CryptoCurrency & BlockChain

密碼貨幣與區塊鏈 (1)

金融科技導論

陳君明

jmchen@crypto.tw

Agenda

- Status of Bitcoin
- Birth of Bitcoin
- Cryptography
- Public Key Cryptography
- Hash Function
- Transactions
- Block Chain
- Consensus
- Block #0
- Summary

Status of Bitcoin

密碼貨幣市值

http://coinmarketcap.com

2021.03.24 10:00

Cryptocurrencies: 8,933 Markets: 36,842 Market Cap: $1,702,938,892,207 24h Vol: $130,151,867,182 Dominance: BTC: 59.8% ETH: 11.4% ETH Gas: 130 Gwei

Slow	Standard	Fast
100 Gwei	130 Gwei	178 Gwei
~72539 secs	~171 secs	~45 secs

CryptoCurrency Market Capitalizations

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$54,485.99	▼ 0.74%	▼ 3.53%	$1,015,983,111,212	$55,889,478,503 1,026,632 BTC	18,662,556 BTC	
2	Ethereum ETH	$1,676.58	▼ 1.07%	▼ 5.62%	$193,214,537,263	$21,554,965,469 12,848,830 ETH	115,174,425 ETH	
3	Tether USDT	$1.00	▼ 0.08%	▲ 0.09%	$39,879,326,471	$87,527,854,161 87,438,267,547 USDT	39,838,509,134 USDT	
4	Binance Coin BNB	$255.34	▼ 1.39%	▼ 0.64%	$39,415,960,841	$2,002,598,733 7,851,316 BNB	154,532,785 BNB	
5	Cardano ADA	$1.11	▼ 1.16%	▼ 8.18%	$35,616,655,078	$4,481,817,494 4,020,211,664 ADA	31,948,309,441 ADA	
6	Polkadot DOT	$34.08	▼ 4.88%	▼ 3.70%	$31,369,477,649	$1,730,265,009 50,900,722 DOT	922,823,408 DOT	
7	XRP XRP	$0.5447	▼ 5.21%	▲ 16.04%	$24,776,132,590	$7,152,342,591 13,107,177,509 XRP	45,404,028,640 XRP	

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

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

Bitcoin Regulation | News

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

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.

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).

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

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

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

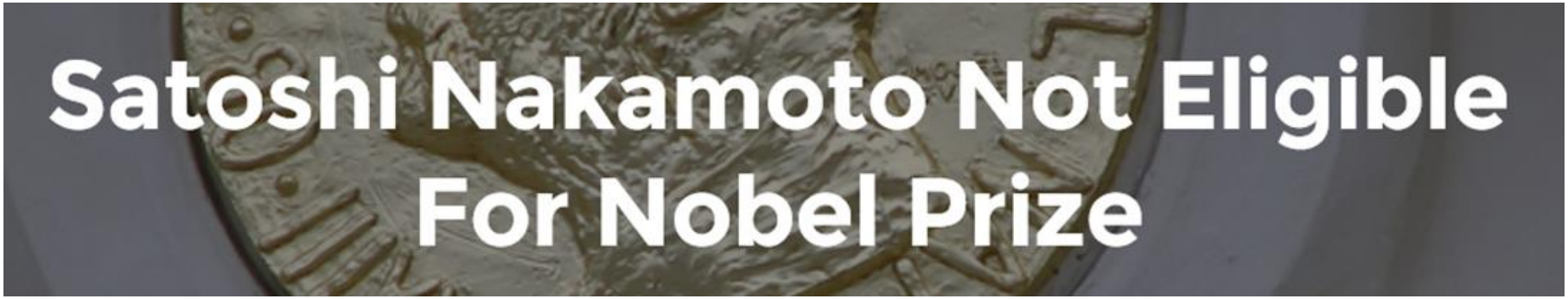
UCLA Prof Wants to Nominate Satoshi Nakamoto for Nobel Prize in Economics

"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.

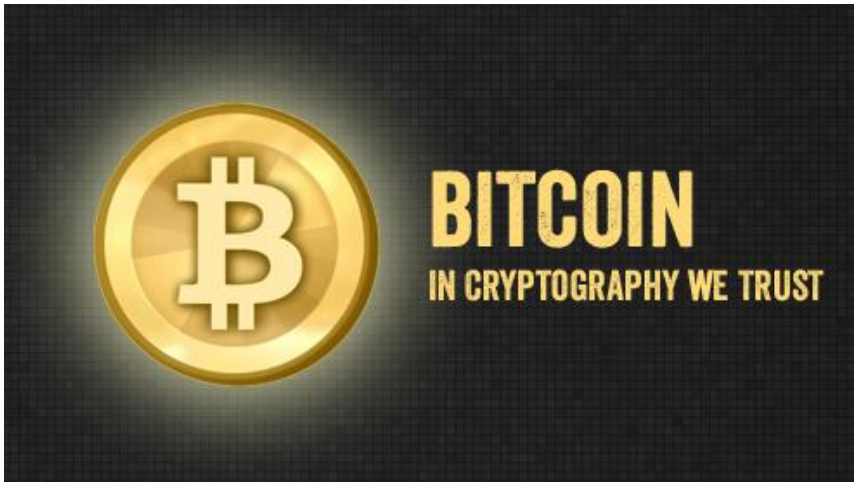
The organization's press officer, Hans Reuterskiöld, told Inverse.com that the prize is never awarded anonymously nor after someone has died.

> *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

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**."

Public Key Cryptography (PKC)

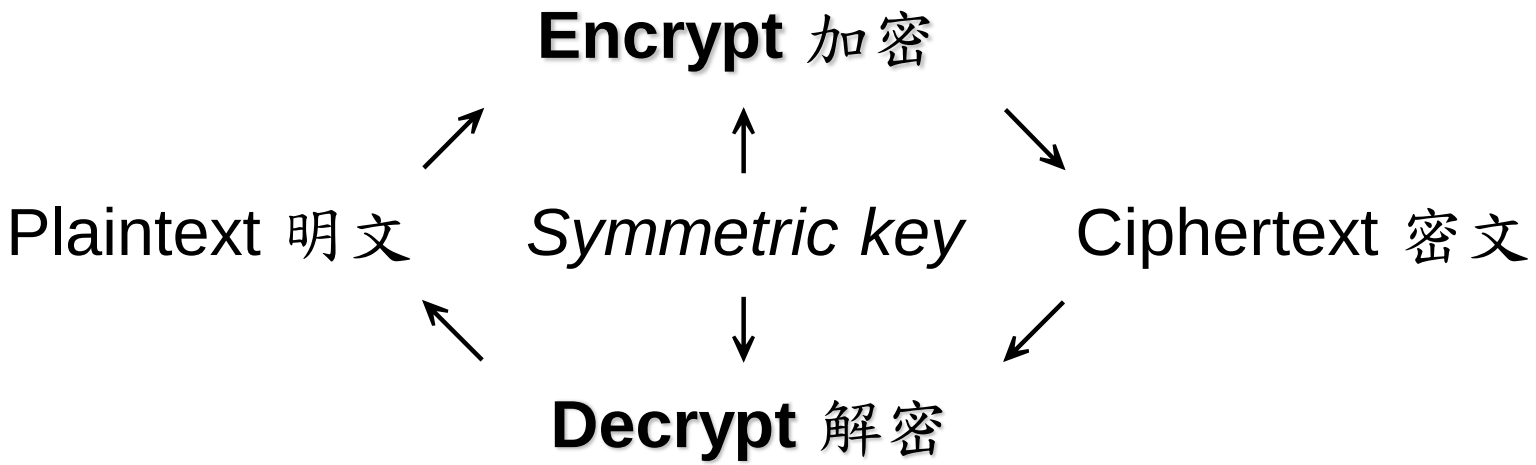
凱撒加密 (Caesar Cipher)

- Gāius Jūlius Caesar (100 BC – 44 BC)
  - 羅馬帝國軍事與政治領導人
- Caesar Cipher
  - 編碼 (Encode): A ↔ 0, B ↔ 1, …, Y ↔ 24, Z ↔ 25
    - 明文 (Plaintext): SPY (18 15 24)
    - 密文 (Ciphertext): VSB (21 18 1)
  - 加密 (Encryption): $c = p + 3 \mod 26$
  - 解密 (Decryption): $p = c - 3 \mod 26$
    - 密鑰 (Key): $k = 3$

Symmetric Cryptography

- 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



DES (Data Encryption Standard)

AES (Advanced Encryption Standard)

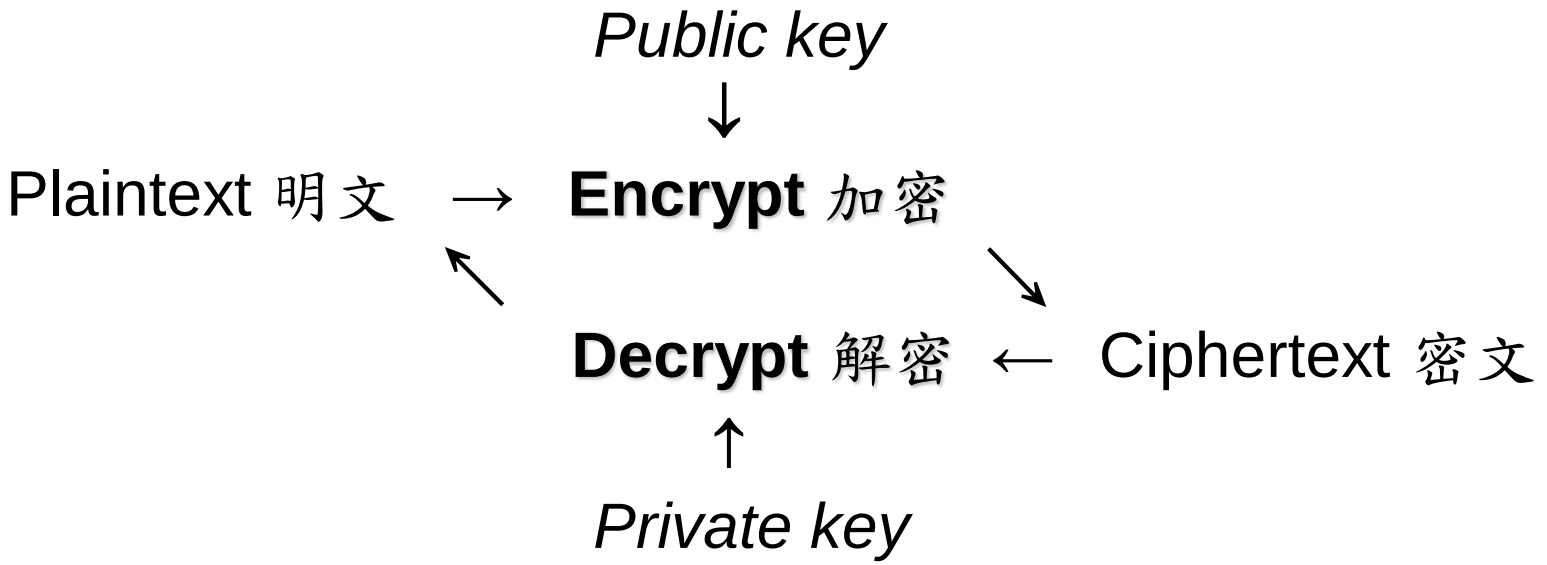
Asymmetric Cryptography

- 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

- Whit Diffie 和 Martin Hellman 於 1976 年提出觀念
- For RSA
  - The multiplication of two large primes (質數) is easy
  - The factorization of a large integer is hard

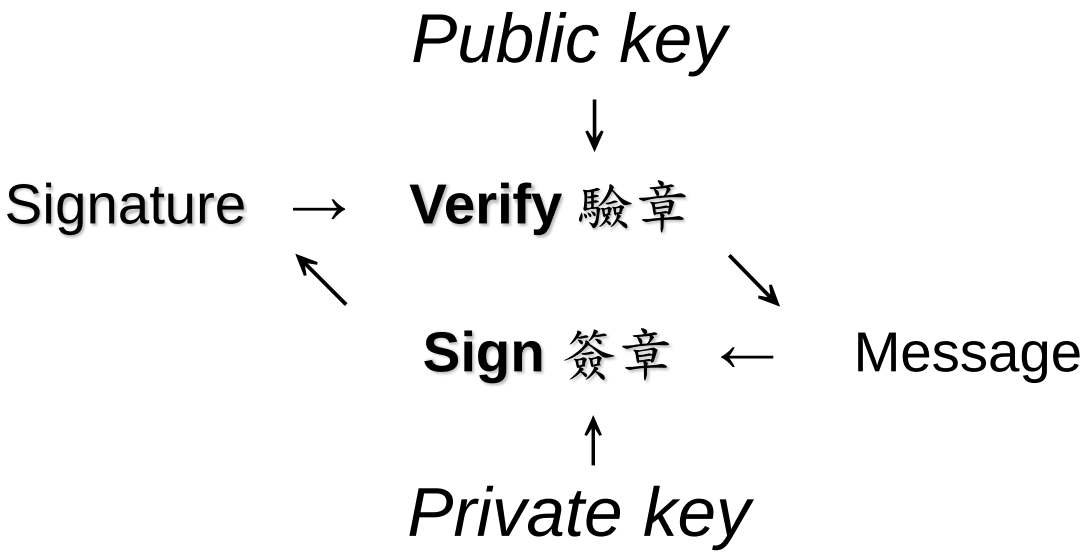
Public Key Cryptosystem 公鑰密碼系統



RSA (Rivest – Shamir – Adleman 1977)

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

Digital Signature 數位簽章



* 資料完整性 (Integrity)
* 身份鑑別性 (Authentication)
* 不可否認性 (Non-Repudiation)

Electronic Signatures Act

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

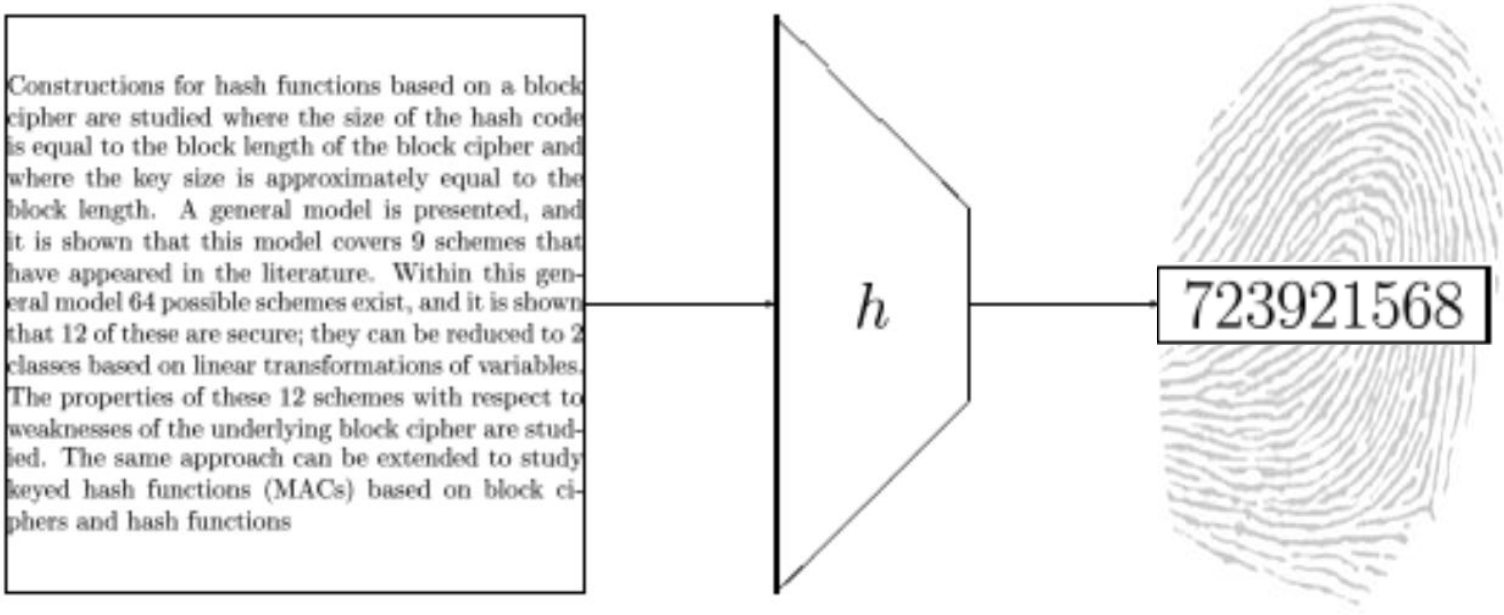
修正日期：民國 103 年 12 月 19 日

臺灣證券交易所 TAIWAN STOCK EXCHANGE

Hash Function

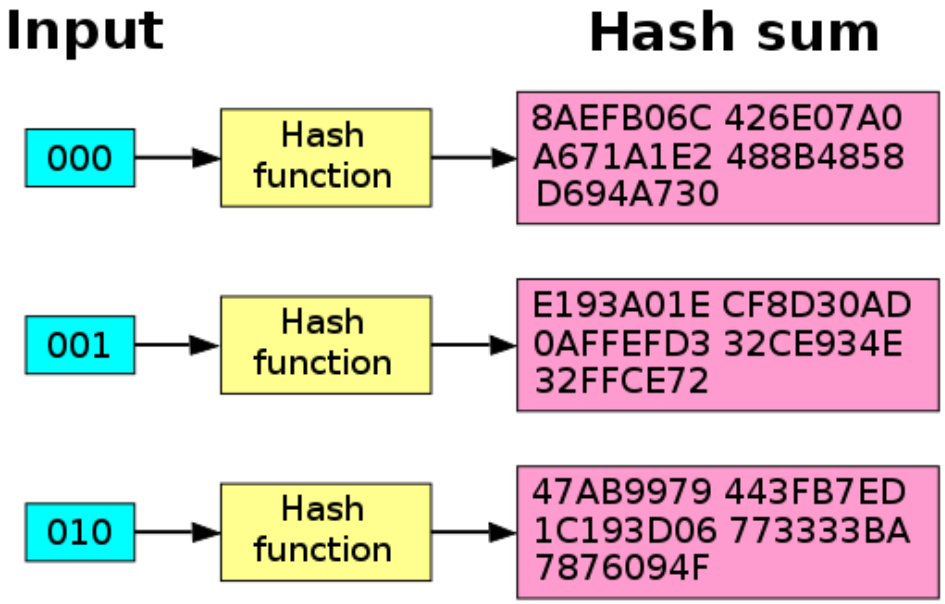
Hash Function 雜湊函數

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



Avalanche Effect 雪崩效應

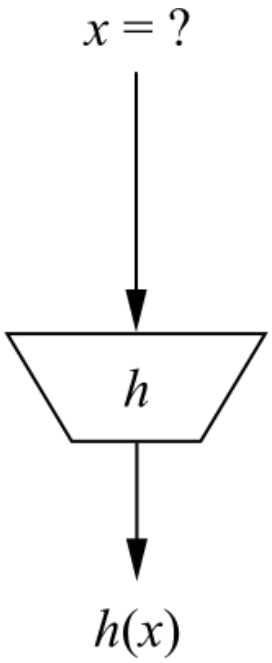
- A desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions
- When an input is changed slightly (e.g., flipping a single bit) the output changes significantly (e.g., half the output bits flip)



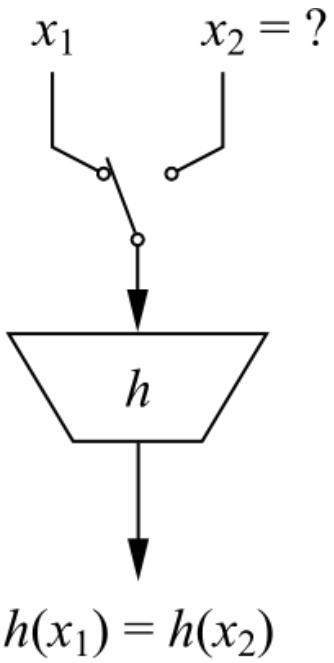
The **SHA-1** hash function exhibits good avalanche effect. When a single bit is changed the hash sum becomes completely different.

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

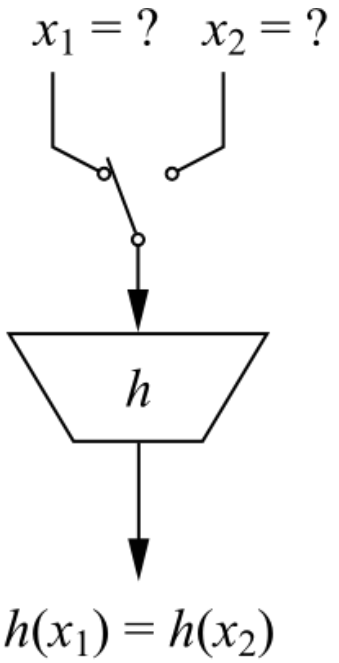
Security Properties



preimage resistance



second preimage resistance



collision resistance

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

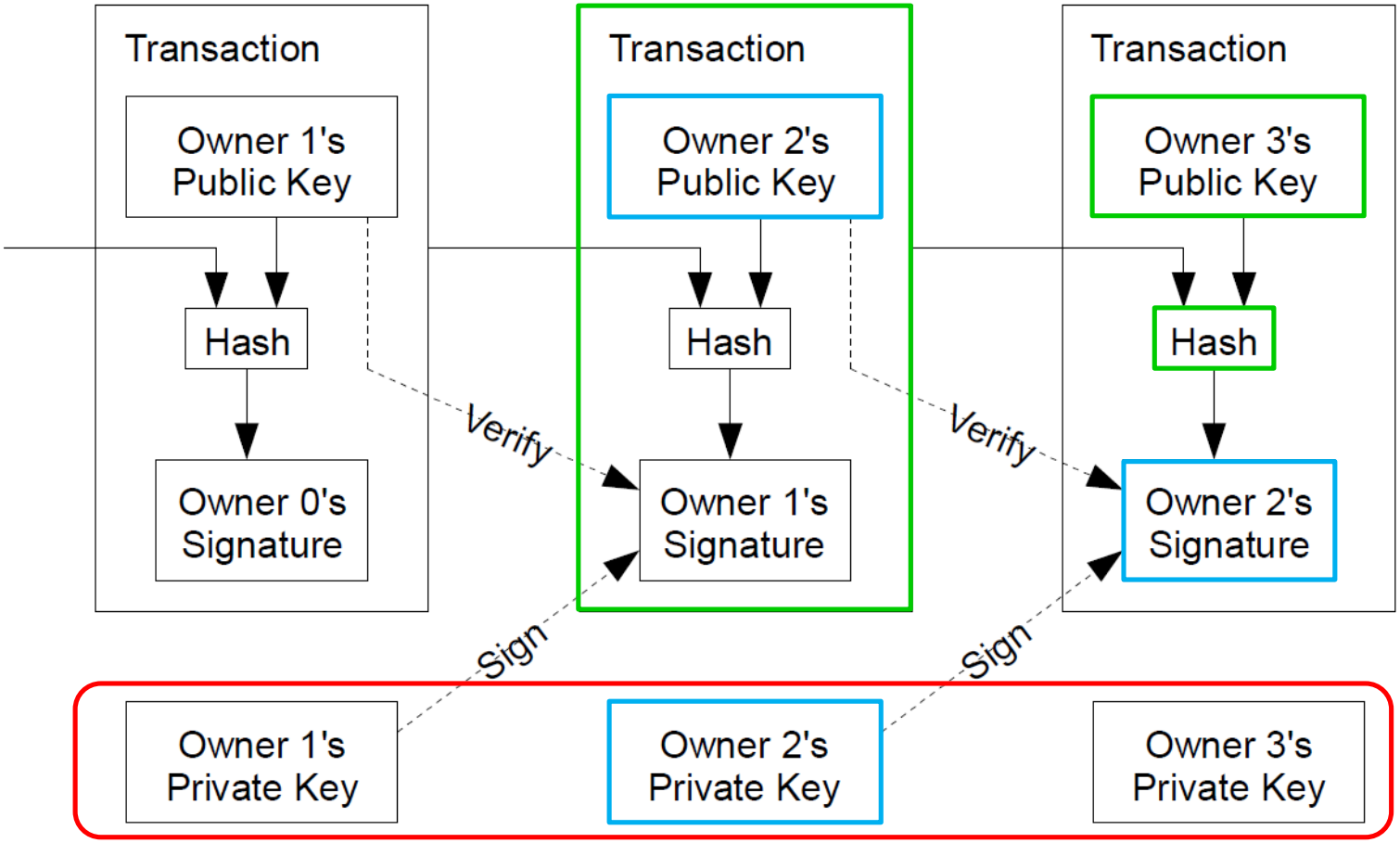
- The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)

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 ($5 \times 5 \times 64$)	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

Transactions

Bitcoin Transactions

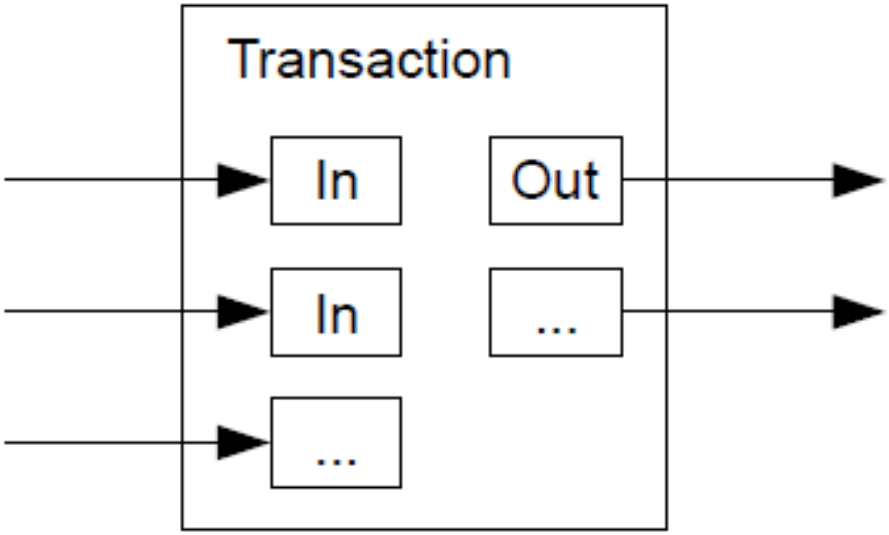


Must be protected very well!!!

http://bitcoin.org/bitcoin.pdf 中本聰

Combining & Splitting Value

- “To allow value to be split and combined, transactions contain multiple inputs and outputs.”



http://bitcoin.org/bitcoin.pdf 中本聰

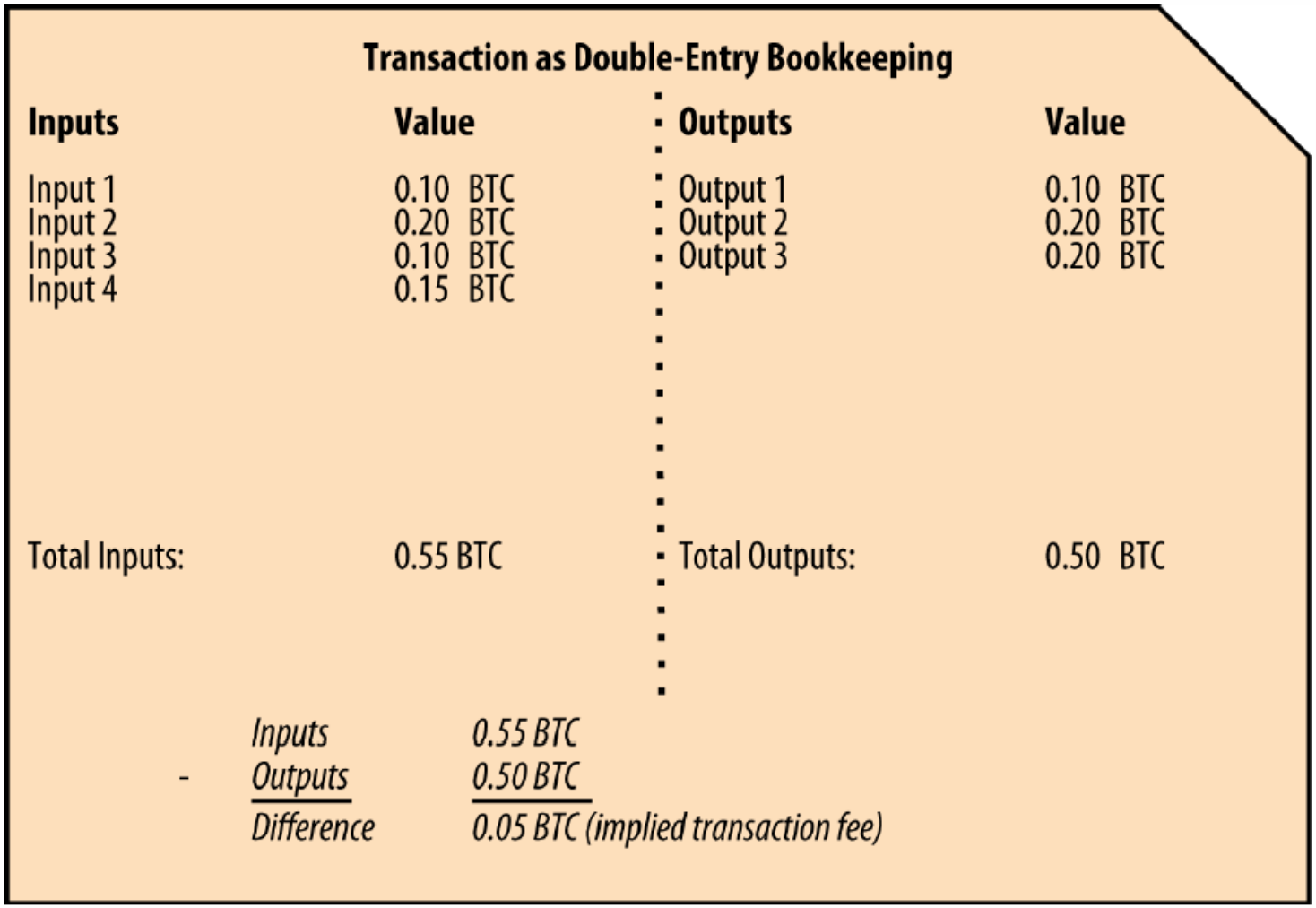


Figure 2-3. Transaction as double-entry bookkeeping

"Mastering Bitcoin" by Andreas M. Antonopoulos

Transaction Fee

- “If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.”

http://bitcoin.org/bitcoin.pdf 中本聰

Transaction Data

- {"hash":"7c4025... "
  - the hash of the remainder of the transaction (Data)
- "ver":1,
  - version 1 of the Bitcoin protocol
- "vin_sz":1,
  - one input
- "vout_sz":1,
  - one output
- "lock_time":0,
  - transaction is finalized immediately
- "size":224,
  - size (in bytes) of the transaction
  - not transaction amount

- "in":[
- {"prev_out":
- {"hash":"2007ae...",
  - where the money from
  - hash of previous transaction
- "n":0},
  - it is the first output from that transaction
- "scriptSig":"304502... 042b2d..."}],
  - signature of the person sending the money
  - the corresponding public key followed by a space
- "out":[
- {"value":"0.31900000",
  - the value of the output
- "scriptPubKey":"OP_DUP OP_HASH160 a7db6f OP_EQUAL
- VERIFY OP_CHECKSIG"}]}
  - Bitcoin's scripting language
  - Bitcoin address of the intended recipient (a7db6f)

http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works

Smart Contract 智慧合約

- “A computer program that directly controls digital assets”
  - *Ethereum: Platform Review* by Vitalik Buterin
- Example
  - ```
    if HAS_EVENT_X_HAPPENED() is true:
            send(party_A, 1000)
    else:
            send(party_B, 1000)
    ```
    ```

Block Chain

Merkle Tree / Hash Tree

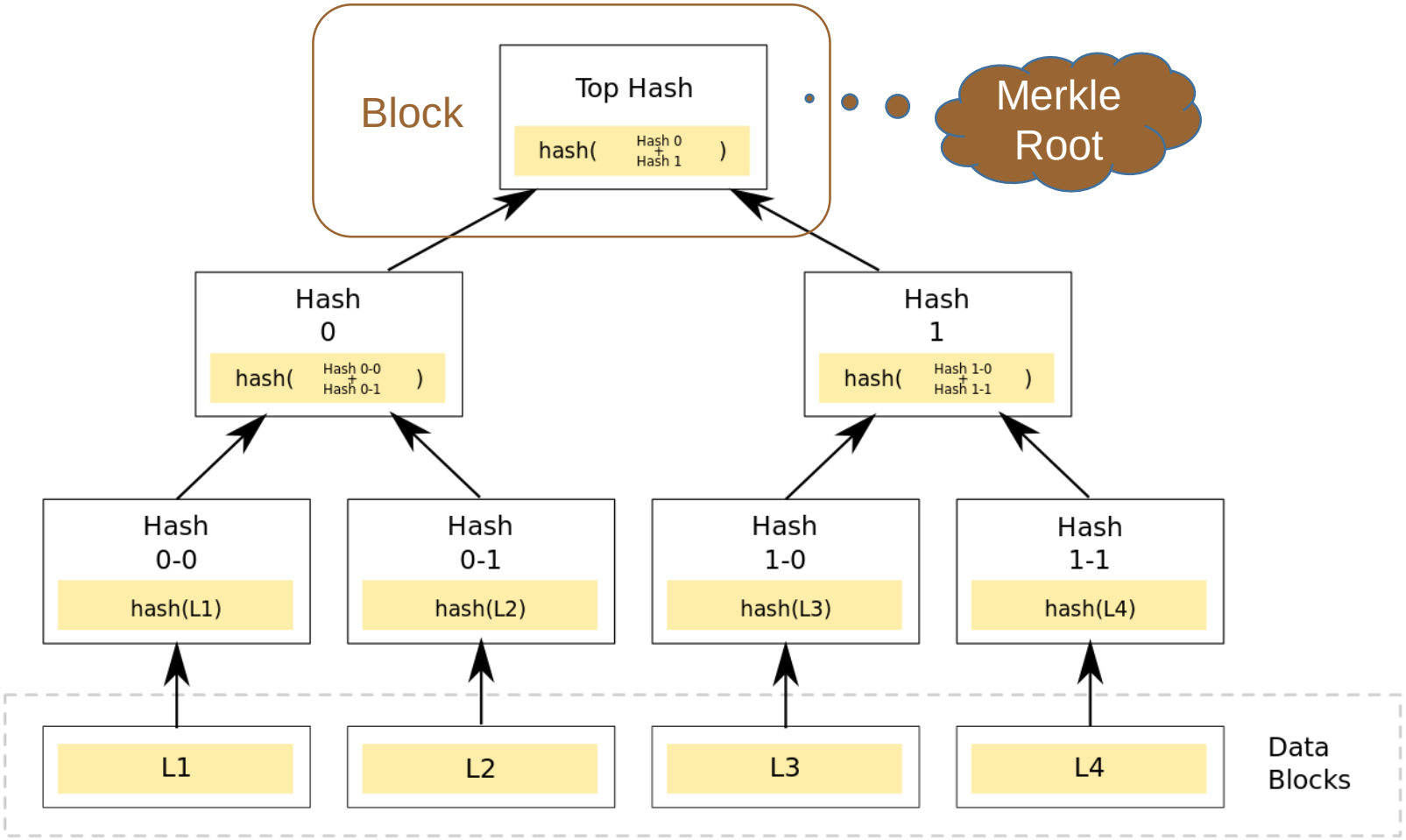
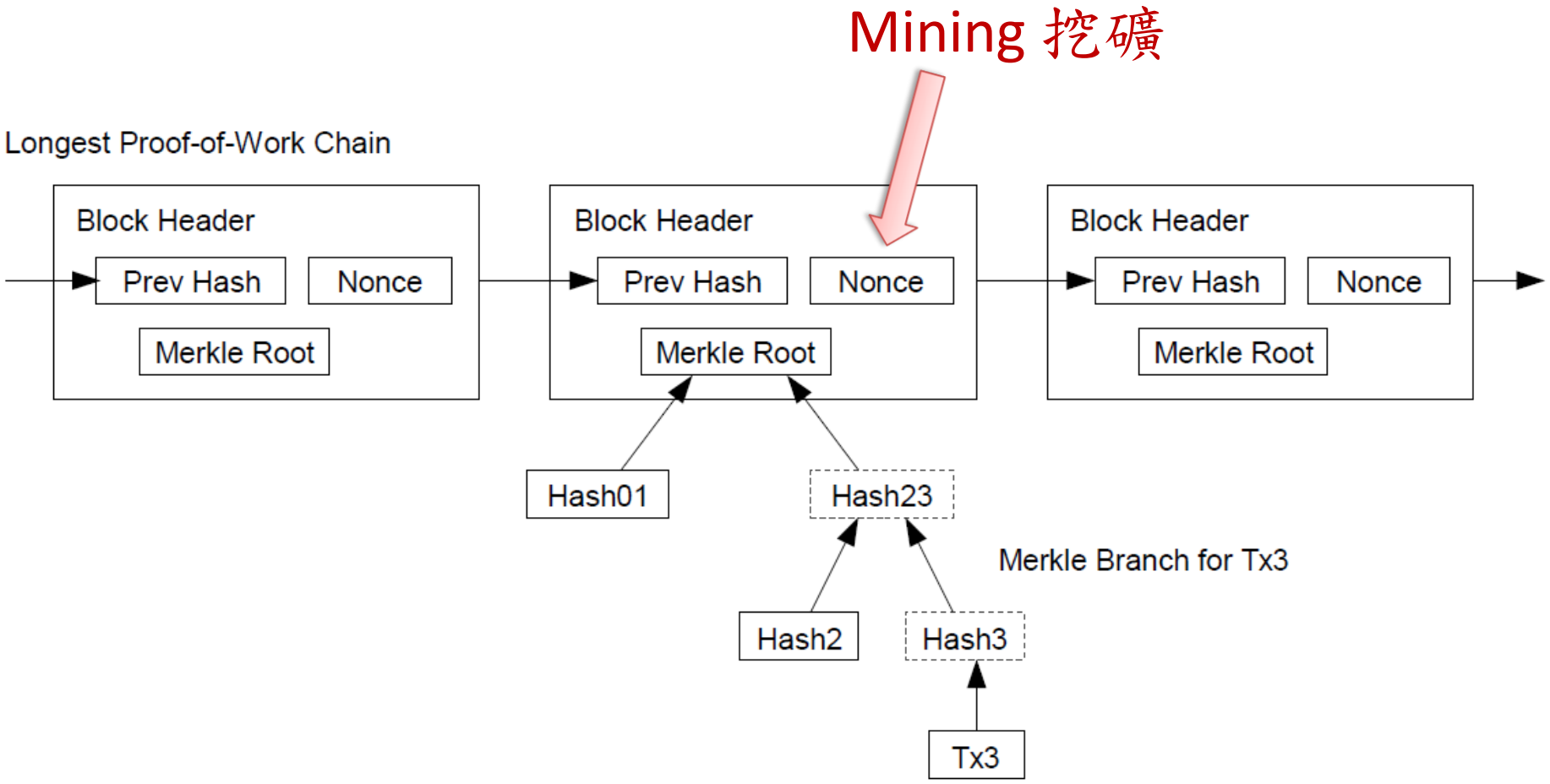


Image Courtesy https://en.wikipedia.org/wiki/Merkle_tree

Block Chain



http://bitcoin.org/bitcoin.pdf 中本聰

Proof-of-Work

- “The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits.”
- [From “Mastering Bitcoin”] Almost 11 minutes after starting to mine block 277,316, one of the hardware mining machines finds a solution and sends it back to the mining node. When inserted into the block header, the nonce 4,215,469,401 produces a block hash of:

  0000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569

  which is less than the target:

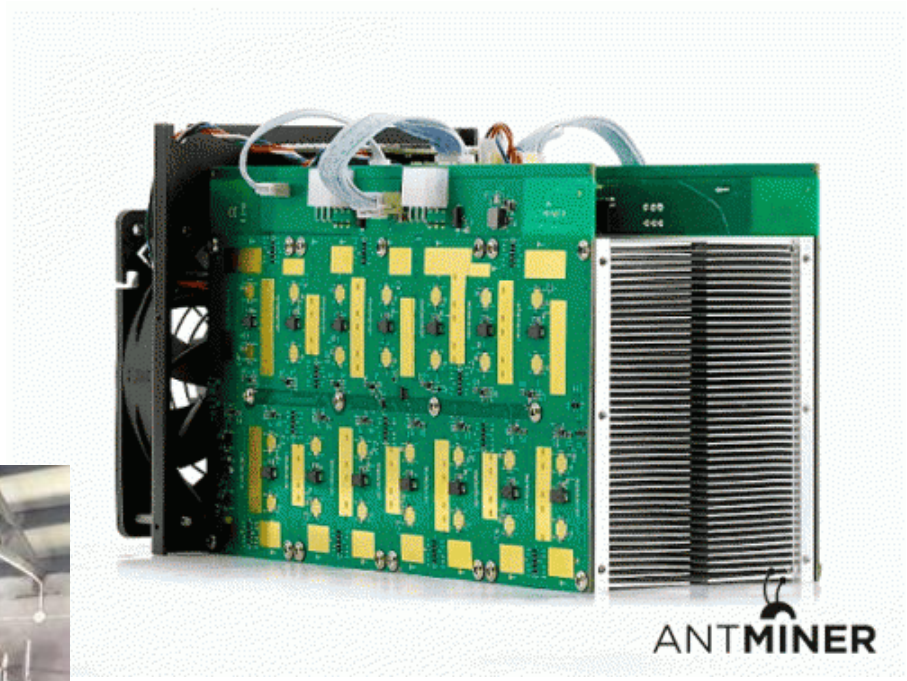
  0000000000000003A30C0000000000000000000000000000000000000000000

Incentive 激勵/誘因

- “By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block.”
  - 2009.1.3 ~ 2012.11.28 (Block #0 ~ #209999) : 50 bitcoins per block
  - 2012.11.28 ~ 2016.7.9 (#210000 ~ #419999) : 25 bitcoins per block
  - 2016.7.9 ~ 2020.5.18 (#420000 ~ #629999) : 12.5 bitcoins per block
  - 2020.5.18 ~ 2024.2.29 (#630000 ~ #839999) : 6.25 bitcoins per block
  - …… Done in 2140: All 21,000,000 bitcoins are issued
- Transaction Fee

http://bitcoin.org/bitcoin.pdf 中本聰

比特幣礦機



比特幣挖礦蜂擁狂吃電，冰島人受不了怒喊「課稅」

作者 數位時代 | 發布日期 2018 年 02 月 20 日 8:06 | 分類 數位貨幣 , 環境科學 , 科技政策

比特幣的價格雖然近期頻頻下挫，不過虛擬貨幣熱潮依然很熱，而電力成本相對低廉的冰島，就成為「挖礦」（mining）的理想地點，吸引大批虛擬貨幣數據中心前往設置。

慾望無窮、資源有限，冰島一家再生能源公司就提出預測數據，2018 年冰島挖礦用電將會超越全國民生用電，投入大量能源生產被認為是投機的虛擬貨幣，冰島議員就提議要針對挖礦獲得的利潤課稅。

先天地理環境優勢，挖礦投資者紛紛湧入

冰島人口約有 34 萬人，幾乎 100% 電力都來自再生能源（70% 來自水力發電、30% 來自地熱），看準豐富的綠色能源以及適合冷卻機器的寒冷氣候，冰島正蓋起一座座虛擬貨幣數據中心，預估今年比特幣挖礦用電將超越冰島的民生用電。

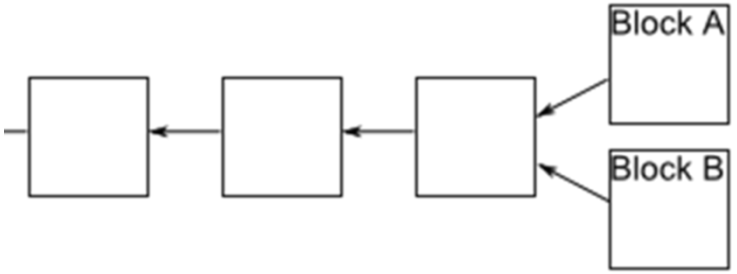
用於挖礦的電腦需要解決負責的運算問題，電腦系統也需要冷卻才能確保運作，因此往往需要耗費大量電力，而冰島天然的地熱、水力發電以及寒冷氣候提供了挖礦的絕佳條件。冰島再生能源公司 HS Orka 提出數據，指出比特幣（Bitcoin）挖礦的能源消耗呈現指數成長。

https://technews.tw/2018/02/20/iceland-will-use-more-electricity-mining-bitcoins-than-powering-homes/

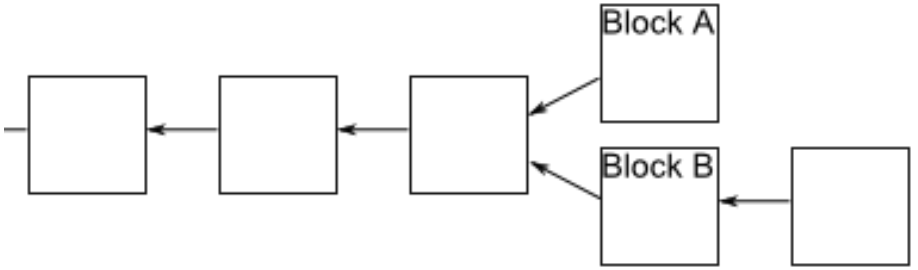
Consensus

Block Forking 區塊分岔

- Occasionally, a fork appears in the block chain, i.e., two miners happen to validate a block of transactions near-simultaneously
  - Some people update their block chain one way, and others update their block chain the other way

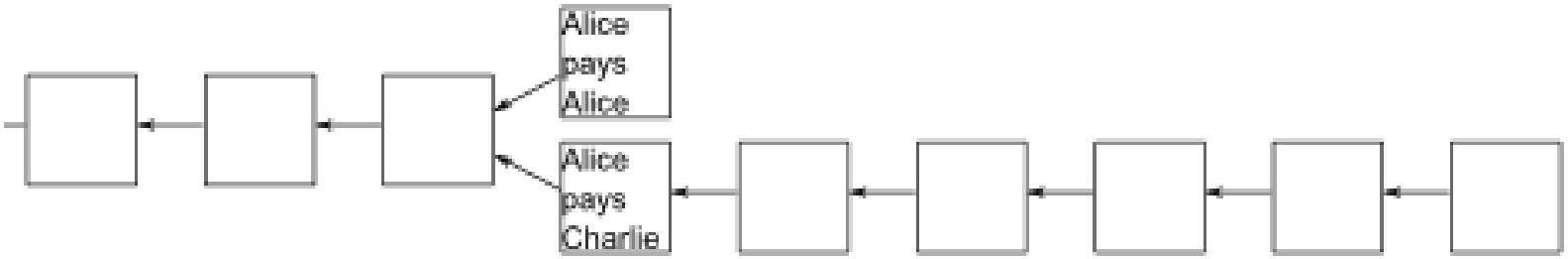


- If a fork occurs, people on the network keep track of both forks
- Miners only work to extend whichever fork is longest in their copy of the block chain



Confirmations

- A transaction is not considered confirmed until
  - It is part of a block in the longest fork
  - At least 5 blocks follow it in the longest fork
  - In this case, we say that the transaction has “6 confirmations”
- 10 minutes per block (in average)
- Payee must wait 60 minutes



Steps to Run the Network

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. Each node works on finding a difficult proof-of-work for its block
4. When a node finds a proof-of-work, it broadcasts the block to all nodes
5. Nodes accept the block only if all transactions in it are valid and not already spent
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash

http://bitcoin.org/bitcoin.pdf 中本聰

Game Theory 賽局理論

- Example: Prisoners' Dilemma 囚徒困境

Prisoner B / Prisoner A	stays silent 沉默 (cooperates 合作)	betrays 認罪 (defects 背叛)
stays silent 沉默 (cooperates 合作)	Each serves 1 year 各服刑一年	Prisoner A: 3 years Prisoner B: goes free
betrays 認罪 (defects 背叛)	Prisoner A: goes free Prisoner B: 3 years	Each serves 2 years 各服刑兩年

- The optimal individual choices leads to a sub-optimal collective outcome

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

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

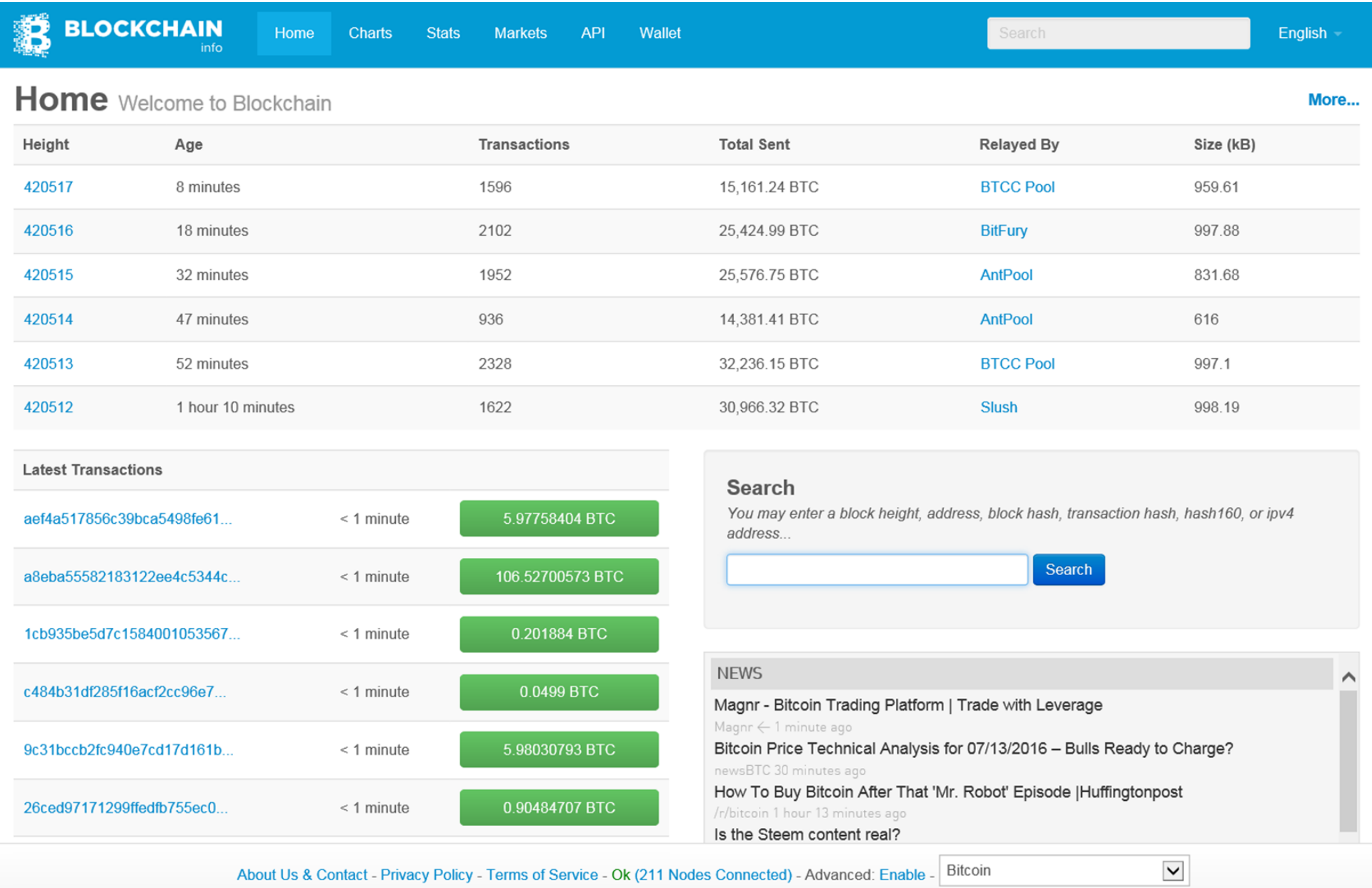
UPDATED on 9th January at 18:11 (GMT)

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



https://blockchain.info

BLOCKCHAIN info | Home | Charts | Stats | Markets | API | Wallet | Search | English

Block #420512

Summary	
Number Of Transactions	1622
Output Total	30,966.32085875 BTC
Estimated Transaction Volume	4,600.97700775 BTC
Transaction Fees	0.32666721 BTC
Height	420512 (Main Chain)
Timestamp	2016-07-13 02:52:35
Received Time	2016-07-13 02:52:35
Relayed By	Slush
Difficulty	213,398,925,331.32
Bits	402990845
Size	998.193 KB
Version	536870912
Nonce	3604645845
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000000452bfa0e4a5721d18eb8332eaac108f4826ef173236c474
Previous Block	0000000000000000004dd60659f290db4b329b8df5d18cc19ae4a44c8e8bd1710
Next Block(s)	000000000000000000025cef84b1e78ff358e60d179072cf0fb53358d4b7117ea3
Merkle Root	a577ad1bdd890323b04a4be14e987de97aa0647773bb2e163317a880a91b70e6

Network Propagation (Click To View)

Transactions

e6984543f9f0f0a07138914f94480517bc481dbc544a7014660ec9f2aab2121f — **2016-07-13 02:52:35**

No Inputs (Newly Generated Coins)	1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE	12.82666721 BTC
		12.82666721 BTC

e698b8aaa677f29db459a85d69f05b152c0f585c1ad557ae3b528deb8a9c81ad — **2016-07-13 02:46:38**

1GiNGZNLNcFt4uQYuvZnNgxCiddXGjaBsh	1BzUyxBBDDrdsHCm7vgsdUGxWF6pSCybtJ	0.01452155 BTC
	1M8hxwYNWWnHkxUjFiF8Y829ni9NXkx3gA	0.05881094 BTC
		0.07333249 BTC

c3bd9ee32ef823c8e4abbcc6bbbb582245f3df1e8ecfb9a0580a69c4359fa83a — **2016-07-13 02:46:49**

12Atx5xZFbJZKJzVkzjcA4iqc6xjzfYeez	1PdsMWgX9MLALb3wAoNoKogU5mZBeYviLP	0.005 BTC
1Kj76Sxe8c3UK85RAQwwdqScAxaBwAY2eb	1JTsidxax1S39ekzbiZWtUru385u1DjFgs	0.0128729 BTC
14r9Gu8xwyb82Ria1boAGJHYfLxi2Vx2k7		
		0.0178729 BTC

029d016635b02bfb7fa7a6a69aa6654228a68a6c66224c59d84f9156b0142d33 — **2016-07-13 02:51:14**

1JXM613U3W2PCGn8ix7Vk3WUjwfWFcukk6	12ebcHoNsUzewercB7FiBhDEsQuaEP5eSu	1.2413474 BTC
	1KTMC82xsr5uHHBULNFjsrF5Vki88ez2pN	1.4393 BTC
		2.6806474 BTC

BLOCKCHAIN info | Home | Charts | Stats | Markets | API | Wallet | Search | English

Bitcoin Address

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

Summary	
Address	1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE
Hash 160	7c154ed1dc59609e3d26abb2df2ea3d587cd8c41
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	7856
Total Received	106,160.37194277 BTC
Final Balance	101.89033403 BTC

Request Payment | Donation Button

Transactions (Oldest First)

Filter

e6984543f9f0f0a0713891 4f94480517bc481dbc544a7014660ec9f2aab2121f — 2016-07-13 02:52:35

No Inputs (Newly Generated Coins) → 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE 12.82666721 BTC

9 Confirmations | 12.82666721 BTC

c0018c0fb39fbc46f62475d7d95400c92a338df89105987e1fbbdf53e8bcb082 — 2016-07-13 01:31:25

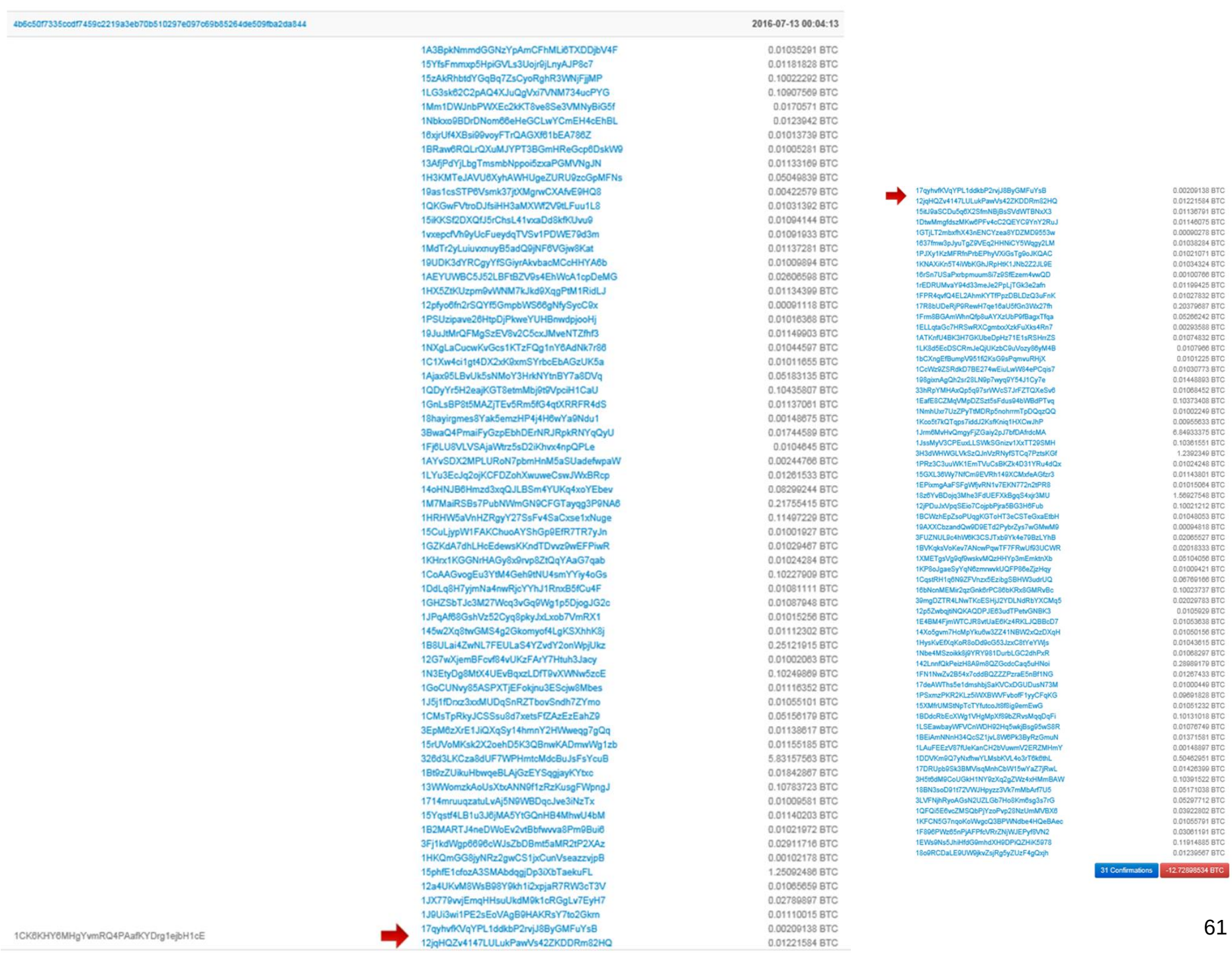
No Inputs (Newly Generated Coins) → 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE 12.56024582 BTC

18 Confirmations | 12.56024582 BTC

1459c9058058b4e20f03a1a2b38573eb9a11acaeea7184d02f14a72bec4e0d58 — 2016-07-13 00:09:04

No Inputs (Newly Generated Coins) → 1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE 12.58155207 BTC

30 Confirmations | 12.58155207 BTC


4b6c50f7335ccdf7459c2219a3eb70b510297e097c69b85264de509fba2da844
2016-07-13 00:04:13
1A3BpkNmmdGGNzYpAmCFhMLi6TXDDjbV4F 0.01035291 BTC
15YfsFmmxp5HpiGVLs3Uojr9jLnyAJP8c7 0.01181828 BTC
15zAkRhbtdYGqBq7ZsCyoRghR3WNjFjjMP 0.10022292 BTC
1LG3sk62C2pAQ4XJuQgVxi7VNM734ucPYG 0.10907569 BTC
1Mm1DWJnbPWXEc2kKT8ve8Se3VMNyBiG5f 0.0170571 BTC
1Nbkxo9BDrDNom66eHeGCLwYCmEH4cEhBL 0.0123942 BTC
16xjrUf4XBsi99voyFTrQAGXf61bEA786Z 0.01013739 BTC
1BRaw6RQLrQXuMJYPT3BGmHReGcp6DskW9 0.01005281 BTC
13AfjPdYjLbgTmsmbNppoi5zxaPGMVNgJN 0.01133169 BTC
1H3KMTeJAVU6XyhAWHUgeZURU9zcGpMFNs 0.05049839 BTC
19as1csSTP6Vsmk37jtXMgrwCXAfvE9HQ8 0.00422579 BTC
1QKGwFVtroDJfsiHH3aMXWfZV9tLFuu1L8 0.01031392 BTC
15iKKSf2DXQfJ5rChsL41vxaDd8kfKUvu9 0.01094144 BTC
1vxepcfVh9yUcFueydqTVSv1PDWE79d3m 0.01091933 BTC
1MdTr2yLuiuvxnuyB5adQ9jNF6VGjw8Kat 0.01137281 BTC
19UDK3dYRCgyYfSGiyrAkvbacMCcHHYA6b 0.01009894 BTC
1AEYUWBC5J52LBFtBZV9s4EhWcA1cpDeMG 0.02606598 BTC
1HX5ZtKUzpm9vWNM7kJkd9XqgPtM1RidLJ 0.01134399 BTC
12pfyo6fn2rSQYf5GmpbWS66gNfySycC9x 0.00091118 BTC
1PSUzipave26HtpDjPkweYUHBnwdpjooHj 0.01016368 BTC
19JuJtMrQFMgSzEV8v2C5cxJMveNTZfhf3 0.01149903 BTC
1NXgLaCucwKvGcs1KTzFQg1nY6AdNk7r86 0.01044597 BTC
1C1Xw4ci1gt4DX2xK9xmSYrbcEbAGzUK5a 0.01011655 BTC
1Ajax95LBvUk5sNMoY3HrkNYtnBY7a8DVq 0.05183135 BTC
1QDyYr5H2eajKGT8etmMbj9t9VpciH1CaU 0.10435807 BTC
1GnLsBP8t5MAZjTEv5Rm5fG4qtXRRFR4dS 0.01137061 BTC
18hayirgmes8Yak5emzHP4j4H6wYa9Ndu1 0.00148675 BTC
3BwaQ4PmaiFyGzpEbhDErNRJRpkRNYqQyU 0.01744589 BTC
1Fj6LU8VLVSAjaWtrz5sD2iKhvx4npQPLe 0.0104645 BTC
1AYvSDX2MPLURoN7pbmHnM5aSUadefwpaW 0.00244766 BTC
1LYu3EcJq2ojKCFDZohXwuweCswJWxBRcp 0.01261533 BTC
14oHNJB6Hmzd3xqQJLBSm4YUKq4xoYEbev 0.08299244 BTC
1M7MaiRSBs7PubNWmGN9CFGTayqg3P9NA6 0.21755415 BTC
1HRHW5aVnHZRgyY27SsFv4SaCxse1xNuge 0.11497229 BTC
15CuLjypW1FAKChuoAYShGp9EfR7TR7yJn 0.01001927 BTC
1GZKdA7dhLHcEdewsKKndTDvvz9wEFPiwR 0.01029467 BTC
1KHrx1KGGNrHAGy8x9rvp8ZtQqYAaG7qab 0.01024284 BTC
1CoAAGvogEu3YtM4Geh9tNU4smYYiy4oGs 0.10227909 BTC
1DdLq8H7yjmNa4nwRjcYYhJ1RnxB5fCu4F 0.01081111 BTC
1GHZSbTJc3M27Wcq3vGq9Wg1p5DjogJG2c 0.01087948 BTC
1JPqAf68GshVz52Cyq8pkyJxLxob7VmRX1 0.01015256 BTC
145w2Xq8twGMS4g2Gkomyof4LgKSXhhK8j 0.01112302 BTC
1B8ULai4ZwNL7FEULaS4YZvdY2onWpjUkz 0.25121915 BTC
12G7wXjemBFcvf84vUKzFArY7Htuh3Jacy 0.01002063 BTC
1N3EtyDg8MtX4UEvBqxzLDfT9vXWNw5zcE 0.10249869 BTC
1GoCUNvy85ASPXTjEFokjnu3EScjw8Mbes 0.01116352 BTC
1J5j1fDrxz3xdMUDqSnRZTbovSndh7ZYmo 0.01055101 BTC
1CMsTpRkyJCSSsu8d7xetsFfZAzEzEahZ9 0.05156179 BTC
3EpM6zXrE1JiQXqSy14hmnY2HWweqg7gQq 0.01138617 BTC
15rUVoMKsk2X2oehD5K3QBnwKADmwWg1zb 0.01155185 BTC
326d3LKCza8dUF7WPHmtcMdcBuJsFsYcuB 5.83157563 BTC
1Bt9zZUikuHbwqeBLAjGzEYSqgjayKYbxc 0.01842867 BTC
13WWomzkAoUsXbxANN9f1zRzKusgFWpngJ 0.10783723 BTC
1714mruuqzatuLvAjs5N9WBDqcJve3iNzTx 0.01009581 BTC
15Yqstf4LB1u3J6jMA5YtGQnHB4MhwU4bM 0.01140203 BTC
1B2MARTJ4neDWoEv2vtBbfwvva8Pm9Bui6 0.01021972 BTC
3Fj1kdWgp8696cWJsZbDBmt5aMR2tP2XAz 0.02911716 BTC
1HKQmGG8jyNRz2gwCS1jxCunVseazzvjpB 0.00102178 BTC
15phfE1cfozA3SMAbdqqjDp3iXbTaekuFL 1.25092486 BTC
12a4UKvM8WsB98Y9kh1i2xpjaR7RW3cT3V 0.01065659 BTC
1JX779vvjEmqHHsuUkdM9k1cRGgLv7EyH7 0.02789897 BTC
1J9Ui3wi1PE2sEoVAgB9HAKRsY7to2Gkrn 0.01110015 BTC
17qyhvfKVqYPL1ddkbP2rvjJ8ByGMFuYsB 0.00209138 BTC
12jqHQZv4147LULukPawVs42ZKDDRm82HQ 0.01221584 BTC
1CK6KHY6MHgYvmRQ4PAafKYDrg1ejbH1cE
17qyhvfKVqYPL1ddkbP2rvjJ8ByGMFuYsB 0.00209138 BTC
12jqHQZv4147LULukPawVs42ZKDDRm82HQ 0.01221584 BTC
15tiJ9aSCDu5q6X2SfmNBjBsSVdWTBNxX3 0.01138791 BTC
1DtwMmgfdszMKw6PFv4cC2QEYC6YnY2RuJ 0.01146075 BTC
1GTjLT2mbxfhX43nENCYzea8YDZMD9553w 0.00090278 BTC
1637fmw3pJyuTgZ9VEq2HHNiCY5VqgyZLM 0.01038284 BTC
1PJXy1KzMFRfnPrbEPhyVXiGsTg9oJKQAC 0.01021071 BTC
1KNAXiKn5T4iWbKGhJRpHtK1JNb2Z2JL9E 0.01034324 BTC
16rSn7USaPxrbpmuum8i7z95fEzem4vwQD 0.00100766 BTC
1rEDRUMvaY94d33meJe2PpLjTGk3e2afn 0.01199425 BTC
1FPR4qvfQ4EL2AhmKYTfPpzDBLDzQ3uFnK 0.01027832 BTC
17R8bUDeRjP6RewH7qe16aU5fGn3Wx27fh 0.20379687 BTC
1Frm8BGAmWhnQfp8uAYXzUbP9fBagxTfqa 0.05266242 BTC
1ELLqtaGc7HRSwRXCgmboXzkFuXks4Rn7 0.00293588 BTC
1ATKnfU4BK3H7GKUbeDpHz71E1sRSHrrZS 0.01074832 BTC
1LK8d5EcDSCRmJeQjUKzbC9uVozy86yM4B 0.0107966 BTC
1bCXngEfBumpV951f62KsG9sPqmvuRHjX 0.0101225 BTC
1CcWz9ZSRdkD7BE274wEiuLwW84ePCqis7 0.01030773 BTC
198gixnAgQh2sr28LN9p7wyq9Y54J1Cy7e 0.01448893 BTC
33hRpYMHAxQp5q97srWvcS7JrFZTQXeSv6 0.01068452 BTC
1EafE8CZMqVMpDZSzt5sFdus94bWBdPTvq 0.10373408 BTC
1NmhUxr7UzZPyTtMDRp5nohrrmTpDQqzQQ 0.01002249 BTC
1Koo5t7kQTqps7iddJ2KsfKniq1HXCwJhP 0.00955633 BTC
1Jrm6MvHvQmgyFjZGaiy2pJ7bfDAfdcMA 6.84933375 BTC
1JssMyV3CPEuxLLSWkSGnizv1XxTT29SMH 0.10361551 BTC
3H3dWHWGLVkSzQJnVzRNyfSTCq7PztsKGf 1.2392349 BTC
1PRz3C3uuWK1EmTVuCsBKZk4D31YRu4dQx 0.01024248 BTC
15GXL36Wy7NfCm9EVRh149XCMxfeAGfzr3 0.01143801 BTC
1EPixmgAaFSFgWfjvRN1v7EKN772n2tPR8 0.01015084 BTC
18z6YvBDojq3Mhe3FdUEFXkBgqS4xjr3MU 1.56927548 BTC
12jPDuJxVpqSEio7CojpbPjra5BG3H6Fub 0.10021212 BTC
1BCWzhEpZsoPUqgKGToHT3eCSTeGxaEtbH 0.01048053 BTC
19AXXCbzandQw9D9ETd2PybrZys7wGMwM9 0.00094818 BTC
3FUZNUL9c4hW6K3CSJTxb9Yk4e79BzLYhB 0.02065527 BTC
1BVKqksVoKev7ANcwPqwTF7FRwUf93UCWR 0.02018333 BTC
1XMETgsVg9qf9wskvMQzHHYp3mEmktnXb 0.05104056 BTC
1KP8oJgaeSyYqN6zmrwvkUQFP86eZjzHqy 0.01009421 BTC
1CqstRH1q6N9ZFVnzx5EzibgSBHW3udrUQ 0.06769166 BTC
16bNcnMEMir2qzGnk6rPC96bKRx8GMRvBc 0.10023737 BTC
39mgDZTR4LNwTKcESHjJ2YDLNdRbYXCMq5 0.02029783 BTC
12p5ZwbqbtNQKAQDPJE63udTPetvGNBK3 0.0105929 BTC
1E4BM4FjmWTCJR8vtUaE6Kz4RKLJQBBcD7 0.01053638 BTC
14Xo5gvm7HoMpYku6w3ZZ41NBW2xQzDXqH 0.01050156 BTC
1HysKvEfXqKoR8oDd9oG53JzxC8tYeYWjs 0.01043615 BTC
1Nbe4MSzoikk8j9YRY981DurbLGC2dhPxR 0.01068297 BTC
142LnnfQkPeizH8A9m8QZGodcCaq5uHNoi 0.28989179 BTC
1FN1NwZv2B54x7oddBQZZZPzraE5nBf1NG 0.01267433 BTC
17deAWThs5e1dmshbjSaK0VCxDGUDusN73M 0.01000449 BTC
1PSxmzPKR2KLz5iWXBWVFvbofF1yyCFqKG 0.09691828 BTC
15XMfrUMStNpTcTYfutcoJt8f8ig9emEwG 0.01051232 BTC
1BDdcRbEcXWg1VHgMpXf89bZRvsMqqDqFi 0.10131018 BTC
1LSEawbayWFVCnWDH92Hq5wkjBsg95wS8R 0.01076749 BTC
1BEiAmNNnH34QcSZ1jvL8W6Pk3ByRzGmuN 0.01371581 BTC
1LAuFEEzV87fUeKanCH2bVuwmV2ERZMHmY 0.00148897 BTC
1DDVKm9Q7yNxfhwYLMsbKVL4o3rT6kf8hL 0.50462951 BTC
17DRUpb9Sk3BMVsqMnhCbW15wYaZ7jRwL 0.01426399 BTC
3H5t6dM8CoUGkH1NY9zXq2gZWz4xHMmBAW 0.10391522 BTC
18BN3soD91t7ZVWJHpyzz3Vk7mMbArf7U5 0.05171038 BTC
3LVFNjhRyoAGs2N2UZLGb7Ho8Km6sg3s7rG 0.05297712 BTC
1QFQi5E6vcZMSQbPjYzoPvp28NzUmMVBX6 0.03922802 BTC
1KFCN5G7nqoKoVWgcQ3BPWNdbe4HQeBAec 0.01055791 BTC
1F896PWz65nPjAFPfcVRtZNjWJEPyf5VN2 0.03061191 BTC
1EWs9Ns5JhiHfdG9mhdXH9DPiQZHiK5978 0.11914885 BTC
18o9RCDaLE9UW9jkvZsjRg5yZUzF4gQxjh 0.01239567 BTC
31 Confirmations
-12.72898534 BTC

Block #0

比特幣發明人果然是他！澳洲企業家Craig Steven Wright終於坦言證實

中本聰一直是個謎樣的人物，2008年發表比特幣（Bitcoin）論文後，不僅創造出全新的金融模式，也發明了如今讓全球金融科技都瘋狂的區塊鏈技術

文/ 王宏仁 | 2016-05-02 發表

http://www.ithome.com.tw/news/105677

比特幣發明者是誰？Wright是中本聰還是騙子？

儘管部份人士相信澳洲企業家Craig Steven Wright就是比特幣發明者，但仍有資安專家、開發者質疑Wright是中本聰的真實性，認為Wright所提出的證據薄弱，要求提出的更有力的證據，例如展示第0區塊的相關私鑰才能證明他真的是中本聰。

文/ 陳曉莉 | 2016-05-03 發表

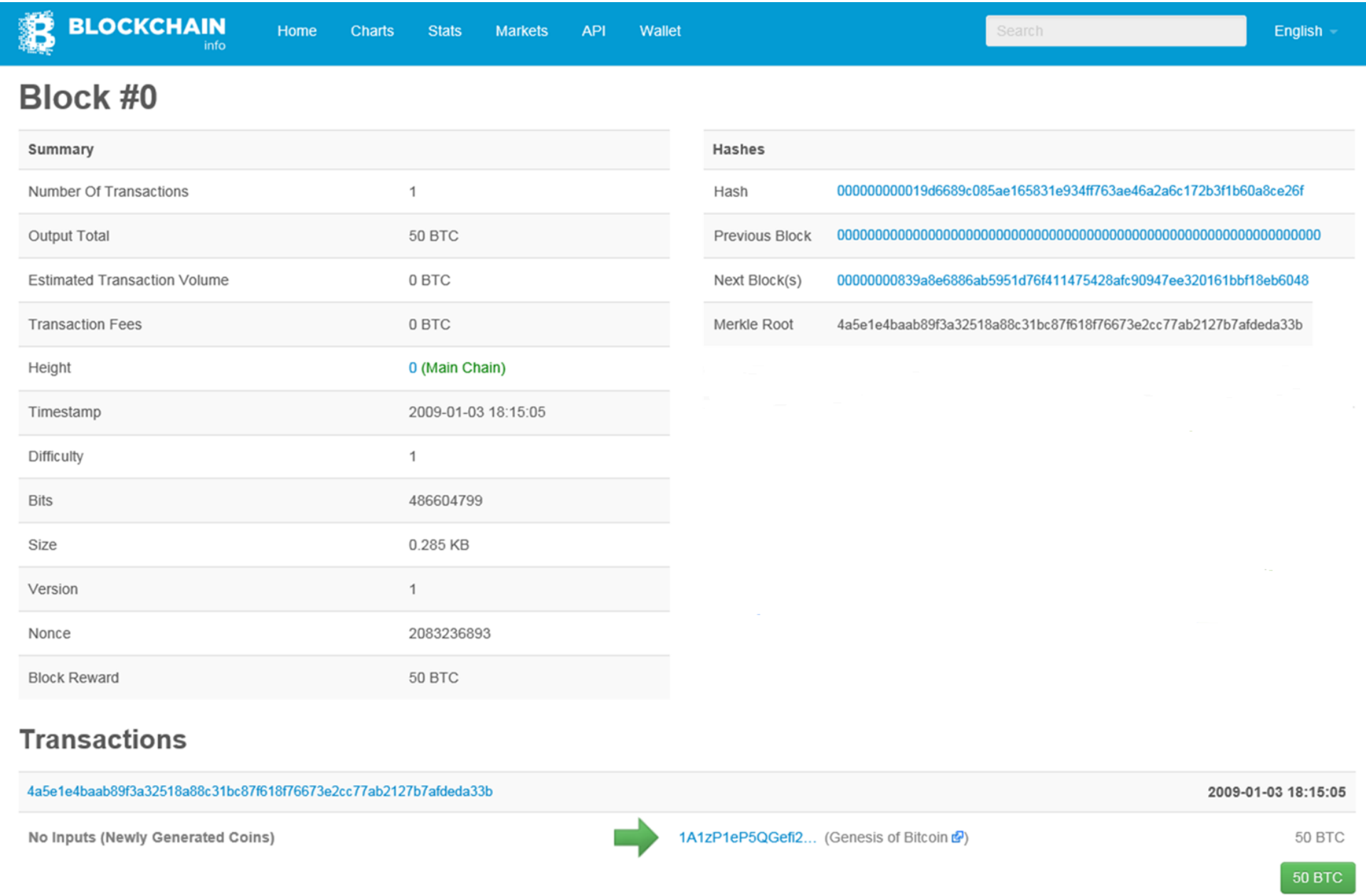
http://www.ithome.com.tw/news/105687

承認是中本聰後質疑聲四起，Wright不想再證明了

Wright向媒體承認自己是中本聰後謠言四起，Wright說，他的能力與性格都受到攻擊，當這些指控被駁回時，新的指控又出現了，他知道他承受不起...向相信他的人道歉。

文/ 陳曉莉 | 2016-05-06 發表

http://www.ithome.com.tw/news/105769


BLOCKCHAIN info
Home
Charts
Stats
Markets
API
Wallet
Search
English
Block #0
Summary
Number Of Transactions 1
Output Total 50 BTC
Estimated Transaction Volume 0 BTC
Transaction Fees 0 BTC
Height 0 (Main Chain)
Timestamp 2009-01-03 18:15:05
Difficulty 1
Bits 486604799
Size 0.285 KB
Version 1
Nonce 2083236893
Block Reward 50 BTC
Hashes
Hash 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block 0000000000000000000000000000000000000000000000000000000000000000
Next Block(s) 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Transactions
4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
2009-01-03 18:15:05
No Inputs (Newly Generated Coins)
1A1zP1eP5QGefi2... (Genesis of Bitcoin)
50 BTC
50 BTC

Genesis of Bitcoin

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

Summary	
Address	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Hash 160	62e907b15cbf27d5425399ebf6f0fb50ebb88f18
Tools	Taint Analysis - Related Tags - Unspent Outputs

Transactions	
No. Transactions	1056
Total Received	66.31917487 BTC
Final Balance	66.31917487 BTC

Request Payment | Donation Button

Transactions (Oldest First)

Filter

1b9a2ef7af3a1a888d3a778a618b8c81033866cc8eb795724b3a4f3fc9273ea8 — 2016-07-09 16:42:23

1EMBaSSyxMQPV2fmUsdB7mMfMoocgfiMNw → Genesis of Bitcoin — 0.0033333 BTC

0.0033333 BTC

d534f62a3f579c063169a642baddab6e57721dbad879e67b9053480103af541f — 2016-07-02 13:58:16

1WriteySQufKZ2pVuM1oMhPrTtTVFq35j → Unable to decode output address
Genesis of Bitcoin — 0 BTC
0.00005 BTC

0.00005 BTC

Public Note: For historical record, John Wnuk and grandson Jayden McAbee have made a donation to the Genesis block that contains the first Bitcoin wallet on June 9, 2016.

456d3d6964d295789959f7e6e270936317a564f03a07227c1249ac292e65b219 — 2016-06-09 20:16:53

14gRnM8MHFszDvHRethXGc3VyfdTuViAqp → Genesis of Bitcoin — 0.0001 BTC

0.0001 BTC

34a89ed9960653f9b073948f8536e2bc0d6c7af7cb53c8f008ffaff0fbf90c66 — 2016-06-09 17:09:30

1ChhZBuU3XLKtWyZ5BfsSzj7m83KjWYDVg → Genesis of Bitcoin — 0.0001 BTC

0.0001 BTC

Summary

區塊鏈特色

- 去中心化 (decentralized)
- 共同維護公開帳本 (public ledger)
- 防止抹滅或竄改 (tamper resistant)
- 具備時戳 (timestamps)
- 自動解決交易衝突 (conflict resolution)

➢ 需要以上特性的應用，才適合導入區塊鏈

常見誤解

- Bitcoin 無「加密」(隱藏資訊)，僅雜湊與數位簽章
  - 中本聰論文的全文無任何 encrypt / encryption，而 sign / signing / signature 出現 12 次
  - Cryptography 在海峽兩岸均翻譯為「密碼學」，CryptoCurrency 應翻譯為「密碼貨幣」
- 區塊鏈及密碼貨幣使用 PKC (Public-Key Cryptography 公鑰密碼學 [數位簽章])，並非 PKI (Public-Key Infrastructure 公鑰基礎建設)；後者為中心化架構，憑證由CA簽發

是嗎？

任正非：區塊鏈安全性在量子計算面前不值一提

作者 MoneyDJ | 發布日期 2019 年 11 月 07 日 14:30 | 分類 手機 分享 Follow 讚 534 分享

https://technews.tw/2019/11/07/ren-zhengfei-blockchain-quantum-computing-safety/

結語

- 區塊鏈來自比特幣，是其記帳機制
- 數位簽章與雜湊函數皆已使用數十年，並非中本聰獨創，但中本聰最早利用上列密碼學工具設計出比特幣與區塊鏈
- 私鑰保護極為重要，常見做法是使用「冷錢包」
- 區塊鏈可應用於金融科技與其他領域，不限於密碼貨幣
- 現有區塊鏈與密碼貨幣，皆可藉由更換數位簽章演算法，抵抗未來量子電腦的威脅