CryptoCurrency and Blockchain (1)

金融科技導論

陳君明

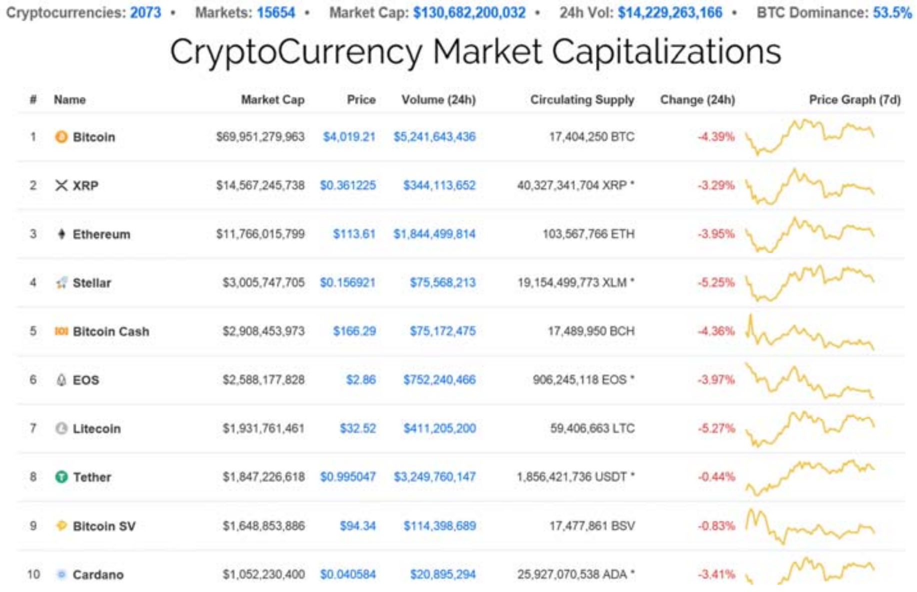
jmchen@crypto.tw

國立臺灣大學 National Taiwan University

Status of Bitcoin

密碼貨幣市值

http://coinmarketcap.com 2018.12.03 12:00



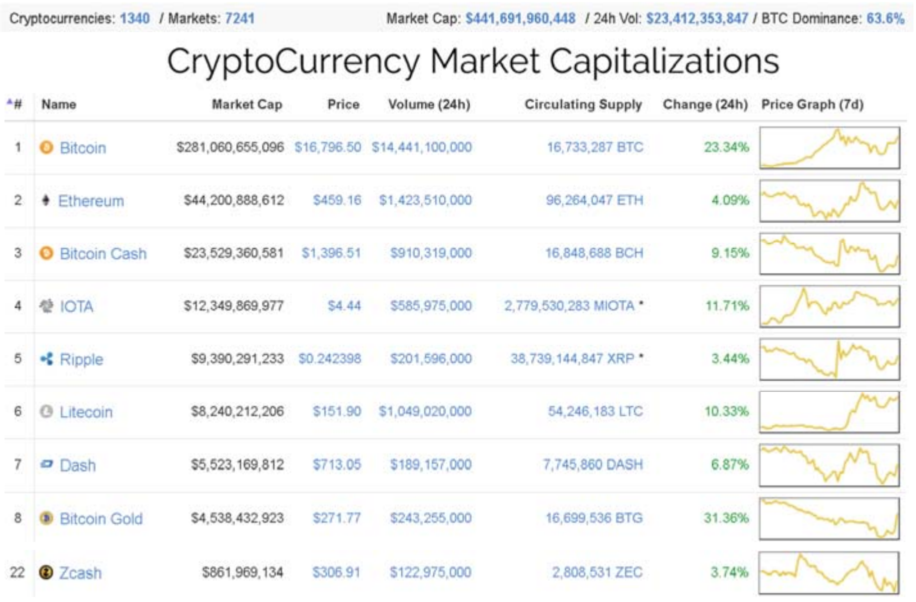
Cryptocurrencies: 2073 • Markets: 15654 • Market Cap: $130,682,200,032 • 24h Vol: $14,229,263,166 • BTC Dominance: 53.5%

CryptoCurrency Market Capitalizations

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$69,951,279,963	$4,019.21	$5,241,643,436	17,404,250 BTC	-4.39%	
2	XRP	$14,567,245,738	$0.361225	$344,113,652	40,327,341,704 XRP *	-3.29%	
3	Ethereum	$11,766,015,799	$113.61	$1,844,499,814	103,567,766 ETH	-3.95%	
4	Stellar	$3,005,747,705	$0.156921	$75,568,213	19,154,499,773 XLM *	-5.25%	
5	Bitcoin Cash	$2,908,453,973	$166.29	$75,172,475	17,489,950 BCH	-4.36%	
6	EOS	$2,588,177,828	$2.86	$752,240,466	906,245,118 EOS *	-3.97%	
7	Litecoin	$1,931,761,461	$32.52	$411,205,200	59,406,663 LTC	-5.27%	
8	Tether	$1,847,226,618	$0.995047	$3,249,760,147	1,856,421,736 USDT *	-0.44%	
9	Bitcoin SV	$1,648,853,886	$94.34	$114,398,689	17,477,861 BSV	-0.83%	
10	Cardano	$1,052,230,400	$0.040584	$20,895,294	25,927,070,538 ADA *	-3.41%	

密碼貨幣市值

http://coinmarketcap.com 2017.12.11 12:00



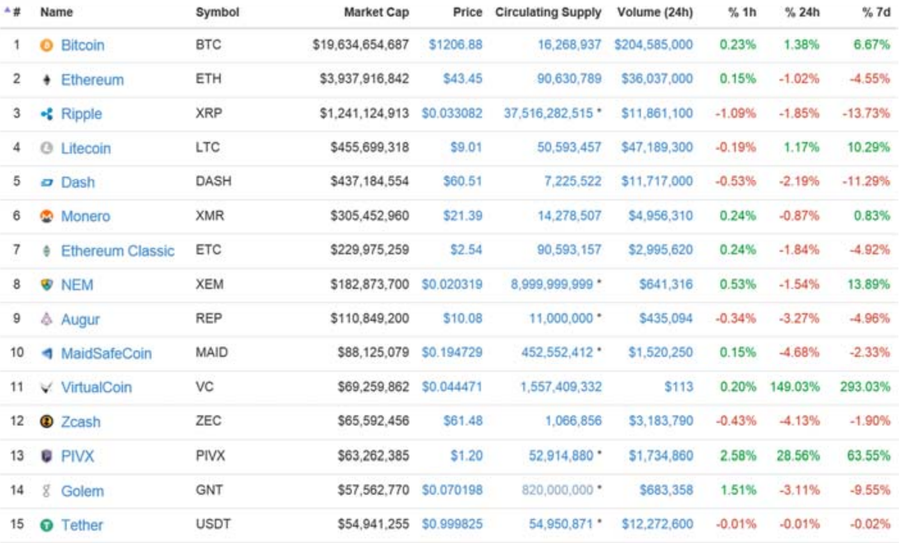
Cryptocurrencies: 1340 / Markets: 7241 Market Cap: $441,691,960,448 / 24h Vol: $23,412,353,847 / BTC Dominance: 63.6%

CryptoCurrency Market Capitalizations

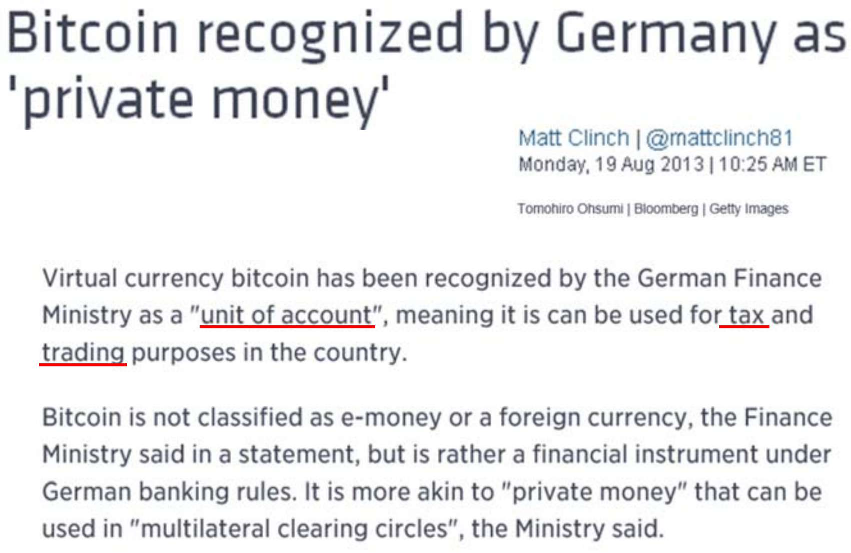
▲#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$281,060,655,096	$16,796.50	$14,441,100,000	16,733,287 BTC	23.34%	
2	Ethereum	$44,200,888,612	$459.16	$1,423,510,000	96,264,047 ETH	4.09%	
3	Bitcoin Cash	$23,529,360,581	$1,396.51	$910,319,000	16,848,688 BCH	9.15%	
4	IOTA	$12,349,869,977	$4.44	$585,975,000	2,779,530,283 MIOTA *	11.71%	
5	Ripple	$9,390,291,233	$0.242398	$201,596,000	38,739,144,847 XRP *	3.44%	
6	Litecoin	$8,240,212,206	$151.90	$1,049,020,000	54,246,183 LTC	10.33%	
7	Dash	$5,523,169,812	$713.05	$189,157,000	7,745,860 DASH	6.87%	
8	Bitcoin Gold	$4,538,432,923	$271.77	$243,255,000	16,699,536 BTG	31.36%	
22	Zcash	$861,969,134	$306.91	$122,975,000	2,808,531 ZEC	3.74%	

密碼貨幣市值

http://coinmarketcap.com 2017.04.12 11:00



#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$19,634,654,687	$1206.88	16,268,937	$204,585,000	0.23%	1.38%	6.67%
2	Ethereum	ETH	$3,937,916,842	$43.45	90,630,789	$36,037,000	0.15%	-1.02%	-4.55%
3	Ripple	XRP	$1,241,124,913	$0.033082	37,516,282,515 *	$11,861,100	-1.09%	-1.85%	-13.73%
4	Litecoin	LTC	$455,699,318	$9.01	50,593,457	$47,189,300	-0.19%	1.17%	10.29%
5	Dash	DASH	$437,184,554	$60.51	7,225,522	$11,717,000	-0.53%	-2.19%	-11.29%
6	Monero	XMR	$305,452,960	$21.39	14,278,507	$4,956,310	0.24%	-0.87%	0.83%
7	Ethereum Classic	ETC	$229,975,259	$2.54	90,593,157	$2,995,620	0.24%	-1.84%	-4.92%
8	NEM	XEM	$182,873,700	$0.020319	8,999,999,999 *	$641,316	0.53%	-1.54%	13.89%
9	Augur	REP	$110,849,200	$10.08	11,000,000 *	$435,094	-0.34%	-3.27%	-4.96%
10	MaidSafeCoin	MAID	$88,125,079	$0.194729	452,552,412 *	$1,520,250	0.15%	-4.68%	-2.33%
11	VirtualCoin	VC	$69,259,862	$0.044471	1,557,409,332	$113	0.20%	149.03%	293.03%
12	Zcash	ZEC	$65,592,456	$61.48	1,066,856	$3,183,790	-0.43%	-4.13%	-1.90%
13	PIVX	PIVX	$63,262,385	$1.20	52,914,880 *	$1,734,860	2.58%	28.56%	63.55%
14	Golem	GNT	$57,562,770	$0.070198	820,000,000 *	$683,358	1.51%	-3.11%	-9.55%
15	Tether	USDT	$54,941,255	$0.999825	54,950,871 *	$12,272,600	-0.01%	-0.01%	-0.02%



Bitcoin recognized by Germany as 'private money'

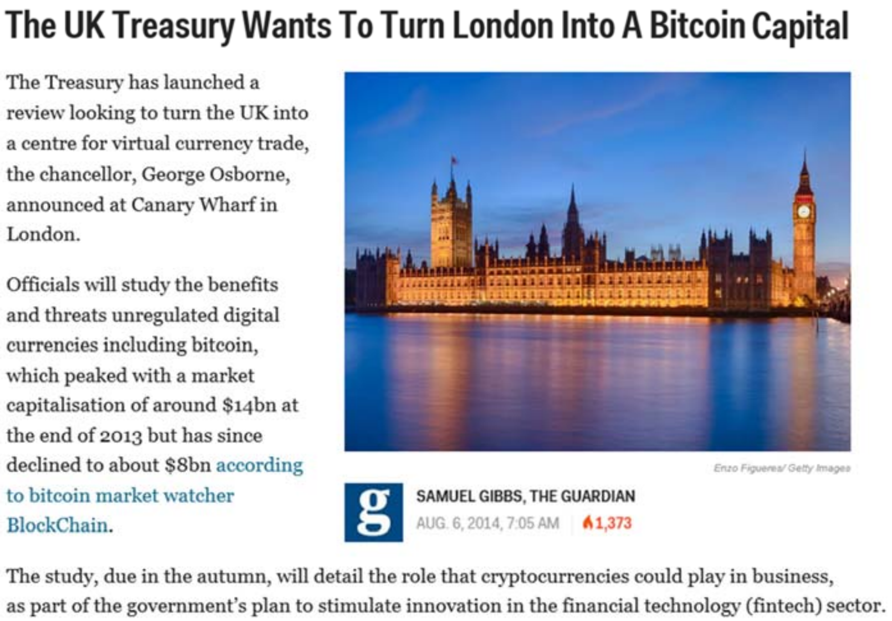
Matt Clinch | @mattclinch81
Monday, 19 Aug 2013 | 10:25 AM ET

Tomohiro Ohsumi | Bloomberg | Getty Images

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.

Bitcoin is not classified as e-money or a foreign currency, the Finance Ministry said in a statement, but is rather a financial instrument under German banking rules. It is more akin to "private money" that can be used in "multilateral clearing circles", the Ministry said.

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.

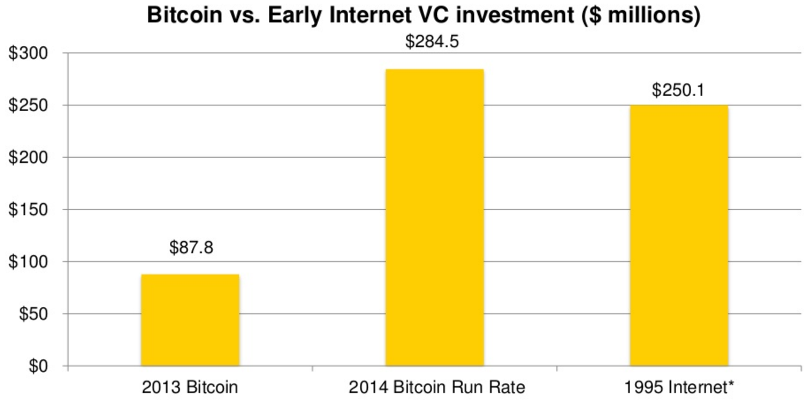
Enzo Figueres/ Getty Images

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.

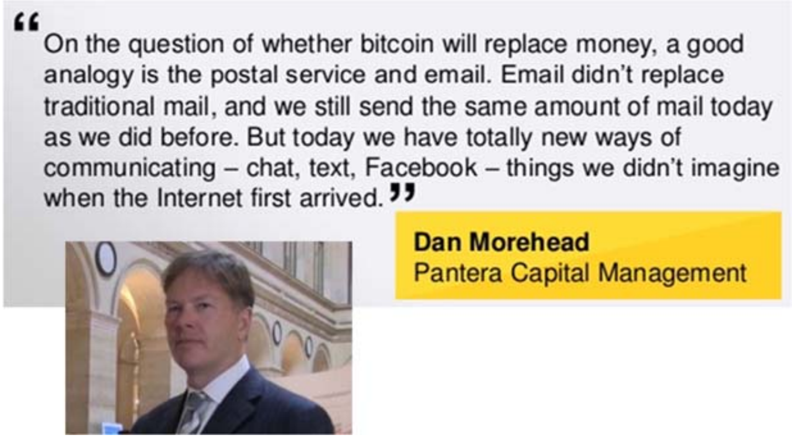
http://www.businessinsider.com/the-uk-treasury-wants-to-turn-london-into-a-bitcoin-capital-2014-8

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



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

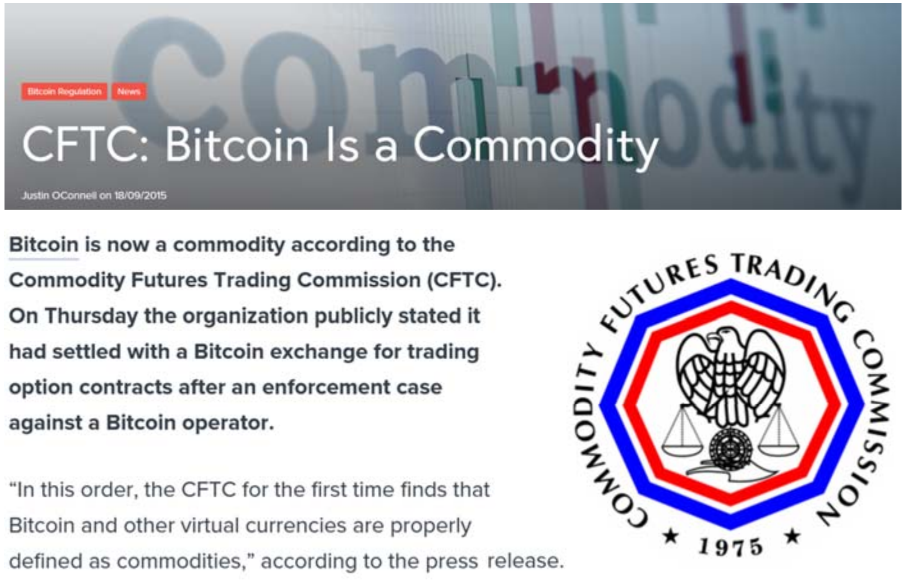
Investor View on Bitcoin



> "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



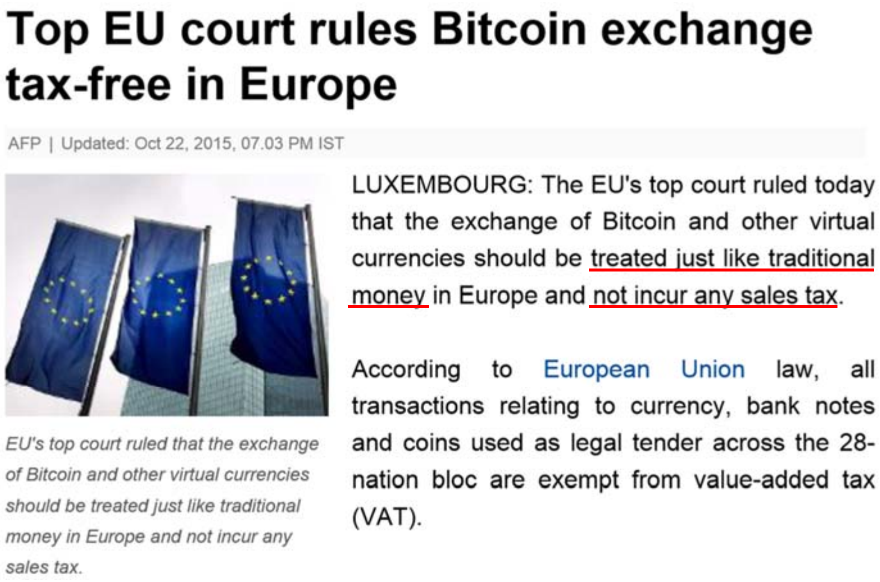
CFTC: Bitcoin Is a Commodity

Justin OConnell on 18/09/2015

Bitcoin is now a commodity according to the Commodity Futures Trading Commission (CFTC). On Thursday the organization publicly stated it had settled with a Bitcoin exchange for trading option contracts after an enforcement case against a Bitcoin operator.

"In this order, the CFTC for the first time finds that Bitcoin and other virtual currencies are properly defined as commodities," according to the press release.

https://www.cryptocoinsnews.com/cftc-bitcoin-commodity



Top EU court rules Bitcoin exchange tax-free in Europe

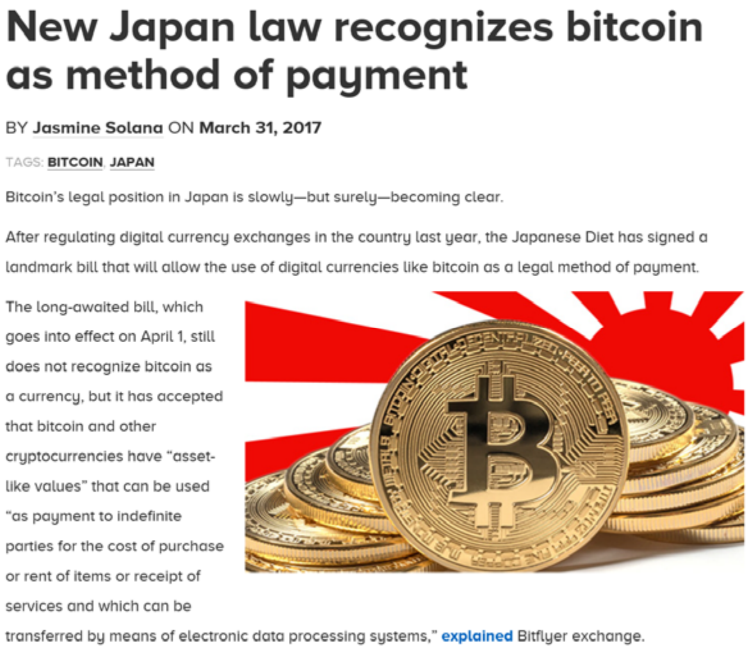
AFP | Updated: Oct 22, 2015, 07.03 PM IST

LUXEMBOURG: The EU's top court ruled today that the exchange of Bitcoin and other virtual currencies should be treated just like traditional money in Europe and not incur any sales tax.

According to European Union law, all transactions relating to currency, bank notes and coins used as legal tender across the 28-nation bloc are exempt from value-added tax (VAT).

EU's top court ruled that the exchange of Bitcoin and other virtual currencies should be treated just like traditional money in Europe and not incur any sales tax.

http://economictimes.indiatimes.com/news/international/business/top-eu-court-rules-bitcoin-exchange-tax-free-in-europe/articleshow/49495088.cms



New Japan law recognizes bitcoin as method of payment

BY **Jasmine Solana** ON **March 31, 2017**

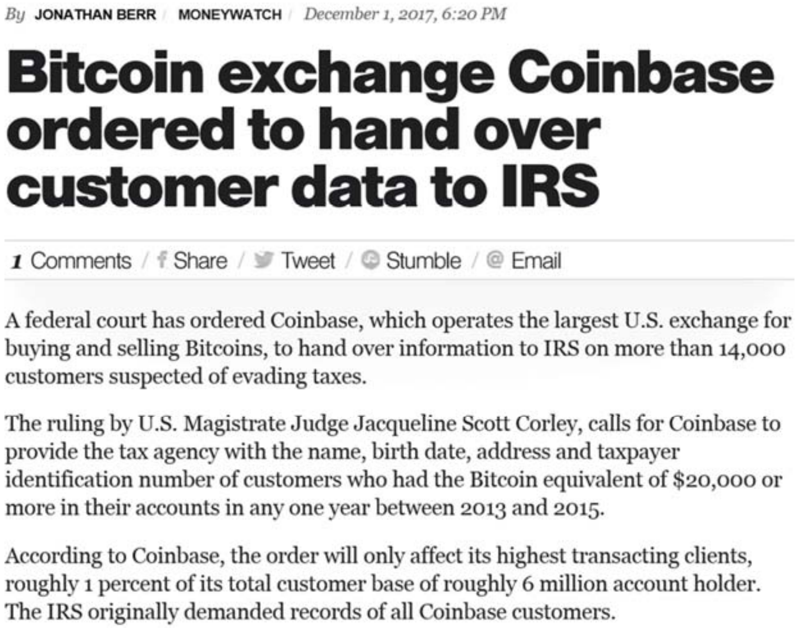
TAGS: **BITCOIN**, **JAPAN**

Bitcoin's legal position in Japan is slowly—but surely—becoming clear.

After regulating digital currency exchanges in the country last year, the Japanese Diet has signed a landmark bill that will allow the use of digital currencies like bitcoin as a legal method of payment.

The long-awaited bill, which goes into effect on April 1, still does not recognize bitcoin as a currency, but it has accepted that bitcoin and other cryptocurrencies have "asset-like values" that can be used "as payment to indefinite parties for the cost of purchase or rent of items or receipt of services and which can be transferred by means of electronic data processing systems," **explained** Bitflyer exchange.

https://calvinayre.com/2017/03/31/bitcoin/new-japan-law-recognizes-bitcoin-method-payment



By JONATHAN BERR / MONEYWATCH / December 1, 2017, 6:20 PM

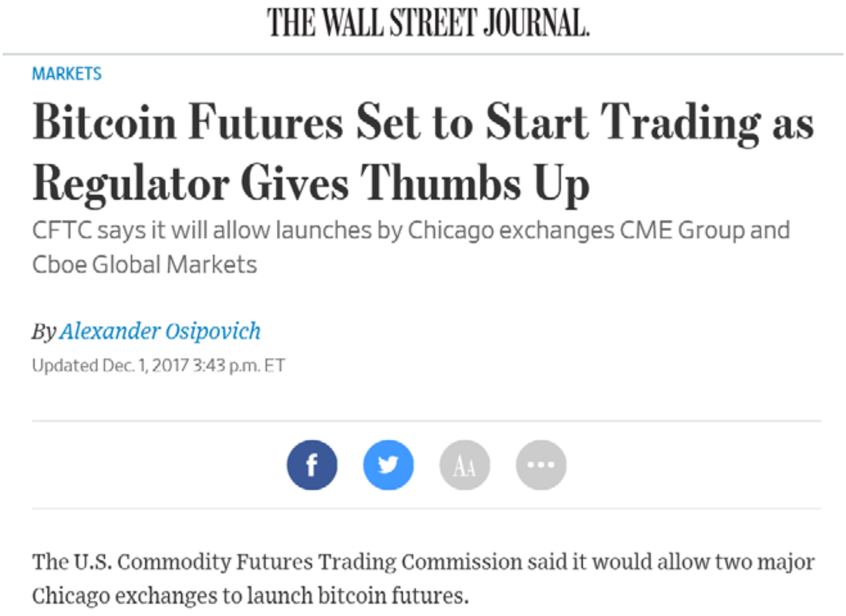
Bitcoin exchange Coinbase ordered to hand over customer data to IRS

A federal court has ordered Coinbase, which operates the largest U.S. exchange for buying and selling Bitcoins, to hand over information to IRS on more than 14,000 customers suspected of evading taxes.

The ruling by U.S. Magistrate Judge Jacqueline Scott Corley, calls for Coinbase to provide the tax agency with the name, birth date, address and taxpayer identification number of customers who had the Bitcoin equivalent of $20,000 or more in their accounts in any one year between 2013 and 2015.

According to Coinbase, the order will only affect its highest transacting clients, roughly 1 percent of its total customer base of roughly 6 million account holder. The IRS originally demanded records of all Coinbase customers.

https://www.cbsnews.com/news/bitcoin-coinbase-ordered-to-hand-over-customer-data-to-irs/



THE WALL STREET JOURNAL.

MARKETS

Bitcoin Futures Set to Start Trading as Regulator Gives Thumbs Up

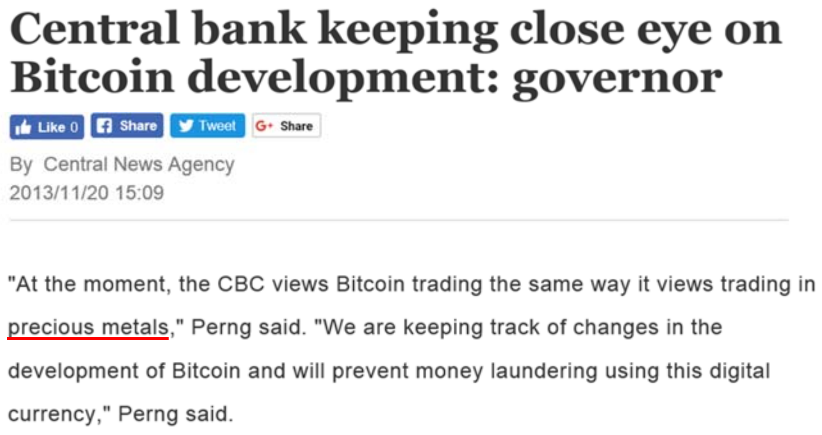
CFTC says it will allow launches by Chicago exchanges CME Group and Cboe Global Markets

By Alexander Osipovich

Updated Dec. 1, 2017 3:43 p.m. ET

The U.S. Commodity Futures Trading Commission said it would allow two major Chicago exchanges to launch bitcoin futures.

https://www.wsj.com/articles/regulator-opens-way-to-bitcoin-futures-1512133201



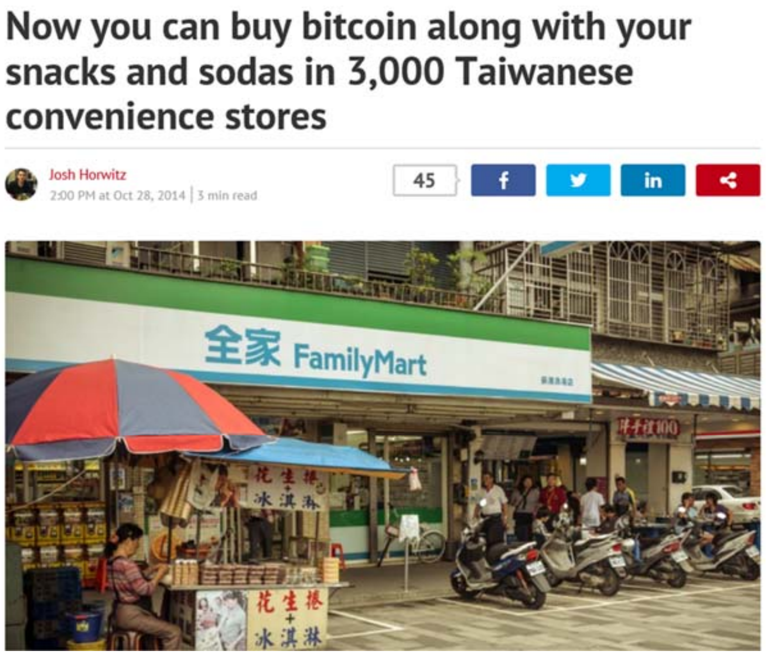
Central bank keeping close eye on Bitcoin development: governor

By Central News Agency
2013/11/20 15:09

"At the moment, the CBC views Bitcoin trading the same way it views trading in precious metals," Perng said. "We are keeping track of changes in the development of Bitcoin and will prevent money laundering using this digital currency," Perng said.

CBC – Central Bank of the Republic of China (Taiwan)
Head : Perng Fai-nan 彭淮南

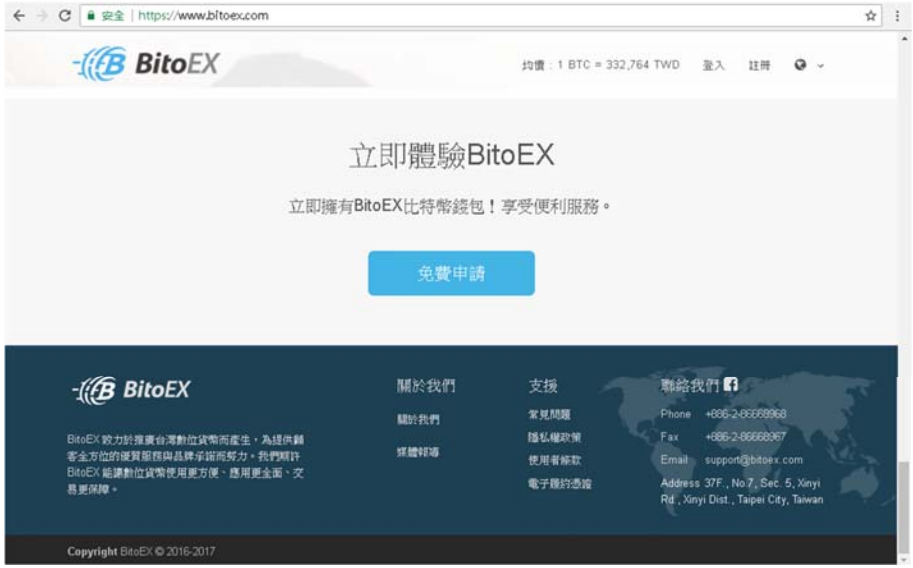
http://www.taiwannews.com.tw/en/news/2349491



Now you can buy bitcoin along with your snacks and sodas in 3,000 Taiwanese convenience stores

Josh Horwitz
2:00 PM at Oct 28, 2014 | 3 min read

https://www.techinasia.com/now-you-can-buy-bitcoin-with-your-red-bull-and-chewing-gum-in-3000-taiwanese-convenience-stores-bitoex-family-mart



https://www.bitoex.com

BitoEX

均價：1 BTC = 332,764 TWD 登入 註冊

立即體驗BitoEX

立即擁有BitoEX比特幣錢包！享受便利服務。

免費申請

BitoEX

BitoEX 致力於推廣台灣數位貨幣而產生，為提供顧客全方位的優質服務與品牌承諾而努力。我們期許 BitoEX 能讓數位貨幣使用更方便、應用更全面、交易更保障。

關於我們
- 關於我們
- 媒體報導

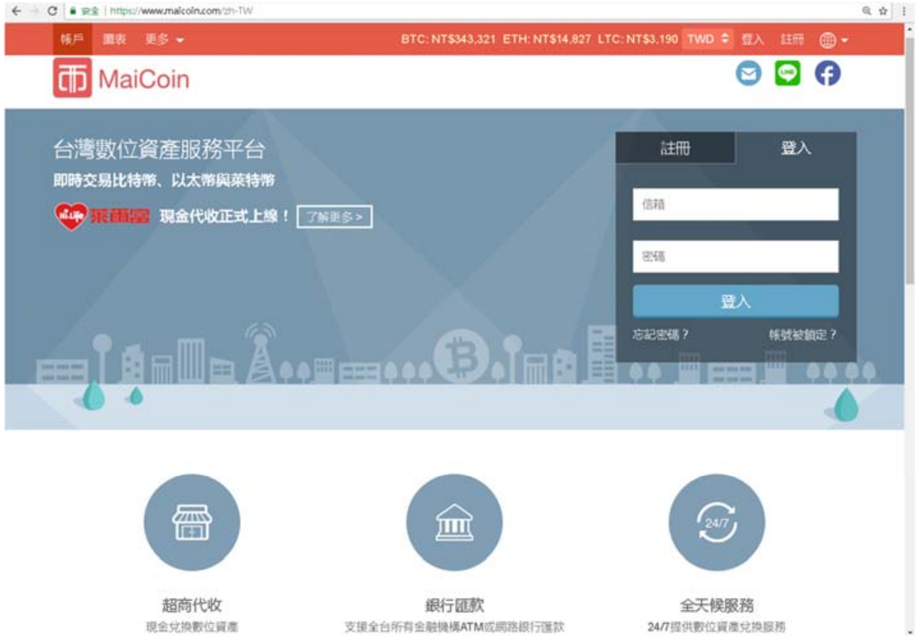
支援
- 常見問題
- 隱私權政策
- 使用者條款
- 電子簽約憑證

聯絡我們

Phone +886-2-86668968
Fax +886-2-86668967
Email support@bitoex.com
Address 37F., No.7, Sec. 5, Xinyi Rd., Xinyi Dist., Taipei City, Taiwan

Copyright BitoEX © 2016-2017

https://www.bitoex.com/



https://www.maicoin.com/zh-TW

帳戶 圖表 更多 BTC: NT$343,321 ETH: NT$14,827 LTC: NT$3,190 TWD 登入 註冊

MaiCoin

台灣數位資產服務平台

即時交易比特幣、以太幣與萊特幣

萊爾富 現金代收正式上線！ 了解更多 >

註冊 登入

信箱

密碼

登入

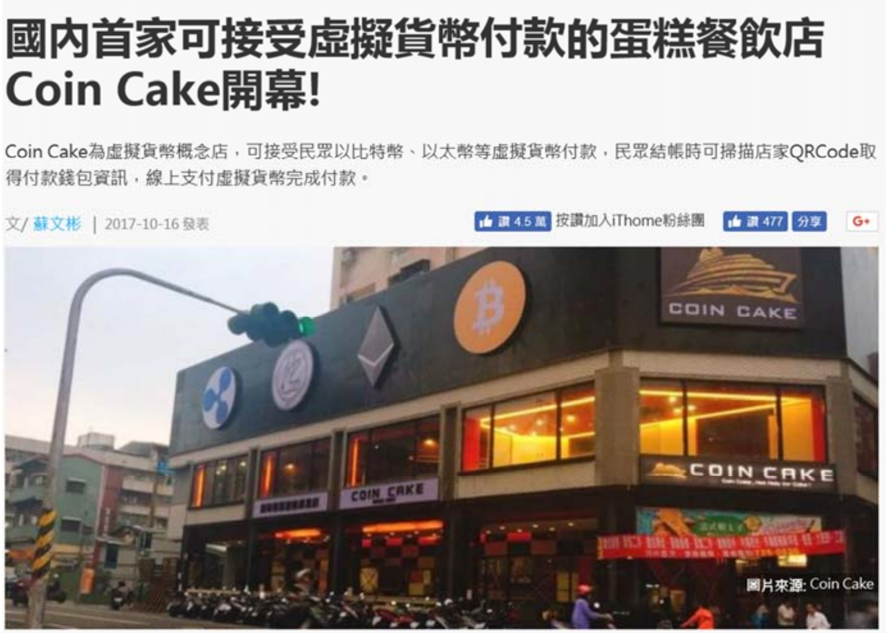
忘記密碼？ 帳號被鎖定？

超商代收
現金兌換數位資產

銀行匯款
支援全台所有金融機構ATM或網路銀行匯款

全天候服務
24/7提供數位資產兌換服務

https://www.maicoin.com/zh-TW



國內首家可接受虛擬貨幣付款的蛋糕餐飲店Coin Cake開幕!

Coin Cake為虛擬貨幣概念店，可接受民眾以比特幣、以太幣等虛擬貨幣付款，民眾結帳時可掃描店家QRCode取得付款錢包資訊，線上支付虛擬貨幣完成付款。

文/ 蘇文彬 | 2017-10-16 發表

讚 4.5 萬 按讚加入iThome粉絲團 讚 477 分享 G+

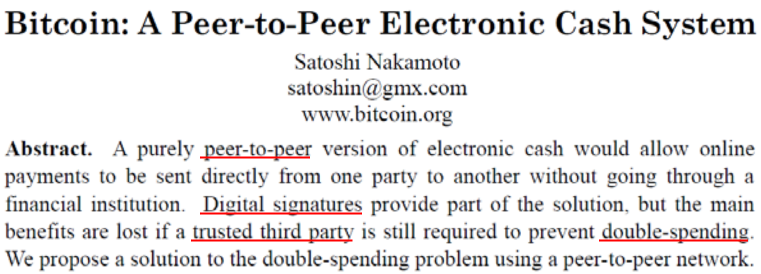
圖片來源: Coin Cake

https://www.ithome.com.tw/news/117488

Birth of Bitcoin

Birth of Bitcoin

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

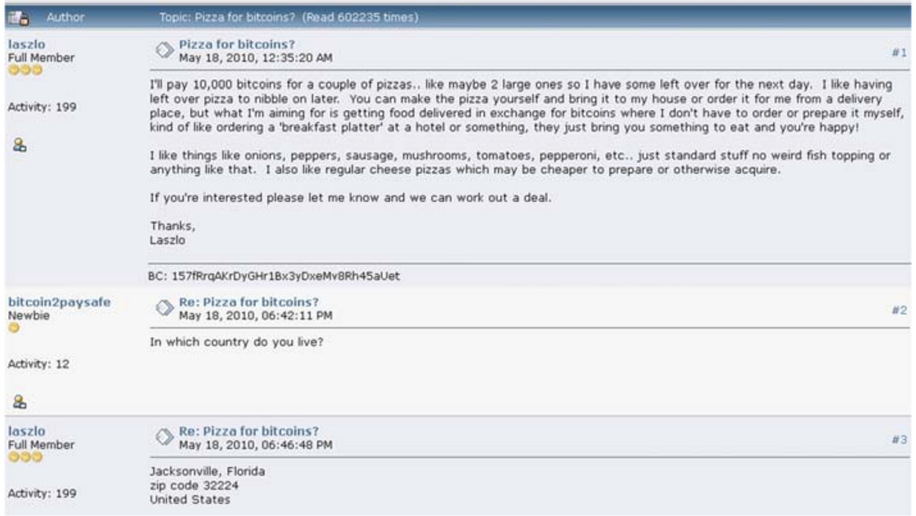


Bitcoin: A Peer-to-Peer Electronic Cash System

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 中本聰



Author | Topic: Pizza for bitcoins? (Read 602235 times)

laszlo
Full Member
Activity: 199

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

bitcoin2paysafe
Newbie
Activity: 12

Re: Pizza for bitcoins?
May 18, 2010, 06:42:11 PM #2

In which country do you live?

laszlo
Full Member
Activity: 199

Re: Pizza for bitcoins?
May 18, 2010, 06:46:48 PM #3

Jacksonville, Florida
zip code 32224
United States

https://bitcointalk.org/index.php?topic=137.0

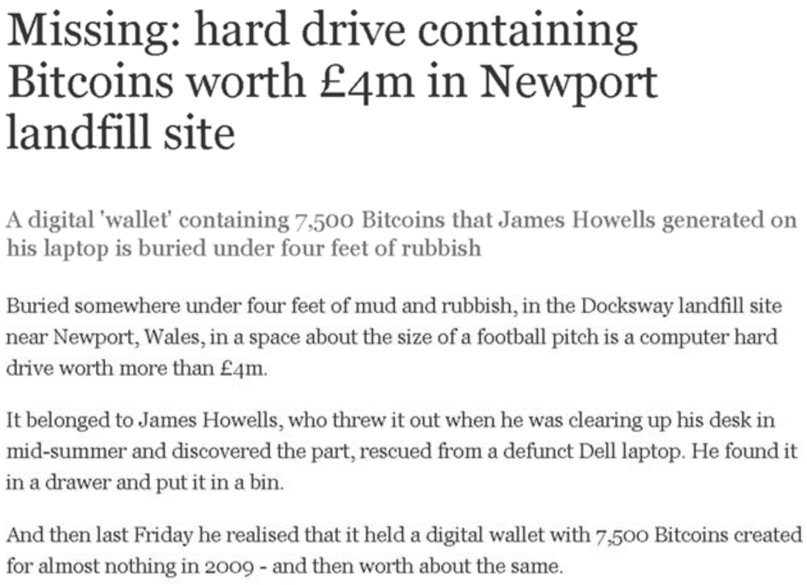
Bitcoin Pizza Day: Celebrating the Pizzas Bought for 10,000 BTC

May 22, 2014 at 19:16 by Grace Caffyn

Today, bitcoiners the world over will celebrate the anniversary of the most expensive pizzas in history.

Bought on 22nd May 2010 by Laszlo Hanyecz, the programmer paid a fellow Bitcoin Talk forum user 10,000 BTC for two Papa John's pizzas. Back then – when the technology was just over a year old – that equated to roughly $25, but is $5.12m by today's exchange rate.

http://www.coindesk.com/bitcoin-pizza-day-celebrating-pizza-bought-10000-btc



Missing: hard drive containing Bitcoins worth £4m in Newport landfill site

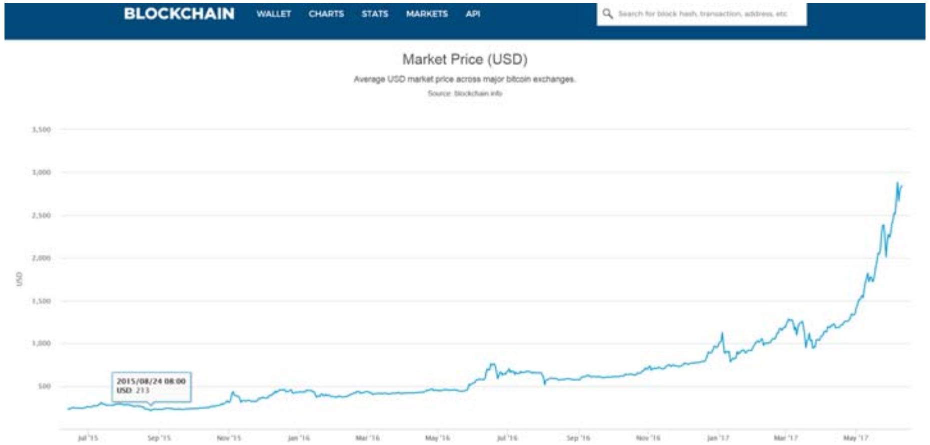
A digital 'wallet' containing 7,500 Bitcoins that James Howells generated on his laptop is buried under four feet of rubbish

Buried somewhere under four feet of mud and rubbish, in the Docksway landfill site near Newport, Wales, in a space about the size of a football pitch is a computer hard drive worth more than £4m.

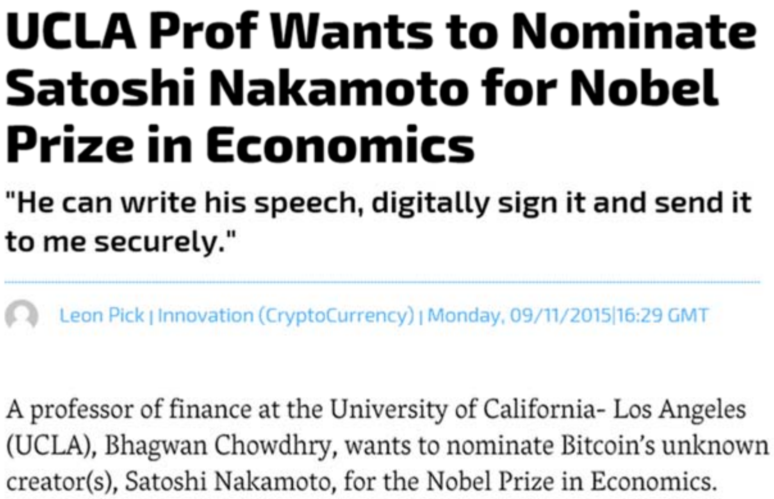
It belonged to James Howells, who threw it out when he was clearing up his desk in mid-summer and discovered the part, rescued from a defunct Dell laptop. He found it in a drawer and put it in a bin.

And then last Friday he realised that it held a digital wallet with 7,500 Bitcoins created for almost nothing in 2009 - and then worth about the same.

https://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site



https://blockchain.info/charts/market-price?timespan=2years



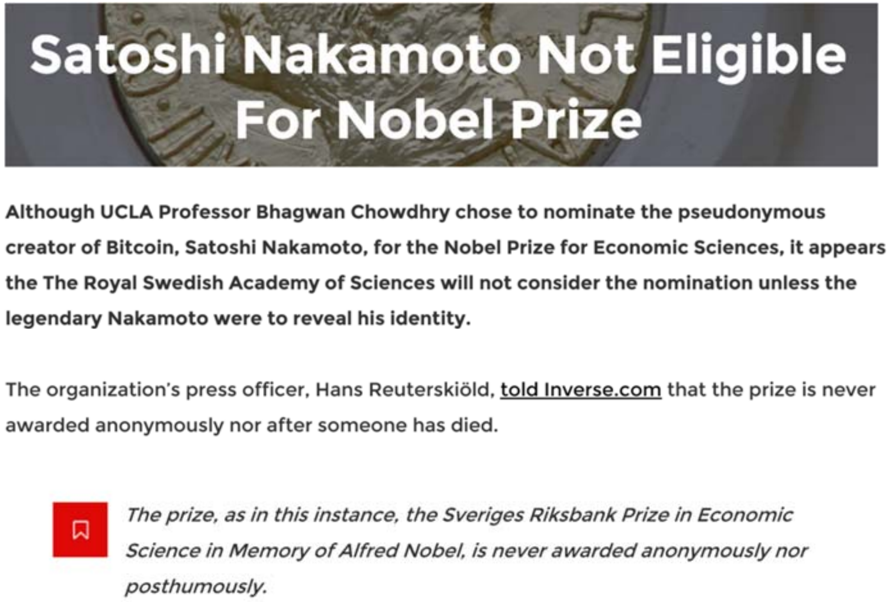
UCLA Prof Wants to Nominate Satoshi Nakamoto for Nobel Prize in Economics

"He can write his speech, digitally sign it and send it to me securely."

Leon Pick | Innovation (CryptoCurrency) | Monday, 09/11/2015|16:29 GMT

A professor of finance at the University of California- Los Angeles (UCLA), Bhagwan Chowdhry, wants to nominate Bitcoin's unknown creator(s), Satoshi Nakamoto, for the Nobel Prize in Economics.

http://www.financemagnates.com/cryptocurrency/innovation/ucla-prof-wants-to-nominate-satoshi-nakamoto-for-nobel-prize-in-economics



Satoshi Nakamoto Not Eligible For Nobel Prize

Although UCLA Professor Bhagwan Chowdhry chose to nominate the pseudonymous creator of Bitcoin, Satoshi Nakamoto, for the Nobel Prize for Economic Sciences, it appears the The Royal Swedish Academy of Sciences will not consider the nomination unless the legendary Nakamoto were to reveal his identity.

The organization's press officer, Hans Reuterskiöld, told Inverse.com that the prize is never awarded anonymously nor after someone has died.

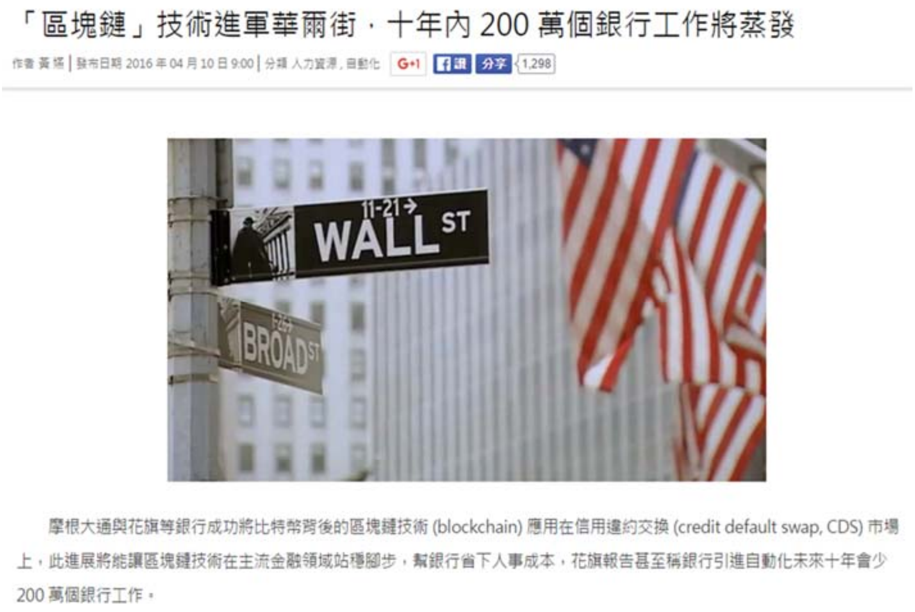
> *The prize, as in this instance, the Sveriges Riksbank Prize in Economic Science in Memory of Alfred Nobel, is never awarded anonymously nor posthumously.*

https://www.cryptocoinsnews.com/satoshi-nakamoto-not-eligible-nobel-prize

FinTech

區塊鏈 Blockchain

- 區塊鏈技術是 Bitcoin 的基礎，受全世界重視的程度已經超越 Bitcoin 本身
- “A blockchain is a decentralized network with memory” (Vitalik Buterin)
- 關鍵：以 hash function 串接資料
  - Hash function – 雜湊函數、赫序函數、哈希函數

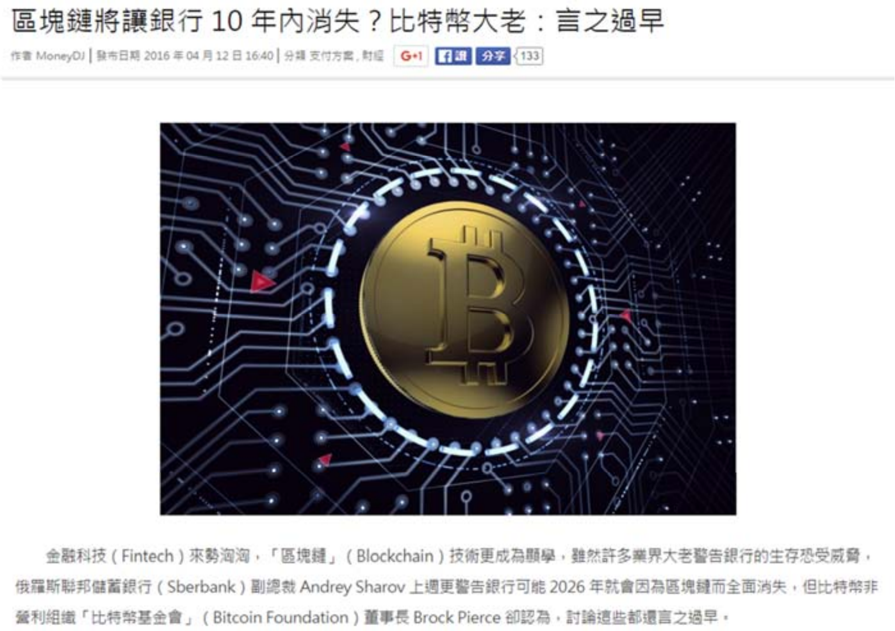


「區塊鏈」技術進軍華爾街，十年內 200 萬個銀行工作將蒸發

作者 黃 嫣 | 發布日期 2016 年 04 月 10 日 9:00 | 分類 人力資源, 自動化 G+1 讚 分享 1,298

摩根大通與花旗等銀行成功將比特幣背後的區塊鏈技術 (blockchain) 應用在信用違約交換 (credit default swap, CDS) 市場上，此進展將能讓區塊鏈技術在主流金融領域站穩腳步，幫銀行省下人事成本，花旗報告甚至稱銀行引進自動化未來十年會少 200 萬個銀行工作。

http://technews.tw/2016/04/10/blockchain-applied-on-wall-street

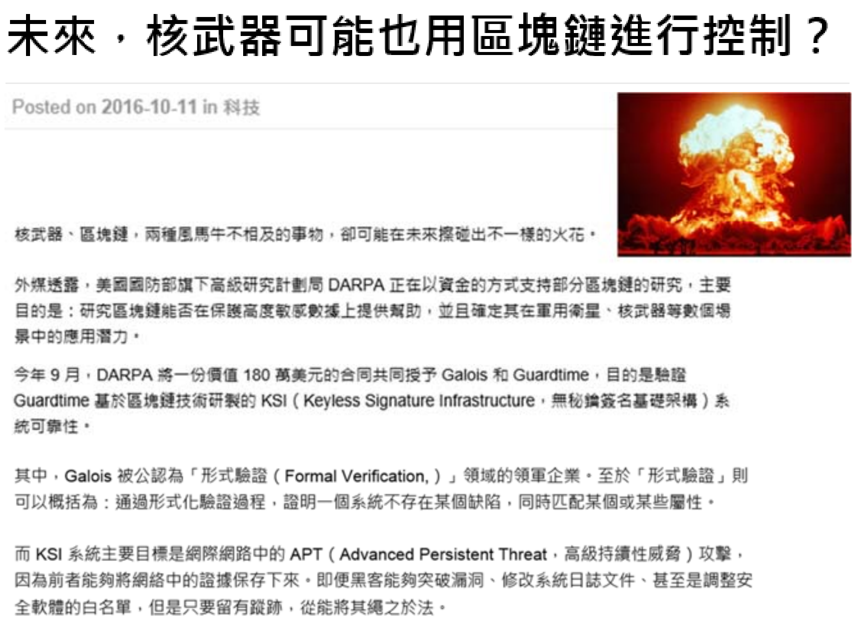


區塊鏈將讓銀行 10 年內消失？比特幣大老：言之過早

作者 MoneyDJ | 發布日期 2016 年 04 月 12 日 16:40 | 分類 支付方案, 財經 G+1 讚 分享 133

金融科技（Fintech）來勢洶洶，「區塊鏈」（Blockchain）技術更成為顯學，雖然許多業界大老警告銀行的生存恐受威脅，俄羅斯聯邦儲蓄銀行（Sberbank）副總裁 Andrey Sharov 上週更警告銀行可能 2026 年就會因為區塊鏈而全面消失，但比特幣非營利組織「比特幣基金會」（Bitcoin Foundation）董事長 Brock Pierce 卻認為，討論這些都還言之過早。

http://finance.technews.tw/2016/04/12/blockchain-bank-fintech



未來，核武器可能也用區塊鏈進行控制？

Posted on 2016-10-11 in 科技

核武器、區塊鏈，兩種風馬牛不相及的事物，卻可能在未來擦碰出不一樣的火花。

外媒透露，美國國防部旗下高級研究計劃局 DARPA 正在以資金的方式支持部分區塊鏈的研究，主要目的是：研究區塊鏈能否在保護高度敏感數據上提供幫助，並且確定其在軍用衛星、核武器等數個場景中的應用潛力。

今年 9 月，DARPA 將一份價值 180 萬美元的合同共同授予 Galois 和 Guardtime，目的是驗證 Guardtime 基於區塊鏈技術研製的 KSI（Keyless Signature Infrastructure，無秘鑰簽名基礎架構）系統可靠性。

其中，Galois 被公認為「形式驗證（Formal Verification,）」領域的領軍企業。至於「形式驗證」則可以概括為：通過形式化驗證過程，證明一個系統不存在某個缺陷，同時匹配某個或某些屬性。

而 KSI 系統主要目標是網際網路中的 APT（Advanced Persistent Threat，高級持續性威脅）攻擊，因為前者能夠將網絡中的證據保存下來。即便黑客能夠突破漏洞、修改系統日誌文件、甚至是調整安全軟體的白名單，但是只要留有蹤跡，從能將其繩之於法。

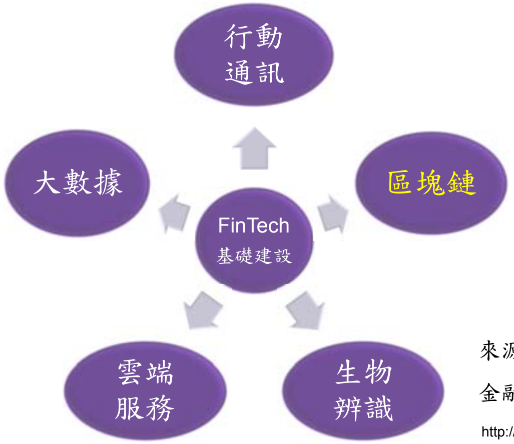
https://kknews.cc/tech/m4kmbp.html

金融科技 FinTech

- **FinTech** (Financial Technology) is a buzzword today
- **FinTech** is an economic industry composed of companies that use technology to make **financial services** more **efficient**
- **FinTech** companies are generally startups founded with the purpose of disrupting incumbent financial systems and corporations that rely less on **software**

https://en.wikipedia.org/wiki/Financial_technology

FinTech 基礎建設

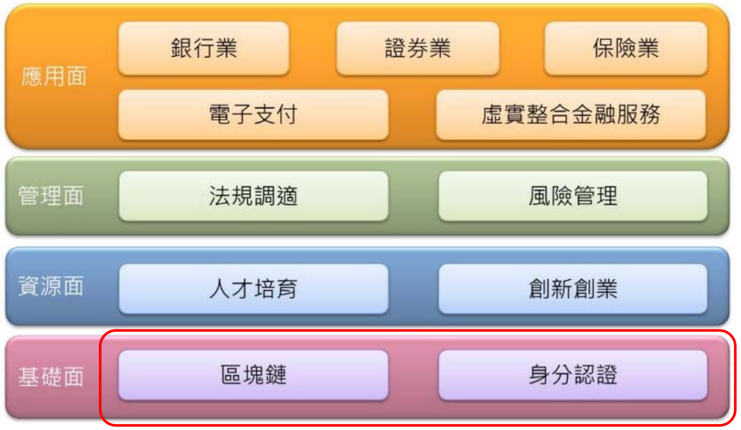


來源 ： 金管會（金融監督管理委員會）

金融科技發展策略白皮書　2016.5.12

http://www.fsc.gov.tw/ch/home.jsp?id=478&parentpath=0,7

政策四大面向 十一項重點



應用面：銀行業、證券業、保險業、電子支付、虛實整合金融服務

管理面：法規調適、風險管理

資源面：人才培育、創新創業

基礎面：區塊鏈、身分認證

Crypto Inside!

Cryptography

Cryptography 密碼學

Bitcoin Tutorial

- **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 security with cryptography. That is why **Bitcoin is at heart a cryptographic protocol**.”

The Book “Mastering Bitcoin”

O'REILLY

Mastering Bitcoin

UNLOCKING DIGITAL CRYPTOCURRENCIES

Andreas M. Antonopoulos

Public Key Cryptography (PKC)

Caesar Cipher

- Gāius Jūlius Caesar (100 BC – 44 BC)
  - A Roman military and political leader and one of the most influential men in world history
  - He played a critical role in the transformation of the Roman Republic into the Roman Empire
- Caesar Cipher
  - Encode: A ↔ 0, B ↔ 1, C ↔ 2, …, Y ↔ 24, Z ↔ 25
    - Plaintext: SPY (18 15 24)
    - Ciphertext: VSB (21 18 1)
  - Encryption: $c = p + 3 \mod 26$
  - Decryption: $p = c - 3 \mod 26$

Symmetric Cryptography

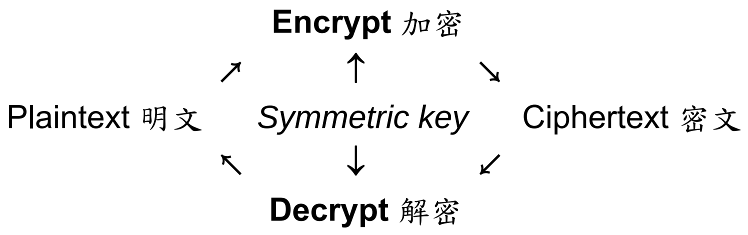
Alice
Bob
K
K

- Analogy: Safe with a strong lock, only Alice and Bob have a copy of the key
  - Alice encrypts

    → locks message in the safe with her key
  - Bob decrypts

    → uses his copy of the key to open the safe

Symmetric Cryptography



Encrypt 加密

Plaintext 明文 *Symmetric key* Ciphertext 密文

Decrypt 解密

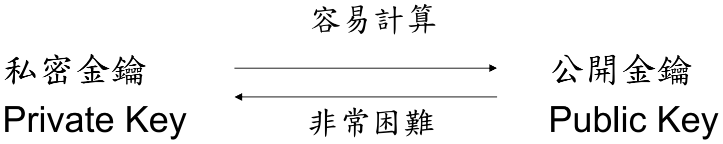
DES (Data Encryption Standard)

AES (Advanced Encryption Standard)

Asymmetric Cryptography

- New Idea: Use the “mailbox” principle
  - Everyone can drop a letter
  - But only the owner has the correct key to open the box

私密金鑰 與 公開金鑰



容易計算

私密金鑰
Private Key

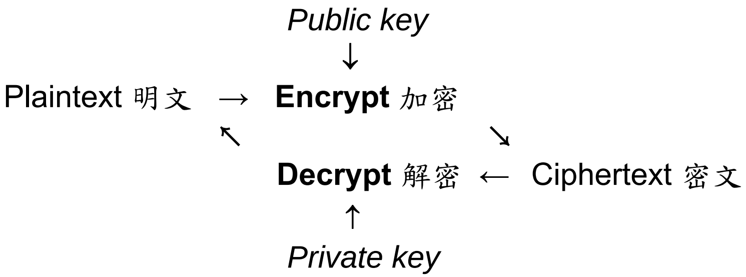
非常困難

公開金鑰
Public Key

藉由數學工具達成此目的

Whit Diffie 和 Martin Hellman 於 1976 年提出此觀念

Public Key Cryptosystem 公鑰密碼系統

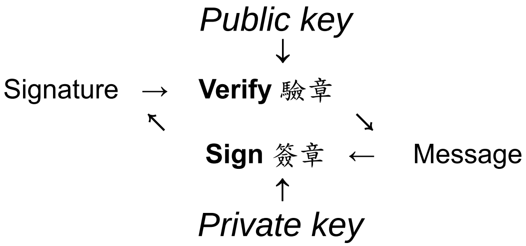


Public key
↓
Plaintext 明文 → **Encrypt** 加密
↖ ↘
Decrypt 解密 ← Ciphertext 密文
↑
Private key

RSA (Rivest – Shamir – Adleman 1977)

ECC (Elliptic Curve Cryptosystem 橢圓曲線密碼系統)

Digital Signature 數位簽章



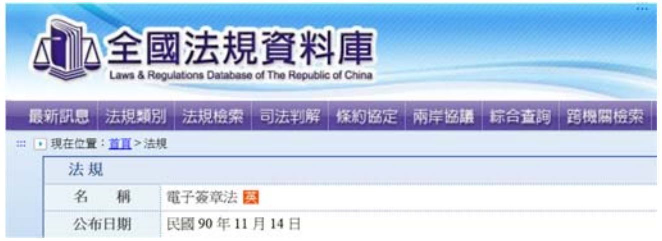
Public key
↓
Signature → **Verify** 驗章
↖ ↘
Sign 簽章 ← Message
↑
Private key

* 資料完整性 (Integrity)

* 身份鑑別性 (Authentication)

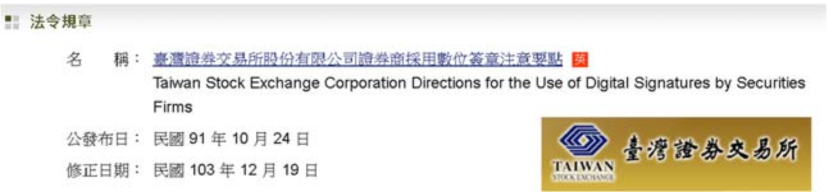
* 不可否認性 (Non-Repudiation)

Electronic Signatures Act



法規

名　稱	電子簽章法 英
公布日期	民國 90 年 11 月 14 日



法令規章

名　稱： 臺灣證券交易所股份有限公司證券商採用數位簽章注意要點 英
Taiwan Stock Exchange Corporation Directions for the Use of Digital Signatures by Securities Firms

公發布日： 民國 91 年 10 月 24 日

修正日期： 民國 103 年 12 月 19 日

Certificate

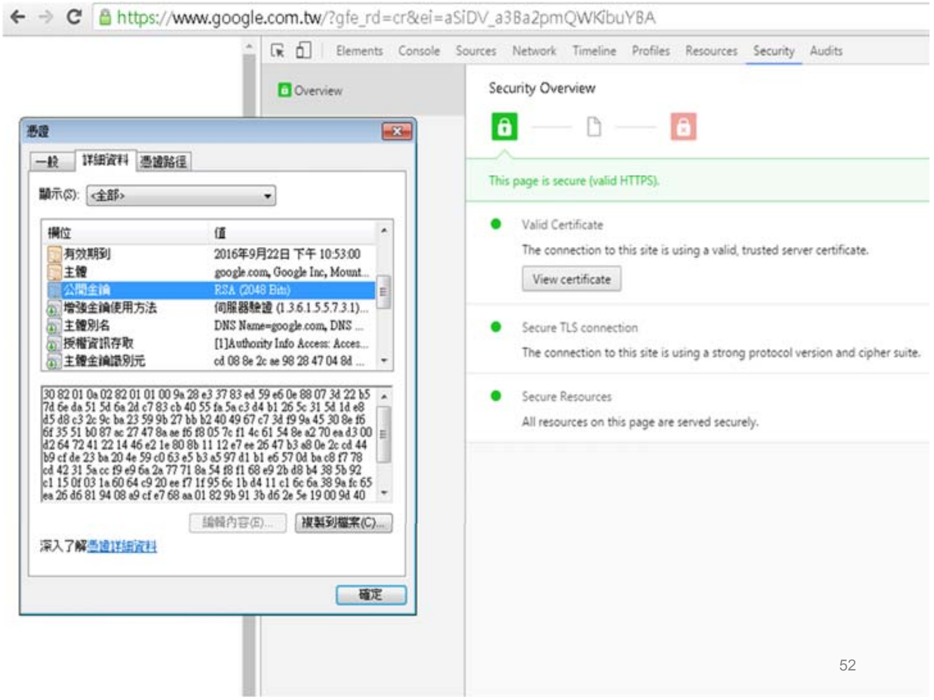
Certificate

- Certificates bind the identity of user to public key
- The trusted authority that issues the certificate is referred to as certification authority (CA)
- The party who receives a certificate, e.g., Bob, verifies Alice's public key using the public key of the CA
- Cert(Alice) =

$(k_{pub_A}, \text{ID(Alice)}, sig_{k_{pr_{CA}}}(k_{pub_A}, \text{ID(Alice)}))$

Google
https://www.google.com.tw/webhp?source=search_app&gws_rd=ssl
Google+ 搜尋 圖片 地圖 Play YouTube 新聞 Gmail 更多 ▾
Google 台灣
Google 搜尋
好手氣
廣告 商業 Google 完全手冊
https://www

HTTPS (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet.



顯示(S): <全部>

欄位	值
有效期到	2016年9月22日 下午 10:53:00
主體	google.com, Google Inc, Mount...
公開金鑰	RSA (2048 Bits)
增強金鑰使用方法	伺服器驗證 (1.3.6.1.5.5.7.3.1)...
主體別名	DNS Name=google.com, DNS ...
授權資訊存取	[1]Authority Info Access: Acces...
主體金鑰識別元	cd 08 8e 2c ae 98 28 47 04 8d ...

```
30 82 01 0a 02 82 01 01 00 9a 28 e3 37 83 ed 59 e6 0e 88 07 3d 22 b5
7d 6e da 51 5d 6a 2d c7 83 cb 40 55 fa 5a c3 d4 b1 26 5c 31 5d 1d e8
d5 d8 c3 2c 9c ba 23 59 9b 27 bb b2 40 49 67 c7 3d f9 9a 45 30 8e f6
6f 35 51 b0 87 ac 27 47 8a ae f6 f8 05 7c f1 4c 61 54 8e a2 70 ea d3 00
d2 64 72 41 22 14 46 e2 1e 80 8b 11 12 e7 ee 26 47 b3 a8 0e 2c cd 44
b9 cf de 23 ba 20 4e 59 c0 63 e5 b3 a5 97 d1 b1 e6 57 0d ba c8 f7 78
cd 42 31 5a cc f9 e9 6a 2a 77 71 8a 54 f8 f1 68 e9 2b d8 b4 38 5b 92
c1 15 0f 03 1a 60 64 c9 20 ee f7 1f 95 6c 1b d4 11 c1 6c 6a 38 9a fc 65
ea 26 d6 81 94 08 a9 cf e7 68 aa 01 82 9b 91 3b d6 2e 5e 19 00 9d 40
```

深入了解憑證詳細資料

Security Overview

This page is secure (valid HTTPS).

Valid Certificate

The connection to this site is using a valid, trusted server certificate.

Secure TLS connection

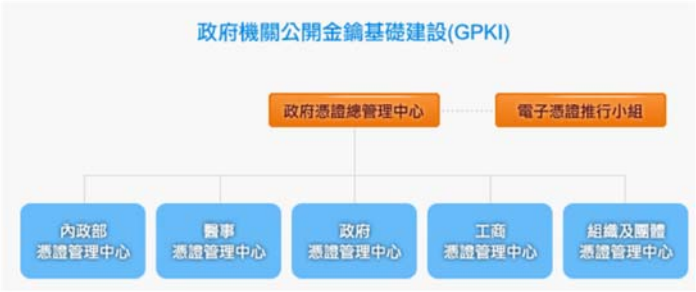
The connection to this site is using a strong protocol version and cipher suite.

Secure Resources

All resources on this page are served securely.

PKI – Public Key Infrastructure

- The entire system that is formed by CAs together with the necessary support mechanisms is called a Public-Key Infrastructure (PKI)



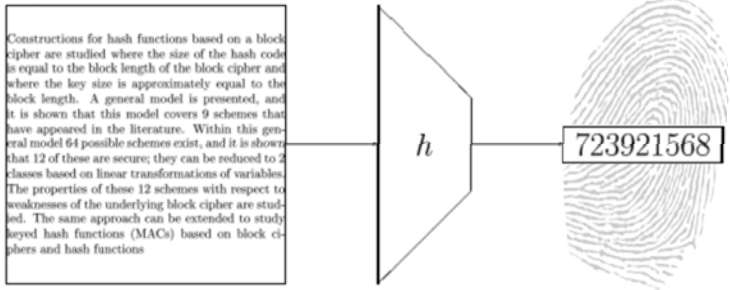
政府機關公開金鑰基礎建設(GPKI)

http://moica.nat.gov.tw/moica.html

Hash Function

Hash Function 雜湊函數

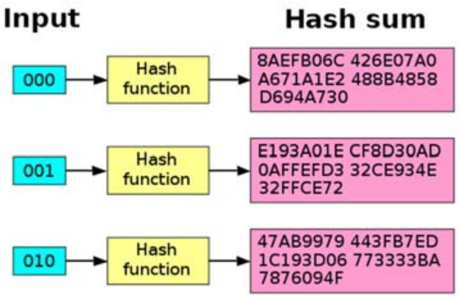
- An efficient function mapping binary strings of **arbitrary length** to binary strings of **fixed length**, called the **hash-value** or **hash-code** (**fingerprint**, **checksum**)



Constructions for hash functions based on a block cipher are studied where the size of the hash code is equal to the block length of the block cipher and where the key size is approximately equal to the block length. A general model is presented, and it is shown that this model covers 9 schemes that have appeared in the literature. Within this general model 64 possible schemes exist, and it is shown that 12 of these are secure; they can be reduced to 2 classes based on linear transformations of variables. The properties of these 12 schemes with respect to weaknesses of the underlying block cipher are studied. The same approach can be extended to study keyed hash functions (MACs) based on block ciphers and hash functions

Avalanche Effect 雪崩效應

- A desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions
- When an input is changed slightly (e.g., flipping a single bit) the output changes significantly (e.g., half the output bits flip)

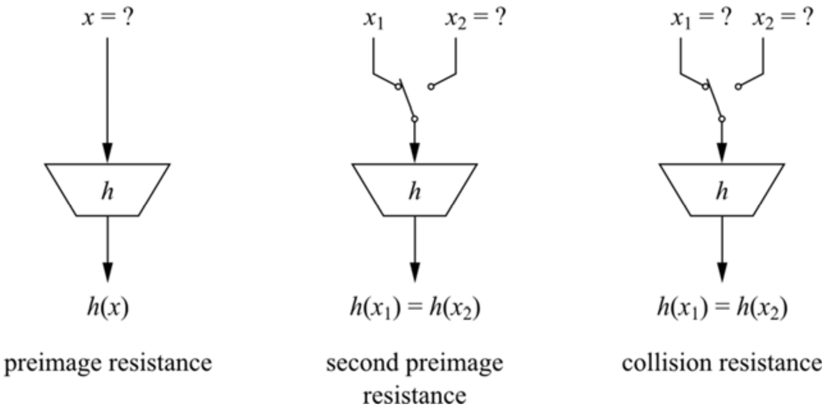


Input
Hash sum
000
Hash function
8AEFB06C 426E07A0 A671A1E2 488B4858 D694A730
001
Hash function
E193A01E CF8D30AD 0AFFEFD3 32CE934E 32FFCE72
010
Hash function
47AB9979 443FB7ED 1C193D06 773333BA 7876094F

The **SHA-1** hash function exhibits good avalanche effect. When a single bit is changed the hash sum becomes completely different.

https://en.wikipedia.org/wiki/Avalanche_effect

Security Properties



Cryptographic Hash Functions

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

SHA: Secure Hash Algorithm

- The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Bitwise operations	Security (bits)
SHA-1 FIPS 180		160	160	512	80	and, or, add, xor, rot	Theoretical attack (2^{61})
SHA-2 FIPS 180	SHA-224	224	256 (8 × 32)	512	64	and, or, xor, shr, rot, add	112
	SHA-256 Bitcoin	256					128
	SHA-384	384	512 (8 × 64)	1024	80	and, or, xor, shr, rot, add	192
	SHA-512	512					256
	SHA-512/224	224					112
	SHA-512/256	256					128
SHA-3 FIPS 202	SHA3-224	224	1600 (5 × 5 × 64)	1152	24	and, xor, rot, not	112
	SHA3-256 Ethereum (Keccak 256)	256		1088			128
	SHA3-384	384		832			192
	SHA3-512	512		576			256

https://en.wikipedia.org/wiki/Secure_Hash_Algorithm

Merkle-Damgård Construction for SHA-1 / SHA-2

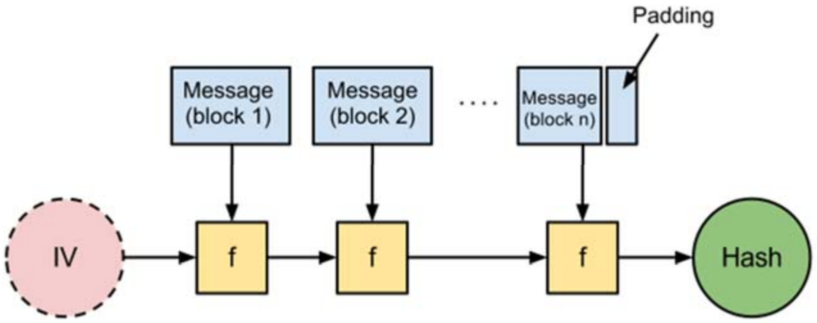


Image Courtesy http://joncave.co.uk/2012/08/i-captured-the-flag

SHA-256

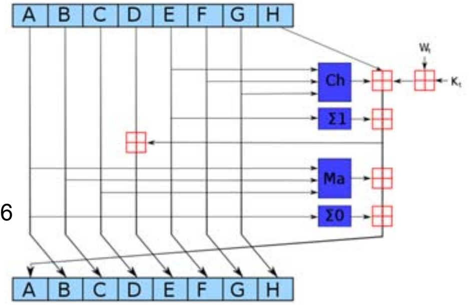
- One iteration in a SHA-2 family compression function
  - The blue components perform the following operations

$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$

$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$

$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$



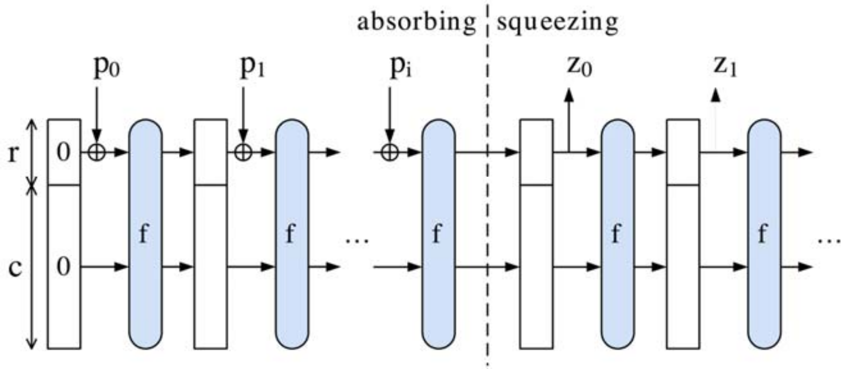
- The bitwise rotation uses different constants for SHA-512
- The given numbers are for SHA-256
  - ⊞ is addition modulo 2^{32}

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

SHA-3 Competition Winner: Keccak

- Designers:
  - Guido Bertoni (Italy) of STMicroelectronics
  - Joan Daemen (Belgium) of STMicroelectronics
  - Gilles Van Assche (Belgium) of STMicroelectronics
  - Michaël Peeters (Belgium) of NXP Semiconductors
- Not very fast in software implementation, but in hardware implementations it is notably faster than all other finalists
- In its largest instance, the state consists of a 5 × 5 array of 64-bit words, 1600 bits total
  - Reduced versions are defined for smaller power-of-2 word sizes w down to 1 bit (25 bits total state)
  - Smaller state sizes can be used to test cryptanalytic attacks
  - Intermediate state sizes (e.g., from $w = 4$, 100 bits, to $w = 32$, 800 bits) also provide practical, lightweight, alternatives

SHA-3 / Keccak: Sponge Construction



Applications

- Verifying the Integrity of Files or Messages
- Password Verification
- File or Data Identifier
- Pseudorandom Generation & Key Derivation
- Proof-of-Work (POW)

https://en.wikipedia.org/wiki/Cryptographic_hash_function

Abstract Algebra

Floor and Ceiling

- **Definition**
  1) The **floor** $\lfloor x \rfloor$ of $x \in \boldsymbol{R}$ is the largest integer $\leq x$
  2) The **ceiling** $\lceil x \rceil$ of $x \in \boldsymbol{R}$ is the smallest integer $\geq x$
- **Example**
  - $\lfloor e \rfloor = 2$, $\lceil e \rceil = 3$, $\lfloor -3.1416 \rfloor = -4$, $\lceil -3.1416 \rceil = -3$
- **Example**
  1) $25 = 3 \times 7 + 4$ [7: divisor, 3: quotient, 4: remainder]
  2) $25 \bmod 7 = 25 - \lfloor 25/7 \rfloor \times 7 = 25 - 3 \times 7 = 25 - 21$

Modular Function

- **Definition**

  $m, n \in \boldsymbol{Z}$, $m > 0$, define

  n* mod *m $= n - \lfloor n/m \rfloor \times m$
  - i.e., the remainder after dividing n by m, which is ≥ 0 and $< m$
- **Example** 58 in the base 3 representation

$a_0 = 58 \bmod 3 = 1$	$19 = \lfloor 58/3 \rfloor$
$a_1 = 19 \bmod 3 = 1$	$6 = \lfloor 19/3 \rfloor$
$a_2 = 6 \bmod 3 = 0$	$2 = \lfloor 6/3 \rfloor$
$a_3 = 2 \bmod 3 = 2$	$0 = \lfloor 2/3 \rfloor$

$(2011)_3 = 2 \times 3^3 + 0 \times 3^2 + 1 \times 3^1 + 1 \times 3^0 = 58$

Group 群

- **Definition** A **group** $(G, *)$ is a set G with an operation $*$, such that the following conditions are satisfied：
  1) Closure $a * b \in G$ for all $a, b \in G$
  2) Associativity $a*(b*c) = (a*b)*c$ for all $a,b,c \in G$
  3) Identity There is an element $e \in G$ such that $a = a * e = e * a$ for each $a \in G$
  4) Inverse For each $a \in G$, there is an element $b \in G$ such that $a * b = b * a = e$

Group

- **Example** Each of the following sets with the specified operation is a group
  - $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ with + (addition)
  - $\boldsymbol{Q}^*$, $\boldsymbol{R}^*$, $\boldsymbol{C}^*$ with × (multiplication)
  - $5\boldsymbol{Z} = \{\, 5a \mid a \in \boldsymbol{Z} \,\}$ with +
  - $\{1, -1\}$ with ×
  - $\boldsymbol{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with + modulo 6
  - $\boldsymbol{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ with × modulo 7
  - $\{(x, y) \in \boldsymbol{R}^2 \mid y^2 = x^3 + ax + b\,\} \cup \{\infty\}$ with point addition and point doubling laws on elliptic curves

Abelian Group 交換群

- **Definition** A group $(G, *)$ is **commutative** or **abelian** if $a * b = b * a$ for all $a, b \in G$
- **Example**
  - $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ with + are commutative
  - $\boldsymbol{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ with [× modulo 9] is commutative
  - $\boldsymbol{Z}_p^* = \{1, 2, \ldots, p-1\}$ with [× modulo p] is commutative for every prime p

×	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Cyclic Group 循環群

- **Definition** A group $(G, *)$ is **cyclic** if there exists a **generator** $g \in G$ such that every $a \in G$ is of the form $a = g * \ldots * g$ (n copies) for some $n \in \boldsymbol{Z}$
- **Example**
  - $(\boldsymbol{Z}, +)$ is cyclic with generators 1 and -1
  - $(\boldsymbol{Z}_7^*, \times)$ is cyclic: $\{1 = 3^0 = 3^6,\ 2 = 3^2,\ 3 = 3^1,\ 4 = 3^4,\ 5 = 3^5,\ 6 = 3^3\}$
  - $(\boldsymbol{Z}_9^*, \times)$ is cyclic with generators 2 and 5
- **Example**
  - $(\boldsymbol{Q}, +)$ is not cyclic
  - $(\boldsymbol{Z}_8^*, \times)$ is not cyclic (Klein 4)

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Group Order

- **Definition** The **order** (denoted as $|G|$) of a group $(G, *)$ is the number of the elements in G
- **Example**
  - $|\boldsymbol{Z}_p| = p$, $|\boldsymbol{Z}_p^*| = p - 1$ for any prime p
  - $|\boldsymbol{Z}_9^*| = 6$
  - $|\boldsymbol{Z}_n^*| = |\{a \in \boldsymbol{Z}_n \mid \gcd(a, n) = 1\}| = \phi(n)$
    - Euler ϕ-function [ϕ : phi]