# How Bitcoin Works:

# A Non-Technical Introduction

The University of Hong Kong

isr institute for SOFTWARE RESEARCH

# Bitcoin

- A non-technical VIDEO:

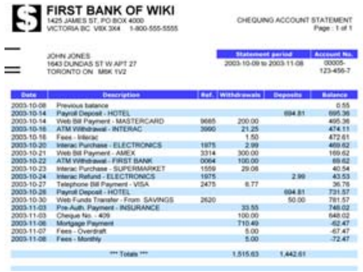
# Token Money

- Represented by a physical object such as a banknote, coin, traveler's cheque, etc.

- Without the token, the value is lost.
- No intermediary required for spending
- But: requires faith in the ISSUER, usually a government

# Notational Money

- Represented by a notation in a ledger, passbook or database
- E.g., a bank account:



FIRST BANK OF WIKI
1425 JAMES ST, PO BOX 4000
VICTORIA BC V8X 3X4 1-800-555-5555

CHEQUING ACCOUNT STATEMENT
Page : 1 of 1

JOHN JONES
1643 DUNDAS ST W APT 27
TORONTO ON M6K 1V2

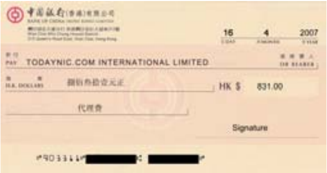
| Statement period | Account No. |
|---|---|
| 2003-10-09 to 2003-11-08 | 00005-123-456-7 |

| Date | Description | Ref. | Withdrawals | Deposits | Balance |
|---|---|---|---|---|---|
| 2003-10-08 | Previous balance | | | | 0.55 |
| 2003-10-14 | Payroll Deposit - HOTEL | | | 694.81 | 695.36 |
| 2003-10-14 | Web Bill Payment - MASTERCARD | 9685 | 200.00 | | 495.36 |
| 2003-10-16 | ATM Withdrawal - INTERAC | 3990 | 21.25 | | 474.11 |
| 2003-10-16 | Fees - Interac | | 1.50 | | 472.61 |
| 2003-10-20 | Interac Purchase - ELECTRONICS | 1975 | 2.99 | | 469.62 |
| 2003-10-21 | Web Bill Payment - AMEX | 3314 | 300.00 | | 169.62 |
| 2003-10-22 | ATM Withdrawal - FIRST BANK | 0064 | 100.00 | | 69.62 |
| 2003-10-23 | Interac Purchase - SUPERMARKET | 1559 | 29.08 | | 40.54 |
| 2003-10-24 | Interac Refund - ELECTRONICS | 1975 | | 2.99 | 43.53 |
| 2003-10-27 | Telephone Bill Payment - VISA | 2475 | 6.77 | | 36.76 |
| 2003-10-28 | Payroll Deposit - HOTEL | | | 694.81 | 731.57 |
| 2003-10-30 | Web Funds Transfer - From SAVINGS | 2620 | | 50.00 | 781.57 |
| 2003-11-03 | Pre-Auth. Payment - INSURANCE | | 33.55 | | 748.02 |
| 2003-11-03 | Cheque No. - 409 | | 100.00 | | 648.02 |
| 2003-11-06 | Mortgage Payment | | 710.49 | | -62.47 |
| 2003-11-07 | Fees - Overdraft | | 5.00 | | -67.47 |
| 2003-11-08 | Fees - Monthly | | 5.00 | | -72.47 |
| | *** Totals *** | | 1,515.63 | 1,442.61 | |

- 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
- Example: personal cheque, Octopus card



中國銀行(香港)有限公司

16 4 2007

PAY TODAYNIC.COM INTERNATIONAL LIMITED

H.K. DOLLARS [illegible] HK $ 831.00

代理費

Signature

⑈903311⑈[redacted] [redacted]⑈

- Can be lost AND requires faith in the ISSUER
- AND requires an intermediary (bank or clearing house) for spending

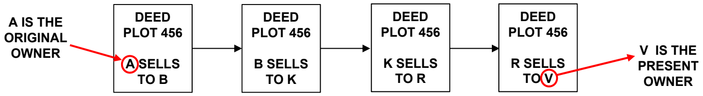
# Virtual Money

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

- 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 does "spending" occur?
- How do you know the spender is the owner?
- What prevents spending the same money twice?

# 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



A IS THE ORIGINAL OWNER
DEED PLOT 456 A SELLS TO B
DEED PLOT 456 B SELLS TO K
DEED PLOT 456 K SELLS TO R
DEED PLOT 456 R SELLS TO V
V IS 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

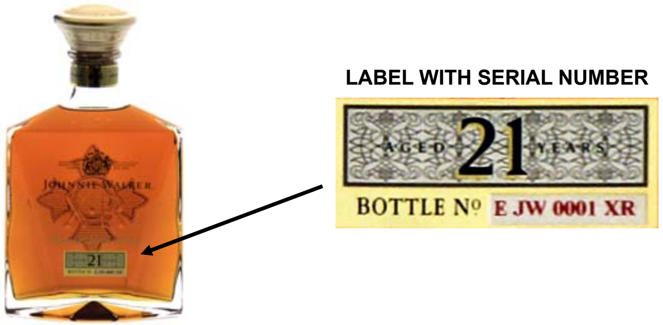
- Ask the network and count the responses! If a majority say that V is the owner, then he is.
- There must be enough honest members that false responses cannot dominate
- This registry is not under government control

# Creating a Currency

- Land is not portable and can’t be “spent”
- Let’s use valuable scotch whisky as money

# Creating a Currency

- Land is not portable and can’t be “spent.”
- Let’s use valuable scotch whisky as money
- Johnnie Walker XR is issued in limited, numbered editions, about HKD 1100 per bottle



LABEL WITH SERIAL NUMBER

# Scotch as Money

- As long as there’s a market for expensive scotch, it will have value
- Scotch drinkers will be able to drink it or trade it
- The value will depend on supply and demand

- Problem: it’s very heavy, can’t be carried easily

# Solution: A Scotch Bank

- Deposit your bottles in a bank
- The bank promises to hand over your bottle when you ask for it
- To prove ownership, they let you keep the label unique to your bottle:

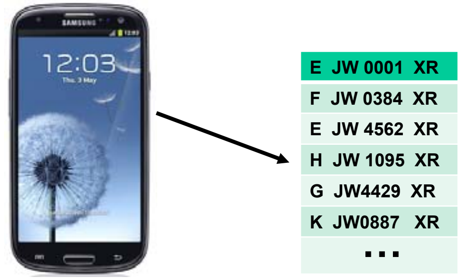
- When you transfer the label, you transfer ownership
- The labels act as money!
- The labels are “backed” by scotch

# Disaster: Scotch is OUTLAWED!

- The Department of Health finds that scotch is poisonous, possibly fatal
- The government orders all of it destroyed, even in your bank
- You have scotch labels but your bank has no more scotch
- What happens to the value of the labels? No longer “backed” by scotch bottles
- Probably declines, but not to zero

# The Label Virtual Currency

- Assume one label is now worth HKD 100.
- You can’t carry all of them around
- You can’t spend them on the Internet
- Let’s “virtualize” them
- Instead of labels, just store their serial numbers in a cellphone app:

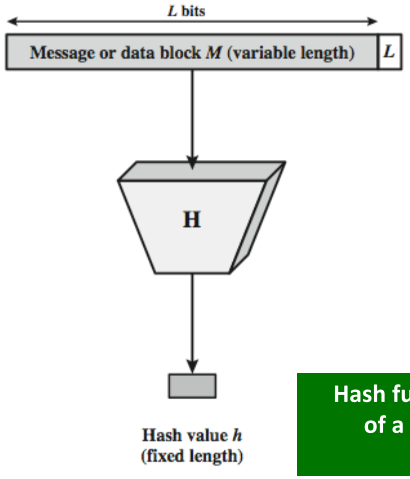


E JW 0001 XR
F JW 0384 XR
E JW 4562 XR
H JW 1095 XR
G JW4429 XR
K JW0887 XR
. . .

# Spending

- To spend a label, you just send its number over the Internet or bump phones
- Problem: you might still have it, but your digital wallet could delete it to prevent double spending
- Problem: How does the recipient know it’s genuine?
- Problem: Who controls the issuance of the numbers?
- Problem: What stops forgery?
- SOLUTION:
  - Make creation of numbers expensive (deters forgery)
  - Limit generation to a fixed quantity of serial numbers
  - Maintain ownership records in a distributed network

# Hash Functions

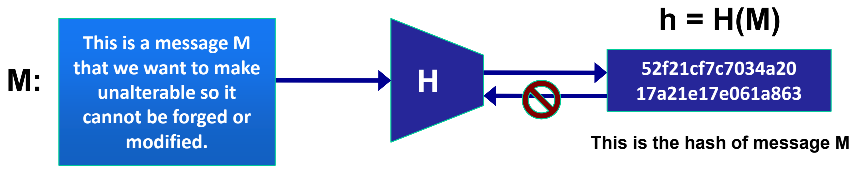


- **A “hash” is a short function of a message**
- **BUT: a hash is not uniquely reversible**
- **Many messages have the same hash**

**Hash function *H* produces a fixed size hash of a 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


M:
This is a message M that we want to make unalterable so it cannot be forged or modified.
H
h = H(M)
52f21cf7c7034a20 17a21e17e061a863
This is the hash of message M

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

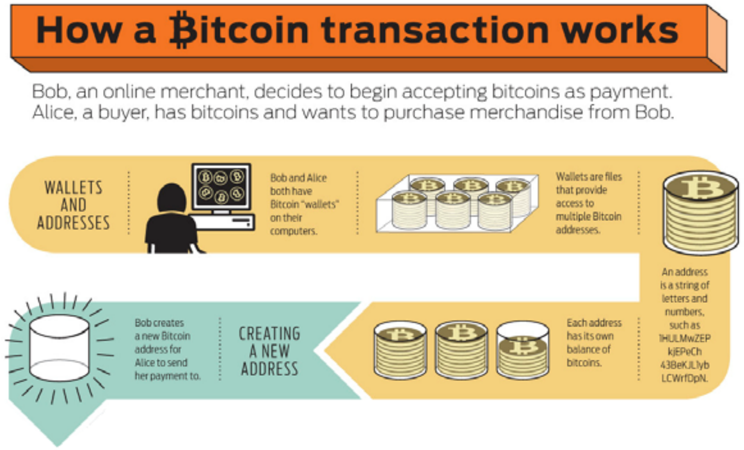
# What is a Bitcoin Really?

- No physical object, not even a character string
- A chain of digitally signed transaction records leading from the original owner to the current holder
- (Very similar to a chain of land deeds)
- The transaction records contain
  (1) hashes that are difficult to find AND
  (2) virtual owner IDs, called addresses
- There is NO bitcoin registry, NO centralization
- Bitcoin chains are broadcast to everyone
- Anyone can verify them

# Bitcoin Protocol

- Bitcoin was invented in 2008 by an anonymous person or team called “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

# How Bitcoin Works 1



How a Bitcoin 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.

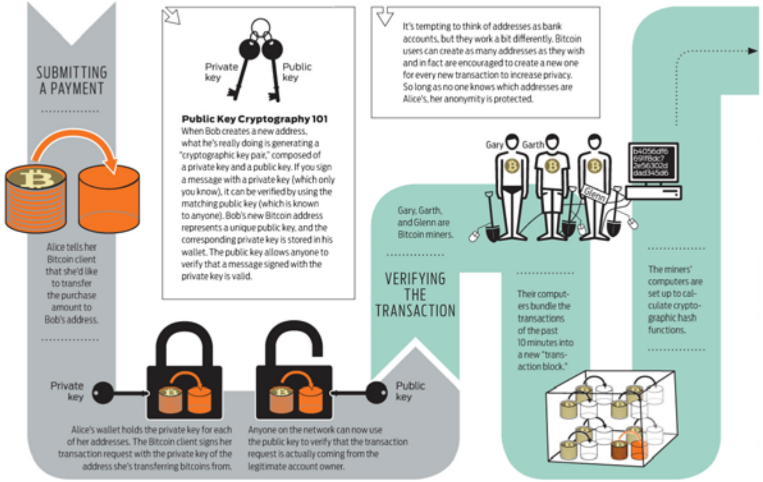
An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

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.

# How Bitcoin Works 2



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

**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.

Gary, Garth, and Glenn are Bitcoin miners.

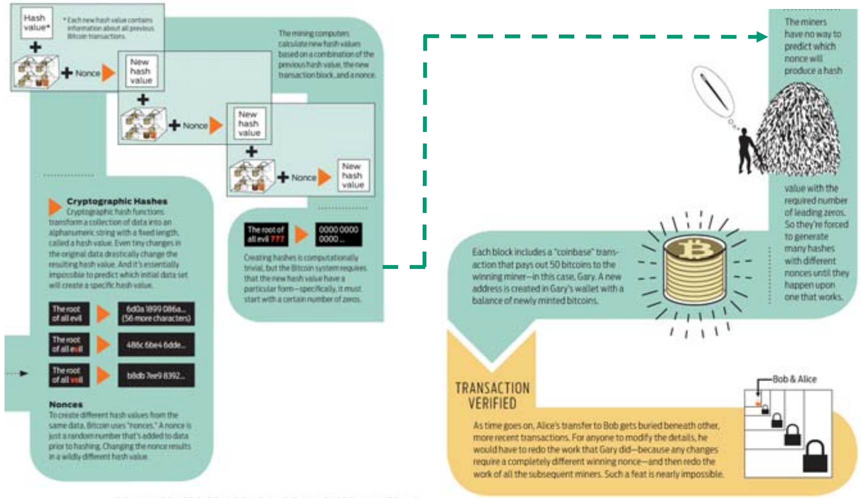
Their computers bundle the transactions of the past 10 minutes into a new "transaction block."

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

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.

# How Bitcoin Works 3



* 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.

**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.

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.

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.

JOSHUA J. ROMERO, BRANDON PALACIO & KARLSSONWILKER INC.

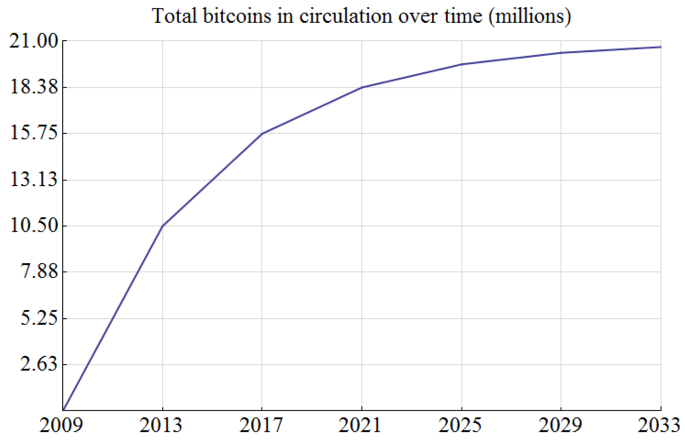
# Bitcoin Addresses

- Bitcoin software generates bitcoin addresses of 25-44 characters for users
- Sample address: 1BBsbEq8Q29JpQr4jygjPof7F7uphqyUCQ
- (The address is actually an elliptic curve public key. 44-character key as secure as a 7000-bit RSA key.)
- To send bitcoins, user specifies a receiving address and amount, and 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.

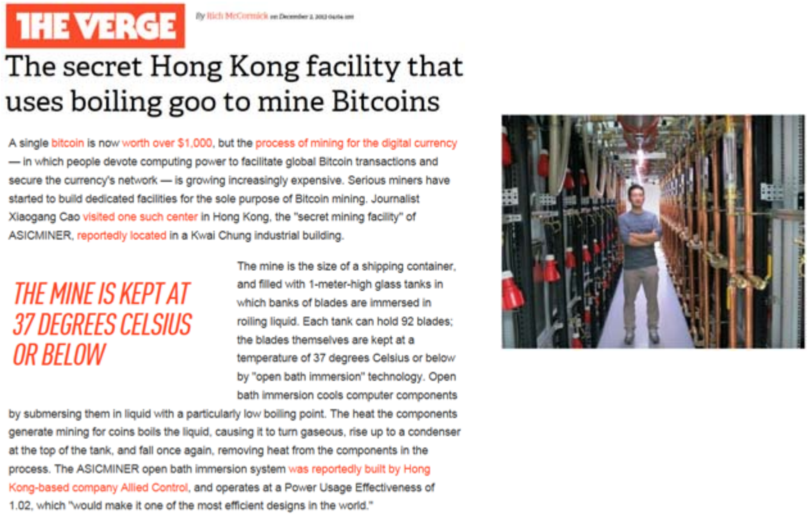
# Bitcoin Mining

- Bitcoin chains begin with data "mined" by performing a large number of hash function computations
- A "miner" tries many different (e.g., 10^15) numbers, trying to find one whose hash value is less than a given threshold
- Success is rewarded with bitcoins
- The threshold declines over time (determined by the protocol)
- Bitcoin hashes are progressively more difficult to find
- There will never be more than 21 million bitcoins. Divisible into units as small as 1/100 millionth of a bitcoin

# Controlled Bitcoin Inflation



# Bitcoin Mining in Hong Kong



THE VERGE By Rich McCormick on December 2, 2013 04:04 am

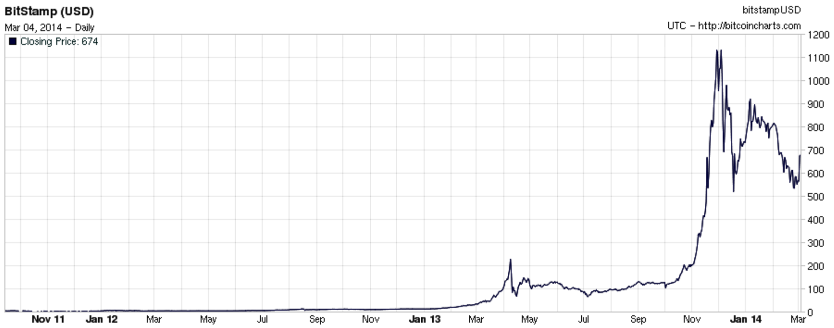
The secret Hong Kong facility that uses boiling goo to mine Bitcoins

A single bitcoin is now worth over $1,000, but the process of mining for the digital currency — in which people devote computing power to facilitate global Bitcoin transactions and secure the currency's network — is growing increasingly expensive. Serious miners have started to build dedicated facilities for the sole purpose of Bitcoin mining. Journalist Xiaogang Cao visited one such center in Hong Kong, the "secret mining facility" of ASICMINER, reportedly located in a Kwai Chung industrial building.

THE MINE IS KEPT AT 37 DEGREES CELSIUS OR BELOW

The mine is the size of a shipping container, and filled with 1-meter-high glass tanks in which banks of blades are immersed in roiling liquid. Each tank can hold 92 blades; the blades themselves are kept at a temperature of 37 degrees Celsius or below by "open bath immersion" technology. Open bath immersion cools computer components by submersing them in liquid with a particularly low boiling point. The heat the components generate mining for coins boils the liquid, causing it to turn gaseous, rise up to a condenser at the top of the tank, and fall once again, removing heat from the components in the process. The ASICMINER open bath immersion system was reportedly built by Hong Kong-based company Allied Control, and operates at a Power Usage Effectiveness of 1.02, which "would make it one of the most efficient designs in the world."

# Bitcoin Value, Sep. ’11 – Mar ’14

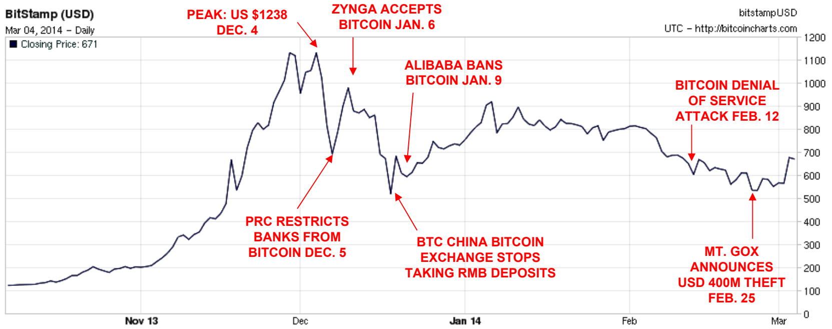


Exchange: BitStamp (USD)

VIEW TRADING CHART

TRANSACTIONS IN REALTIME

# Bitcoin Value, Oct ’13 – Mar ’14



PEAK: US $1238 DEC. 4

ZYNGA ACCEPTS BITCOIN JAN. 6

ALIBABA BANS BITCOIN JAN. 9

BITCOIN DENIAL OF SERVICE ATTACK FEB. 12

PRC RESTRICTS BANKS FROM BITCOIN DEC. 5

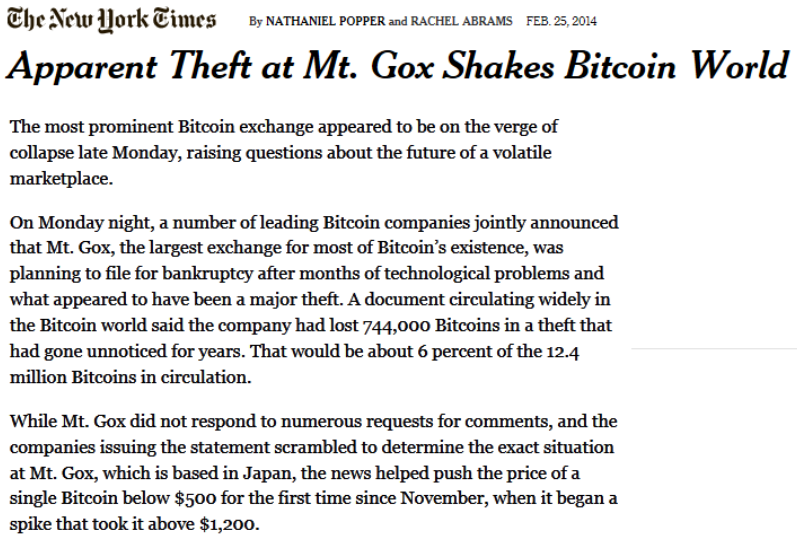
BTC CHINA BITCOIN EXCHANGE STOPS TAKING RMB DEPOSITS

MT. GOX ANNOUNCES USD 400M THEFT FEB. 25

Exchange: BitStamp (USD)

VIEW TRADING CHART

TRANSACTIONS IN REALTIME



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.

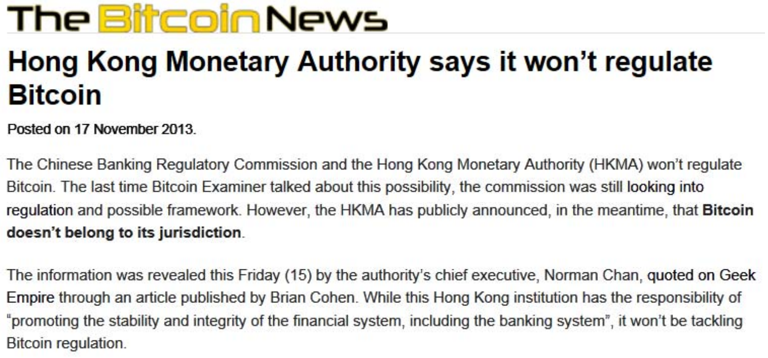
On Monday night, a number of leading Bitcoin companies jointly announced that Mt. Gox, the largest exchange for most of Bitcoin's existence, was planning to file for bankruptcy after months of technological problems and what appeared to have been a major theft. A document circulating widely in the Bitcoin 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.

# Possible Vulnerabilities

- No way to reverse a transaction without the payee's cooperation
- Transaction malleability (alterability)
- Should to wait 60 minutes or more to confirm a large transaction
- Software bugs
- Bank robbery by hackers (e.g. Mt. Gox)
- Malware attacks against wallets
- Government attempts to control
  - – Silk Road raided by US FBI in Oct 2013
- Competing digital currencies easy to create

# Bitcoin in Hong Kong



The Bitcoin News

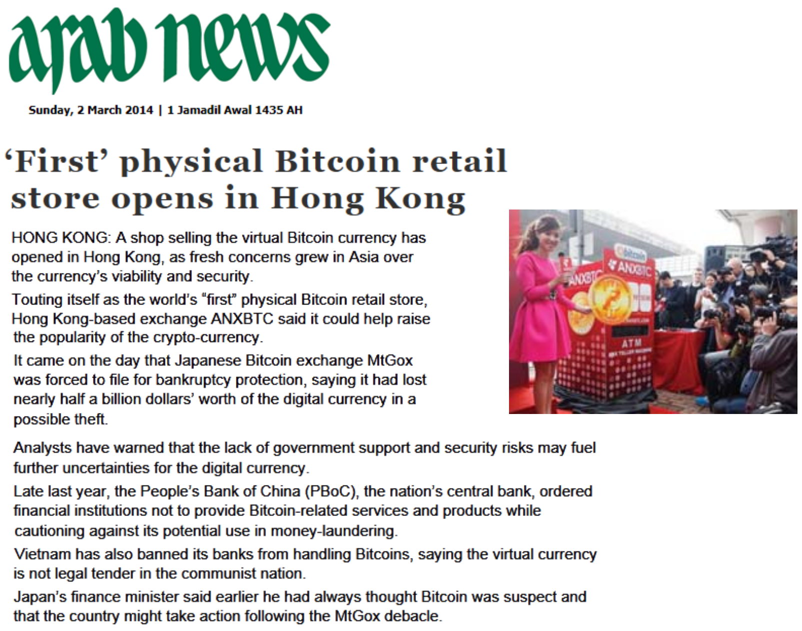
## Hong Kong Monetary Authority says it won't regulate Bitcoin

Posted on 17 November 2013.

The Chinese Banking Regulatory Commission and the Hong Kong Monetary Authority (HKMA) won't regulate Bitcoin. The last time Bitcoin Examiner talked about this possibility, the commission was still looking into regulation and possible framework. However, the HKMA has publicly announced, in the meantime, that **Bitcoin doesn't belong to its jurisdiction**.

The information was revealed this Friday (15) by the authority's chief executive, Norman Chan, quoted on Geek Empire through an article published by Brian Cohen. While this Hong Kong institution has the responsibility of "promoting the stability and integrity of the financial system, including the banking system", it won't be tackling Bitcoin regulation.

- This created speculation that HK would become a hotbed of Bitcoin activity



arab news

Sunday, 2 March 2014 | 1 Jamadil Awal 1435 AH

## 'First' physical Bitcoin retail store opens in Hong Kong

HONG KONG: A shop selling the virtual Bitcoin currency has opened in Hong Kong, as fresh concerns grew in Asia over the currency's viability and security.

Touting itself as the world's "first" physical Bitcoin retail store, Hong Kong-based exchange ANXBTC said it could help raise the popularity of the crypto-currency.

It came on the day that Japanese Bitcoin exchange MtGox was forced to file for bankruptcy protection, saying it had lost nearly half a billion dollars' worth of the digital currency in a possible theft.

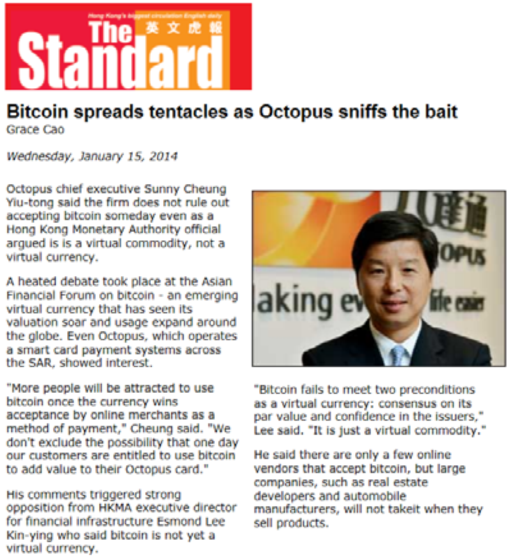
Analysts have warned that the lack of government support and security risks may fuel further uncertainties for the digital currency.

Late last year, the People's Bank of China (PBoC), the nation's central bank, ordered financial institutions not to provide Bitcoin-related services and products while cautioning against its potential use in money-laundering.

Vietnam has also banned its banks from handling Bitcoins, saying the virtual currency is not legal tender in the communist nation.

Japan's finance minister said earlier he had always thought Bitcoin was suspect and that the country might take action following the MtGox debacle.

# Octopus + Bitcoin?



Hong Kong's biggest circulation English daily
The Standard 英文虎報

## Bitcoin spreads tentacles as Octopus sniffs the bait

Grace Cao

*Wednesday, January 15, 2014*

Octopus chief executive Sunny Cheung Yiu-tong said the firm does not rule out accepting bitcoin someday even as a Hong Kong Monetary Authority official argued is is a virtual commodity, not a virtual currency.

A heated debate took place at the Asian Financial Forum on bitcoin - an emerging virtual currency that has seen its valuation soar and usage expand around the globe. Even Octopus, which operates a smart card payment systems across the SAR, showed interest.

"More people will be attracted to use bitcoin once the currency wins acceptance by online merchants as a method of payment," Cheung said. "We don't exclude the possibility that one day our customers are entitled to use bitcoin to add value to their Octopus card."

His comments triggered strong opposition from HKMA executive director for financial infrastructure Esmond Lee Kin-ying who said bitcoin is not yet a virtual currency.

"Bitcoin fails to meet two preconditions as a virtual currency: consensus on its par value and confidence in the issuers," Lee said. "It is just a virtual commodity."

He said there are only a few online vendors that accept bitcoin, but large companies, such as real estate developers and automobile manufacturers, will not takeit when they sell products.

# Q&A