

# 貨幣和比特幣

## CURRENCY AND BITCOIN

Sam Wong  
2017-05-26

## 說明

呢個Deck有小量動畫同大量嘅文字筆記做補充

如果睇唔到，可以喺呢度下載其他格式

<https://github.com/sam0737/brownbag>

我嘅Bitcoin銀包: 1J9MKzB2KNoPofgACqXwtNb48DMyeDCAoT

本Deck以CC-SA 3.0發佈

圖片使用嘅版權喺筆記中詳細說明

▪ 放棄金本位 CC-SA 3.0: Will O'Neil



錢到底係乜嘢？

CC0: <http://maxpixel.freegreatpicture.com/Cash-Exchange-Financial-Currency-Banknote-Money-1309887>



銀紙可以食㗎咩？古代用糧食做貨幣最實際。  
為五斗米而折腰有無聽過？

Public Domain:

[https://commons.wikimedia.org/wiki/File:%E0%B4%AC%E0%B4%B8%E0%B5%81%E0%B4%AE%E0%B4%A4%E0%B4%BF\\_%E0%B4%85%E0%B4%B0%E0%B4%BF.JPG](https://commons.wikimedia.org/wiki/File:%E0%B4%AC%E0%B4%B8%E0%B5%81%E0%B4%AE%E0%B4%A4%E0%B4%BF_%E0%B4%85%E0%B4%B0%E0%B4%BF.JPG)



問題:

一般商品都易爛 (而鹽曾幾何時都試過係貨幣一種，政府規定唔可以私自提煉竟然有發生過，哈哈)

量多 – 唔方便拎。周街拎住幾斤米咩。

難以標準化

加上國際貿易興起和需求 (用米嘅話運到過去都爛晒啦，何況鬼老都唔食米)

所以興起以貴金屬作為貨幣。

Public Domain: <https://commons.wikimedia.org/wiki/File:China-1Yuan-1914.jpg>

## 金/銀本位貨幣有乜問題先？

礦產地分佈唔平均

挖礦速度、生產力變化/需求唔協調，亦唔係話變就變

- 發現新金礦對金融系統帶來衝擊
- 20世紀生產力爆發
- 打仗

三藩市又叫舊金山，因為在**1848**年發現金礦

如果挖礦仲慢過生產力嘅增幅，即係收埋收埋啲金銀等到未來購買力會更大嘅話，就即係通縮。

最後大家就收埋啲錢唔會使，經濟循環崩潰。

針對實物貨幣呢個問題，有兩招: 部份準備金制度、紙幣

## 部份準備金制度 FRACTIONAL-RESERVE BANKING

1. 存100蚊入銀行
2. 銀行按法例只需要保留10% (x%)
3. 90蚊可以借出去
4. 借出去嘅90蚊最後都係入銀行㗎啦  
又可以借81蚊出去
5. 最終100蚊就變咗做 $100/x\%$ ，即係有1000蚊喺街 (M2貨幣)

### 2016年中國存款準備金規定

- 大型金融機構: 16.50%
- 中小金融機構: 13.00%

原本100蚊嘅金銀，銀行玩兩玩就變成1000蚊



## 紙幣

20世紀初戰事頻繁，要真金白銀畀軍餉。有國共內戰、美國南北內戰、第一次世界大戰等等...

紙幣最初發行嘅時候，通常政府都承諾可以隨時兌換返做真金白銀 (即係「憑票即付」)

強勢嘅政權可能會強迫人民上繳金銀，私藏即屬違法。

無論點都好，一般政府自己都會認自己發嘅紙幣 – 例如可以用來交稅。

但打仗始終要好多錢，亦會損耗自己一國嘅生產力(GDP)，最後都會被擠提或通貨過份膨脹，因為根本無足夠嘅生產力去支持濫發嘅貨幣，大家開始失去信心，然後大幅偏值。

國民政府都有發過「法幣」取代銀圓，1948・49年仲強迫上繳金銀去換所謂嘅金圓券、銀圓券，唔使一年就變晒廢紙。

[https://zh.wikipedia.org/wiki/File:ROC\\_Fabi.jpg](https://zh.wikipedia.org/wiki/File:ROC_Fabi.jpg)

Believed to be in Fair Use





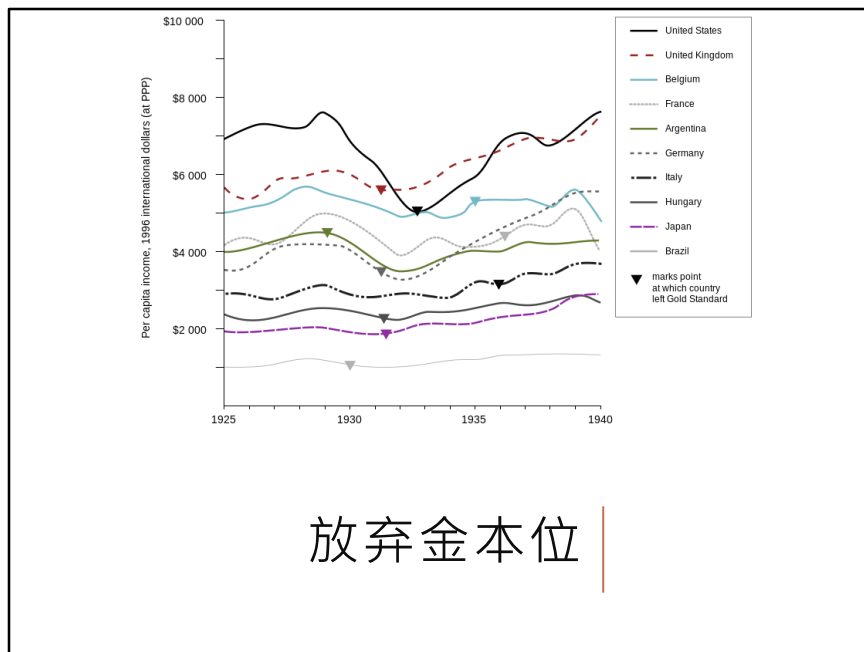
睇返世界其他地方，一打仗就要大幅偏值、通脹，去支付軍餉  
打輸嘅德國就慘豬豬咯...馬克銀紙拎來當牆紙貼，燒咗佢暖下個身仲平過買柴來  
燒。



轉眼打完仗，之後舞照跑馬照跳，大家返去做嘢嘅做嘢，食飯嘅食飯。經濟有所改善，但突然整個經濟大蕭條。

原因有兩大講法：

1. 紐約股災，然後出現信心危機，之後銀行被擠提倒閉，一發不可收拾
  2. 一戰之後大家收緊銀根 (因為之前通脹、太多“熱錢”)，回復到戰前承諾嘅兌換率。一個唔覺意收得太緊，搞到有流動性問題，然後通縮。
- 個雪球一碌就碌咗十幾年。



## 放棄金本位

有啲國家就放棄金本位，即係相等宜家嘅QE、匯率自由浮動、開印鈔機。希望整返多啲「錢」，做咗通脹。

睇一睇個圖，美國放棄金本位嗰下之後人均收入就升返。早知就早啲放棄啦？

CC-SA 3.0: Will O'Neil

[https://commons.wikimedia.org/wiki/File:Graph\\_charting\\_income\\_per\\_capita\\_througout\\_the\\_Great\\_Depression.svg](https://commons.wikimedia.org/wiki/File:Graph_charting_income_per_capita_througout_the_Great_Depression.svg)



又過咗陣 - 又打仗喇！例牌又通脹。

## BRETTON WOODS 布雷頓森林體系

1944年7月在布雷頓森林公園所定嘅協議

以美元為儲備貨幣

- 美國聯儲局保證隨時可以按官價將美元兌成黃金
- 提供足夠嘅美元作為國際清償手段  
噉就避免咗挖礦速度跟不上生產力嘅問題

轉下眼又打完仗。

今次大家就唔想返去金本位喇 (見過鬼仲唔怕黑?)

但二戰嘅時候自由浮動亦太得人驚。

而呢一刻，美國就係最強，成個戰事差唔多就係求其掙咗兩粒原子彈。其他曾如德、英、法、中、日有參戰嘅就元氣大傷。

所以啲盟國去美國Bretton Woods開個會傾個方案。

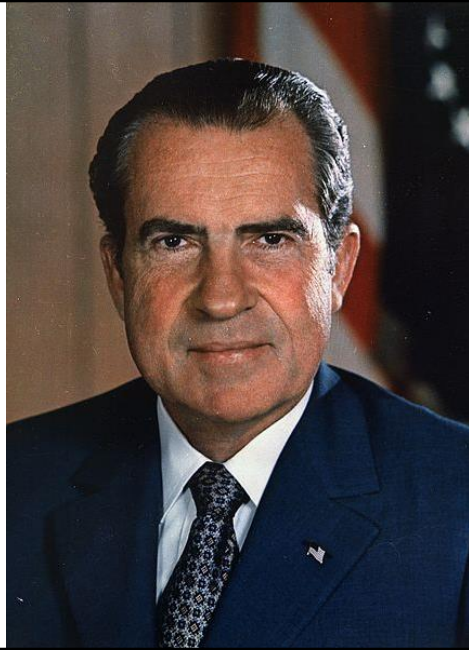
結論就係大家都信美金，尤如信黃金一樣。



今次到美國打仗。一打廿年，國力幾強都有佢嘅限度。  
外國信心不足，開始向美國兌黃金。

## 尼克遜衝擊 NIXON SHOCK

1971



時任美國總統尼克遜 – 就喺1971某日突然就話唔再兌黃金，而且加進口稅，希望國民內部消費。

本來講係90日嘅臨時政策，但係根本返唔到轉頭。

風水佬呢你十年八年...美國都叫捱義氣頂咗27年。(咁又唔係話Bretton Woods無佢著數)

全世界嘅貨幣就由呢一日起變成自由浮動，同金、銀都無晒關係。

Public Domain:

[https://commons.wikimedia.org/wiki/File:Richard\\_M.\\_Nixon,\\_ca.\\_1935\\_-\\_1982\\_-\\_NARA\\_-\\_530679.jpg](https://commons.wikimedia.org/wiki/File:Richard_M._Nixon,_ca._1935_-_1982_-_NARA_-_530679.jpg)

## 法定貨幣 FIAT CURRENCY

唔食得，講穿咗其實乜都唔係  
但至少可以用來交稅

到咗法幣時代，一個幣到底有咩意義就只係法律裏面寫住㗎咋。(啱晒法治社會)

之後**1987**年某日香港發生股災，單日插水跌幅拍得住經濟大蕭條個鑊。  
但係今鋪就醒喇，因為都係大家法幣，所以可以通過貨幣政策做啲嘢，對民生嘅影響無咁大，  
甚至日本之後仲光輝咗好幾年 (然後因為印太多錢爆煲搞到「失去的十年」)，  
不過都無經濟大蕭條個期咁大鑊。

後面**2000**年金融風暴、**2008**年次按危機、QE量化寬鬆、美國開印鈔機、中國央行調整存款準備金等，大家都比較熟啦。



## 貨幣總結

一句到尾，錢值幾多只係信心，由一國嘅GDP頂住。  
現代主流經濟學認為，維持2%左右低通脹係啱啱好。

比特幣 |

# 比特幣 BITCOIN/BTC

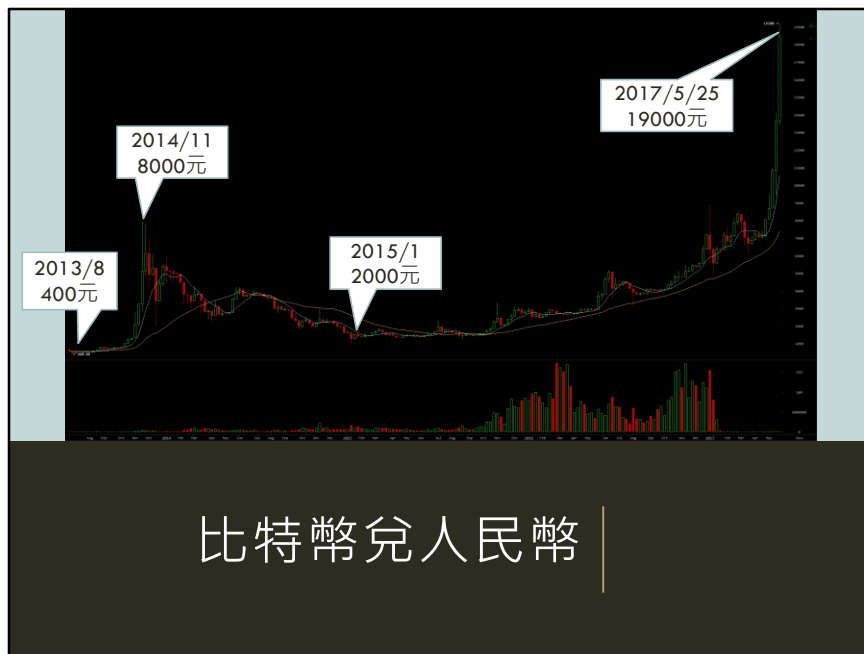
世界第一隻Cryptocurrency (加密貨幣)

2009-01-03開始

由一個叫中本聰 (Nakamoto Shatoshi)嘅仁兄發明

目前用過最細嘅交易單位係百万份之一個BTC，亦叫做Shatoshi  
• 但技術上可以去到更加細，總之唔一定要一個一個BTC交易

中本聰只係個網名，真人係乜水無人知。



Bitcoin在Okcoin.cn上的价格

2013年8月 – 400

2014年11月 – 8000

2017年5月25日 – 19000

2017年5月26日 – 16000 (單日就跌咗15%)

(截自bitcoinwisdom.com)

## 比特幣價值

信則有、不信則無

有好多交易所提供與法幣兌換服務

因中國政府管制，2017年2月起中國國內嘅交易所並唔可以提幣出去

BTC嘅定價，同外匯、股票、甚至黃金都差唔多。邊個願意用呢個價買、邊個願意賣，就係咁。

雖然唔可以用來交稅，但據講都有上十萬個商號收比特幣。最少仲可以用來交WannaCry嘅贖金？(註：一款Ransomware)

一句到尾，信就有，唔信就無。

交易所並無漲停板、跌停板嘅機制。

同現時紙黃金(ETF)有啲唔同，紙黃金一定係部份準備金制，買一兩並唔代表佢背後真係有一兩金專屬畀你。

但目前嘅BTC交易所都聲稱係完全準備金制，某啲交易所仲用過特定算法公開Audit過，當然你睇唔睇得明、信唔信得過就自己諗下先。

史上亦有發生過mt.gox事件 – 一間當時最大嘅交易所因為據稱被黑，畀人偷晒啲coins而執笠。

又或者可以參考1637年荷蘭鬱金香狂熱嘅歷史。

## 比特幣特性

無人監管、亦無單人可以隻手干預  
發行量固定而且可預知，唔會有QE  
賬目公開  
錢包匿名

後面講點解，聽住先。

QE即量化寬鬆 (Quantitative easing)

# 比特幣規則

## 產生

- 平均每10分鐘就會有新嘅區塊(Block)被挖出
- 挖到嗰個人可以得到獎金。呢個途徑係唯一比特幣嘅產生辦法。
- 獎金一開始係定做50BTC，隨後每挖出210000個區塊(約4年)就減半
  - 宜家係12.5BTC一個區塊，已挖出約80%嘅總量
- 每挖2016個區塊(約2星期)會調整挖礦計算難度
  - 無論有幾多部電腦一齊挖，都會維持約10分鐘挖出一個

## 消費限制

- 一蚊唔可以使兩次 (Double Spending)  
廢話...可以使兩次嘅叫乜做貨幣？

先唔好問點解。例如點解係每10分鐘，點解係每四年減半...  
一開始中本聰定咗係噉就係噉。

就好似一齊玩包剪揼，點解剪係贏到包？一齊玩就要跟呢個規矩。

後面會解釋點解大家都跟呢套遊戲規則玩。

## PROOF OF WORK (POW)

$$x^2 - 15x + 54 = 0$$

$$x = 6 \text{ or } x = 9$$

咁乜嘢係區塊，乜嘢係挖礦？  
先要講講Proof of Work

呢個二次元方程大家中學都有學過，一眼睇落去唔知道答案 – 計一計就知原來  
 $x=6$ 或 $x=9$

但講個答案出來，其他人要驗證係咪啱就好容易，一代入去就知。



## HASH 雜湊函數

```
sha256("UCO IS GOOD") =  
a603ecea9c7efa4f27f32d2ca3f6deb508a8d95c4ad562db3e66c44d061ced9f
```

```
sha256("UCO IS GOOD!") =  
d5aac8c5f0a407bc8fcd75cac423dbcd585133c80a11dfcfbfc42e7c13c72a41
```

```
sha256("UCO IS GOOD0") =  
6ee2f7f9b8904aa51339fafba4d8618b35f9dabaa06e0afb27b16266dc24b57c
```

```
sha256("UCO IS GOOD1") =  
9a659c5b991cae2a4e3012a4d7d63872d02ae94212de7e29b82177ec42fb3dd1
```

難題: "UCO IS GOOD"後跟個乜嘢數目字, sha256計出來先至係0開頭?

答案: 3

```
sha256("UCO IS GOOD3") =  
0c578d1440d99dc601730cfb2f0c9ebe36b63b0d04ec1d00d413b3b72dc5e25f
```

3就是呢一次嘅nonce

當然要電腦去解個二次元方程就太易啦, 喺bitcoin實際上係用雜湊函數, 其中呢一款sha256就係實際上用嘅POW算法。

所有雜湊函數都一樣, 只要放入去嘅原文改一改, 計出來嘅結果都會變到阿媽都唔認得。

而簡單來講, 係無可能從結果嗰串數字(雜湊值)去推敲返個原文。

註: a603...嗰串係16進制數字; 16進制係以0-9, 然後abcde分別代表11、12、13、14、15。

所以要搵nonce, 唯一辦法就係逐個撞。當然符合零開頭嘅答案唔只係3, 可能幾十、幾百、幾萬有好N個撞得出係0開頭嘅雜湊值。

但如果問題改一改做「請講出一個可以計到有5個0開頭嘅nonce」, 咁就要啲時間去撞喇。

## 區塊

最大1MB嘅文件

要雜湊嘅內容:

- N筆交易資料，包括獎金入賬呢一筆交易
- 上面呢堆資料會計出一個32 bytes嘅雜湊值 (亦即Merkle Tree嘅根節點)
- 上一個區塊嘅支針

噉挖礦即係乜？

- 搵一個nonce而sha256(區塊內容+nonce)係比難度值細
- 搵到之後就向其他電腦廣傳呢個區塊內容+nonce

Q: 如果我hack咗某部挖礦電腦，佢咁啱計出一個nonce，我就搶咗佢個nonce首先廣播出去，噉我會唔會搶埋佢份獎金？

A: 唔會。因為嗰個nonce只會係對應佢所編集嘅交易資料 – 當中包括嗰條「俾12.5BTC落我袋」呢一段 – 嘅雜湊值

如果你要將「落我袋」改成「落你袋」，所需要嘅nonce根本就唔一樣。

## 節點 NODE – 執行規則者

1. 收到之前講嘅挖礦結果
2. 驗證係咪符合規則
  1. 確保區塊信息正確、無爛data
  2. 檢驗nonce無計錯，而且計出來嘅sha256雜湊值符合當前難度要求
  3. 確保交易資料都係符合規則，包括獎金啱唔啱數，有無一蚊使兩次等等

驗證通過 → 就會加到區塊鏈上面(Blockchain)，同時廣播出去  
生得最高個區塊就係當前「公認」嘅Bitcoin系統狀態

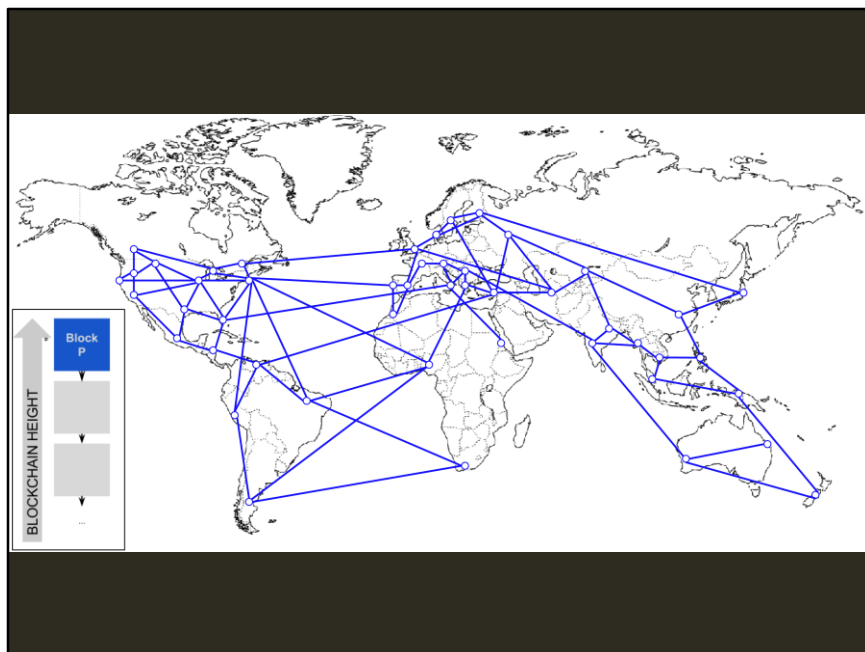
挖礦電腦喺收到新嘅區塊消息嘅時候，就會放棄手上挖緊個一塊。否則挖完都係得個吉，其他節點根本就唔會再理。

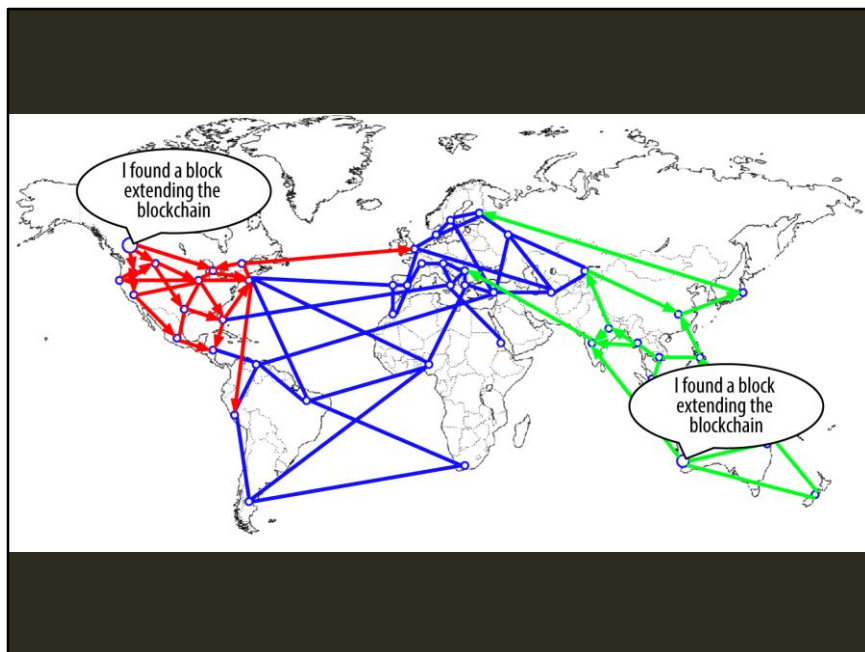
難度值 – 就係前幾版話每兩星期/2016個區塊調整一次，將難度控制喺平均十分鐘挖出一次。

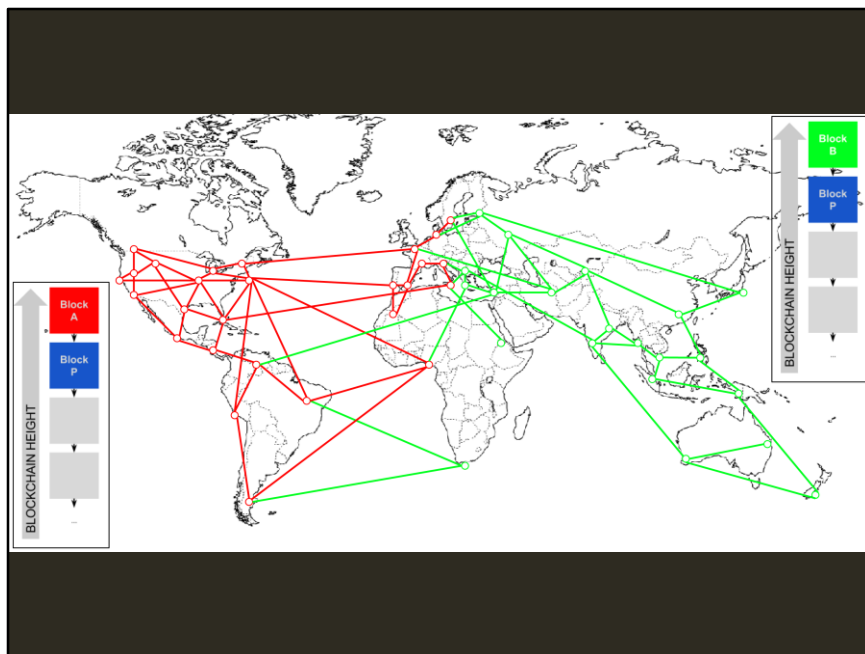


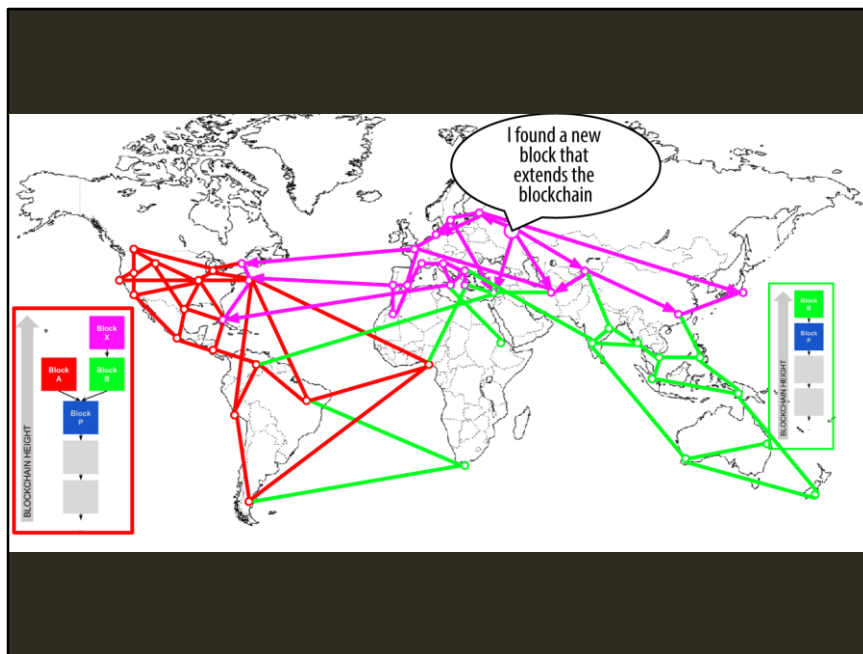
## BLOCKCHAIN分岐 |

如果全世界有兩個地方同時挖到新區塊會點？同步都要時間嘛

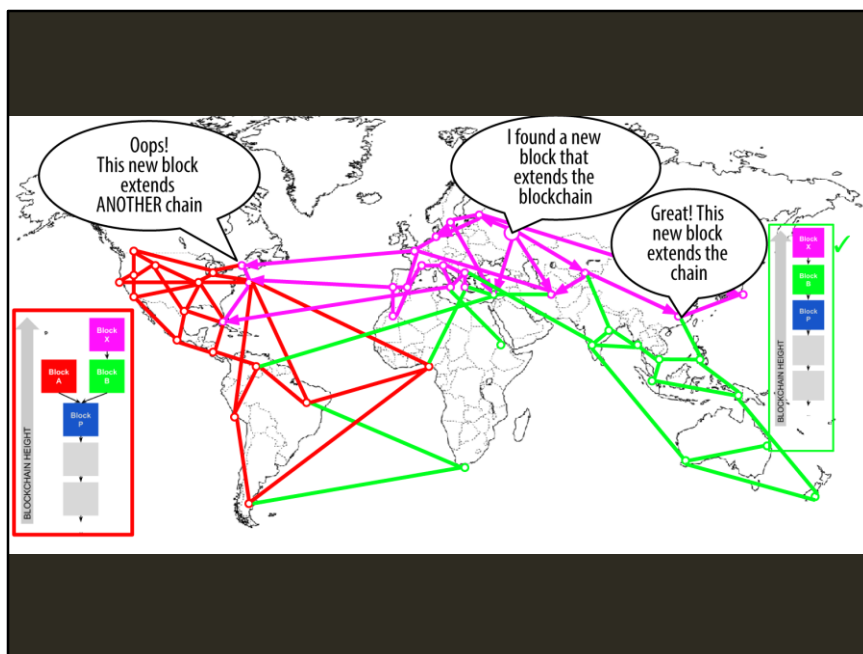












最終都會變返做一條鏈，因為大家都按規則玩，只會喺最長嗰一條鏈繼續挖。紅色嗰一舊區塊A就會好似「八萬五政策」一樣，唔存在喇！裏面嘅交易等同無發生過。

實際上，出現一層分歧嘅機率係一星期一遇，但兩層就微乎其微。如果一個交易係收埋喺第3幾個區塊之下，基本上都無人可以推得翻。

有一啲交易，例如將BTC入交易所，可能會要求等3個確認（三層咁深）先算數，呢個純粹係雙方自己定嘅事 – 睇下大家接受到嘅風險同埋時間，同係Bitcoin規則本身無關。

## BITCOIN=就是嗰一套規則

>50%節點話係咁，就係咁

出Bug時、要改規則時 – 需要>50%節點升級 (Hard Fork)

Bitcoin 2013年3月

- v0.7版不能對應某交易資料，v0.8可以
- v0.7認為v0.8所認受嘅區塊係錯，唔接受。
- 兩個版本使用嘅電腦相當 (按挖礦能力計)
- 區塊鏈變成有雙頭龍，維持咗好幾個鐘
- 最尾點收科：幾個大礦池(後面講)共識先落返去v0.7
- v0.8個條鏈就當無發生過，放入雪櫃。

Ethereum 以太坊 2016年6月

- 有bug，被hack
- Hard fork咗而變成兩種貨幣 (Ethereum Classic和Ethereum)

中本聰同佢之後接棒嘅人係有一個「官方組織」去商討制定Bitcoin技術，而且有放一個公版客戶端設計 (Reference Client)

(有啲似Nvidia嘅Founder's Edition? XD)

公版係開源嘅，通訊協議都係公開。用唔用公版大家自己揀，就好似HTTP一樣，大家都可以用唔同嘅瀏覽器上網。

出名嘅客戶端好似有兩三個，史上都出現過某一版本有Bug而計唔出數。但只要>50%嘅運算力都傾向支持某一個規則，嗰個就係Bitcoin。

官方亦可以挖爛塊面無啦啦推一個新版本，改成挖一個Block就有50000個BTC。但係大家會唔會跟風跟住用？呢樣嘢唔係一個組織控制得到。

又或者好似Ethereum嘅，搞到變咗兩個貨幣出來，因為兩套規則都各自有佢嘅「擁躉/信徒」去投放資源run節點

---

Q1: 節點係伺服器(Server)嗎？

A1: 其實只要係電腦就得，其實Server都係電腦㗎。實際上可能係個Raspberry Pi、可能係行Windows、可能係行Linux、可能係Router仔（就係唔講Mac...噢唔覺意都講咗）

而只係做規則驗證所需要嘅電費，比起挖礦嘅都低好多。(返到去POW個原理)

舉例就好似用Bittorrent (BT)一樣，阿某君想download嘢就自然要開一個BT App，其實亦即係一個BT節點。

越想守護Bitcoin規則嘅人，就越有誘因去用小小電去行一個節點，例如佢可能係個商家、投資者、投機者...

Q2: 出bug要hard fork嘅時候，可唔可以直接update客戶端？


A2: 其實係要大家去升級。有啲client可能有自動更新功能 (如同Windows Update)，有啲可能要自己download。

情況如某日你用舊版BT App發現要更新先download到嘢，但係因為你又好想download某樣嘢，所以自自然然會去更新。

挖礦嘅都唔想挖出來嘅變廢物，所以亦有誘因去跟大隊去升級。

Q3: 感覺就好似一個Game咁，BTC就係裏面嘅貨幣

A3: 差唔多啦，都係數字一個 (其實你銀行入面嘅都係數字一個)。但就無營運商 - 唔會無啦啦話「今日抽SSR機率改成X%」，而係玩家夾埋嘅共識作準。

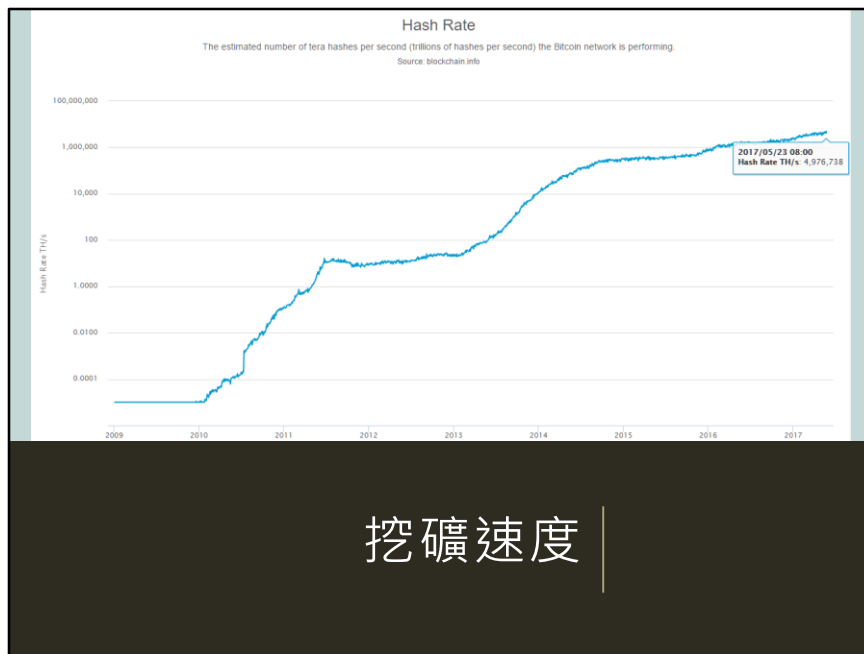


點樣拎到BTC？ |

咁有乜方法入手先？有三招：交易所買賣、挖、交易收款

## 交易所買賣

存入法幣，同買賣貴金屬、股票差唔多



自己一个挖基本上唔會中獎

一部機嘅運算能力係幾每秒幾百K個hash咁上下。

今日(2017-05-23)參與成個Bitcoin挖礦嘅速度係4976738T個hash咁上下。

機率有幾低自己計啦吓。

順便講:

1T=1000G

1G=1000M

1M=1000K

1K=1000

## 挖礦池 MINING POOL

大家一齊挖，邊個挖到就拎出來，然後按返每部機嘅速度平分

# 公私金鑰加密法

先隨機生產兩組好特別嘅數字

- **公鑰**(Public Key)是指公開畀人睇嘅一組
- **私鑰**(Private Key)是指自己收埋保存嘅一組

密鑰用法

- 原文x → 用**公鑰**加密 → 密文Y → 可用**私鑰**解密 → 原文X
- 原文x → 用**私鑰**加密 → 密文Y → 可用**公鑰**解密 → 原文X  
其實掉返轉都得，數學上無話邊個公邊個私，兩個一樣嘅  
只係在乎你收埋咗邊一個

簽名

- 原文嘅**雜湊值** → 用**私鑰**加密 → 得出對應嘅Signature，即**簽名**
- **簽名** → 用**公鑰**解密，就可以比較同原文嘅**雜湊值**一唔一樣
- 唔使講出**私鑰**但又可以證明自己擁有**私鑰**

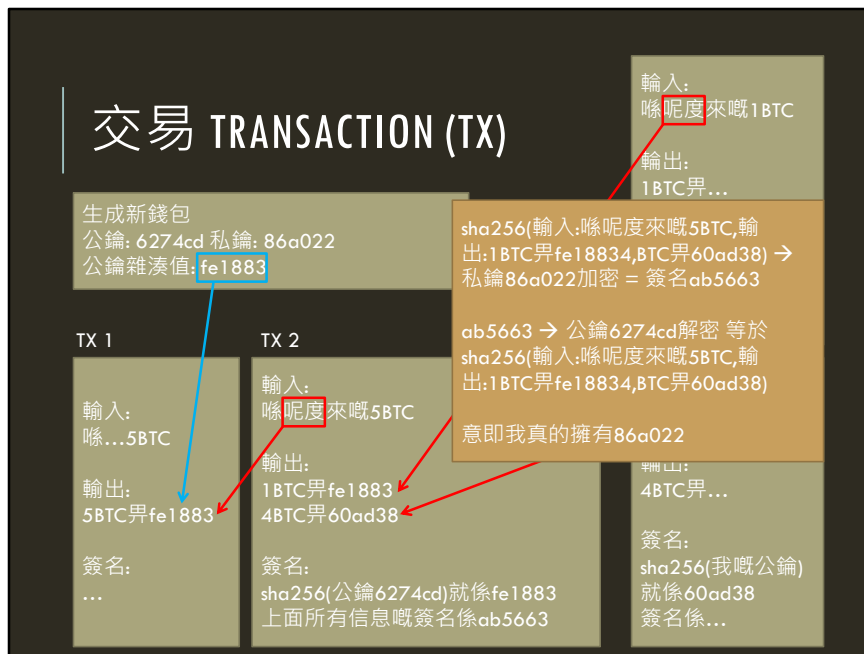
第三就係有人畀BTC你 (可能因為你賣咗其他嘢畀佢)  
呢度要先講講公私金鑰嘅概念

同現實嘅公司印差唔多

其他人見到你喺份文件上吸咗個公司印(如同**簽名**一樣)，就知道我真係有個公司印(私鑰)喺手，即使我從來都唔使拎個公司印實物(私鑰)出來畀人睇。

通過數學保證，無人可以單單透過睇過份吸咗印嘅文件，就可以雕返一模一樣嘅印仔出來。





簡單版，先唔提腳本(Script)

生成新錢包，即係公私金鑰對，將公鑰嘅雜湊值(基本上即錢包地址)畀想轉BTC你嘅人

之後收到BTC又點樣使？（唔使得嘅就唔係錢啦）

睇圖，其實一個TX就係跟住一個TX環環扣住，除咗獎金係無上一個TX之外。

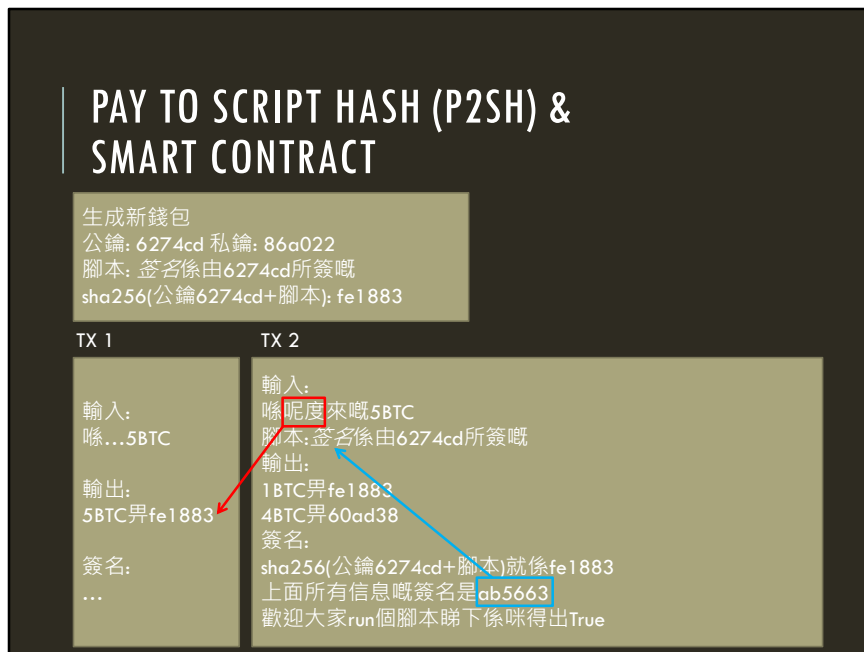
節點會驗證區塊入面嘅TX係咪符合規則，無問題先會納入Blockchain，例如：

- 公鑰嘅雜湊值就係同上手錢包地址一樣，而且簽名正確
- 輸入總金額係細過輸出總金額 (除咗獎金交易)
- 仲有剩嘅係會俾咗挖到礦嘅人

## 進行交易

1. 簽好名，把TX資料廣播出去
2. 祈求有挖礦者將你嘅TX放入佢挖嘅區塊裏面
  - 可以提供交易費作誘因...，宜家通常係0.001BTC
  - 越多越響香，越快有人理
  - 所以挖礦者都會盡量想包晒所有TX入個區塊裏面

挖到一個包含你嘅TX的區塊出來，廣播出去又被廣泛接納嘅話，就會成為歷史嘅一部份



實際上一個交易資料係稍為複雜少少，睇圖

腳本唔一定係呢個。Bitcoin腳本係用佢一套特定嘅語言去寫成，例如腳本可以話係

- 需要多個簽名先至True
- 直接return true都得

呢個腳本語言係特登設計成非Turing Complete嘅，費事有人玩嘢啦...Halting Problem呀

# 比特幣特性

## 無人監管

- 要>50%節點達成共識，無一人可隻手遮天

## 發行量固定且可預知

- 由規則控制，規則是>50%節點嘅共識

## 賬目公開

- 區塊鏈

## 錢包匿名

- 公私金鑰係可以自己隨便生成，要幾多有幾多

回顧一下點解比特幣有呢啲特性

## ALT-COIN (其他加密貨幣)

### Litecoin (2011年)

- 採用scrypt而唔係sha256作為pow
- 2.5分鐘一個block

仲有幾十種樓上，有唔同嘅參數，但原理大同小異

### Ethereum 以太坊

- 腳本語言係Turing Complete，使POW唔係白白晒電而係做一啲有義意嘅運算



## Q & A

投資、投機？  
價格可跌可升...

法幣嘅歷史係由1971年開始，Bitcoin係2009年。未來兩樣嘢會點嘅樣，有早知無乞兒兼夾中埋3T。

早期就曾經有人用幾萬個BTC買一塊Pizza。

Bitcoin同法幣嘅購買力終歸究底係乜？兩樣都唔可以食落肚，最終都係講個信字。