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
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Price</th>
<th>24h %</th>
<th>7d %</th>
<th>Market Cap</th>
<th>Volume(24h)</th>
<th>Circulating Supply</th>
<th>Last 7 Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin BTC</td>
<td>$54,485.99</td>
<td>-0.74%</td>
<td>3.53%</td>
<td>$1,015,983,111,212</td>
<td>$55,889,478,503</td>
<td>18,662,556 BTC</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum ETH</td>
<td>$1,676.58</td>
<td>1.07%</td>
<td>5.62%</td>
<td>$193,214,537,263</td>
<td>$21,554,965,469</td>
<td>115,174,425 ETH</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
<tr>
<td>3</td>
<td>Tether USDT</td>
<td>$1.00</td>
<td>-0.08%</td>
<td>0.09%</td>
<td>$39,879,326,471</td>
<td>$87,527,854,161</td>
<td>39,838,509,134 USDT</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
<tr>
<td>4</td>
<td>Binance Coin BNB</td>
<td>$255.34</td>
<td>1.39%</td>
<td>0.64%</td>
<td>$39,415,960,841</td>
<td>$2,002,598,733</td>
<td>154,532,785 BNB</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
<tr>
<td>5</td>
<td>Cardano ADA</td>
<td>$1.11</td>
<td>-1.16%</td>
<td>8.18%</td>
<td>$35,616,655,078</td>
<td>$4,481,817,494</td>
<td>31,948,309,441 ADA</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
<tr>
<td>6</td>
<td>Polkadot DOT</td>
<td>$34.08</td>
<td>-4.88%</td>
<td>3.70%</td>
<td>$31,369,477,649</td>
<td>$1,730,265,009</td>
<td>922,823,408 DOT</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
<tr>
<td>7</td>
<td>XRP XRP</td>
<td>$0.5447</td>
<td>5.21%</td>
<td>16.04%</td>
<td>$24,776,132,590</td>
<td>$7,152,342,591</td>
<td>45,404,028,640 XRP</td>
<td><img src="https://via.placeholder.com/150" alt="Chart" /></td>
</tr>
</tbody>
</table>
Central bank keeping close eye on Bitcoin development: governor

"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

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.

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.
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
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).

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.

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
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: 157RqAKrDyGHR1Bx3yDxeMv8Rh45aUet

In which country do you live?

Jacksonville, Florida
zip code 32224
United States
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.
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."

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.
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 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
  - “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](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
    \[ \rightarrow \text{locks message in the safe with her key} \]
  - Bob decrypts
    \[ \rightarrow \text{uses his copy of the key to open the safe} \]
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  ->  公開金鑰
Private Key  ->  Public Key

非常困難

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

Plaintext → Encrypt → Ciphertext

Public key

Decrypt ← Ciphertext

Private key

RSA (Rivest – Shamir – Adleman 1977)

ECC (Elliptic Curve Cryptosystem)
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

名稱： 台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
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
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
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).

<table>
<thead>
<tr>
<th>Algorithm and variant</th>
<th>Output size (bits)</th>
<th>Internal state size (bits)</th>
<th>Block size (bits)</th>
<th>Rounds</th>
<th>Bitwise operations</th>
<th>Security (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SHA-1</strong> FIPS 180</td>
<td>160</td>
<td>160</td>
<td>512</td>
<td>80</td>
<td>and, or, add, xor, rot</td>
<td>Theoretical attack (2^{61})</td>
</tr>
<tr>
<td>SHA-224</td>
<td>224</td>
<td>256 (8 × 32)</td>
<td>512</td>
<td>64</td>
<td>and, or, xor, shr, rot, add</td>
<td>112</td>
</tr>
<tr>
<td>SHA-256</td>
<td>256</td>
<td>(8 × 32)</td>
<td>512</td>
<td>64</td>
<td>and, or, xor, shr, rot, add</td>
<td>128</td>
</tr>
<tr>
<td>SHA-384</td>
<td>384</td>
<td>512 (8 × 64)</td>
<td>1024</td>
<td>80</td>
<td>and, or, xor, shr, rot, add</td>
<td>192</td>
</tr>
<tr>
<td>SHA-512</td>
<td>512</td>
<td>512 (8 × 64)</td>
<td>1024</td>
<td>80</td>
<td>and, or, xor, shr, rot, add</td>
<td>256</td>
</tr>
<tr>
<td>SHA-512/224</td>
<td>224</td>
<td>512 (8 × 64)</td>
<td>1024</td>
<td>80</td>
<td>and, or, xor, shr, rot, add</td>
<td>112</td>
</tr>
<tr>
<td>SHA-512/256</td>
<td>256</td>
<td>512 (8 × 64)</td>
<td>1024</td>
<td>80</td>
<td>and, or, xor, shr, rot, add</td>
<td>128</td>
</tr>
<tr>
<td><strong>SHA-2</strong> FIPS 180</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA3-224</td>
<td>224</td>
<td>1600 (5 × 5 × 64)</td>
<td>1152</td>
<td></td>
<td>and, xor, rot, not</td>
<td>112</td>
</tr>
<tr>
<td>SHA3-256</td>
<td>256</td>
<td>1600 (5 × 5 × 64)</td>
<td>1152</td>
<td></td>
<td>and, xor, rot, not</td>
<td>128</td>
</tr>
<tr>
<td>SHA3-384</td>
<td>384</td>
<td>1600 (5 × 5 × 64)</td>
<td>1152</td>
<td></td>
<td>and, xor, rot, not</td>
<td>192</td>
</tr>
<tr>
<td>SHA3-512</td>
<td>512</td>
<td>1600 (5 × 5 × 64)</td>
<td>1152</td>
<td></td>
<td>and, xor, rot, not</td>
<td>256</td>
</tr>
<tr>
<td><strong>SHA-3</strong> FIPS 202</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- Transaction
  - Owner 1's Public Key
  - Hash
  - Owner 0's Signature

- Transaction
  - Owner 2's Public Key
  - Hash
  - Owner 1's Signature

- Transaction
  - Owner 3's Public Key
  - Hash
  - Owner 2's Signature

Must be protected very well!!!
Combining & Splitting Value

“To allow value to be split and combined, transactions contain multiple inputs and outputs.”
## Transaction as Double-Entry Bookkeeping

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Value</th>
<th>Outputs</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input 1</td>
<td>0.10 BTC</td>
<td>Output 1</td>
<td>0.10 BTC</td>
</tr>
<tr>
<td>Input 2</td>
<td>0.20 BTC</td>
<td>Output 2</td>
<td>0.20 BTC</td>
</tr>
<tr>
<td>Input 3</td>
<td>0.10 BTC</td>
<td>Output 3</td>
<td>0.20 BTC</td>
</tr>
<tr>
<td>Input 4</td>
<td>0.15 BTC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total Inputs:** 0.55 BTC  
**Total Outputs:** 0.50 BTC

\[
\begin{align*}
\text{Inputs} & : 0.55 \text{ BTC} \\
- \quad \text{Outputs} & : 0.50 \text{ BTC} \\
\text{Difference} & : 0.05 \text{ BTC (implied transaction fee)}
\end{align*}
\]

*Figure 2-3. Transaction as double-entry bookkeeping*
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.”
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-protocolactually-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

Longest Proof-of-Work Chain

Block Header
- Prev Hash
- Nonce

Merkle Root

Hash01

Hash23

Merkle Branch for Tx3

Hash2

Hash3

Tx3

Mining 挖礦

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:

\[
0000000000000002a7b7d25a417c0374cc55261021e8a9ca74442b01284f0569
\]

which is less than the target:

\[
0000000000000003a30c000000000000000000000000000000000000000000
\]
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荷的運算問題，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
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
## Game Theory 賽局理論

- **Example: Prisoners’ Dilemma** 囚徒困境

<table>
<thead>
<tr>
<th></th>
<th>Prisoner B</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Prisoner A</td>
<td>stays silent (cooperates 合作)</td>
<td>stays silent 沉默</td>
<td>betrays 認罪 (defects 背叛)</td>
</tr>
<tr>
<td></td>
<td>Each serves 1 year 各服刑一年</td>
<td>Prisoner A: 3 years 各服刑三年</td>
<td>Prisoner B: goes free 各服刑兩年</td>
</tr>
</tbody>
</table>

- 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.

<table>
<thead>
<tr>
<th>Height</th>
<th>Age</th>
<th>Transactions</th>
<th>Total Sent</th>
<th>Relayed By</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>420517</td>
<td>8 minutes</td>
<td>1596</td>
<td>15,161.24 BTC</td>
<td>BTCC Pool</td>
<td>959.61</td>
</tr>
<tr>
<td>420516</td>
<td>18 minutes</td>
<td>2102</td>
<td>25,424.99 BTC</td>
<td>BitFury</td>
<td>997.88</td>
</tr>
<tr>
<td>420515</td>
<td>32 minutes</td>
<td>1952</td>
<td>25,578.75 BTC</td>
<td>AntPool</td>
<td>831.68</td>
</tr>
<tr>
<td>420514</td>
<td>47 minutes</td>
<td>936</td>
<td>14,381.41 BTC</td>
<td>AntPool</td>
<td>616</td>
</tr>
<tr>
<td>420513</td>
<td>52 minutes</td>
<td>2328</td>
<td>32,236.15 BTC</td>
<td>BTCC Pool</td>
<td>997.1</td>
</tr>
<tr>
<td>420512</td>
<td>1 hour 10 minutes</td>
<td>1622</td>
<td>30,966.32 BTC</td>
<td>Slush</td>
<td>998.19</td>
</tr>
</tbody>
</table>

Latest Transactions:
- ae4a517856c39bca5498fe61<br>  < 1 minute 5,977,584.04 BTC
- a8eba55582183122ee4c5344c<br>  < 1 minute 106,527,005.73 BTC
- 1cb935be5d7c1584001053567<br>  < 1 minute 0.201884 BTC
- c484b31df285f16acf2cc96e7<br>  < 1 minute 0.0499 BTC
- 9c31bcb2f6c940e7cd17d161b<br>  < 1 minute 5,980,307.93 BTC
- 26ced97171299ffedf755ec0<br>  < 1 minute 0.90484707 BTC

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

NEWS
- Magnr - Bitcoin Trading Platform | Trade with Leverage
  - 1 minute ago
- Bitcoin Price Technical Analysis for 07/13/2016 – Bulls Ready to Charge?
  - newsBTC 30 minutes ago
- How To Buy Bitcoin After That 'Mr. Robot' Episode | Huffingtonpost
  //bitcoin 1 hour 13 minutes ago
- Is the Steem content real?

https://blockchain.info
## Block #420512

**Summary**

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Of Transactions</td>
<td>1622</td>
</tr>
<tr>
<td>Output Total</td>
<td>30,966.32085875 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>4,600.97700775 BTC</td>
</tr>
<tr>
<td>Transaction Fees</td>
<td>0.32666721 BTC</td>
</tr>
<tr>
<td>Height</td>
<td>420512 (Main Chain)</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2016-07-13 02:52:35</td>
</tr>
<tr>
<td>Received Time</td>
<td>2016-07-13 02:52:35</td>
</tr>
<tr>
<td>Relayed By</td>
<td>Slush</td>
</tr>
<tr>
<td>Difficulty</td>
<td>213,398,925,331.32</td>
</tr>
<tr>
<td>Bits</td>
<td>402990845</td>
</tr>
<tr>
<td>Size</td>
<td>998.193 KB</td>
</tr>
<tr>
<td>Version</td>
<td>536870612</td>
</tr>
<tr>
<td>Nonce</td>
<td>3604645845</td>
</tr>
</tbody>
</table>

**Hashes**

- **Hash**: 0000000000000000000000452bfa0e4a5721d18eb8332eaac108f4826ef173236c474
- **Previous Block**: 00000000000000000000004dd60659f290db4b329b8df5d18cc19ae4a44c8e6bd1710
- **Next Block(s)**: 000000000000000000000025ce8b4b1e788f358e60d179072cf0fbb533564b7117ea3
- **Merkle Root**: a577ad1b3d890323b304a4be14e987de97aa0647773bb2e163317a880a91b70e6

**Network Propagation (Click To View)**

[Map Image]
Transactions

No Inputs (Newly Generated Coins)

<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>Date</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>e6994543f900a0713891f94480517bc481dbc544a7014660ec9f2aab2121f</td>
<td>2016-07-13 02:52:35</td>
<td>1CK6kHY6MHgYvmRQ4PAa1KYDrg1ejbH1cE</td>
</tr>
<tr>
<td>689b8aaa6777f29db459a85d69f05b152c0f585c1ad557ae3b528deb8a9c81ad</td>
<td>2016-07-13 02:46:38</td>
<td>1BzUywBBDDrdsHCm7vgsdUGxWF6pSCybU 1M8hwwYNWWhKxUJF1tF8Y829ni9NXx3gA</td>
</tr>
<tr>
<td>c3bd9ee32ef323c8e4abbc96bb58224f3df1e8ecfb9a0580a69c4359fa83a</td>
<td>2016-07-13 02:46:49</td>
<td>1PdsMWgX9MLALb3wAoKnKoU5mZBeWiLP 1JTsidxa1S39eozbiZWTUru385u1Dfgs</td>
</tr>
<tr>
<td>029d018635b02bfb7fa7a6a69aa654228a89a8c68224c59d84f9156b0142d33</td>
<td>2016-07-13 02:51:14</td>
<td>1XkM613U3W2PCGn8ik7VkJWUwmWFcukk6 1KzMc82k55u1HBULNFjsrF5Vkl88ez2pN</td>
</tr>
</tbody>
</table>
Bitcoin Address

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

Summary

Address: 1CKKHY6MhgYrM4PAafKYoDrg1ejbH1cE
Hash 160: 7c154ed1dc59609e3d26abb2df2ea3d587cd8c41
Tools: Taint Analysis - Related Tags - Unspent Outputs

Transactions

No. Transactions: 7856
Total Received: 106,160.37194277 BTC
Final Balance: 101,890,33403 BTC

Request Payment
Donation Button

Transactions (Oldest First)

2016-07-13 02:52:35

No Inputs (Newly Generated Coins)

1CK6HY6MHgYrmRQ4PAafKYDrg1ejbH1cE
9 Confirmations
12.82666721 BTC

2016-07-13 01:31:25

No Inputs (Newly Generated Coins)

1CK6HY6MHgYrmRQ4PAafKYDrg1ejbH1cE
18 Confirmations
12.56024582 BTC

2016-07-13 00:09:04

No Inputs (Newly Generated Coins)

1CK6HY6MHgYrmRQ4PAafKYDrg1ejbH1cE
30 Confirmations
12.58155207 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

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。

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。


## Block #0

### Summary

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Of Transactions</td>
<td>1</td>
</tr>
<tr>
<td>Output Total</td>
<td>50 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>0 BTC</td>
</tr>
<tr>
<td>Transaction Fees</td>
<td>0 BTC</td>
</tr>
<tr>
<td>Height</td>
<td>0 (Main Chain)</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2009-01-03 18:15:05</td>
</tr>
<tr>
<td>Difficulty</td>
<td>1</td>
</tr>
<tr>
<td>Bits</td>
<td>486604799</td>
</tr>
<tr>
<td>Size</td>
<td>0.285 KB</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Nonce</td>
<td>2083236893</td>
</tr>
<tr>
<td>Block Reward</td>
<td>50 BTC</td>
</tr>
</tbody>
</table>

### Hashes

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>0000000000000019d6689c085ae165831e934f763ae46a2a6c172b3f1b60a8ce26f</td>
</tr>
<tr>
<td>Previous Block</td>
<td>000000000000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>Next Block(s)</td>
<td>000000000839a8e6886ab5951d76f411475428af90947ee320161bb18eb6048</td>
</tr>
<tr>
<td>Merkle Root</td>
<td>4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b</td>
</tr>
</tbody>
</table>

### Transactions

- **4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b** 2009-01-03 18:15:05
  - No Inputs (Newly Generated Coins)
  - Output: 1A2zP1eP5QGefi2... (Genesis of Bitcoin)
  - 50 BTC
Genesis of Bitcoin
Addresses are identifiers which you use to send bitcoins to another person.

Summary
Address: 1A1zP1e5QGeft2DMPTTL5SLmv7DivmNa
Hash: 62e907b15cbr27d5425399ebf60fb50ebb88f18
Tools: Taint Analysis - Related Tags - Unspent Outputs

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

Transactions (Oldest First)

1b9a2ef7af3a1a888d3a778a618b8c81033866cc8eb795724b3a4f3fc9273ea8 2016-07-09 16:42:23
1EMaSSyxMQPv2fmUsdB7mMfMoocgf1MNw

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.

456d3d6964d295789959f7e6e270936317a564f03a017227c1249ac292e65b219 2016-06-20 20:16:53
14gRnM8MHFszDvHRethXG3VvdTuVlAq2

34a89ed996b63f9b073948f8536e2bc0d6c7af7cb53c8f008ffaf0fbf90c66 2016-06-17 17:09:30
1ChhZBuU3XLtWyzZ5BfssZj7m83KjWYDvG

456d3d6964d295789959f7e6e270936317a564f03a017227c1249ac292e65b219 2016-06-20 20:16:53
14gRnM8MHFszDvHRethXG3VvdTuVlAq2

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.

1ChhZBuU3XLtWyzZ5BfssZj7m83KjWYDvG
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，才適合導入區塊鍊
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
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