CryptoCurrency and Blockchain (3)

金融科技導論

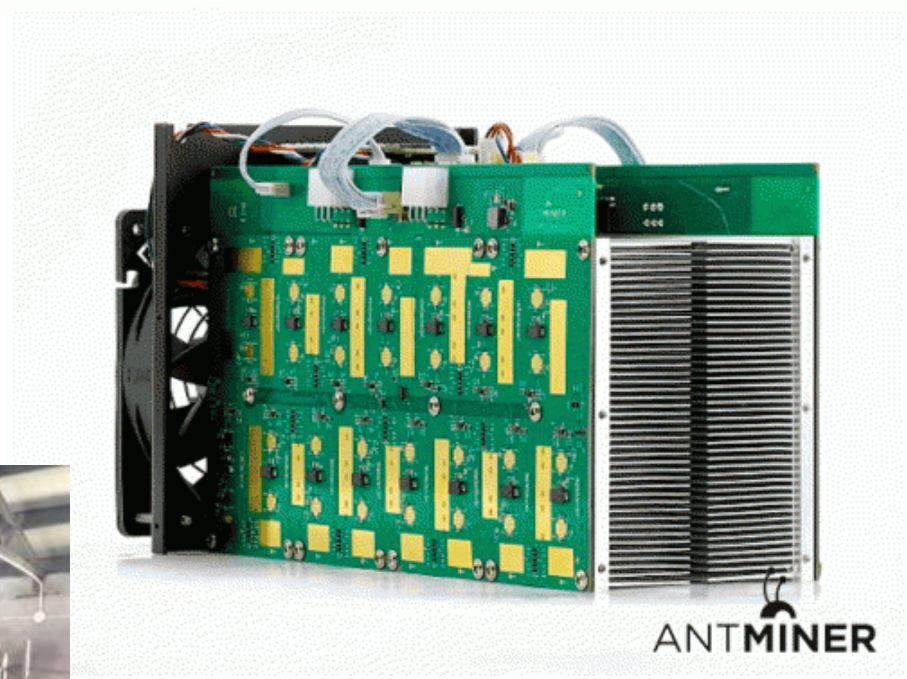
陳君明

jmchen@ntu.edu.tw

國立臺灣大學 National Taiwan University

Mining

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/

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

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

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

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/

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

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

挖礦顯示卡需求強勁 Nvidia 首季相關收益達 2.89 億美元

◇ 企業趨勢 by Antony Shum on 五月 14, 2018

近年隨着加密貨幣的盛行，挖礦的需求也不斷增加。由於挖礦需要用到大量的 GPU 運算，因此同時帶動了顯示卡的銷量提升。最近 Nvidia 的業績就透露了他們在首季於挖礦顯示卡方面錄得大幅增長。

Nvidia 表示，在第一季的收入之中，挖礦相關市場的銷售額佔了 9% 以上，亦佔了 OEM 收入的 76%，比上季增加 115%，總共帶來 2.89 億美元的收入。Nvidia CEO Jensen Huang 解釋，由於挖礦用家對顯示卡的需求增加，導致價格上漲，使他們收益超出預期。

這次是 Nvidia 首次公開挖礦市場在收入之中佔多少，不過 Nvidia 方面亦估計，下一季來自挖礦市場的銷量可能會下跌三分之二，這一方面是因為價格上漲令需求降低，也是因為年初開始加密貨幣的價格大幅下跌，加上挖礦難度提升，「礦工」擴充挖礦規模的意欲也會因此下跌。

除了 Nvidia 之外，AMD 亦有受惠於挖礦需求，不過他們就強調這方面的需求並不是主要帶來公司成長的因素。AMD 在 4 月份的資料顯示挖礦相關的銷售收入佔整體的 10% 左右。雖然挖礦相關的銷售強勁，但這個市場的需求亦可以相當不穩定，因此晶片公司不願意全力投放資源開發這方面的產品也是可以理解。

來源：Bloomberg https://unwire.pro/2018/05/14/nvidia-reports-first-quarter-crypto-sales/news

比特大陸密訪台積 聚焦新挖礦晶片合作

2018-06-04 02:00 經濟日報 記者謝佳雯／台北報導 讚 91 分享

業界傳出，全球虛擬貨幣挖礦機龍頭比特大陸（Bitmain）共同創辦人暨共同執行長詹克團上周旋風式來台，密訪台積電、力晶等供應鏈夥伴，尋求為新一代高效能挖礦晶片展開合作，並商討比特大陸轉型發展人工智慧（AI）應用後的合作方向。

至昨（3）日截稿前，台積電未對詹克團是否拜會有任何回應；比特大陸和力晶發言窗口則表示，不清楚相關行程。台積電預計明（5）日舉行股東會，不僅是董事長張忠謀的退休前告別秀，與比特大陸接下來的合作發展，預料也是小股東關切的議題。

業界消息指出，詹克團此次來台，力晶創辦人暨執行長黃崇仁，以及將升任台積電總裁的共同執行長魏哲家親自接待，凸顯兩家公司對比特大陸的重視。

近期虛擬貨幣價格震盪激烈，比特幣一度面臨7,000美元大關保衛戰，市場對虛擬貨幣市場產生疑慮，並傳出比特大陸對供應鏈拉貨力道顯著放緩，砍單聲四起。

比特大陸為台積電大客戶，外資擔憂後市，接連出脫持股，使得台積電股價走勢受影響。詹克團上周訪台與台積電、力晶談新合作案，意味比特大陸仍會持續強化與台積電等夥伴合作，破除外界砍單傳聞，不僅牽動虛擬貨幣未來動態，也關係到創意、智原等挖礦機相關業者接單。

https://money.udn.com/money/story/5612/3178193

NVIDIA營收連四降，最佳CEO黃仁勳的麻煩到底出在哪？

撰文者：張庭瑋

商周頭條 | 2019.11.17 12,219

繪圖晶片龍頭輝達（NVIDIA），上週公布第三季財報，營收比去年同期下降了5%，這已是連續4季下降。財報表現落漆，甫被選為「最佳CEO」的執行長黃仁勳，肩上究竟擔著多少挑戰？而他的應戰策略，竟然是：轉型為軟體公司！

輝達過去一年真的過得很不好。德銀（Deutsche Bank）最近一篇研究報告指出，過去一年的眾多營運困境中，最嚴重的就是，加密貨幣挖礦需求銳減。

挑戰1：加密貨幣挖礦潮的「宿醉」

「加密貨幣狂歡後的宿醉，持續的比我想像中的還久。」黃仁勳去年曾無奈的在電話法說會上表示。

由於繪圖晶片特別適合用在加密貨幣「挖礦」，在2017年底到2018年初之間，比特幣等加密貨幣價格狂飆，導致晶片需求大增。《CNBC》報導，當時配備高階繪圖晶片的顯示卡，在市面上甚至一卡難求，讓股價已經被AI（人工智慧）晶片題材拱高的輝達，在去年10月1日達到股價巔峰289美元。

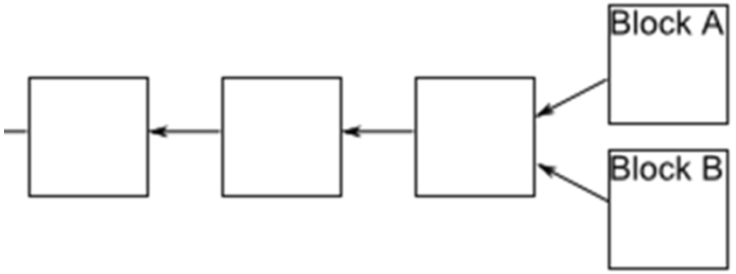
然而，危機就藏在繁榮中。去年底以來，加密貨幣挖礦潮退去，加上遊戲業務需求不振，讓輝達營運陷入低潮。

https://www.businessweekly.com.tw/focus/blog/3000751

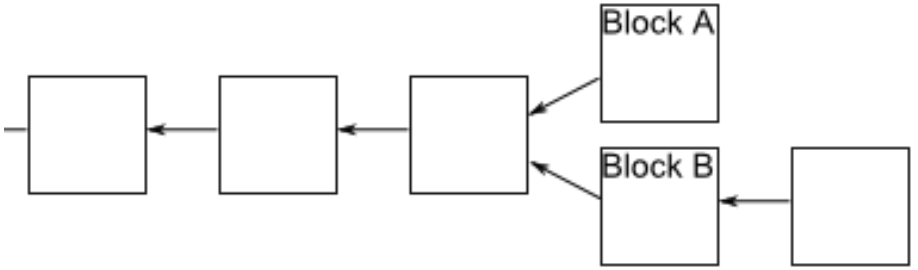
Consensus

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

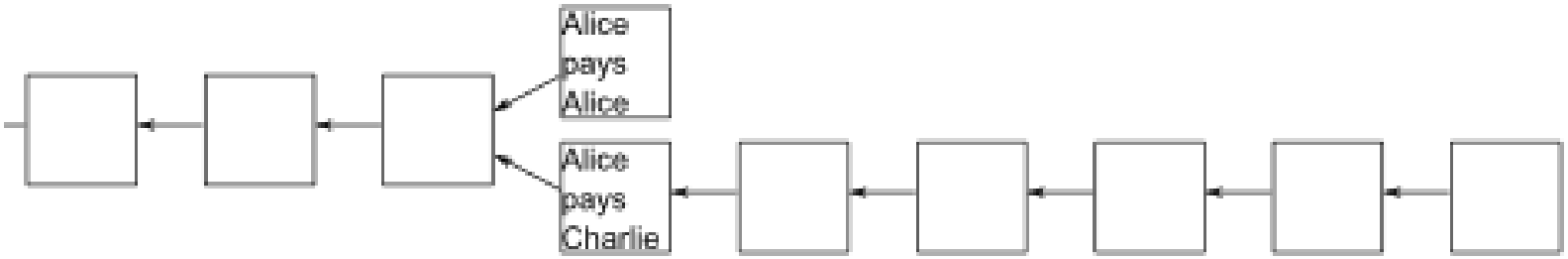


- If a fork occurs, people on the network keep track of both forks
- Miners only work to extend whichever fork is longest in their copy of the block chain



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

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

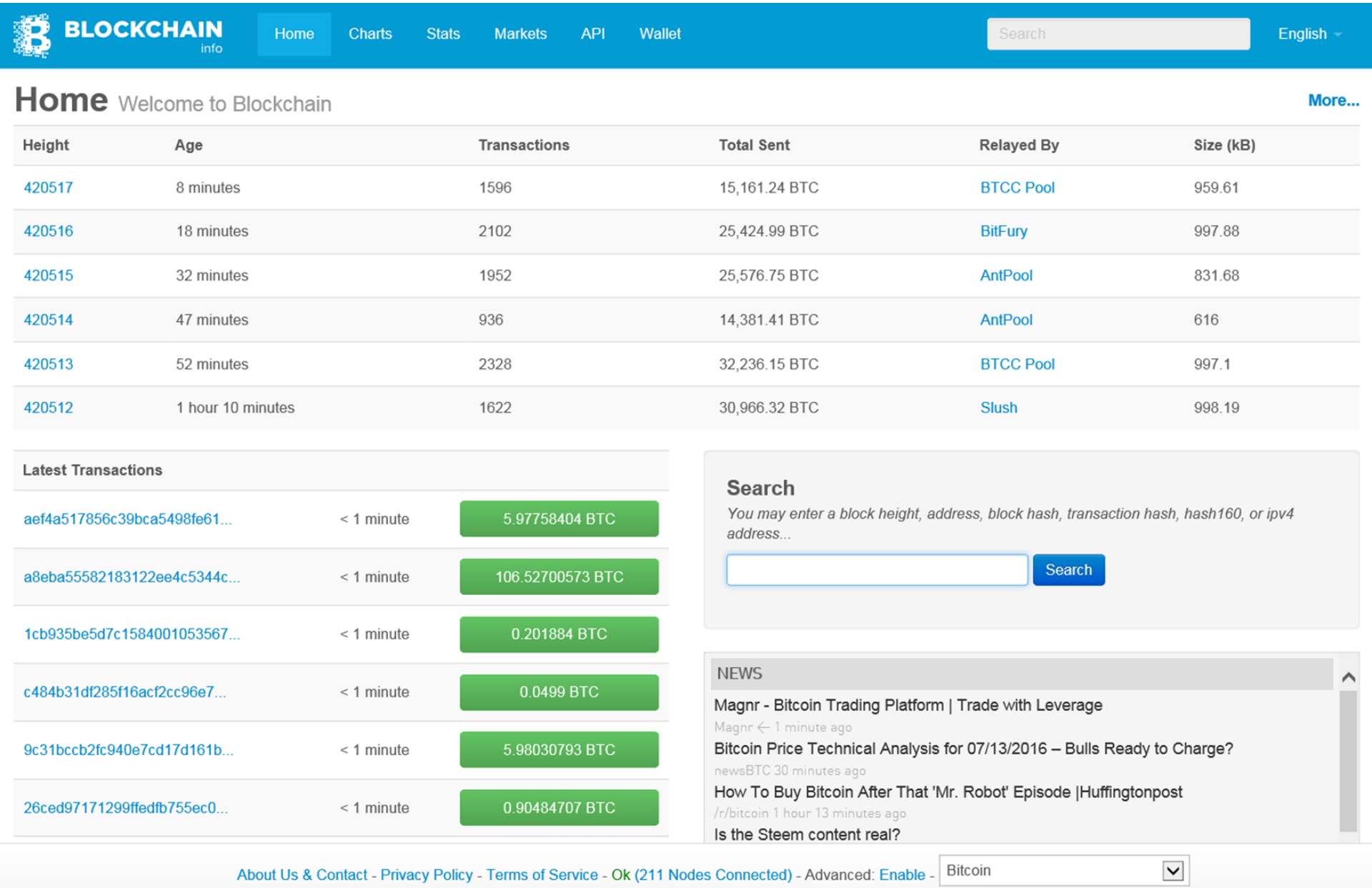
UPDATED on 9th January at 18:11 (GMT)

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 1Kj76Sxe8c3UK85RAQwwdqScAxaBwAY2eb 14r9Gu8xwyb82Ria1boAGJHYfLxi2Vx2k7	→	1PdsMWgX9MLALb3wAoNoKogU5mZBeYviLP — 0.005 BTC 1JTsidxax1S39ekzbiZWtUru385u1DjFgs — 0.0128729 BTC

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

e6984543f9f0f0a07138914f94480517bc481dbc544a7014660ec9f2aab2121f — 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
1BRaw6RQLrQXuMJYPT3BGmHReGcp8DskW9	0.01005281 BTC
13AfjPdYjLbgTmsmbNppoi5zxaPGMVNgJN	0.01133169 BTC
1H3KMTeJAVU8XyhAWHUgeZURU9zcGpMFNs	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
15tiU9aSCDu5q6X2SfmNBjBsSVdWTBNxX3	0.01138791 BTC
1DtwMmgfdszMKw6PFv4cC2QEYC6YnY2RuJ	0.01146075 BTC
1GTjLT2mbxfhX43nENCYzea8YDZMD9553w	0.00090278 BTC
1637fmw3pJyuTgZ9VEq2HHNiCY5Wqgy2LM	0.01038284 BTC
1PJXy1KzMFRfnPrbEPhyVXiGsTg9oJKQAC	0.01021071 BTC
1KNAXiKn5T4iWbKGhJRpHtK1JNb2Z2JL9E	0.01034324 BTC
16rSn7USaPxrbpmuum8i7z95fEzem4vwQD	0.00100766 BTC
1rEDRUMvaY94d33meJe2PpLjTGk3e2afn	0.01199425 BTC
1FPR4qvfQ4EL2AhmKYTfPpzDBLDzQ3uFnK	0.01027832 BTC
17R8bUDeRjP9RewH7qe16aU5fGn3Wx27fh	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
1HysKvEfXqKoR8oDd9cG53JzxC8tYeYWjs	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
3H5t6dM8CoUGkH1NY9zXq2gZVz4xHMmBAW	0.10391522 BTC
18BN3soD91t7ZVWJHpyzz3Vk7mMbArf7U5	0.05171038 BTC
3LVFNjhRyoAGs5N2UZLGb7Ho8Km6sg3s7rG	0.05297712 BTC
1QFQi5E6vcZMSQbPjYzoPvp28NzUmMVBX6	0.03922802 BTC
1KFCN5G7nqoKoVWgcQ3BPWNdbe4HQeBAec	0.01055791 BTC
1F896PWz65nPjAFPfcVRrZNjWJEPyf5VN2	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

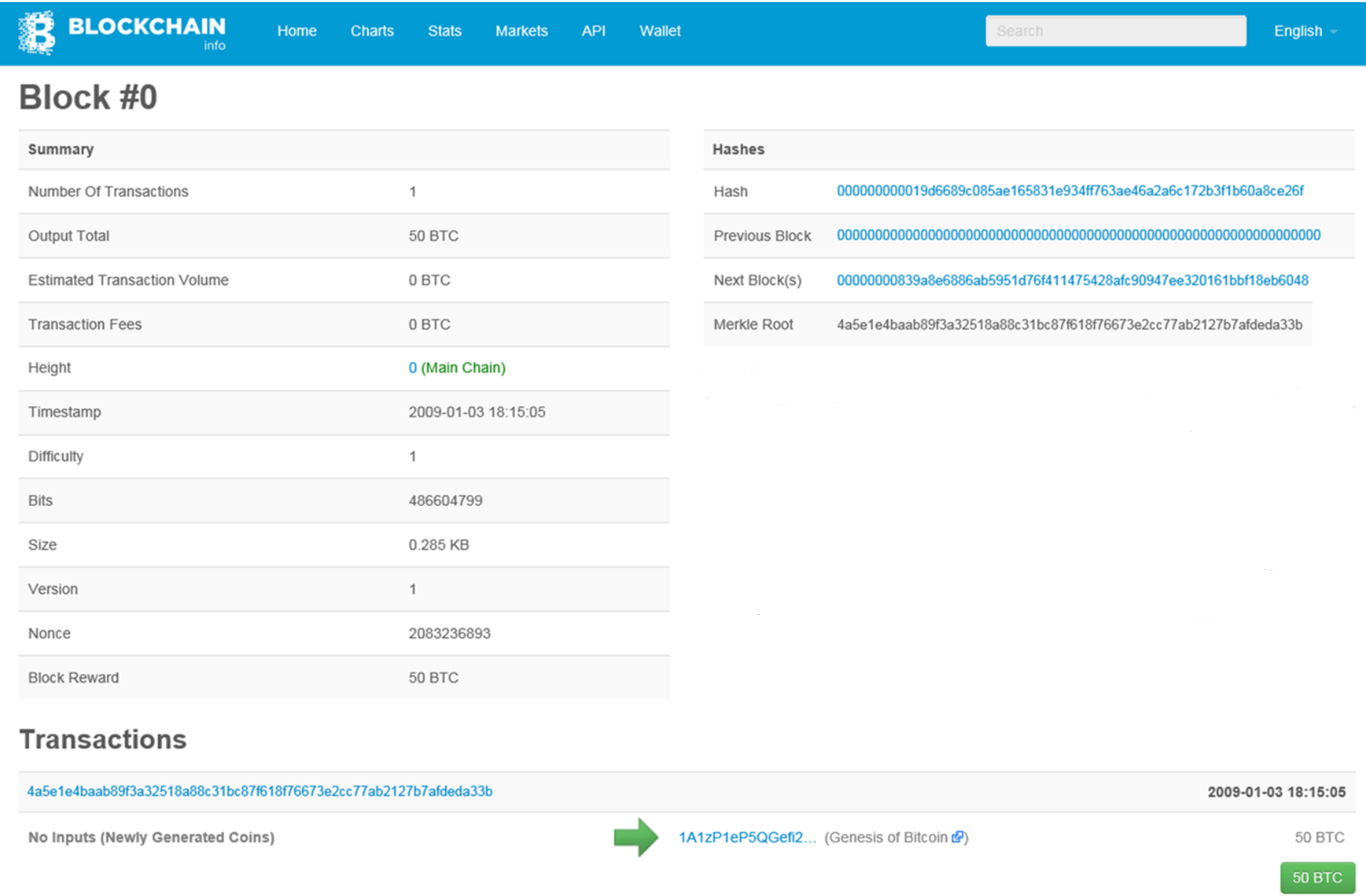
http://www.ithome.com.tw/news/105687

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

ECDSA
(Elliptic Curve Digital Signature Algorithm)

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 $e = \mathrm{HASH}(m)$, 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 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

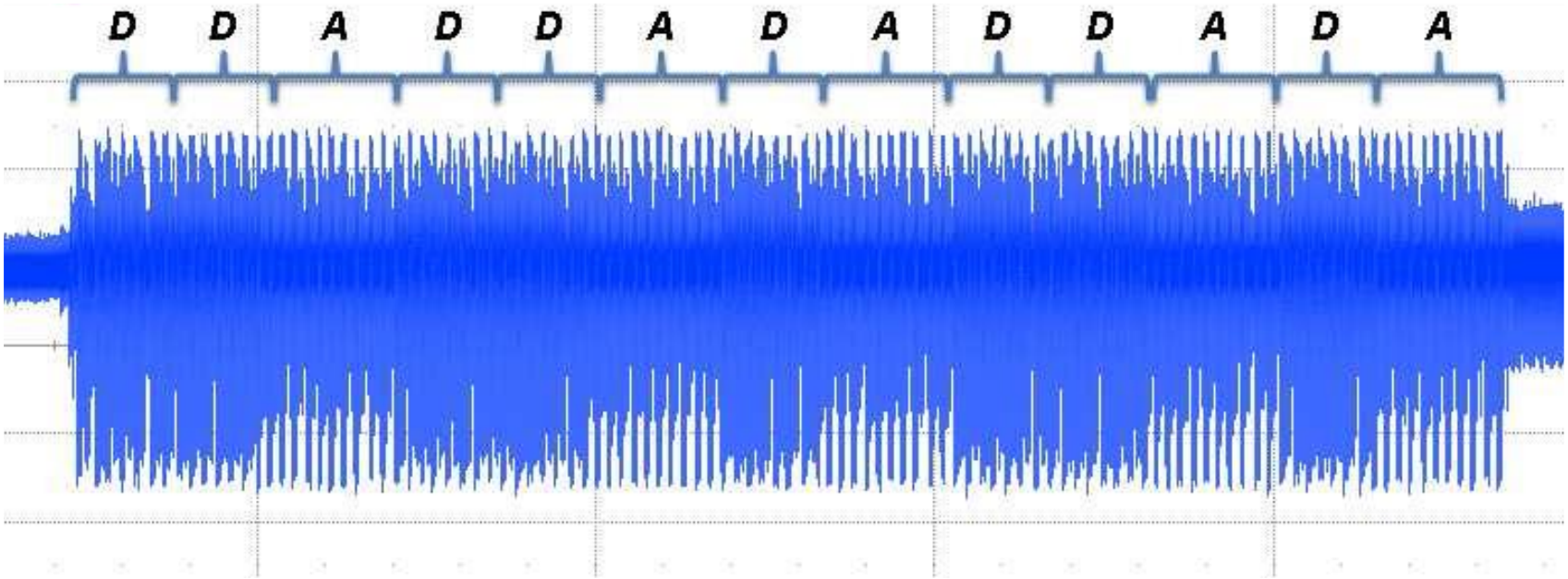
Ephemeral Key & RNG

- [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.
  - 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**

Side Channel Attack (SCA)


Side Channel Attack
旁通道攻擊！

Side-Channel Attacks 旁通道攻擊



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

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

隔空抓「鑰」： 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

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

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。

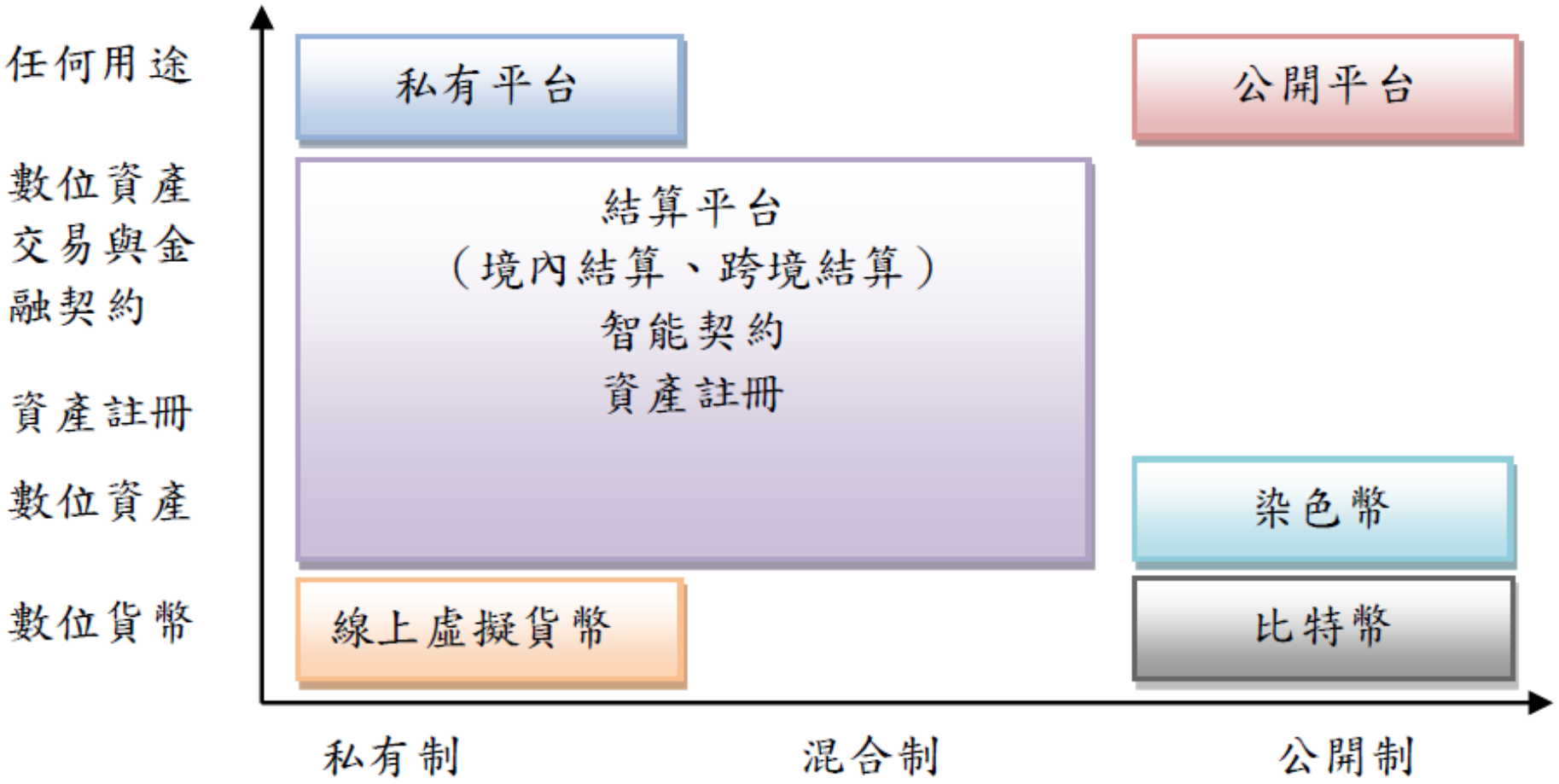
區塊鏈分類

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。

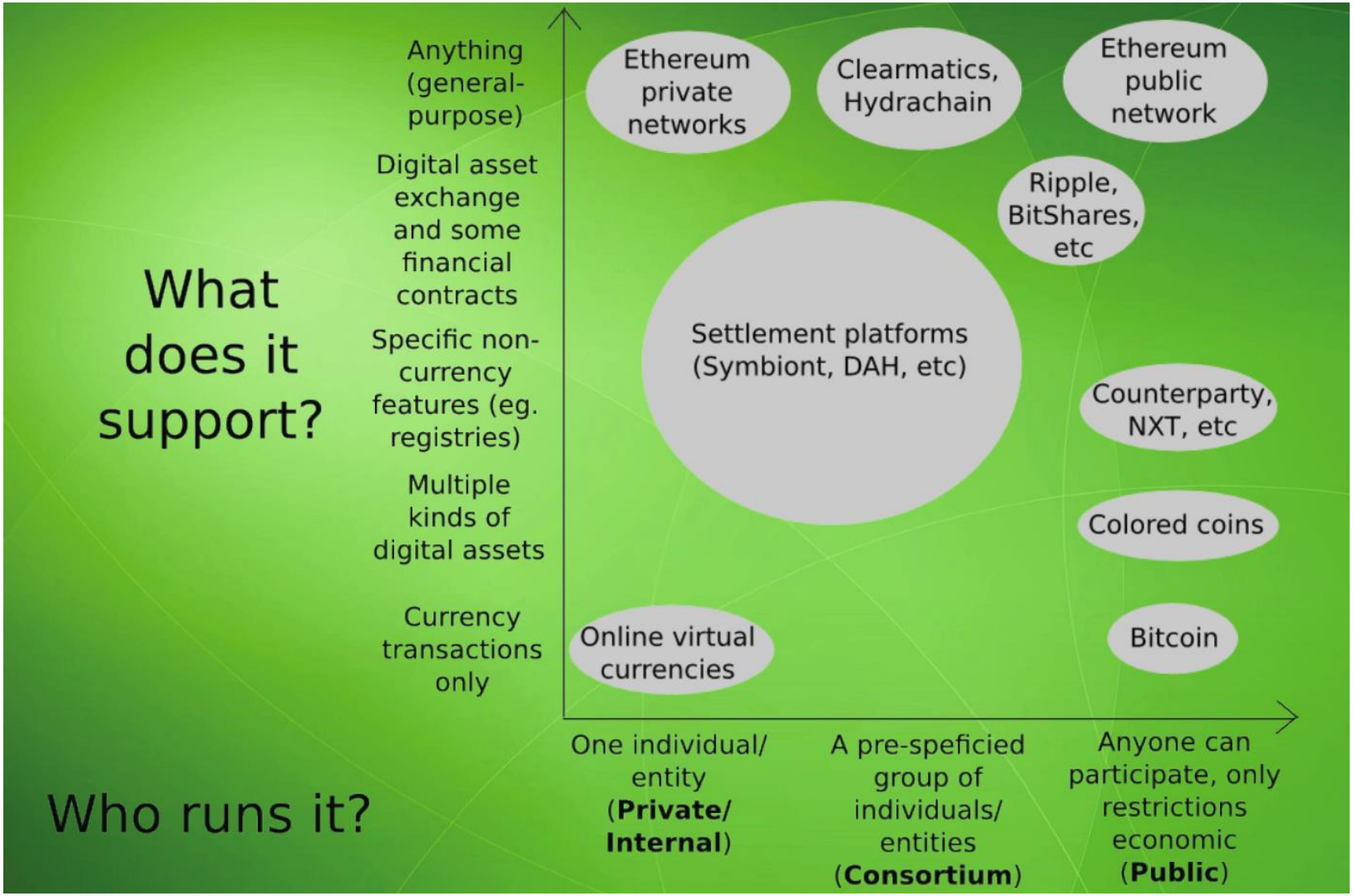
金融科技發展策略白皮書　p.94

區塊鏈分類

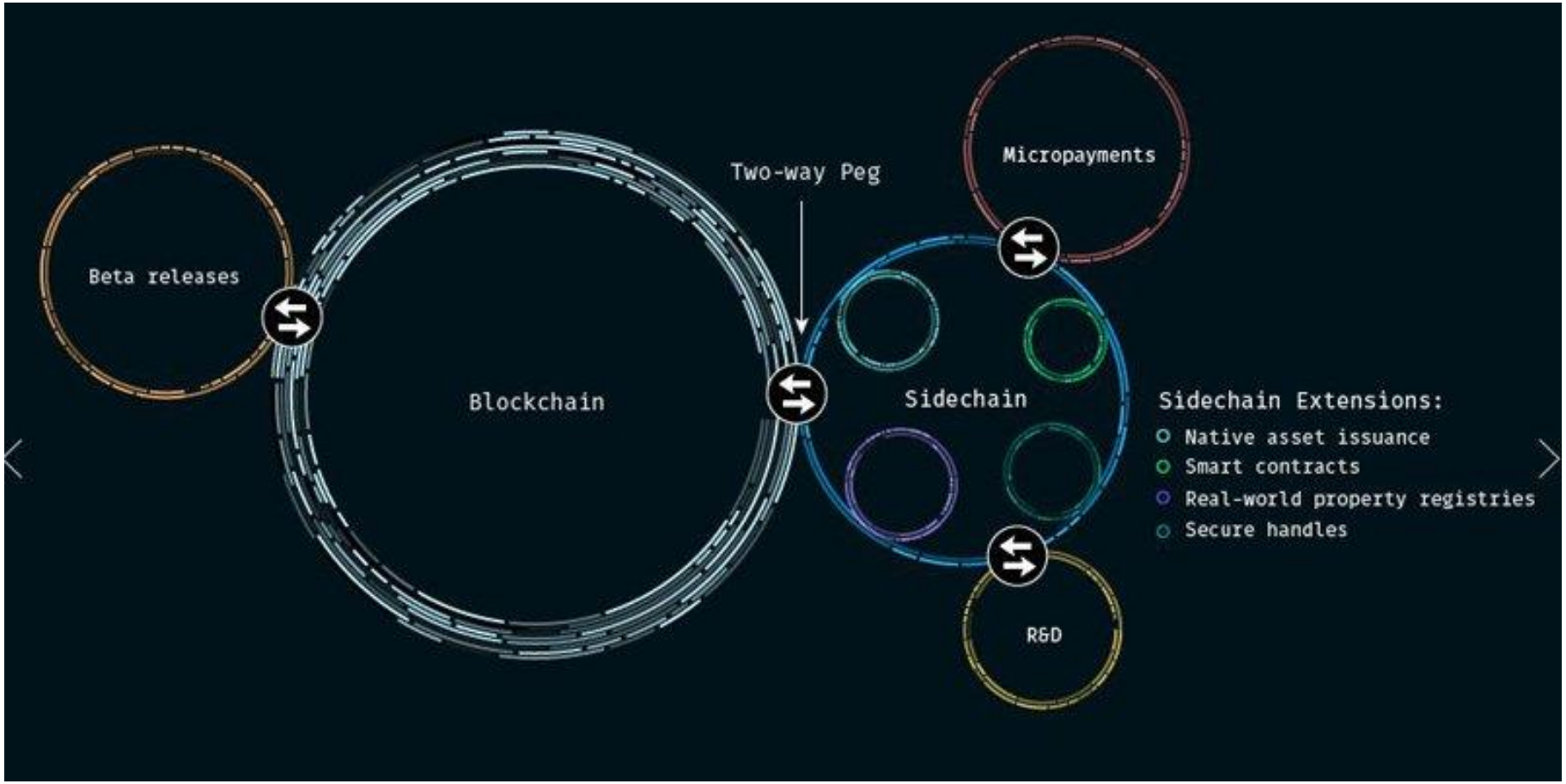


金融科技發展策略白皮書　p.94

區塊鏈分類


What does it support?
Anything (general-purpose)
Digital asset exchange and some financial contracts
Specific non-currency features (eg. registries)
Multiple kinds of digital assets
Currency transactions only
Ethereum private networks
Clearmatics, Hydrachain
Ethereum public network
Ripple, BitShares, etc
Settlement platforms (Symbiont, DAH, etc)
Counterparty, NXT, etc
Colored coins
Online virtual currencies
Bitcoin
Who runs it?
One individual/ entity (Private/ Internal)
A pre-speficied group of individuals/ entities (Consortium)
Anyone can participate, only restrictions economic (Public)

Sidechain 側鏈



Two-way Peg: 雙向錨定

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

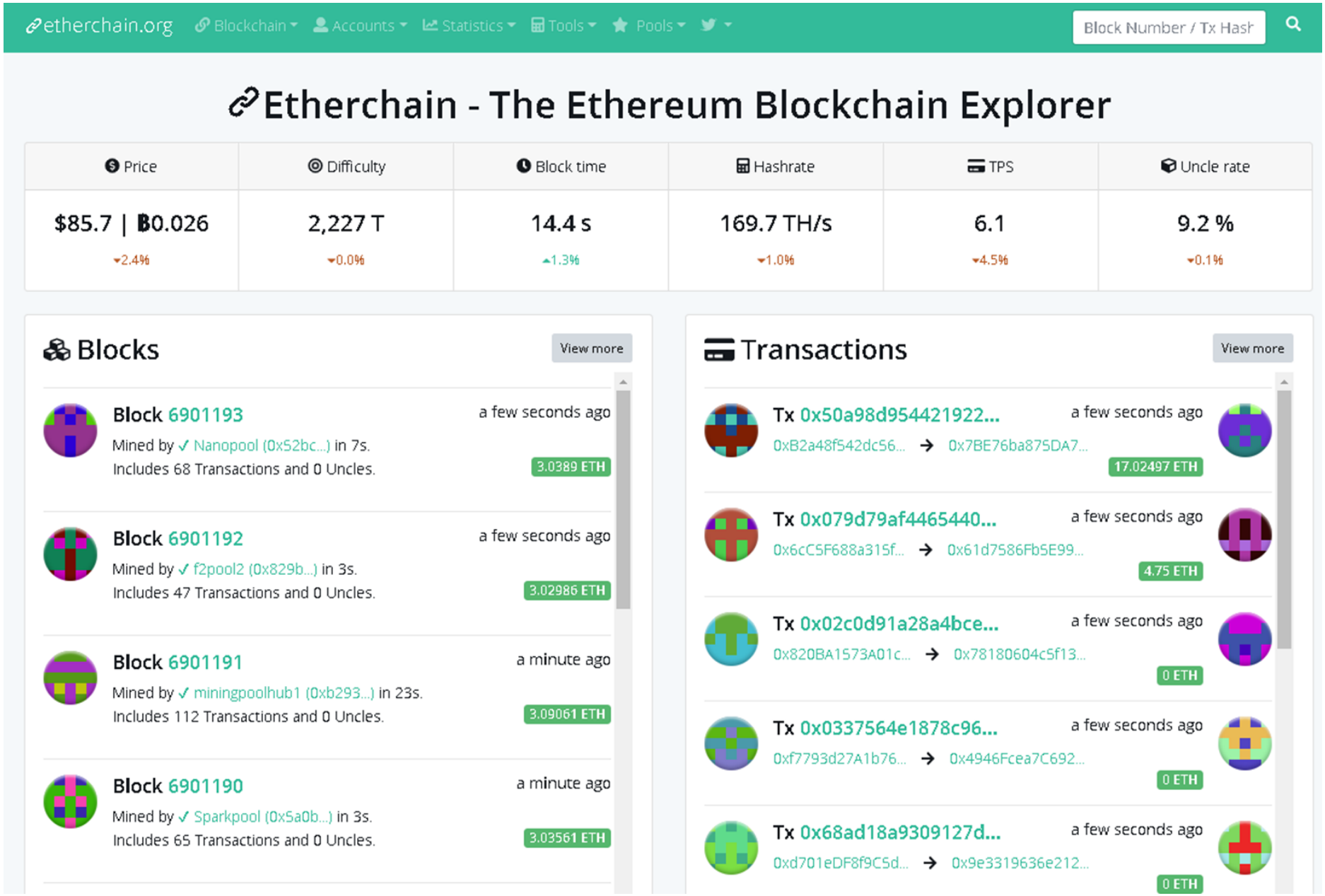
- Ethereum was initially proposed by Vitalik Buterin in late 2013, and the genesis block, marking the live release of the Ethereum project, occurred on 30 July 2015

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://www.etherchain.org

Proof of Stake

Proof of Work (PoW)

- A **Proof-of-Work** (**PoW**) system (or protocol) is a consensus mechanism, which deters denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer
- A key feature of these schemes is their asymmetry: the work must be moderately hard (yet feasible) on the requester side but easy to check for the service provider
- The concept was invented by Cynthia Dwork and Moni Naor as presented in a 1993 journal article, and the term "Proof of Work" or PoW was first coined and formalized in a 1999 paper by Markus Jakobsson and Ari Juels

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

Proof of Stake (PoS)

- The proof of stake model requires a user to lock his Ethers (for the case of Ethereum) into smart contracts in order to be eligible for validating blocks
- The equivalency of having a large hashrate in PoW is staking more money in the case of PoS
- A person with a higher hashrate had more probability of validating a block in PoW, similarly, a person who staked more has the same powers here

https://blockpublisher.com/pos-will-bring-more-security-to-ethereum-than-pow-vitalik-buterin/

Proof of Stake (PoS)

- For a hacker to add blocks in the blockchain, he would have to stake a lot of money
- Even after the adding of blocks, there would be a time for a challenger to check and see whether there is a sign of suspicious activity or wrong validations on the blockchain in which case he would challenge the validation and the hacker would lose all of his staked money

https://blockpublisher.com/pos-will-bring-more-security-to-ethereum-than-pow-vitalik-buterin/

課後閱讀

- 「評論：JPMCoin與Schneier教授的“區塊鏈無用論”」，孟岩
- 「揭秘中共大推區塊鏈的目的和前景」，大紀元時報
  - https://hk.epochtimes.com/news/2019-11-08/6222804
- 「坐困愁城的 Libra」，天遠律師事務所
  - 細看 Libra，千瘡百孔
    - https://www.inside.com.tw/amparticle/17020-facebook-Libra-has-a-lot-of-problems
  - 傳統金融體系需要當頭棒喝，但這根棒子是 Libra 嗎?
    - https://www.inside.com.tw/article/17033-Can-Libra-solve-the-problems-of-traditional-finance
  - Libra：困死台灣八陣圖內
    - https://www.inside.com.tw/amparticle/17051-Libra-will-have-a-lot-of-difficulties-in-Taiwan