

程式人

十分鐘系列

本文衍生自維基百科



區塊鏈

（比特幣背後的關鍵技術）

陳鍾誠

2020 年 10 月 1 日

這幾年

- 程式領域最熱門的技術
- 應該是這兩項：
 - 深度學習
 - 區塊鏈

昨天

- 我們已經談過深度學習背後的《梯度下降法》



A screenshot of a Facebook post by 陳鍾誠 (Chen Zhongcheng), posted 15 hours ago. The post text says: "很久沒寫十分鐘系列了，這次的主題是《梯度下降法》。這是所有《深度學習技術背後共同演算法》，不考慮執行速度的話，可以用短短的 20 行程式實作完成！(不依賴深度學習套件)" (I haven't written the 10-minute series for a long time, this time the topic is 'Gradient Descent'. This is the common algorithm behind all deep learning technologies, if we don't consider execution speed, it can be implemented with just 20 lines of code! (No deep learning libraries required)). The post includes a video player showing a presentation slide titled "梯度下降法" (Gradient Descent) with the subtitle "(隱藏在深度學習背後的演算法)" (Algorithm hidden behind deep learning). The slide also credits 陳鍾誠 and the date 2020 年 9 月 30 日. Below the video, the text "SLIDESHARE.NET" is visible, followed by the title "梯度下降法 (隱藏在深度學習背後的演算法) -- 十分鐘系列" and a reference link "參考程式 -- https://github.com/ccckmit/ai/blob/master/python/...". At the bottom, it shows engagement metrics: "Fred Chien、Bridan Wang和其他174人" (Fred Chien, Bridan Wang, and 174 others) and "3則留言 54次分享" (3 comments, 54 shares).

陳鍾誠
15 小時 · 🌐

很久沒寫十分鐘系列了，這次的主題是《梯度下降法》
這是所有《深度學習技術背後共同演算法》，不考慮執行速度的話，
可以用短短的 20 行程式實作完成！(不依賴深度學習套件)

十分鐘系列

梯度下降法
(隱藏在深度學習背後的演算法)
陳鍾誠
2020 年 9 月 30 日

SLIDESHARE.NET

梯度下降法 (隱藏在深度學習背後的演算法) -- 十分鐘系列
參考程式 -- <https://github.com/ccckmit/ai/blob/master/python/...>

Fred Chien、Bridan Wang和其他174人 3則留言 54次分享

今天

- 就讓我們來研究一下區塊鏈

傳統上

- 當你想學一門技術

你可能會去找書

於是你找到區塊鏈的書

search.books.com.tw/search/query/key/區塊鏈/cat/all

博客來 售票網 企業採購 福利平台 海外專館

登入 加入會員 購物金 會員專區 電子書櫃 線上客服

百寶(11)
電子書(56)
看全館分類

縮小搜尋範圍

- ☐ 作者/演唱/譯/編/繪
- ☐ 出版社
- ☐ 現在可購買商品
- ☐ 可超商取貨
- ☐ 可港澳店取
- ☐ 可新加坡店取
- ☐ 可菲律賓店取
- ☐ 可海外宅配
- ☐ 一個月內上市新品
- ☐ 本週上市新品
- ☐ 名稱含此關鍵字
- ☐ 免費電子書
- ☐ 適合手機平板閱讀
- ☐ 適合平板閱讀

從 到 元

篩選

最近查詢的關鍵字

☐  **2030世界未來報告書：區塊鏈、AI、生技與新能源革命、產業重新洗牌，接下來10年的工作與商機在哪裡？**
中文書，傑羅姆·格倫 朴英淑 宋佩芬 高寶，出版日期：2020-04-15
優惠價 79 折 332 元
根據你的心情所挑選的音樂、影集放鬆，度過愉快的一天。以上情節都將在10年內發生，你準備好迎接未來世界了嗎？本書將發展趨勢分成了以下7大部分：1.區塊鏈：即將走進商業、醫療、不動產、文化等領域，各大產業將徹底轉變。2..... [more](#)

☐  **圖解區塊鏈2：通證經濟**
中文書，徐明星 李雲月 王沐凝 吳嘉慧 基峰，出版日期：2020-08-31
優惠價 9 折 405 元
區塊鏈快速發展之後所產生的全新經濟模式：通證經濟 區塊鏈的快速發展，與經濟學理論、密碼學相互激盪之後，產生了一種全新的經濟模式：通證經濟。「通證」是可流通的加密數位憑證，是區塊鏈網路的記帳方式，在網路上可自由流通且有密碼學加持..... [more](#)

☐  **區塊鏈技術與應用**
中文書，華為區塊鏈技術開發團隊，五南，出版日期：2020-07-25
優惠價 95 折 399 元
本書詳實地介紹了區塊鏈技術和應用，主要包括三大部分：由淺入深地介紹了區塊鏈技術緣起、演進過程、技術原理和發展趨勢；分享並解析實際應用案例，以華為雲端區塊鏈服務為例示範了區塊鏈應用實踐的過程；分析探究區塊鏈的價值、未來發展趨勢以及有關區塊鏈錄..... [more](#)

☐  **區塊鏈社會學**
中文書，高重建，天窗出版有限公司，出版日期：2020-08-20
優惠價 9 折 585 元
區塊鏈掀起「無大台、有共識」革命，即將徹底改變我們對生活、經濟、社會，以至家國的觀念！「區塊鏈只是以各種方式演繹世界，然而關鍵是，改變它。」今天認識區塊鏈，相當於九十年代了解互聯網。區塊鏈，一個無大台、不可篡改、流動民主的..... [more](#)

還真是不少

- 光博客來網站就有 617 筆

然後你看了幾本

- 會發現自己還是搞不懂
- 到底甚麼是區塊鏈！

有人說

- 免費的東西，其實是最貴的！

但我說

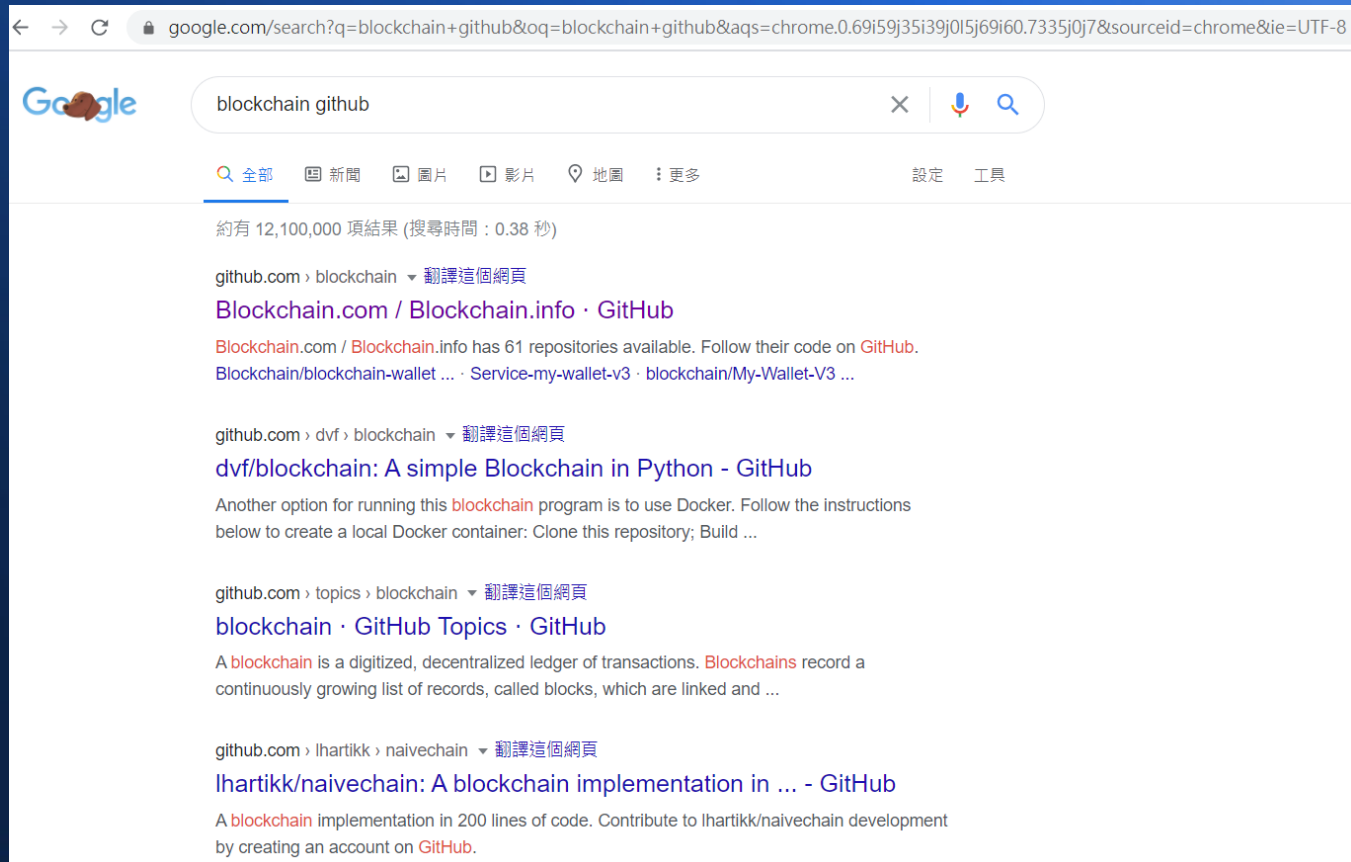
- 在程式的領域，最好的東西經常都是免費的！

只要懂得找 gi thub

- 又何必看那些，連程式碼都沒有的書呢？

在 github 上

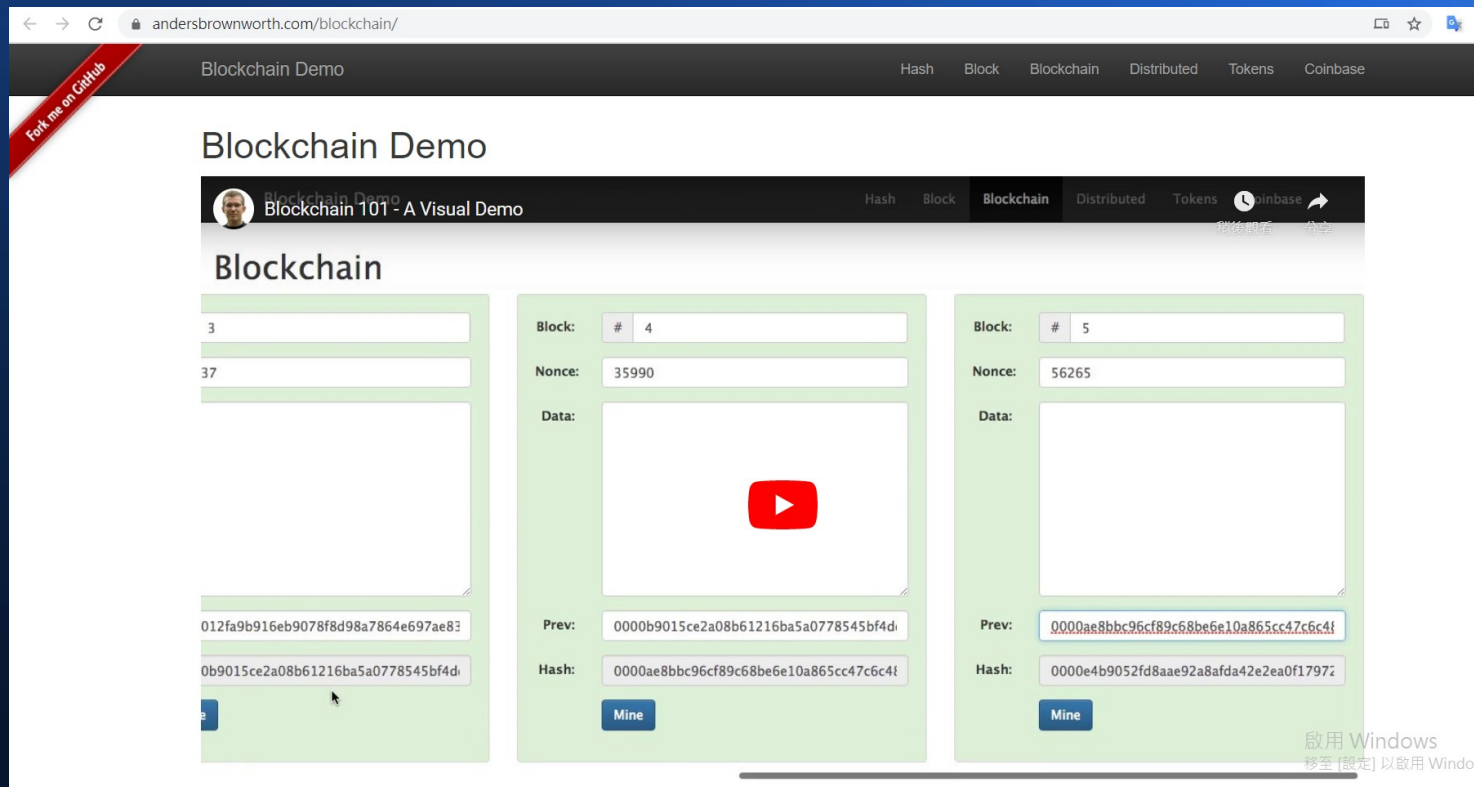
- 你可以找到各式各樣的區塊鏈實作
- 各種程式語言都有！



<https://www.google.com/search?q=blockchain+github>

其中這個專案

- 是我最喜歡的一個！



不只有程式碼

The screenshot shows the GitHub interface for the repository `anders94/blockchain-demo`. The page includes a navigation bar with links for Pull requests, Issues, Marketplace, and Explore. Below the repository name, there are tabs for Code, Issues, Pull requests (6), Actions, Projects, Wiki, Security, and Insights. The main content area displays a list of files and folders with their commit history and timestamps.

Repository: `anders94 / blockchain-demo` (217 Watchers)

Navigation: `<> Code` | `! Issues` | `🔗 Pull requests 6` | `🎬 Actions` | `📁 Projects` | `📖 Wiki` | `🛡 Security` | `📈 Insights`

Branches: `master` | `6 branches` | `0 tags` | `Go to file` | `Add file` | `Code`

Recent Activity: `anders94 Merge pull request #82 from anders94/dependabot/npm_and_yarn/lod... 3faf785 on 19 Jul 100 commits`

File/Folder	Commit Message	Time Ago
<code>bin</code>	initial import	4 years ago
<code>locales</code>	reverts	14 months ago
<code>public</code>	Update blockchain.js	3 years ago
<code>routes</code>	initial import	4 years ago
<code>views</code>	migrate from jade to pug so we get continued security updates. jad...	14 months ago
<code>.dockerignore</code>	add a Docker setup for blockchain-demo	4 years ago
<code>.gitignore</code>	add a Docker setup for blockchain-demo	4 years ago

<https://github.com/anders94/blockchain-demo/>

只要你有基本的程式觀念

- 看完這兩段影片
- 勝過看完博客來的那 617 本書！

現在

- 就讓我們跟著影片
- 來學學區塊鏈吧！

比特幣的區塊鏈運作

- 是依靠一種稱為 SHA256 的雜湊函數

SHA256 Hash

Data:

anders

Hash:

19ea4ac2e1a53b1267fe5a61a3b6b81f760ce4223a25b495a5e2b6183da68717

不同的輸入會有不同的雜湊值

SHA256 Hash

Data:

anders|

Hash:

19ea4ac2e1a53b1267fe5a61a3b6b81f760ce4223a25b495a5e2b6183da68717

SHA256 Hash

Data:

oihs
sdc
|

Hash:

d29f3cc6be8f759034e0fb9f242d4e9fd8aa31cf5c1d2cf4d70c1019c9b43f2f

一個區塊

- 是一筆包含雜湊值的紀錄

Block

Block:

1

Nonce:

10

Data:

hi

Hash:

8c28724f6e93be2b70e6dffd2cdefc081f6b96cca1e60f94de9fa4bf3639f6c1

Mine

而挖礦的過程

- 就是要找出紀錄上填入甚麼 nonce 值，才會讓 hash 有指定位數的前導零（例如下圖中 hash 為 0000d742....，那就是有 4 個字的前導零）

Block

Block:

1

Nonce:

59396

Data:

hi

Hash:

0000d742711b9c79c3464eaacdfa0153206221aeed749612b48f22475a96f912

Mine

比特幣的挖礦

- 是根據前十分鐘的挖礦難易度
決定下次的前導零數量

像是這個區塊就有 18 個前導零

Blockchain.com

Wallet

Exchange

Explorer

Block 606566

Hash	000000000000000001152e2388e54eed7a19dfd29b2c5f18c02bf088dbcf14b
Confirmations	44,181
Timestamp	2019-12-04 13:10
Height	606566
Miner	Poolin
Number of Transactions	1,270
Difficulty	12,973,235,968,799.78
Merkle root	acc7b594f74a35b75d56b5f25ea324e18765446dc4f87df991d6d99b6ad1d091
Version	0x20000000
Bits	387,297,854
Weight	1,433,767 WU

<https://www.blockchain.com/btc/block/000000000000000001152e2388e54eed7a19dfd29b2c5f18c02bf088dbcf14b>

將 16 進位換成 2 進位

- 一個 16 進位對應 4 個 bits
- 所以 18 個前導零相當於 $18 \times 4 = 72$ 個 bit 的零
- 要找到這樣的 nonce，機會只有 $1/2^{72}$
- 這也是為何挖礦要很多算力的原因！
- 因為你的程式平均要嘗試 2^{72} 次才能找到一個符合的 nonce 填上。

所以

- 比特幣的挖礦，基本上就是個猜 nonce 的遊戲！

和猜謎不同的是

- 電腦可以用全速去猜，速度愈快的電腦，可以猜愈多次，猜中的機會也就愈大！

然後

- 我們就可以講解《區塊鏈》
的觀念了！

在區塊鏈上

- 後面的區塊必須記錄前面的 hash 值
而且填入的 nonce 還要讓自己區塊有足夠的前導零

Blockchain

Block: # 1	Block: # 2	Block: # 3
Nonce: 11316	Nonce: 35230	Nonce: 12937
Data:	Data:	Data:
Prev: 00000000000000000000000000000000	Prev: 000015783b764259d382017d91a36d206d0f	Prev: 000012fa9b916eb9078f8d9
Hash: 000015783b764259d382017d91a36d206d0f	Hash: 000012fa9b916eb9078f8d98a7864e697ae83	Hash: 0000b9015ce2a08b61216b
Mine	Mine	Mine

於是

- 區塊一個串一個，每個都要滿足前導零的要求
- 任何一個不滿足，都很容易被快速檢查出來
- 這就是區塊鏈的《易檢查、難填充》特性！

如果你想竄改區塊中的任何一個字

- 會造成雜湊值不正確

Blockchain

783b764259d382017d91a36d206d0i

fa9b916eb9078f8d98a7864e697ae83

Block: # 3

Nonce: 12937

Data: hi

Prev: 000012fa9b916eb9078f8d98a7864e697ae83

Hash: 9d1c04689c2d59a121a136282616445aa1f8c

Mine

Block: # 4

Nonce: 35990

Data:

Prev: 9d1c04689c2d59a121a136282616445aa1f8c

Hash: 663a1eb093aeb59dd9f4b1161e10dd5038ffa

Mine

唯一的解決方法

- 就是把竄改紀錄後的那些區塊，全部重新挖一遍！

Blockchain

783b764259d382017d91a36d206d0i

fa9b916eb9078f8d98a7864e697ae83

Block: # 3

Nonce: 12937

Data: hi

Prev: 000012fa9b916eb9078f8d98a7864e697ae83

Hash: 9d1c04689c2d59a121a136282616445aa1f8c

Mine

Block: # 4

Nonce: 35990

Data:

Prev: 9d1c04689c2d59a121a136282616445aa1f8c

Hash: 663a1eb093aeb59dd9f4b1161e10dd5038ffa

Mine

但是當你竄改了

- 其他人所記錄的區塊鏈並沒有改
- 根據多數決法則，你很容易就被發現是竄改的！

於是

- 區塊鏈的不可竄改性就得到了確保！

這就是

- 比特幣為何在沒有中央控管的狀況下
- 卻可以達到分散式認證的原因了！

而以太坊

- 則是在區塊鏈上又加入了智能合約
- 導致以太坊有可能成為分散式金融

DeFi (Decentralize Finance) 的主要技術！

比特幣的紀錄

- 其實還記載了交易資訊

Tokens

Peer A

Block: # 1

Nonce: 26486

Tx:	\$	25.00	From:	Darcy	->	Bingle
	\$	4.27	From:	Elizat	->	Jane
	\$	19.22	From:	Wickl	->	Lydia
	\$	106.4	From:	Lady	->	Collin
	\$	6.42	From:	Charl	->	Elizat

Prev: 00000000000000000000000000000000

Hash: 000049015089c7b64125575f5cf78fa3d2bba

Mine

更多影片

Block: # 2

Nonce: 82590

Tx:	\$	97.67	From:	Ripley	->	Lamb
	\$	48.61	From:	Kane	->	Ash
	\$	6.15	From:	Parke	->	Dallas
	\$	10.44	From:	Hicks	->	Newt
	\$	88.32	From:	Bisho	->	Burke
	\$	45.00	From:	Huds	->	Gorm
	\$	92.00	From:	Vasqi	->	Aponi

Prev: 000049015089c7b64125575f5cf78fa3d2bba

Hash: 0000f843c73a7b3f5f3af6b7a4f5690a377326

Mine

Block: # 3

Nonce: 40596

Tx:	\$	3.14	From:	Sylve
	\$	2.12	From:	Twee
	\$	1.99	From:	Daffy

Prev: 0000f843c73a7b3f5f3af6b7a

Hash: 0000a9dd50de891b2de8601

Mine

於是你可以買賣比特幣

- 或者用比特幣消費！

但如果你

- 想用比特幣來買珍珠奶茶

那可能會大失所望！

因為每十分鐘

- 全世界只會產生一個大小約 4MB 的
比特幣區塊

如果用比特幣買珍奶

- 勢必得等到下一個區塊驗證好

於是你

- 得在奶茶店等十分鐘 ...
- 才知道交易是否成功
- 你的奶茶消費有沒有成功被排入下一個區塊 ...

所以

- 別總是想著用比特幣買珍奶

雖然

- 早期真的有人用比特幣買披薩
- 而且還真的成功了！
- 這個交易成了歷史上的傳奇

史稱《比特幣披薩日》



<https://www.blocktempo.com/bitcoin-pizza-day-event-may-twenty-second/>

最後要提醒大家

- 比特幣的交易紀錄，並不是像下圖中採用人名而是以《電子錢包》的《公開金鑰》紀載的，只是個代號，所以你並不會知道交易者的姓名！

Peer A

Block: # 1

Nonce: 26486

Tx:

\$ 25.00	From: Darcy	->	Bingle
\$ 4.27	From: Elizab	->	Jane
\$ 19.22	From: Wickl	->	Lydia
\$ 106.4	From: Lady	->	Collin
\$ 6.42	From: Charl	->	Elizab

Prev: 00000000000000000000000000000000

Hash: 000049015089c7b64125575f5cf78fa3d2bba

Mine

Block: # 2

Nonce: 82590

Tx:

\$ 97.67	From: Ripley	->	Lamb
\$ 48.61	From: Kane	->	Ash
\$ 6.15	From: Parke	->	Dallas
\$ 10.44	From: Hicks	->	Newt
\$ 88.32	From: Bisho	->	Burke
\$ 45.00	From: Huds	->	Gorm
\$ 92.00	From: Vasq	->	Apon

Prev: 000049015089c7b64125575f5cf78fa3d2bba

Hash: 0000f843c73a7b3f5f3af6b7a4f5690a377326

Mine

Block: # 3

Nonce: 40596

Tx:

\$ 3.14	From: Sylve	->	
\$ 2.12	From: Twee	->	
\$ 1.99	From: Daffy	->	

Prev: 590a377326957b38666d53d

Hash: 0000a9dd50de891b2de8601

Mine

更多影片

14:29 / 17:49

YouTube

還有一個技術問題是

- 如果你的比特幣錢包沒有錢，卻又假裝有錢去和別人做交易，那會怎麼樣呢？

關於這點你不用擔心

- 由於比特幣是以 coinbase 的方式控管的，所以沒錢的不能假裝有錢去交易！

這類的驗證

- 就牽涉到比特幣背後的《公鑰 / 私鑰》機制
- 也就是密碼學中的非對稱式加解密的 RSA 算法和橢圓演算法所確保的。

進一步的內容

- 還是請大家直接看影片，會更生動活潑且清楚！

對了

- 如果你想寫個簡易的挖礦程式，可以參考這個 node.js 範例

```
const crypto = require('crypto');

let record = {
  nonce: 0,
  data: 'john => mary : $2.7; george => john : $1.3',
}

function hash (text) {
  return crypto.createHmac('sha256', '').update(text).digest('hex')
}

function mining(record) {
  for (var nonce=0; nonce<1000000000000; nonce++) {
    record.nonce = nonce
    let h = hash(JSON.stringify(record))
    if (h.startsWith('0000')) return { nonce: nonce, hash: h }
  }
}

console.log(mining(record))
```

程式非常簡單

就是一直調整 nonce
後算雜湊值，看看 hash
是否有夠多的前導零
有的話就是挖到了！

```
const crypto = require('crypto');

let record = {
  nonce: 0,
  data: 'john => mary : $2.7; george => john : $1.3',
}

function hash (text) {
  return crypto.createHmac('sha256', '').update(text).digest('hex')
}

function mining(record) {
  for (var nonce=0; nonce<1000000000000; nonce++) {
    record.nonce = nonce
    let h = hash(JSON.stringify(record))
    if (h.startsWith('00000')) return { nonce: nonce, hash: h }
  }
}

console.log(mining(record))
```

當然也可以用亂數挖

- 這樣就算別人程式比你快，你還是會有點機會挖到的！

```
1  const crypto = require('crypto');
2
3  let record = {
4    nonce: 0,
5    data: 'john => mary : $2.7; george => john : $1.3',
6  }
7
8  function hash (text) {
9    return crypto.createHmac('sha256', '').update(text).digest('hex')
10 }
11
12 function mining(record) {
13   // for (var nonce=0; nonce<1000000000000; nonce++) {
14   while (true) {
15     let nonce = Math.floor(Math.random()*100000000)
16     record.nonce = nonce
17     let h = hash(JSON.stringify(record))
18     if (h.startsWith('00000')) return { nonce: nonce, hash: h }
19   }
20 }
21
22 console.log(mining(record))
```

這就是

- 比特幣中區塊鏈技術的原理

希望您會喜歡

我們今天的

- 十分鐘系列！

我們下次見

Bye bye !