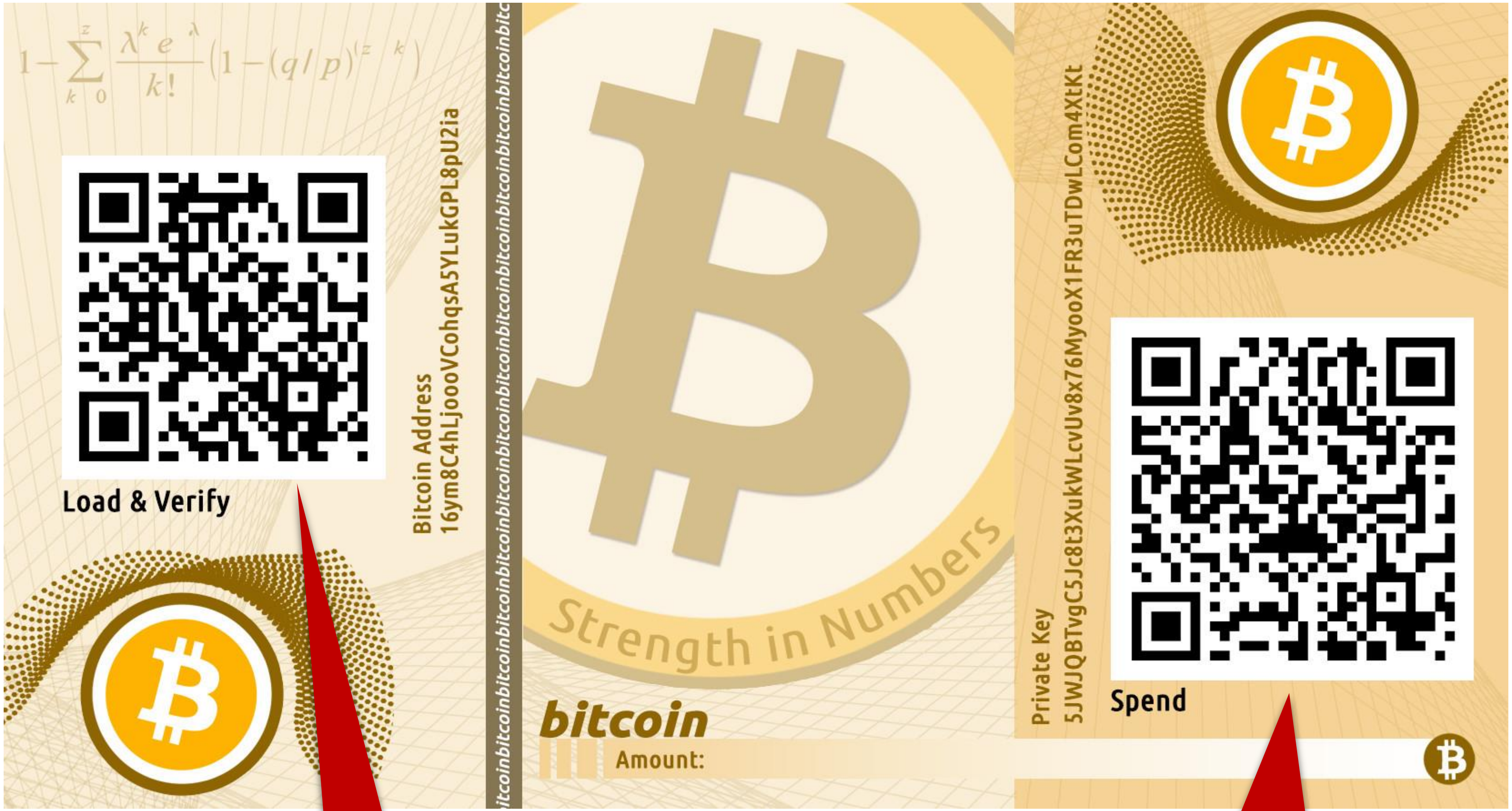
常見問題

- 我要怎麼開始？
- 我要如何使用MaiCoin？
- 我要如何購買比特幣？
- 我要怎麼賣比特幣？
- 使用比特幣安全嗎？

更多

https://www.maicoin.com

Paper Wallet


Load & Verify
Bitcoin Address
16ym8C4hLjoooVCohqsA5YLukGPL8pU2ia
Strength in Numbers
bitcoin
Amount:
Private Key
5JWJQBTvgC5Jc8t3XukWLcvUv8x76MyooX1FR3uTDwLCom4XtKt
Spend

Bitcoin Address

Bitcoin Private Key

https://blog.safello.com/index.php/2014/02/13/how-to-redeem-and-use-a-bitcoin-paper-wallet

Piper

Piper is the most secure and easy-to-use **Bitcoin paper wallet printer**
Learn More
bitcoin
Piper

"Paper wallets are universally regarded as the most secure way to store bitcoin"

"Piper makes creating paper wallets as easy as pressing a button"

"If you invest in bitcoin ... it could be a lifesaver."

http://cryptographi.com

How to Secure Bitcoin Wallets?

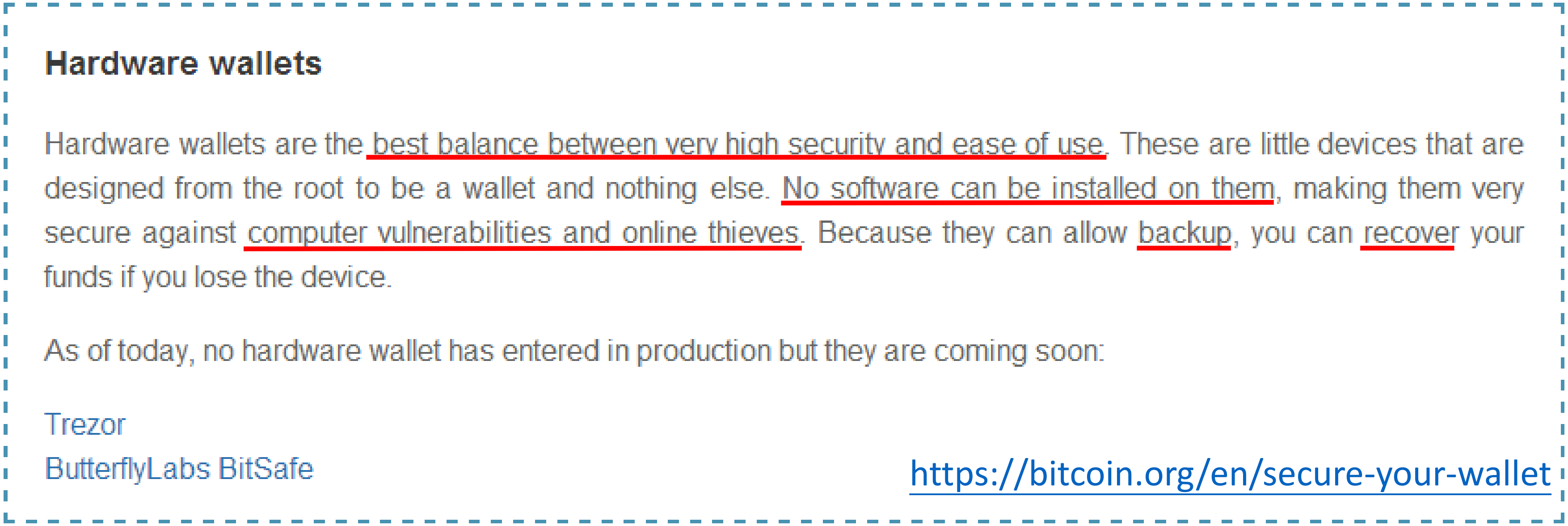
- Backup the wallet
  - Backup entire wallet
  - Encrypt online backups
  - Use many secure locations
  - Make regular backups
- Encrypt the wallet
  - User a strong password and never forget it
- Keep the software up to date

https://bitcoin.org/en/secure-your-wallet

Hack
How to ~~Secure~~ Bitcoin Wallets?

- Backup the wallet → **Steal User’s File**
  - Backup entire wallet
  - Encrypt online backups
  - Use many secure locations
  - Make regular backups
- Encrypt the wallet → **Brute Force / Key Logger / Social Engineering / …**
  - User a strong password and never forget it
- Keep the software up to date → **Fake Update Site**
- Offline wallet for savings → **Need More Work ☺**
  - **Offline transaction signing**
  - **Hardware wallets**

Hardware Wallets



Hardware wallets

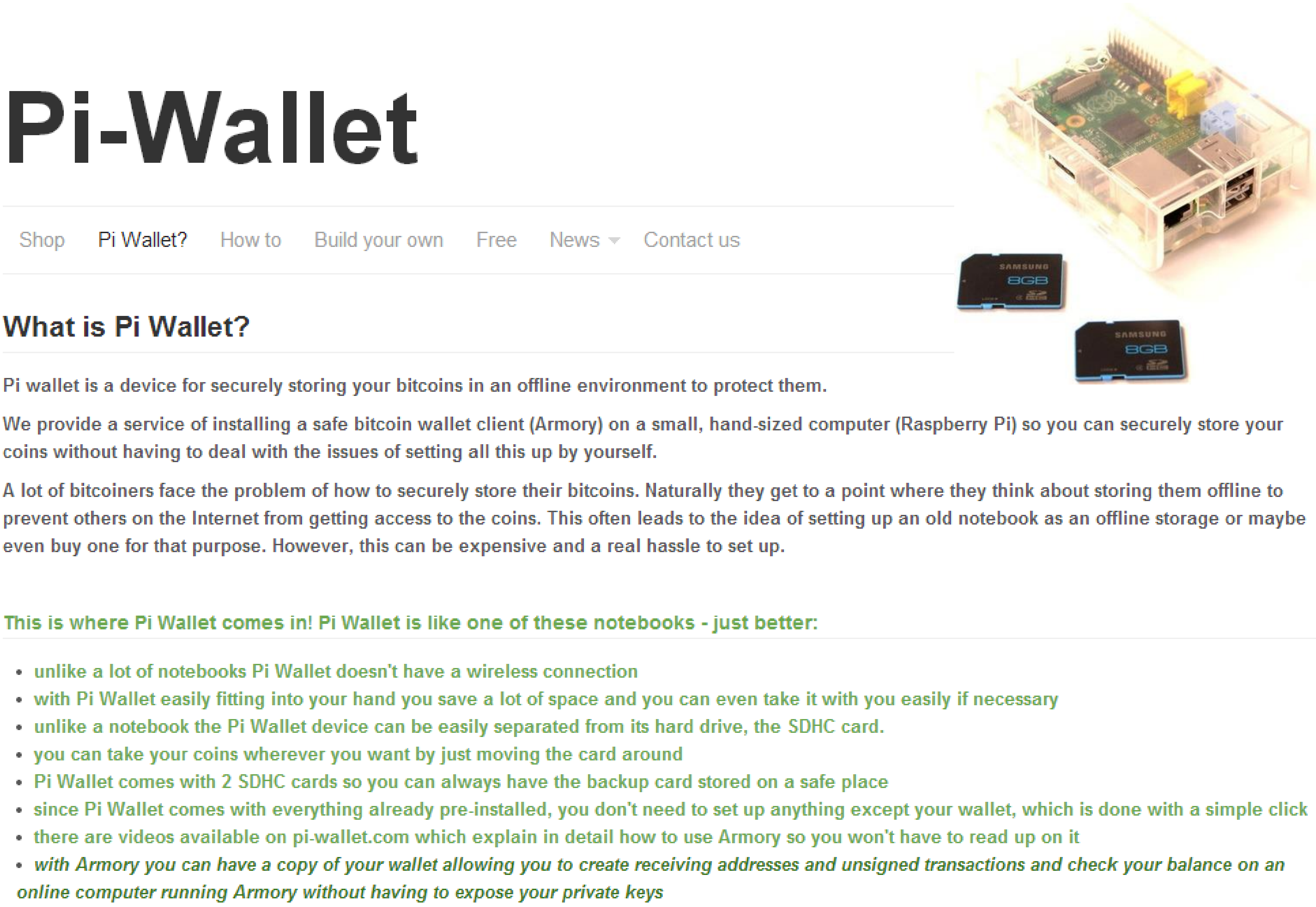
Hardware wallets are the best balance between very high security and ease of use. These are little devices that are designed from the root to be a wallet and nothing else. No software can be installed on them, making them very secure against computer vulnerabilities and online thieves. Because they can allow backup, you can recover your funds if you lose the device.

As of today, no hardware wallet has entered in production but they are coming soon:

Trezor
ButterflyLabs BitSafe

https://bitcoin.org/en/secure-your-wallet

- Best balance between very high secure and ease of use
- No software can be installed on them
  - Very secure against computer vulnerabilities
- Backup and Recovery



Pi-Wallet

What is Pi Wallet?

Pi wallet is a device for securely storing your bitcoins in an offline environment to protect them.

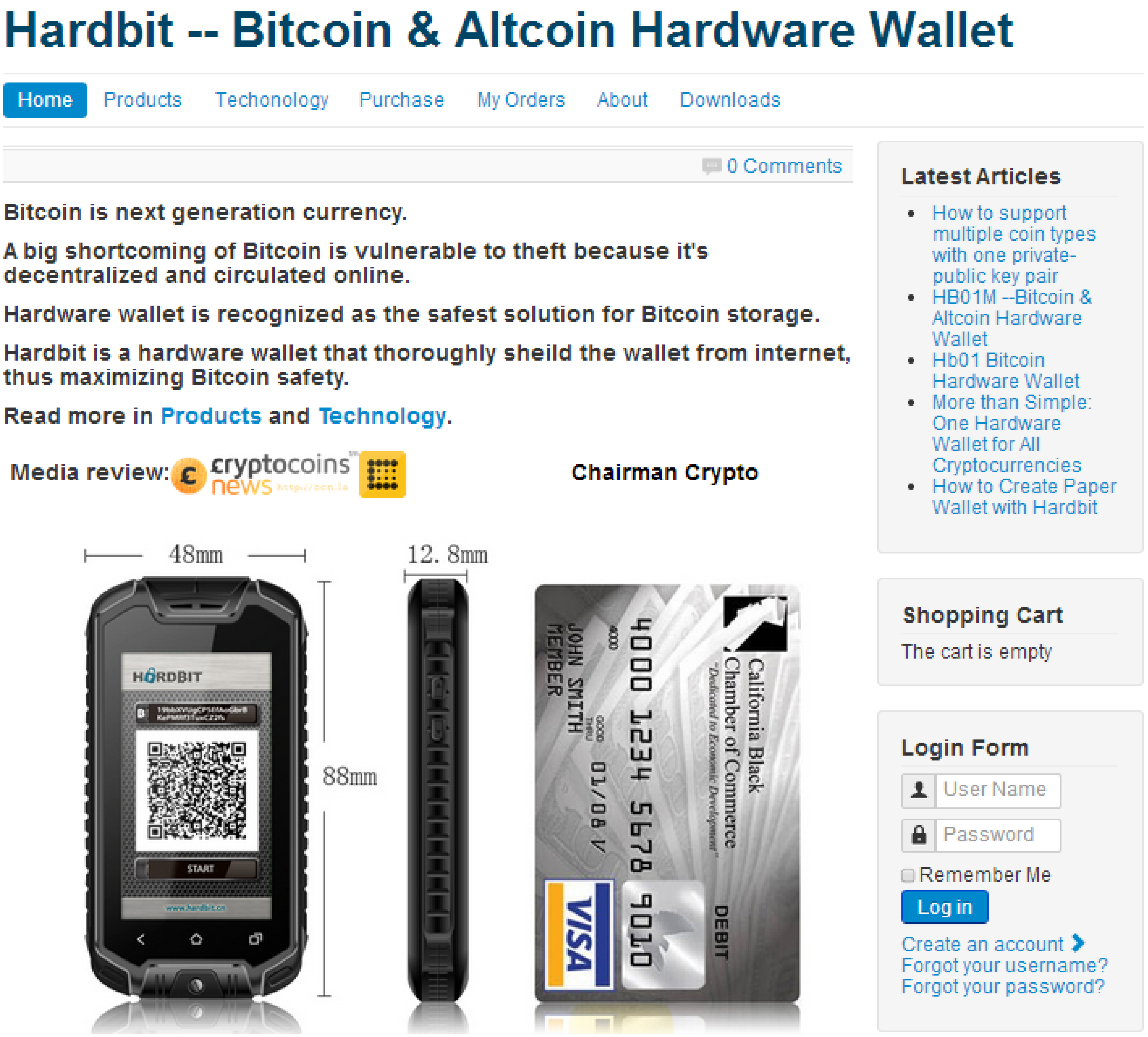
We provide a service of installing a safe bitcoin wallet client (Armory) on a small, hand-sized computer (Raspberry Pi) so you can securely store your coins without having to deal with the issues of setting all this up by yourself.

A lot of bitcoiners face the problem of how to securely store their bitcoins. Naturally they get to a point where they think about storing them offline to prevent others on the Internet from getting access to the coins. This often leads to the idea of setting up an old notebook as an offline storage or maybe even buy one for that purpose. However, this can be expensive and a real hassle to set up.

This is where Pi Wallet comes in! Pi Wallet is like one of these notebooks - just better:

- unlike a lot of notebooks Pi Wallet doesn't have a wireless connection
- with Pi Wallet easily fitting into your hand you save a lot of space and you can even take it with you easily if necessary
- unlike a notebook the Pi Wallet device can be easily separated from its hard drive, the SDHC card.
- you can take your coins wherever you want by just moving the card around
- Pi Wallet comes with 2 SDHC cards so you can always have the backup card stored on a safe place
- since Pi Wallet comes with everything already pre-installed, you don't need to set up anything except your wallet, which is done with a simple click
- there are videos available on pi-wallet.com which explain in detail how to use Armory so you won't have to read up on it
- *with Armory you can have a copy of your wallet allowing you to create receiving addresses and unsigned transactions and check your balance on an online computer running Armory without having to expose your private keys*

http://www.pi-wallet.com



Hardbit -- Bitcoin & Altcoin Hardware Wallet

Home | Products | Techonology | Purchase | My Orders | About | Downloads

0 Comments

Bitcoin is next generation currency.

A big shortcoming of Bitcoin is vulnerable to theft because it's decentralized and circulated online.

Hardware wallet is recognized as the safest solution for Bitcoin storage.

Hardbit is a hardware wallet that thoroughly sheild the wallet from internet, thus maximizing Bitcoin safety.

Read more in Products and Technology.

Media review: cryptocoins news **Chairman Crypto**

Latest Articles

- How to support multiple coin types with one private-public key pair
- HB01M --Bitcoin & Altcoin Hardware Wallet
- Hb01 Bitcoin Hardware Wallet
- More than Simple: One Hardware Wallet for All Cryptocurrencies
- How to Create Paper Wallet with Hardbit

Shopping Cart

The cart is empty

Login Form

User Name

Password

□ Remember Me

Log in

Create an account ›
Forgot your username?
Forgot your password?

http://www.hardbit.cn

Trezor

- Specification
  - 59 x 30 x 6 mm, OLED with 128 x 64 pixels
  - I/O Interface: Micro USB (HID Class), Two buttons
  - Supported software wallet: bitcoincore, MultiBit, …
  - Supported web wallet: blockchain, myTrezor, …
- Security Features
  - Generate private keys internally and never leave it
  - On device transaction signing
  - PIN protection (Dynamic PIN pad)
  - Backup by a seed (BIP0039, Bitcoin Improve Proposal)
  - Open-source include software and hardware

http://www.bitcointrezor.com

Comparison of Hardware Wallets

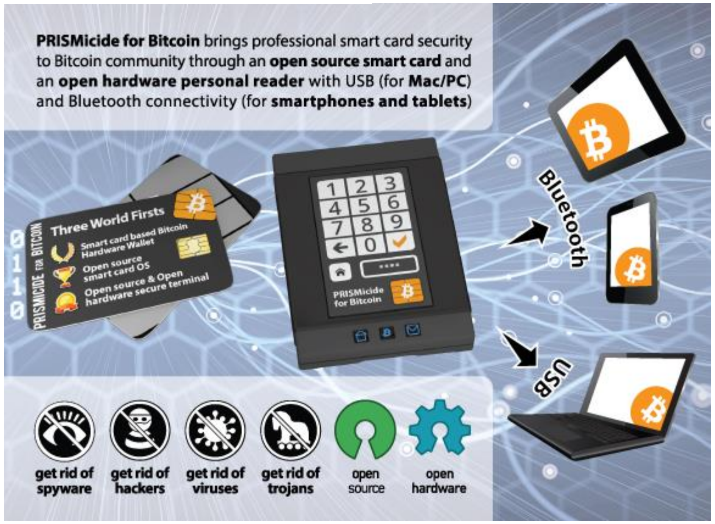
Category		Trezor	Hardbit
Interface	*Communication Interface*	Micro USB	Camera
Security Features	*Store Private Key Security Levels*	Encrypted Flash	Flash
	Backup	Seed	QR Code
	Pin Protection	Special Pin	Input on Device
Software Support	*Wallet Software Integration*	Multi-Bit Electrum Block-chain MyTrezor Web	Customized POS
	Source Code	Open	Closed

Other Hardware Wallets

BitSafe

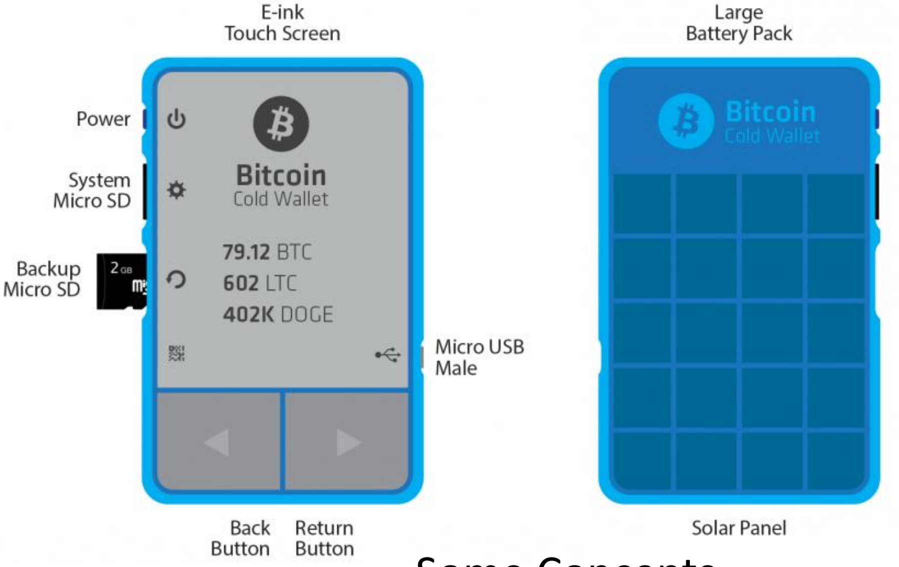
Mycelium Bitcoincard

BTChip

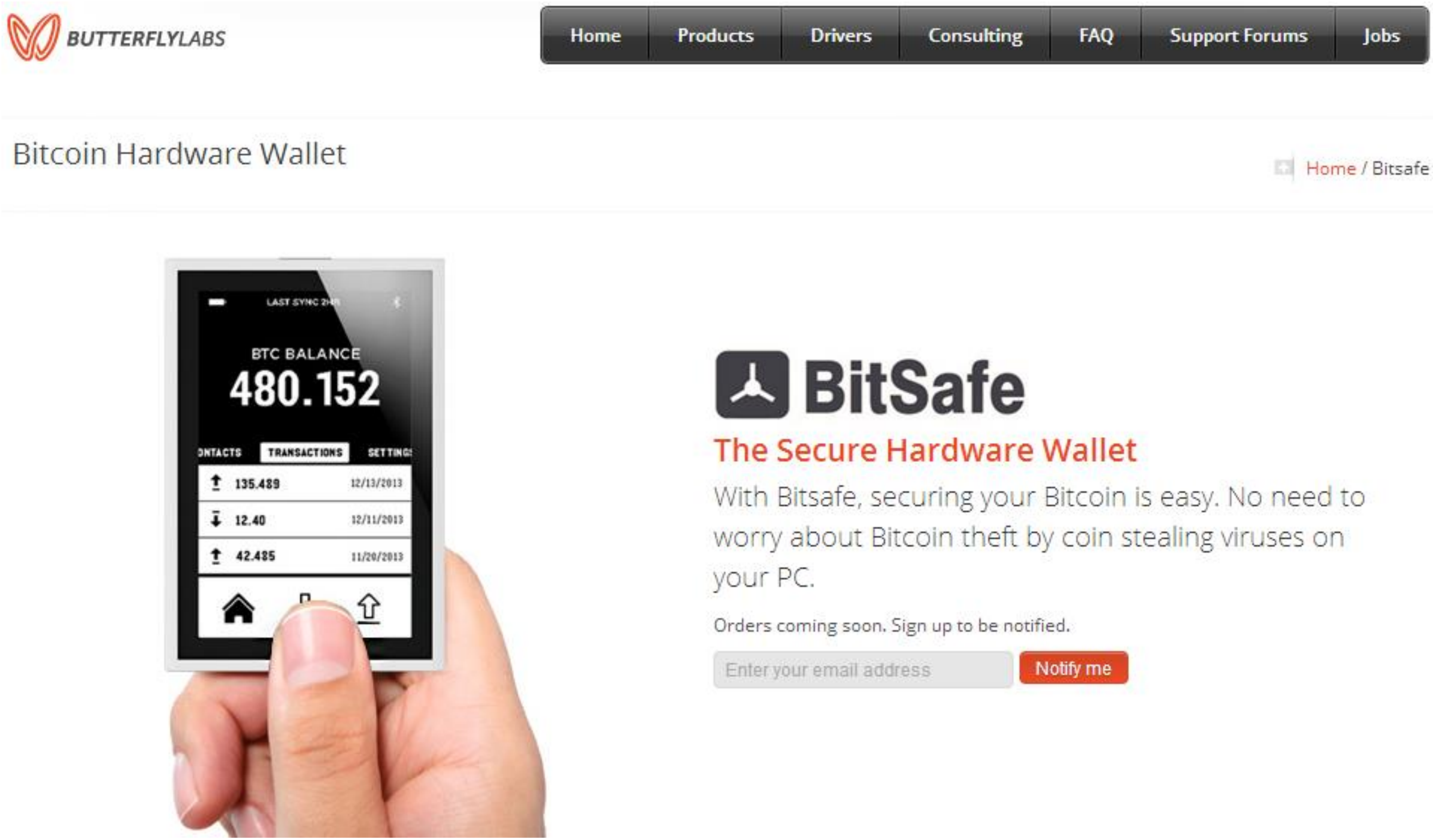


PRISMicide for Bitcoin brings professional smart card security to Bitcoin community through an **open source smart card** and an **open hardware personal reader** with USB (for **Mac/PC**) and Bluetooth connectivity (for **smartphones and tablets**)

PRISMicide



Some Concepts



Bitcoin Hardware Wallet

BitSafe

The Secure Hardware Wallet

With Bitsafe, securing your Bitcoin is easy. No need to worry about Bitcoin theft by coin stealing viruses on your PC.

Orders coming soon. Sign up to be notified.

http://www.butterflylabs.com/bitcoin-hardware-wallet

Mycelium Bitcoincard

The reliability of the **Bitcoin** system is assured primarily by cryptography.

The system's main vulnerability is the Bitcoin wallet, created as a **file** on a computer.

If a hacker (or a computer virus) gains access to a computer and can read this file, they will be able to transfer all money to their **anonymous** account, where it will be nearly impossible to find.

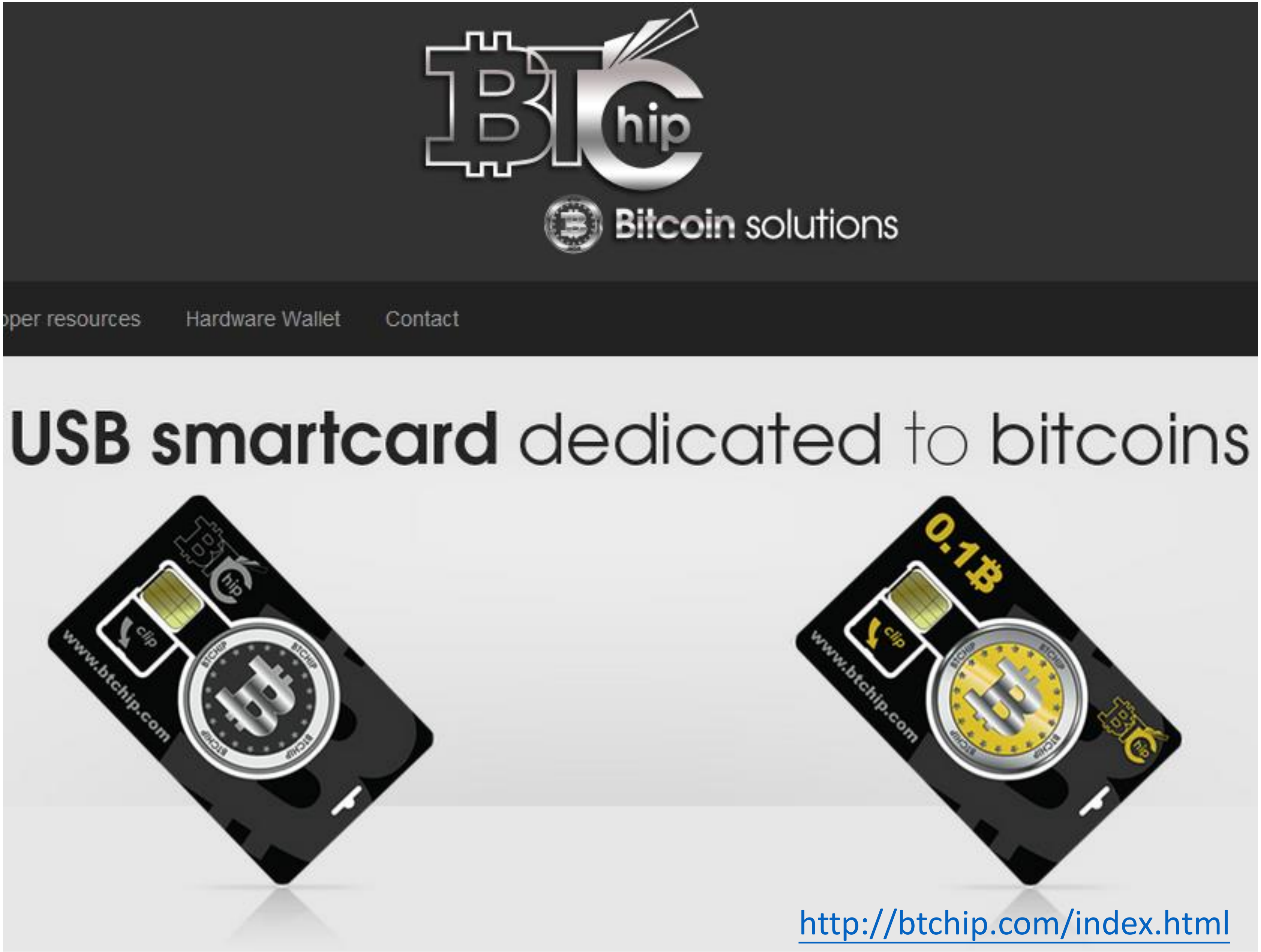
It will also be impossible to prove to anyone that you **yourself** did not transfer the money to your own anonymous account.

Our Bitcoincard, a stand-alone device that acts as an electronic wallet, can be used to **secure** the wallet in a safe place (outside the computer, making it inaccessible to hackers).

Device is in final stages of development.

Radio enabled supersmartcards as a self-sustainable wireless media without immediate internet connection needed

https://mycelium.com/bitcoincard



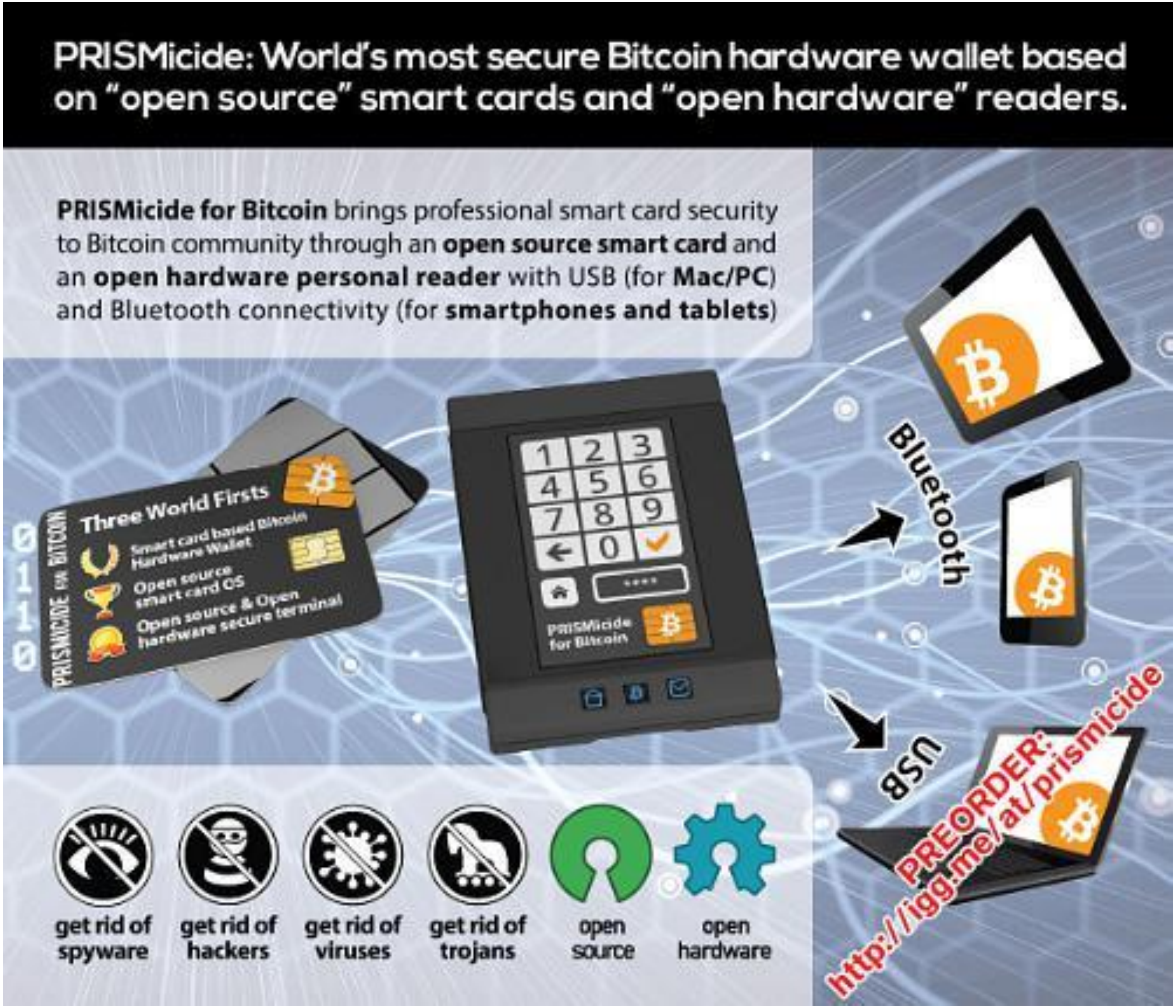
BTChip

Bitcoin solutions

per resources Hardware Wallet Contact

USB smartcard dedicated to bitcoins

http://btchip.com/index.html

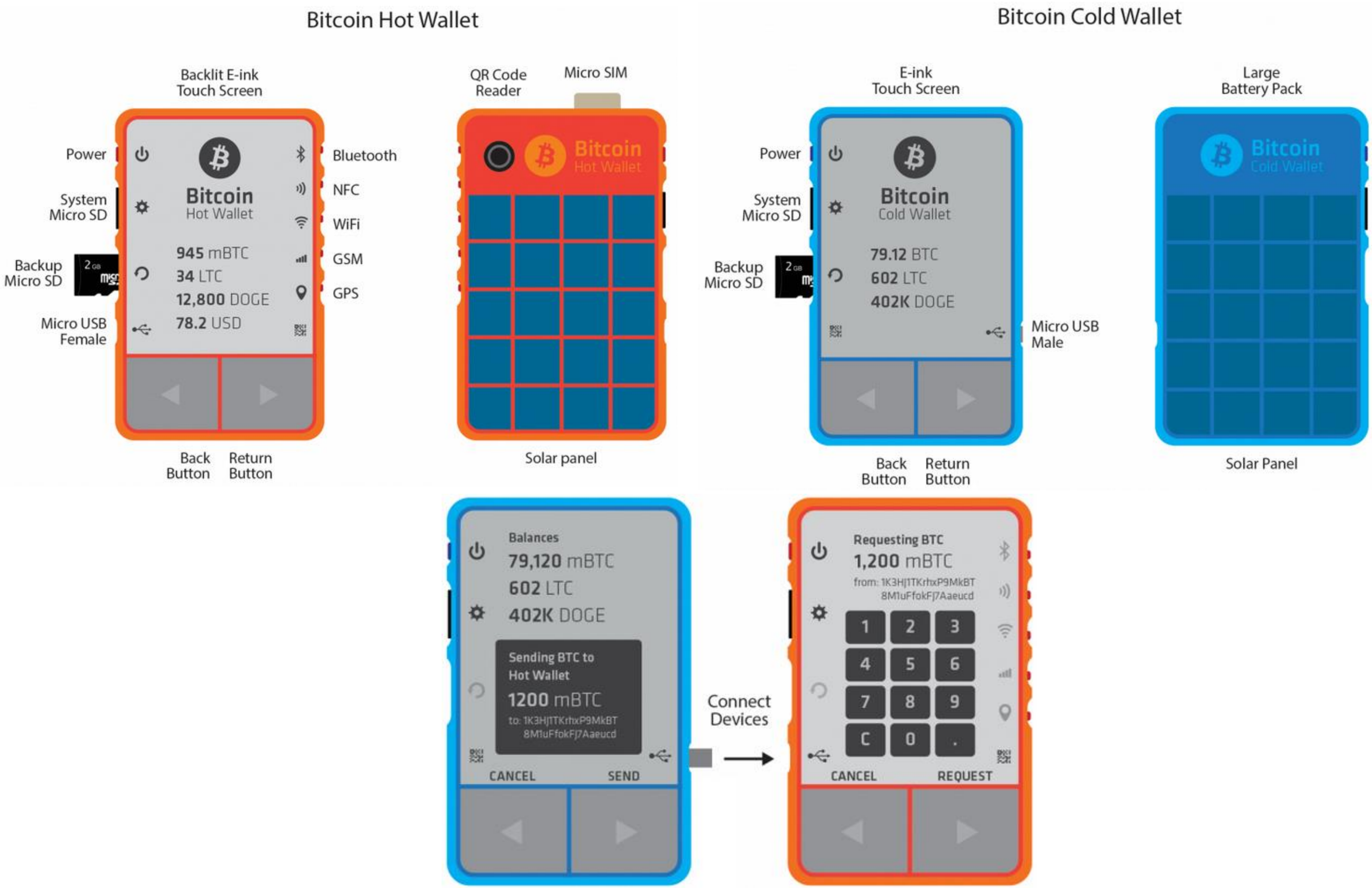


PRISMicide: World's most secure Bitcoin hardware wallet based on "open source" smart cards and "open hardware" readers.

PRISMicide for Bitcoin brings professional smart card security to Bitcoin community through an **open source smart card** and an **open hardware personal reader** with USB (for **Mac/PC**) and Bluetooth connectivity (for **smartphones and tablets**)

https://www.indiegogo.com/projects/prismicide-world-s-most-secure-bitcoin-hardware-wallet-and-anti-prism-platform

Bitcoin Hot & Cold Wallet Concept



http://news.insidebitcoins.com/bitcoin-cold-hot-wallet-concept

What Should a Hardware Wallet Be?

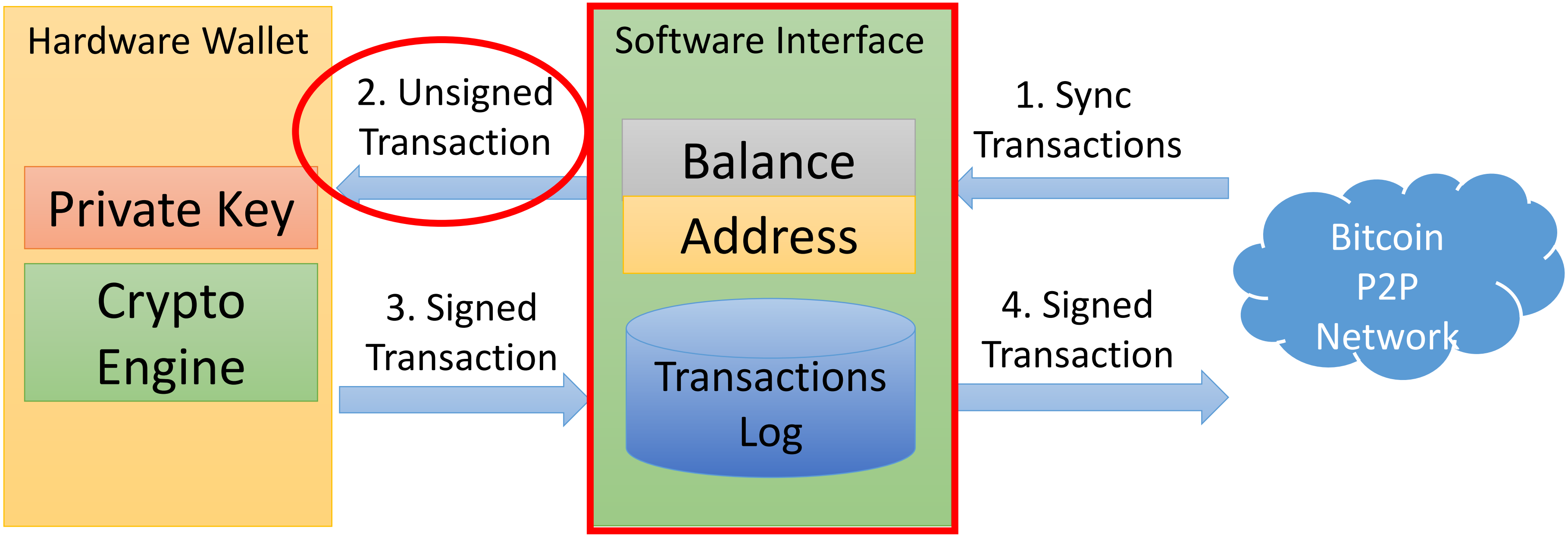
- Security
  - Private keys protected in the device and **never exposed in plaintext**
  - Device authentication
  - Sign the bitcoin transaction **“offline”** with decent **RNG**
  - Able to **backup** and **restore** when hardware failure or lose
  - Solid hardware and firmware against thieves
  - Using **secure chip** against **hardware hack**

- Easy of use
  - Easy to understand
  - Easy to operate
  - Easy to carry

- Advanced Features
  - HD wallet (BIP0032)
  - Multi-signature feature

https://en.bitcoin.it/wiki/Hardware_wallet https://en.bitcoin.it/wiki/Smart_card_wallet

Scenario of Using a Hardware Wallet



- How to prevent unauthorized signing request?
- How to prevent manipulated signing request?

A Demo of a Smartcard Wallet

bitcoin
[testnet]
位元幣核心
Version v0.9.1.0-g026a939-beta
© 2009-2014 位元幣核心開發人員
正在驗證區塊資料

Demo Environment

Hardware Features

- Common Criteria EAL 5+
- ARM Secure Core SC300TM
- Secure Flash (Active Shield)
- TRNG
- Coprocessor for ECDSA
- Unique ID

Firmware Features

- On card transaction signing
- On card ECDSA/AES/SHA256
- 1000+ Bitcoin address and private key pairs
- Host binding
- User PIN (optional PUK)
- Wallet management

Recap

- Bitcoin economy is boosting
- Bitcoin is essentially a cryptographic protocol, which is brilliant and beautiful
- Watch out various aspects of Bitcoin security
- Bitcoin private keys are so crucial that must be protected with extreme care
- Offline Bitcoin hardware wallets integrated with mobile devices seem to be one of the future trends

Bitcoin Rocks!

Appendix. The Script about Bitcoin from Cryptographers' Panel, RSA Conference 2014

https://www.youtube.com/watch?v=gMc9fHvc78Y

__Kocher__ {31:57}: As you speak about decentralized systems and splitting trust, that brings up the topic in Bitcoin, which has been getting a lot of attention recently. It's been called everything from a dangerous technology that should be banned, to the currency in the future, to a great investment, to a bubble. Do you use it? What's your thought about it? Where do you think crypto-currencies will sit in the future?

__Rivest__: I don't use it. It's a fun research topic.

__Shamir__ {32:21}: I think that it is an example of a project which had a lot of potential, but almost everything that could go wrong with it did. Let's look at some of the aspects. It was supposed to be a decentralized system, which no one would be in control of. It turns out that there were a few organizations which, a few exchanges which dominated the market. Almost nobody can mine Bitcoins at the moment. So if you want to make any money out of the mining operation, you have to buy these very very expensive ASICs. And therefore again, it's highly centralized. Almost everything is highly centralized. If you think about how many cases are reported, in which Bitcoins are stolen from computers – from electronic wallets kept in your computer – it shows that the currency on the Internet cannot be kept on the Internet, which I find very ironic.

Diffie {33:33}: I thought indeed in its original vision as a totally decentralized thing, that was tremendously exciting. I mean we’ve been trying, we’ve been chasing, some people particularly chasing the will of the wisp of electronic, decentralized, anonymous, this, that, and the other electronic banking; now for about three decades. So this struck me as a big leap forward in that direction. And Bitcoin is now just one, you know, it needn't be perfect as a design, there are related designs that attempt to debug it. The kind of centralization you’re talking about is very hard to eliminate in anything. Biology does fairly well. But if you go one level deeper, you find the heavy elements manufactured in supernovas, which are expensive, right? So whether you can build, a competitive society, whatever, that doesn’t have centralized resources; whether that can out-compete one that does, I think it is very far from clear.

LaMacchia {34:36}: So first I don’t use Bitcoin currently. I played around a little bit just to try mining early on, didn’t really find anything. And I will admit that when the coin – when it got above a thousand dollars a Bitcoin, I did the digital equivalent of hunting around in the cushions of your couch, looking to see if I had managed to leave any little digital coins around. Cause it would have been interesting though I didn't have anything left on disk. But what I find most interesting is the amount of computing power that’s going into it. So I did a quick check last night. You go to blockchain.org [blockchain.info actually] which publishes all the stats on the Bitcoin blocks. And currently the Bitcoin mining network is generating about 29 million giga-hashes per second. That’s about 2 to the 55 [2^{55}] hashes, SHA-2 hashes, per second is going into this effort.

Diffie: […] reading someone's DES traffic.

LaMacchia: Well that’s the point. If you have that much of compute power that's been specialized you can basically apply it to a DES key in a second or two. Or finding SHA-1 collisions if the theoretical bounds under 2 to 64 [2^{64}] are correct, could do it in under an hour of time. So there is a lot of compute power that’s being thrown into this.

Rivest {35:46}: So we're getting security because those resources are not being devoted towards breaking these cryptosystems, but they're off doing Bitcoin things. Right? […]

LaMacchia: Something like a honey-pot.

Shamir: I’m actually surprised that the green movement is not trying to intervene, because so much electricity is being lost making their Bitcoins that somebody should do it.

Rivest {36:07}: That‘s a great technical question as how do you implement something like the Bitcoin public ledger in a way that doesn’t waste all this electricity. I‘d love to see a good solution to that. Following up on that just a little bit if I may: I think there’s a convergence of interest here between Bitcoin and some other applications. In Bitcoin you‘ve got this distributed public ledger basically where you can append records at the end of that. That abstraction is one that we see in other applications as well. The certificate transparency project by Google has the same abstraction needed. And also a lot of electronic voting applications need a public ledger where you can append only and so on to. So I think we’re seeing an identification of a common abstraction we need to have well implemented. I think the Bitcoin implementation is wasteful for electricity. If we can solve that problem of doing what‘s done there without the electricity waste, we may have a home-run. {36:59}

Recorders: 林樂寬 (Niklas Lemcke), 童御修