CryptoCurrency and Blockchain (3)

金融科技導論

陳君明

jmchen@crypto.tw

國立臺灣大學 National Taiwan University

Blockchain, Mining

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:

  0000000000000003A30C00000000000000000000000000000000000000000000

Hash Function Usages

- Double SHA256, i.e., SHA256(SHA256())
  - Merkle Tree
  - Block Hash
  - Transaction ID
- RIPEMD160(SHA256())
  - Bitcoin Address

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
  - …… Done in 2140: All 21,000,000 bitcoins are issued
- "The incentive can also be funded with transaction fees."
  - "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

比特幣礦機

Cryptocurrency miners are renting entire Boeing 747s just to stay in the game

BI Peter Farquhar, Business Insider Australia
Jul. 31, 2017, 2:31 AM 79,047

FACEBOOK LINKEDIN TWITTER EMAIL PRINT

In a mining boom, buy the shovels.

It's one of the oldest investing axioms, and anyone with shares in chipmakers AMD and Nvidia are reaping the rewards right now.

As the price of Bitcoin and Ethereum explodes, cryptocurrency miners are in a race to beat each other to the riches, and graphics processors are the tools they need.

A China Airlines Boeing 747. Bayne Stanley/Zuma Press/PA Images

http://www.businessinsider.com/cryptocurrency-miners-rent-boeing-747s-2017-7

比特幣飆破6,000美元...全球瘋挖礦，台廠滿訂單

2017/10/22 | 科技脈動

產品	公司	10月20日 收盤價（元）	10月20日 漲跌幅（%）
板卡廠	華　碩（2357）	258.00	0.58
	微　星（2377）	74.50	2.90
	技　嘉（2376）	40.60	0.12
	撼　訊（6150）	65.50	-4.10
ASIC晶片	創　意（3443）	290.50	-6.59
晶圓代工廠	台積電（2330）	237.50	-0.63

https://www.ctee.com.tw/News/ViewCateNews.aspx?newsid=164785&cateid=kjmd

正因為比特幣已可在部份國家進行支付，而且比特幣價格持續看漲，自然有愈來愈多人投入挖礦行列。事實上，目前全球有7成的比特幣是來自大陸的礦工，因為大陸地廣人稀、電費低廉，大陸業界也流傳一句話，「深圳的礦機加上四川的水電」，成就了大陸比特幣的挖礦大業。

數千台到上萬台的挖礦機、數十台的大型風扇或冷卻設備，每天24小時不停的挖礦，但能挖到的比特幣已愈來愈少，比特幣價值也愈來愈高，不僅大陸人瘋挖礦，包括日本、台灣、韓國等地都有人建置挖礦專業平台。但挖礦帶來的負面問題也不少，如台灣日前就發生有人在民宅設立挖礦機導致電線走火。而挖比特幣需要耗費大量電力，挖出1塊錢比特幣的耗電量，幾乎是正常家庭3～4個月的用電量。

所以，礦工們要持續升級挖礦機，也塑造出難以想像的比特幣挖礦生態圈，為挖礦機打造特殊應用晶片（ASIC）的創意接單暢旺，記憶體廠如威剛、宜鼎等亦滿手訂單，就連台積電也看到挖礦的好行情。台積電共同執行長劉德音在日前法說會中就指出，第三季加密型虛擬貨幣的挖礦相關晶片需求強勁，並帶來了3.5～4億美元營收。

https://www.ctee.com.tw/News/ViewCateNews.aspx?newsid=164785&cateid=kjmd

十月 4, 2017

【區塊客專訪】與台灣第一家挖礦機公司創辦人宋倬榮談挖礦及區塊鏈前景

應用介紹 / 精選主題

區塊客：有沒有什麼是投入挖礦前必須知道的行業內幕呢？

其實這對業內人士來說也不算甚麼秘辛，有一些礦機商生產完挖礦機美其名為替客戶測試，其實是「自己先挖」，甚至有時候宣稱延遲出貨，事實上都是自己在挖，等越來越難挖了再把礦機賣到市面上，而且這台礦機的開發費還是客戶分攤，因此選擇一間有誠信的礦機公司很重要。

區塊客：該如何選擇挖礦機呢？

目前只有 3 種幣有 ASIC 挖礦機：比特幣、萊特幣和達世幣（Dash），其他的幣用顯示卡挖就好了。只要在挖礦計算機輸入電費成本、顯卡型號、幣的價值和挖礦難度等等，就可以知道能不能回本。

區塊客：後來您從挖礦轉到區塊鏈及應用開發的契機是什麼？

我最早接觸這個行業的時候，沒甚麼人在講區塊鏈，當時最紅的是做挖礦。而比特幣紅了以後，大家覺得它的底層技術區塊鏈應該會滿有用處，而我自己也研究了一陣子。

https://blockcast.it/2017/10/04/blockcast-interview-first-mining-machine-in-taiwan/

「天堂文件」：小米CEO雷軍 靠私下投資比特幣設備商賺錢

鉅亨網編譯黃意文 2017/11/27 17:09

Bitmain 主宰比特幣礦業，除了製造專門的挖礦鑽機外，它們也設計機器內部的矽，以及經營採礦池，允許每一位礦工投入處理能力至更大的挖礦群體，進而提高他們的支出回報。Bitmain 在內蒙古和新疆自治區營運大型數據中心，因為那些地方的電力、土地與勞力較便宜。

比特幣分析師 Jimmy Song 預測，Bitmain 今年推出的新型鑽機，利潤約為 2.5 億美元。《Quartz》並報導，Bitmain 擁有良好的財務能力，去年可能付給台積電 4 億美元的晶片製作費用，為 AntMiner 鑽機訂製客製化晶片，而在最近一次的法說會上，台積電亦透露數位加密貨幣客戶在其總營收中占了 5%。

網站《Quartz》嘗試與「國際調查記者同盟」取得細節，但它們沒有回應，小米拒絕回應，Bitmain 則是無回應。

https://news.cnyes.com/news/id/3974142

QUARTZ

MINE CRAFT

The three stocks to watch for a cryptocurrency earnings boost this quarter

TSMC, the world's largest independent chip maker, said last week (Oct. 19) that its third-quarter earnings were boosted by gear popular among crypto-miners. "We saw continued strength from automotive, [internet of things] and high-performance computing, which includes a surge demand from cryptocurrency mining," TSMC co-CEO Mark Liu said in a conference call (pdf).

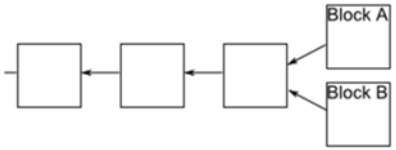
Bitmain, likely the largest maker of crypto-mining rigs, contracts with TSMC to produce customized silicon. It's unclear which other mining rig manufacturers have the scale to contract with TSMC, but Liu said crypto-miners accounted for between $350 and $400 million in revenue last quarter, or up to around 5% of the company's overall sales. "So it's pretty big and it's a pick up from the third quarter and stay on for the fourth quarter," Liu said on the call. TSMC's US-listed shares are up around 40% so far this year.

https://qz.com/1109011/tsmc-tsm-nvidia-nvda-amd-are-getting-a-boost-from-bitcoin-and-ethereum-miners

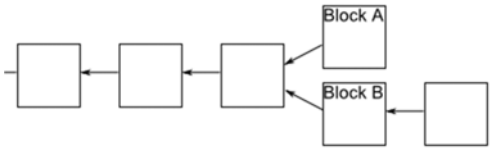
Consensus, Network

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

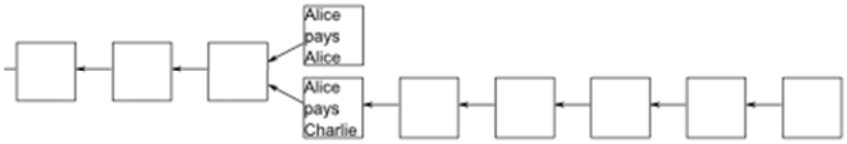


- If a fork occurs, people on the network keep track of both forks
- Miners only work to extend whichever fork is longest in their copy of the block chain



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

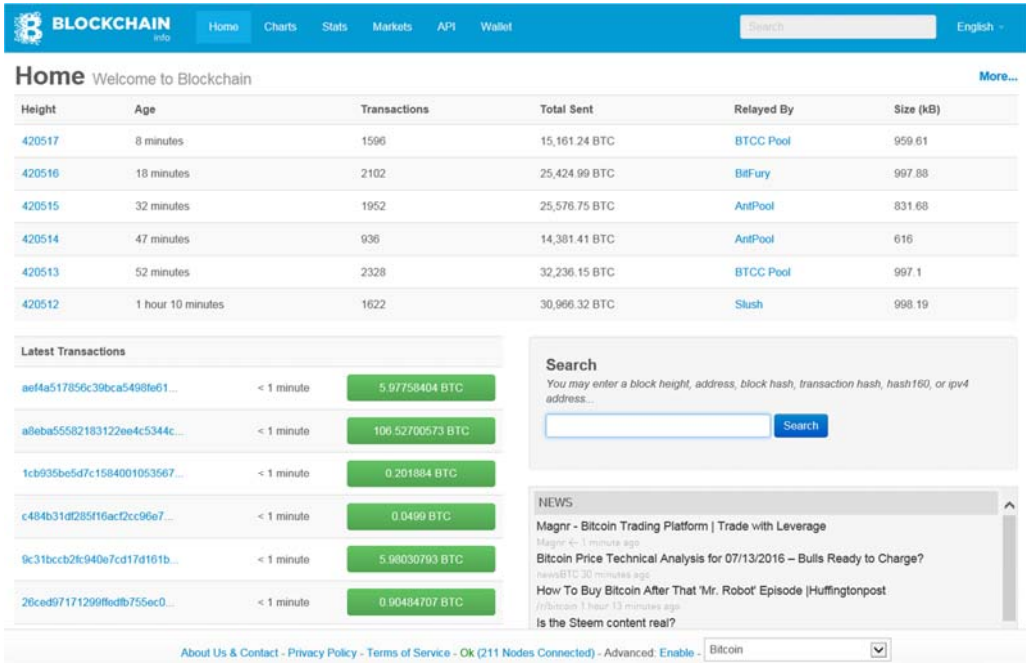
1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. Each node works on finding a difficult proof-of-work for its block
4. When a node finds a proof-of-work, it broadcasts the block to all nodes
5. Nodes accept the block only if all transactions in it 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

Game Theory 賽局理論

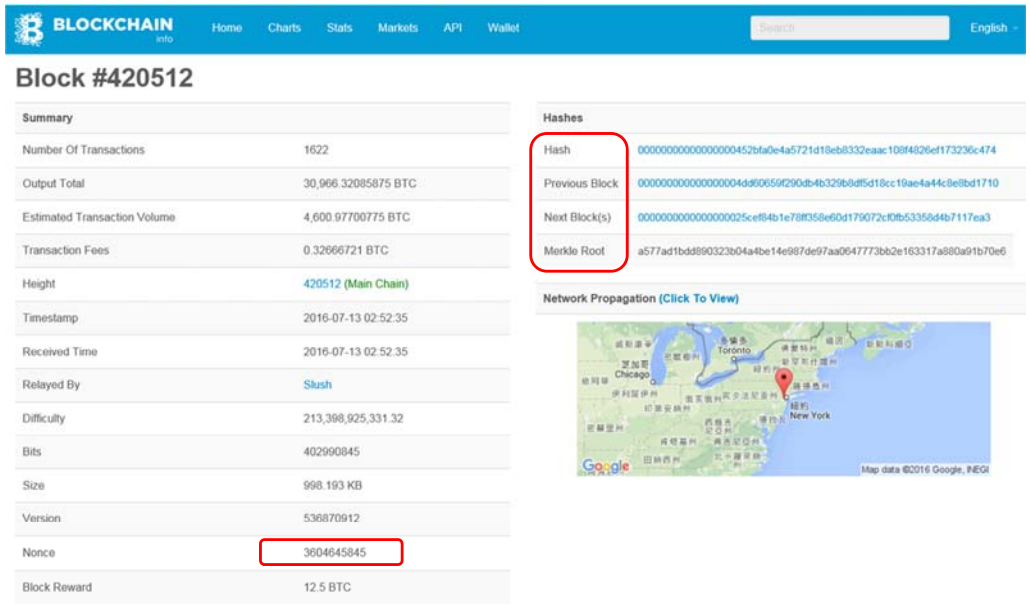
- Example: Prisoners' Dilemma 囚徒困境

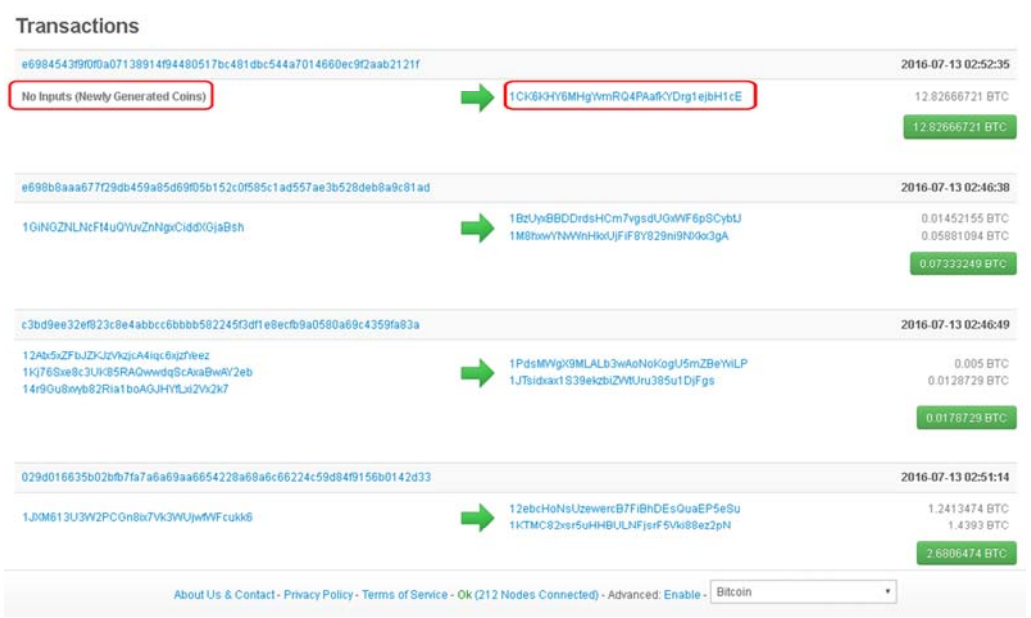
Prisoner B / Prisoner A	stays silent 沉默 (cooperates 合作)	betrays 認罪 (defects 背叛)
stays silent 沉默 (cooperates 合作)	Each serves 1 year 各服刑一年	Prisoner A: 3 years Prisoner B: goes free
betrays 認罪 (defects 背叛)	Prisoner A: goes free Prisoner B: 3 years	Each serves 2 years 各服刑兩年

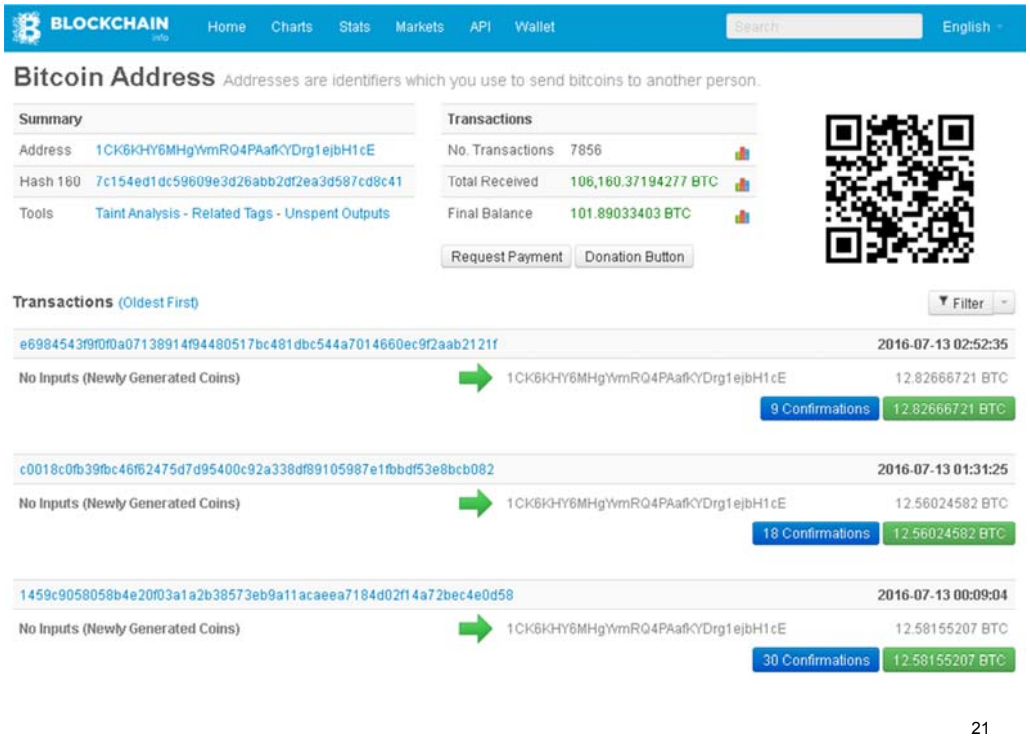
- The optimal individual choices leads to a sub-optimal collective outcome

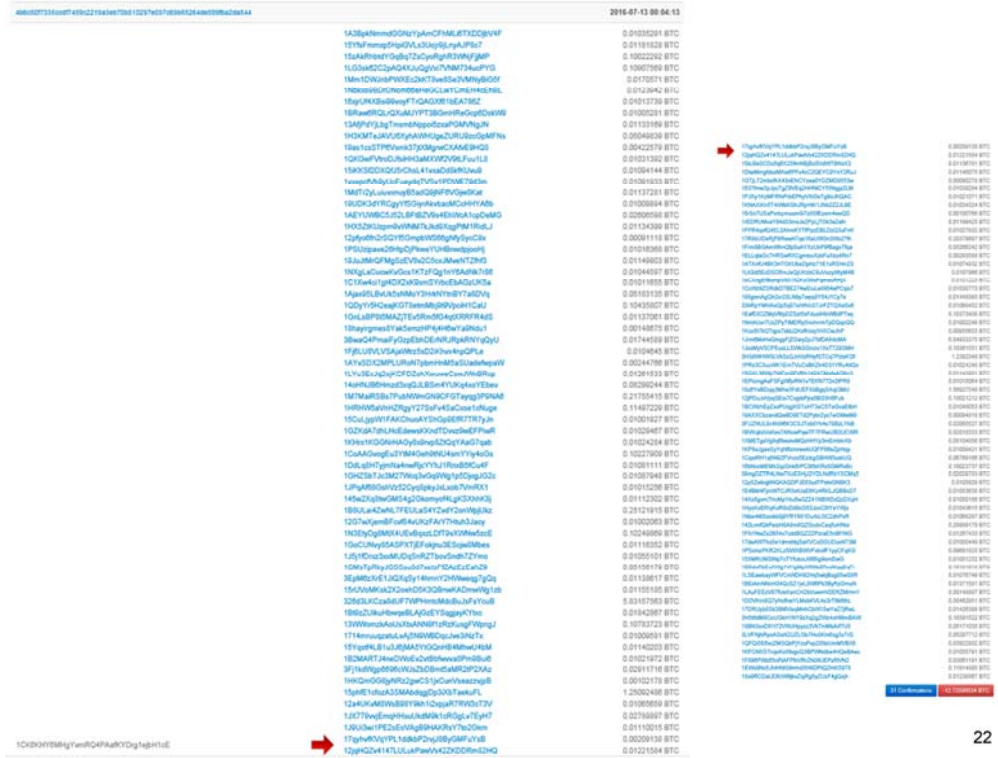


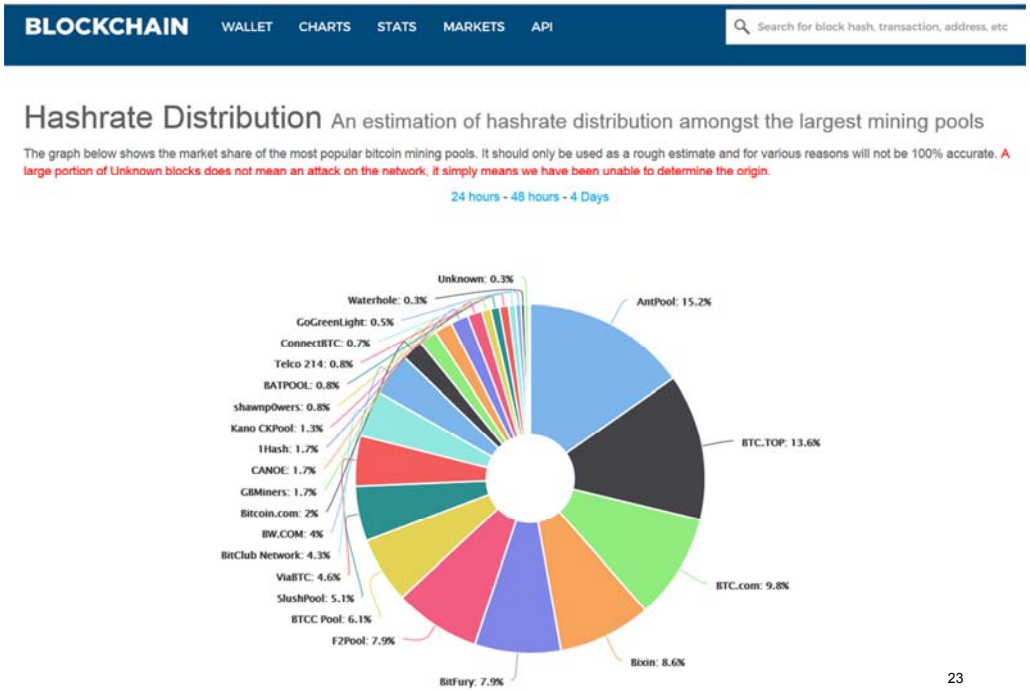
https://blockchain.info











誤解：區塊鏈使用 PKI ?!

- 數位簽章等公鑰密碼系統，屬於 PKC (Public-Key Cryptography 公鑰密碼學) 的範圍
  - https://en.wikipedia.org/wiki/Public-key_cryptography
- 由 CA (Certificate Authority 憑證管理中心)、RA、Certificate、CRL、... 組成的架構才稱為 PKI (公鑰基礎建設)
  - https://en.wikipedia.org/wiki/Public_key_infrastructure
- Bitcoin, Ethereum 等區塊鏈使用 PKC，並非 PKI
- 區塊鏈強調去中心化，不會有 CA

金融科技發展策略白皮書　p.93

區塊鏈加密技術是數種技術集合的統稱，最底層的帳冊記錄數位化的資產，自創始後無縫且持續增加的交易資料，通過公私鑰簽章加解密方法，讓數位資產可以在不同持有人之間移轉並記入帳冊，交易無需在任何第三方的主持下發生，結合密碼學加密技術，依時間序定期或定量將交易資料寫入資料區塊（block）內，再通過驗證程序確認，最新驗證過的區塊，會附加到先前已驗證過的區塊之後，形成區塊鏈帳冊，由所有參與成員構成的網路節點內電腦協同一致維護及儲存，共識即確保成員同意那些交易是根據什麼程序來運作，這些數位資產將無法與帳冊分割使用，意即不能離鏈交易。

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

讚 2.7 萬 按讚加入iThome粉絲團　分享 1,443　G+1 4

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。

讚 2.7 萬 按讚加入iThome粉絲團　分享 55　G+1 3

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。

讚 2.7 萬 按讚加入iThome粉絲團　分享 112　G+1 0

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

14gRnM8MHFszDvHRethXGc3WyfdTuVAqp → Genesis of Bitcoin 0.0001 BTC

0.0001 BTC

34a89ed9960653f9b073948f8536e2bc0d6c7af7cb53c8f008faff0fbf90c66 2016-06-09 17:09:30

1ChhZBuU3XLKtWyZ5BfsSzj7m83KjWYDVg → Genesis of Bitcoin 0.0001 BTC

0.0001 BTC

Security

ECDSA Signing 簽章

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

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

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

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

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

k : ephemeral key

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

ECDSA Verification 驗章

For Bob to authenticate Alice's signature, he must have a copy of her public-key curve point Q_A. Bob can verify Q_A is a valid curve point as follows:

1. Check that Q_A is not equal to the identity element O, and its coordinates are otherwise valid
2. Check that Q_A lies on the curve
3. Check that $n * Q_A = O$

After that, Bob follows these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. Calculate $e = \mathrm{HASH}(m)$, where HASH is the same function used in the signature generation.
3. Let z be the L_n leftmost bits of e.
4. Calculate $w = s^{-1} \bmod n$.
5. Calculate $u_1 = zw \bmod n$ and $u_2 = rw \bmod n$.
6. Calculate the curve point $(x_1, y_1) = u_1 * G + u_2 * Q_A$.
7. The signature is valid if $r \equiv x_1 \pmod n$, invalid otherwise.

Note that using Straus's algorithm (also known as Shamir's trick) a sum of two scalar multiplications $u_1 * G + u_2 * Q_A$ can be calculated faster than with two scalar multiplications.[3]

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

Ephemeral Key & RNG

- The **entropy**, **secrecy**, and **uniqueness** of the DSA/ECDSA **random ephemeral key *k*** is critical
  - Violating any one of the above three requirements can reveal the entire private key to an attacker
  - Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA / ECDSA
- [December 2010] The ECDSA private key used by **Sony** to sign software for the **PlayStation 3** game console was recovered, because Sony implemented *k* as static instead of random

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

Ephemeral Key & RNG

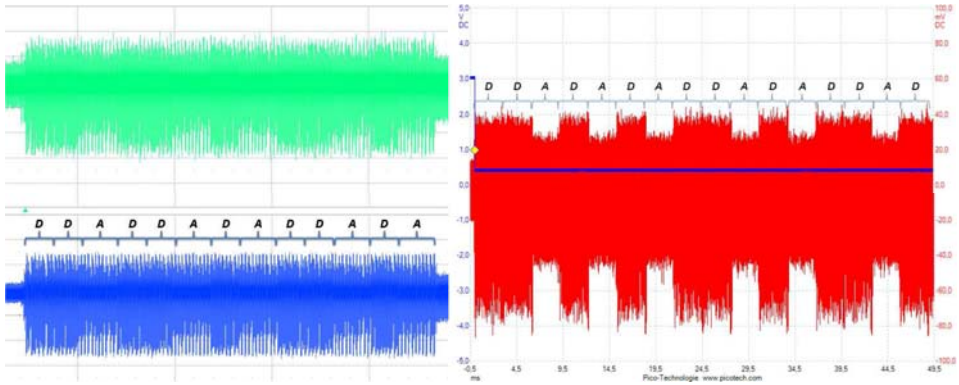
- [August 2013] Bugs in some implementations of the Java class *SecureRandom* sometimes generated collisions in *k*, allowing in stealing **bitcoins** from the containing wallet on **Android app**
  - http://www.theregister.co.uk/2013/08/12/android_bug_batters_bitcoin_wallets
- [August 2013] 158 accounts had used the same signature nonces *r* value in more than one signature. The total remaining balance across all 158 accounts is only 0.00031217 BTC. The address, 1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj, appears to have stolen bitcoins from 10 of these addresses. This account made 11 transactions between March and October 2013. These transactions have netted this account over 59 bitcoins (approximately $12,000 USD).
  - http://eprint.iacr.org/2013/734.pdf
- This issue can be prevented by deriving *k* deterministically from the **private key** and the **message hash**, as described by **RFC 6979**

ECDSA (Elliptic-Curve Digital Signature Algorithm)

- 必須安全計算點的倍數

Key creation	
Choose secret signing key $1 < s < q-1$. Compute $V = sG \in E(\mathbb{F}_p)$. Publish the verification key V.	
Signing	
Choose document $d \bmod q$. Choose random element $e \bmod q$. Compute $eG \in E(\mathbb{F}_p)$ and then, $s_1 = x(eG) \bmod q$ and $s_2 \equiv (d + ss_1)e^{-1} \pmod q$. Publish the signature (s_1, s_2).	

Side-Channel Attacks



D (double) or **A** (add) depends on the bits of **Private Key**

Image Courtesy https://eprint.iacr.org/2015/354.pdf

ECDSA Key Extraction from Mobile Devices

- Fully extract secret signing keys from OpenSSL and CoreBitcoin running on iOS devices

Sourse: https://www.tau.ac.il/~tromer/mobilesc

Applications, Evolutions

區塊鏈特色

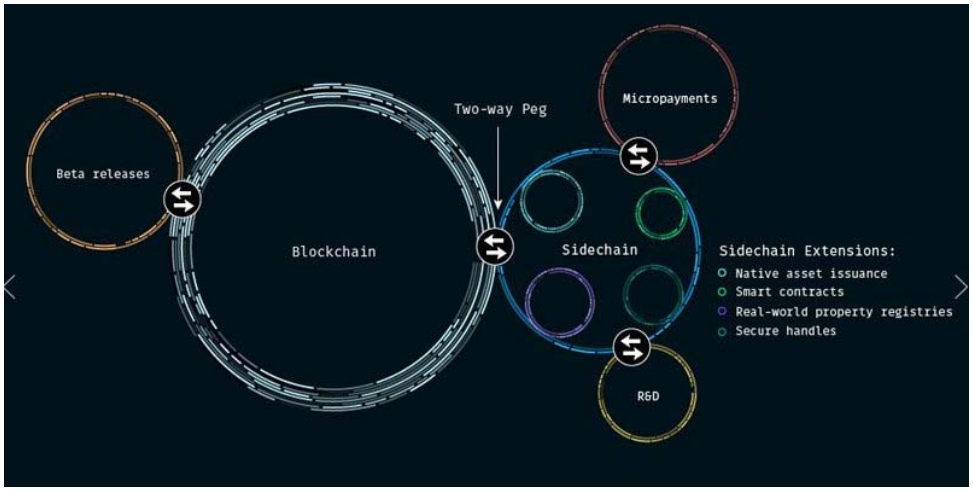
- 去中心化 (decentralized)
- 共同維護公開帳本 (public ledger)
- 防止抹滅或竄改 (tamper resistant)
- 具備時戳 (timestamps)
- 自動解決交易衝突 (conflict resolution)

區塊鏈應用領域

- 銀行
- 支付與轉帳
- 網路安全
- 學術驗證
- 投票
- 汽車租賃與銷售
- 物聯網
- 智慧合約
- 分析與預測
- 線上音樂
- 出行共享
- 證券交易
- 醫療
- 公證
- .....
- (族繁不及備載)

http://www.bnext.com.tw/ext_rss/view/id/1336998
http://tech.gmw.cn/2016-02/16/content_18893346.htm

Sidechain 側鏈



Two-way Peg: 雙向錨定

區塊鏈分類

1.公開制或非許可制區塊鏈（Permissionless Blockchain）：

系統採開放存取架構，無中央管控的組織，任何人欲加入應用社群網路，僅需認同其制定的遊戲規則，無需通過任何審查程序即可用匿名方式參加，並自動取得發起或接受交易的授權，不受任何現有法規制度或規範限制，主要應用在鏈結（on-chain）系統內生性創造之資產（例如比特幣）的交易帳冊。

2.私有制或許可制區塊鏈（Permissioned Blockchain）：

許可制通常用於大型企業或政府，基於組織內部某些共通性的應用，建立限制使用範圍與對象的區塊鏈系統，具備中央管理的機制，成員為預先選定不對外開放加盟。

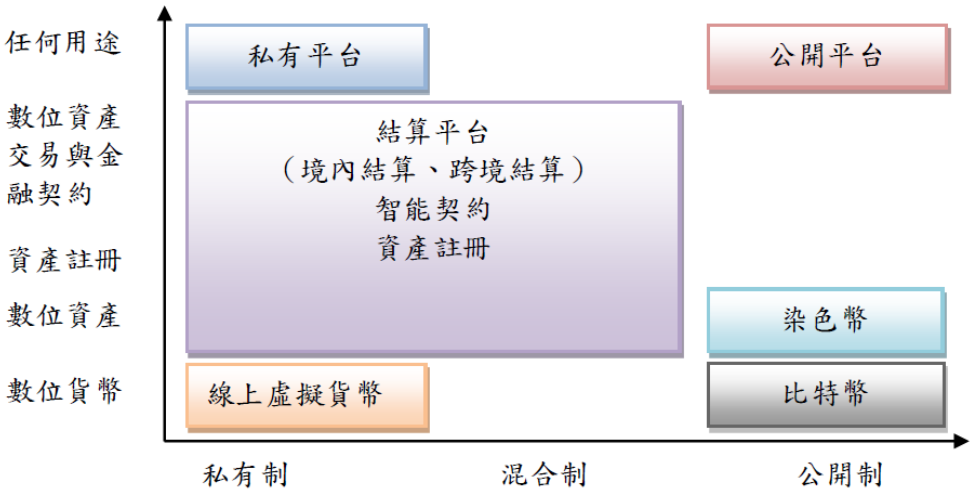
區塊鏈分類

3.混合制或聯盟制（Consortium blockchains）：

混合制為結合公開制與私有制之區塊鏈應用，通常用於提供相同服務且具備互通需求的產業，由核心成員發起組成聯盟，制定合意之相關規範與流程，後續參與者需要經過核心成員審核，並同意遵循相關契約規定或法律規範，可採行權限管控設定，相較於公開制具備高度的擴展性。

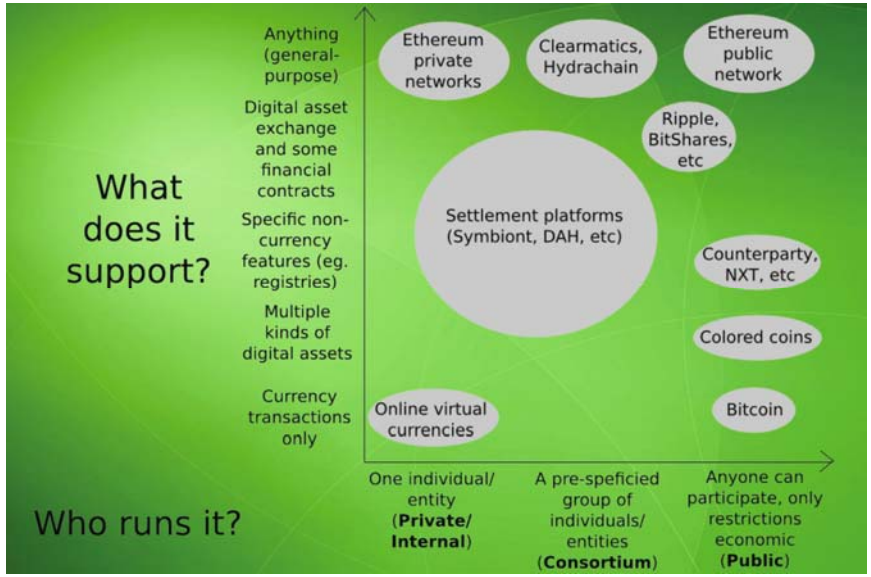
金融科技發展策略白皮書 p.94

區塊鏈分類



金融科技發展策略白皮書 p.94

區塊鏈分類



Ethereum

Ethereum 以太坊 / 以色龍

- Ethereum is a public blockchain platform with programmable transaction functionality
- It provides a decentralized virtual machine that can execute peer-to-peer contracts using a crypto asset called Ether (unofficial code ETH)

https://www.ethereum.org

Vitalik Buterin

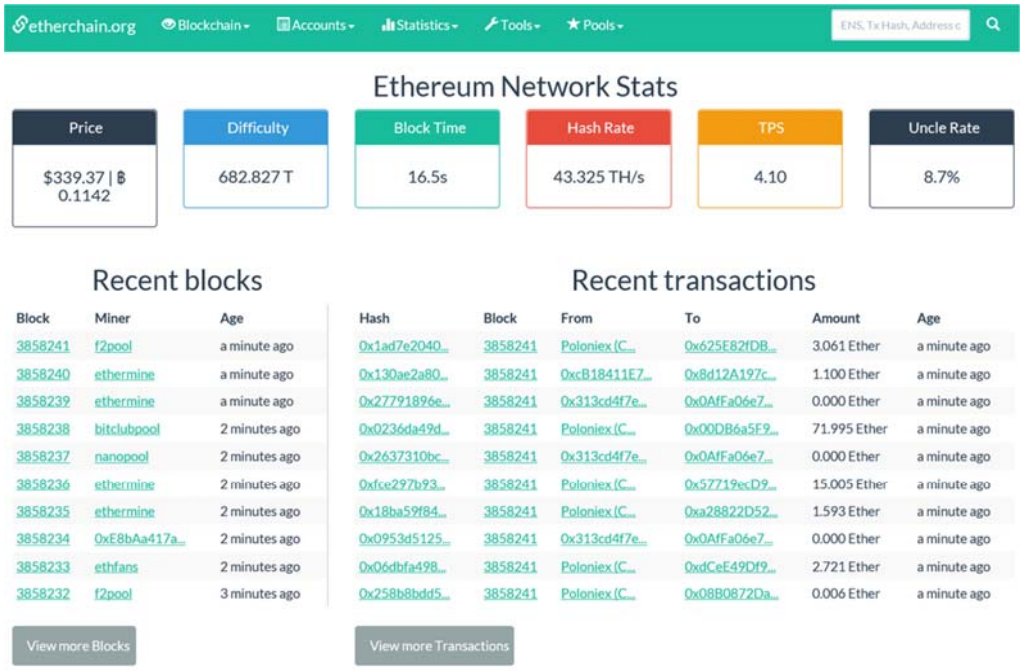
- Ethereum was initially proposed by Vitalik Buterin in late 2013, and the genesis block, marking the live release of the Ethereum project, occurred on 30 July 2015

Born	January 31, **1994** Moscow, Russia
Residence	Switzerland
Citizenship	Russia, Canada
Fields	Digital contracts, Digital currencies, Game theory

Image Courtesy
http://www.coinfox.info/news/video/5460-vitalik-buterin-o-blokchejne-i-nadezhnosti-ethereum-2

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)
    ```

https://etherchain.org

zk-SNARKs
    ```

交易隱私保護：zk-SNARKs

Zerocash: Decentralized Anonymous Payments from Bitcoin

Eli Ben-Sasson* Alessandro Chiesa† Christina Garman‡ Matthew Green‡
Ian Miers‡ Eran Tromer§ Madars Virza†

May 18, 2014

Abstract

Bitcoin is the first digital currency to see widespread adoption. Although payments are conducted between pseudonyms, Bitcoin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zerocoin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet it still reveals payment destinations and amounts, and is limited in functionality.

In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in *zero-knowledge Succinct Non-interactive ARguments of Knowledge* (zk-SNARKs).

zk-SNARKs

- zk-SNARKs: You can verify the correctness of computations without having to execute them and you will not even learn what was executed – just that it was done correctly

Zcash

https://z.cash

號稱終極匿名的數位貨幣 ZCash 強勢發表，它究竟有什麼好處？

作者 雷鋒網 | 發布日期 2016 年 11 月 01 日 7:30 | 分類 Fintech , 網路 G+1 讚 分享 251

日前，基於區塊鏈技術的替代數位貨幣 ZCash 正式發表，開發者宣稱，ZCash 利用加密隱藏用戶的身分，是第一種真正匿名的數位貨幣。據悉，ZCash 發表之初便異常火爆，火爆到了甚至還沒開始挖礦，Bitmex 上的期貨價格最高能達到 1.98TC。

http://technews.tw/2016/11/01/zcash