貨幣和比特幣
CURRENCY AND BITCOIN

Sam Wong
2017-05-26

說明

這個Deck有小量動畫和大量的文字筆記做補充

如果看不見，可以從這裏下載其他格式的

https://github.com/sam0737/brownbag

我的Bitcoin錢包: 1J9MKzB2KNoPofgACqXwtNb48DMyeDCAoT

本Deck係以CC-SA 3.0發佈

圖片使用的授權在筆記中詳細說明

- 放棄金本位 CC-SA 3.0: Will O'Neil

錢到底是什麼？

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

糧食

紙幣可以吃的嗎？古代還是用糧食做貨幣來得實際。
為五斗米而折腰有聽過不？

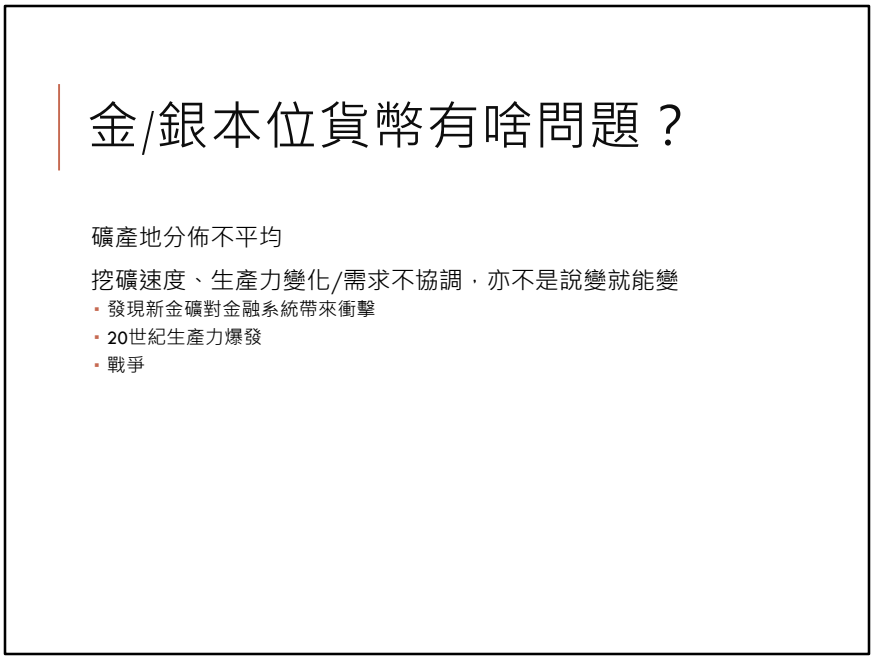
Public Domain:
https://commons.wikimedia.org/wiki/File:%E0%B4%AC%E0%B4%B8%E0%B5%81%E0%B4%AE%E0%B4%A4%E0%B4%BF_%E0%B4%85%E0%B4%B0%E0%B4%BF.JPG


銀圓

問題:
一般糧食都是易腐的 (而鹽曾幾何時也是貨幣的一種，政府規定不可以私自提煉竟然有發生過，哈哈哈)
量多 – 攜帶不便。總不能扛著幾斤米到處走。
難以標準化
加上國際貿易興起和需求 (用米的話運到目的地都爛得七七八八了，更何況老外不吃米飯)

所以興起以貴金屬作為貨幣。

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



舊金山之所以是舊金山，是因為在1848年發現有金礦

如果挖礦比生產力的增幅慢，亦即把金銀藏走來等到未來反而有更大的購買力的話，就是我們說的通縮。
最後大家就會把錢留著不花，經濟循環隨即崩潰。

針對實物貨幣這個問題，有兩招可解: 部份準備金制度、紙幣

部份準備金制度
FRACTIONAL-RESERVE BANKING

1. 存100元進銀行
2. 銀行按法例只需要保留10% (x%)
3. 90元又可以借出去
4. 借出去的90元到最後還不是存進銀行？
   又可以借81元出去
5. 最终100元就變成了100/x%，即是變成有1000元 (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元的金銀，在銀行轉兩圈變個魔術就變成1000元

紙幣

20世紀初戰事頻繁，需要真金白銀以支軍餉。有國共內戰、美國南北內戰、第一次世界大戰等等…

紙幣最初發行的時候，通常政府都承諾可以隨時兌換回去真金白銀
強勢點的政權可能會強迫人民上繳金銀，不得私藏。
無論點如何，一般政府都會承認自己發的紙幣 – 譬方說可以用來交稅。
但戰爭免不了勞民傷財，會損耗自己一國的生產力(GDP)，最後都會被擠兌或通貨過份膨脹，因為根本再没有足夠的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。

國民政府曾發行過「法幣」取代銀圓，1948・49年還強迫上繳金銀去換所謂的金圓券、银圓券，不消一年就變成廢紙s。

https://zh.wikipedia.org/wiki/File:ROC_Fabi.jpg
Believed to be in Fair Use

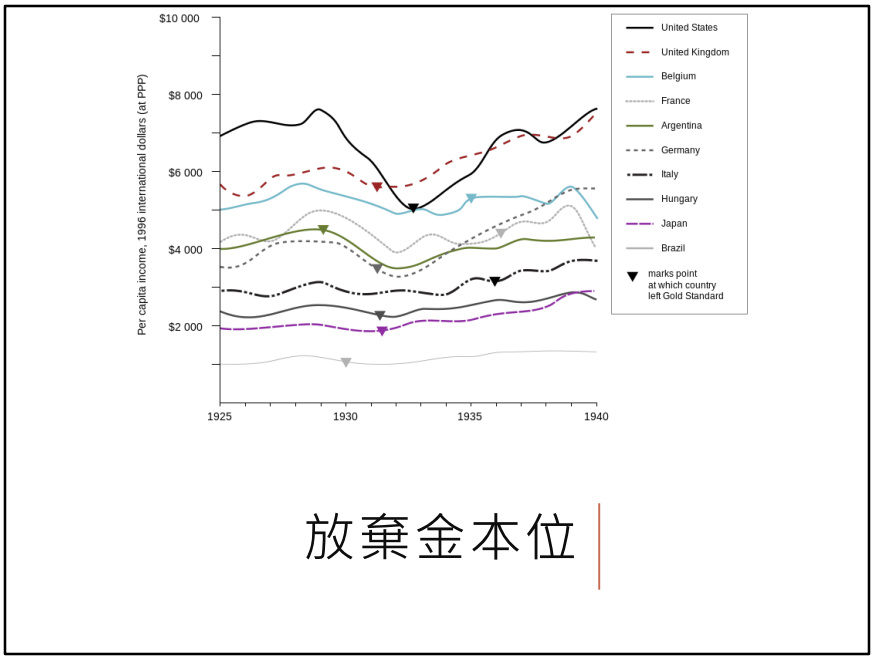
放眼看世界其他地方，一有戰事貨幣就要大幅偏值、通彭，去支付軍餉
打輸了一戰的德國就可慘了...馬克紙幣拿來當牆紙來貼，把它燒掉暖暖身子比買柴還划算。

一轉眼一戰就結束，然後「舞照跑、馬照跳」，大家該幹活的幹活，經濟有所改善，但突然來個經濟大蕭條。

原因有兩大說法:

1. 某日紐約發生股災，然後出現信心危機，接著銀行被擠兌倒閉，一發不可收拾
2. 一戰之後大家開始收緊銀根 (因為之前通彭、太多"熱錢")，回復到戰前所承諾的兌換率。一時大意收得太緊，導致出現流動性問題，然後發生通縮。

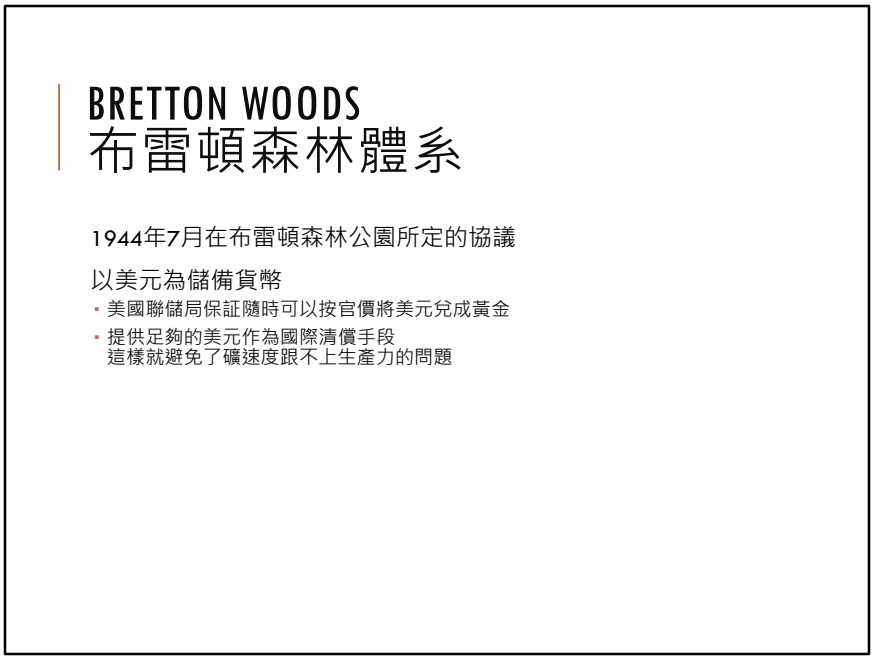
這作雪球一滾就滾了十幾年。



有一些國家就放棄金本位，即是相等於現在的量化寬鬆、匯率自由浮动、開動印鈔機。希望弄多點「錢」出來，製造通彭。
看一看這圖，美國在放放棄金本位之後一刻人均收入就脫離谷底。早知道就…

CC-SA 3.0: Will O'Neil
https://commons.wikimedia.org/wiki/File:Graph_charting_income_per_capita_throughout_the_Great_Depression.svg

又過了一會 - 又打仗啦！通彭已經是預料之內了吧？



轉一下眼又打完。
今次大家就不想回到金本位了
但二戰時自由浮動亦太可怕。

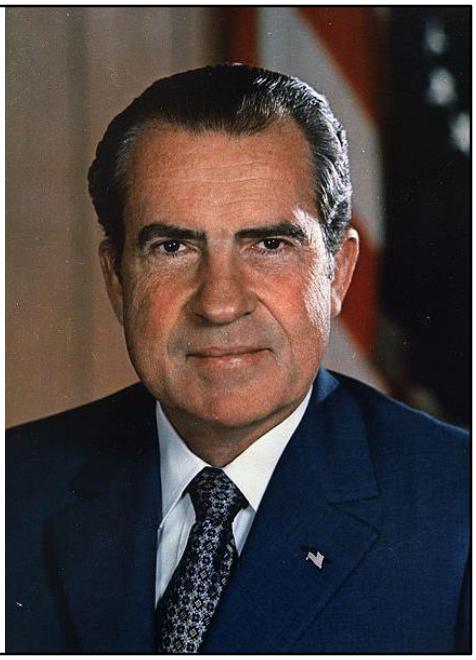
而在這一刻，美國就是全球最強，整個戰事就僅僅是丟了兩顆原子彈。其他如德、英、法、中、日有參戰的都元氣大傷。
所以盟國都跑去美國Bretton Woods開會討論商議對策。

結論就是大家都信美金，如同相信黃金一樣。

這事就到美國起事端。一打就廿年，國力有多強也是有個限度。
外國信心不足，開始向美國兌換黃金。

尼克森衝擊
NIXON SHOCK

1971



時任美國總統尼克森 – 就於1971某天突然宣佈不再兌換黃金，而且增加進口稅，希望國民在內部消費。
本來說是個90天的臨時政策，但根本就回不去。
風水師編你十年八載…美國這老大哥扛了27年也算是盡了情義。(不過倒不是說Bretton Woods對她沒好處)

全世界的貨幣就由呢一日起變成自由浮動，與金、銀完全脫離關係。

Public Domain:
https://commons.wikimedia.org/wiki/File:Richard_M._Nixon,_ca._1935_-_1982_-_NARA_-_530679.jpg

到了法幣時代，一個幣到底有什麼意義就只是由法律所賦予。

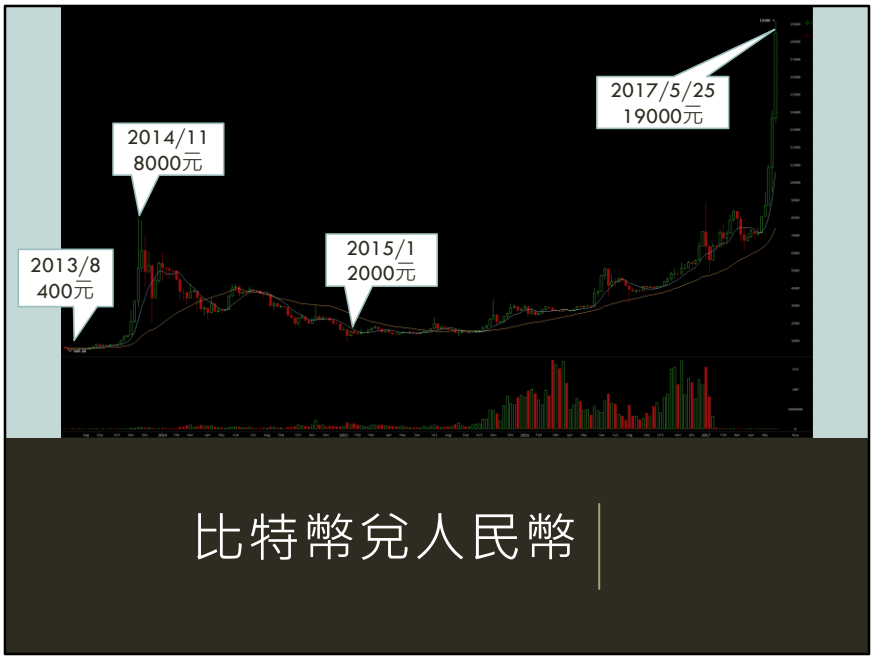
之後1987年某天香港發生股災，單日跌幅比得出經濟大蕭條的那天。
但這一次大家都學聰明了，因為都是大家法幣，所以可以通過貨幣政策去緩解，對民生影響相對細得多，
甚至日本之後還光輝了好幾年 (然後因為印太多錢而泡沫爆破，迎來「失去的十年」)，不過都未至於經濟大蕭條那時期這麼糟。

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

一句到底，錢值多少全憑信心，由一國的GDP支撐。
現代主流經濟學認為，維持2%左右的低通就剛剛好。


比特幣

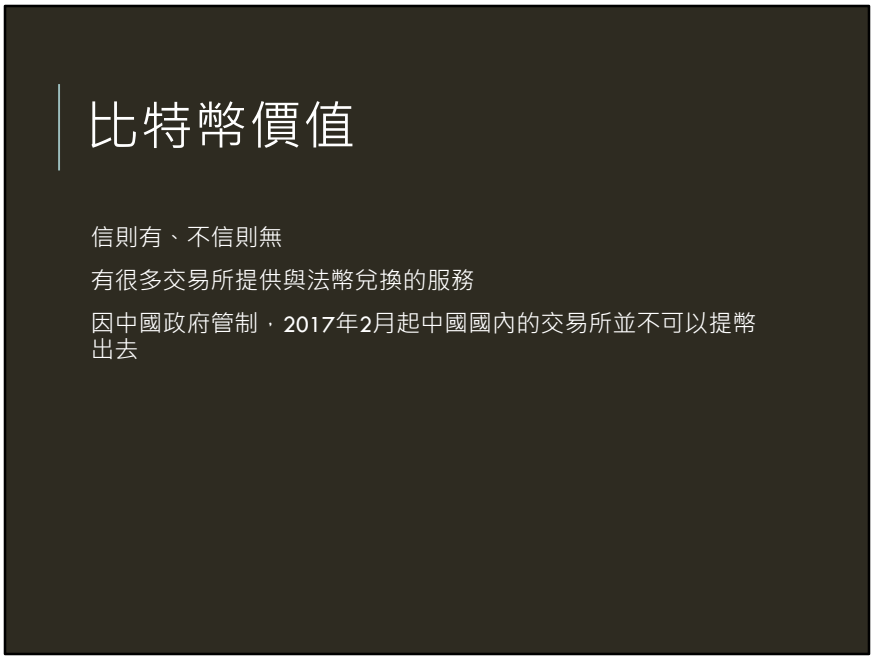
中本聡其實只是個網名，真人到底是誰天曉得？



Bitcoin在Okcoin.cn上的價格

2013年8月 – 400
2014年11月 – 8000
2017年5月25日 – 19000
2017年5月26日 – 16000 (單日就丟了15%)

(截自bitcoinwisdom.com)



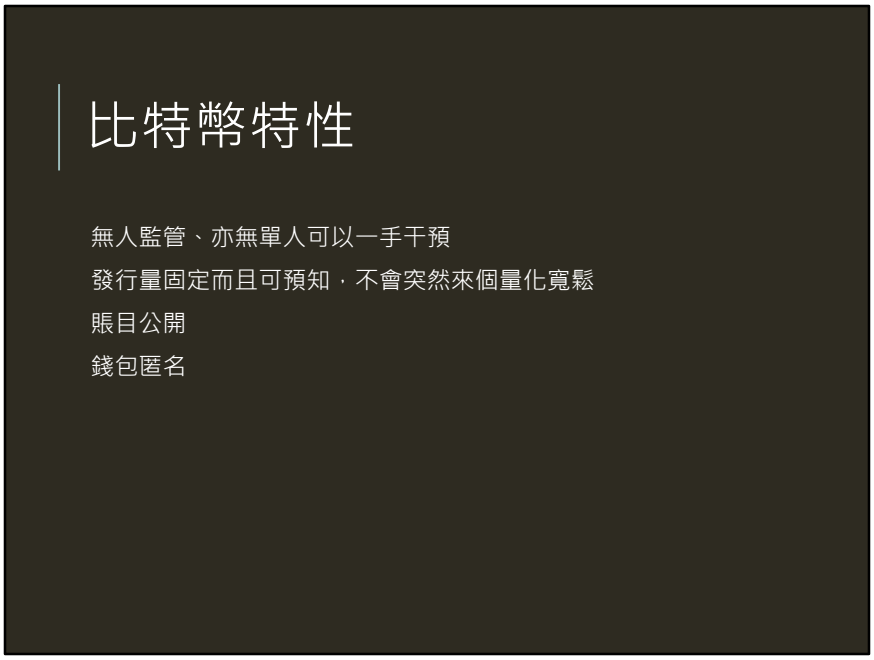
BTC的定價，與外匯、股票、甚至黃金都差唔多。誰願意用某一價格買、誰願意賣，這樣就定下來了。
雖然不可以用來交稅，但據統計也有上十萬個商號接受比特幣。最起碼還可以用來繳WannaCry的贖金？XD (註: 一款勒索病毒)

一句到尾，信則有，不信則無。

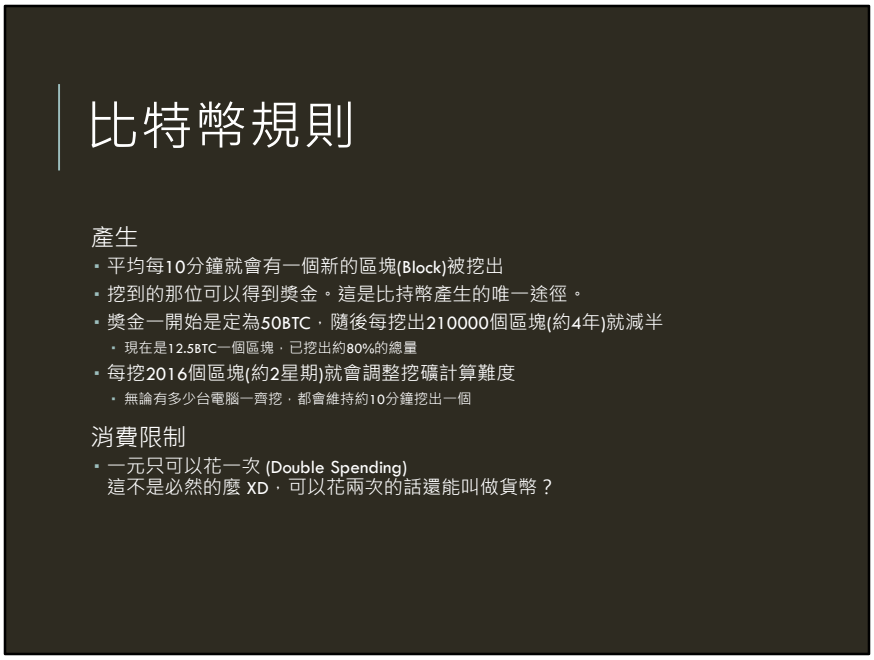
交易所並無漲停板、跌停板的機制。

和現時紙黃金(ETF)稍有不同，紙黃金一定是部份準備金制，買一克並唔代表佢背後真的有一克金專屬歸你。
但目前的BTC交易所都**聲稱**是完全準備金制，某些交易所還曾經用過特定算法公開審計過，當然你看不看得懂那算法、信不信得過就自己先想想。
史上亦有發生過mt.gox事件 – 一間當時最大的交易所因為據稱被黑，被偷光了coins而關門大吉。

又或者可以參考1637年荷蘭鬱金香狂熱的歷史。



後面會說明為什麼，先聽著。



先不要問為什麼，例如為什麼就是每10分鐘，為什麼就是四年減半...
一開始中本聰定了下來是這樣就這樣。

就像玩剪刀石頭布，為什麼剪刀就是贏布？一起玩就要跟著這一個規則。

後面會解釋為什麼大家都心甘情願跟著這一套遊戲規則玩。

PROOF OF WORK (POW)

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

$$x = 6 \; or \; x = 9$$

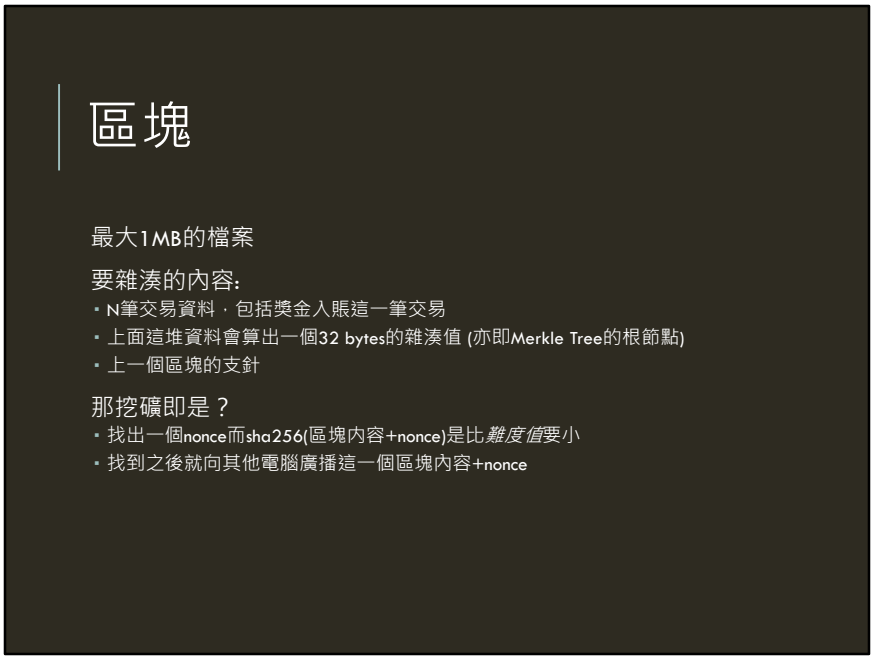
那到底什麼是區塊、什麼是挖礦？
這個就要先從Proof of Work說起。

相信大家在初中就學過二次元方程式的解法，一眼看上去未必馬上知道答案，但稍為算一算就知道原來根是6或9。
但若某人把答案說出來，其他人要驗証一下是否正確則是非常容易的事，把數值代到方程式裏頭就知道。

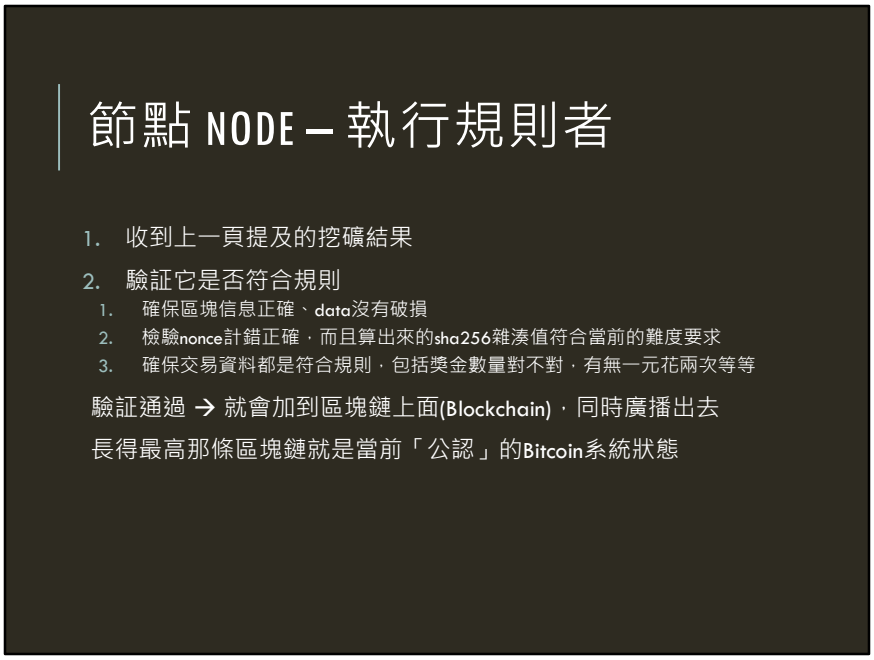
當然要電腦去解二次元方程就實在太容易啦，在bitcoin中實際上是用sha256這一款雜湊函數作為POW算法。

所有雜湊函數都一樣，只要代進去的原文稍為改一改，算出來的結果都截然不同。
而簡單來說，是並沒有可能從結果(雜湊值)去推敲出原文是長什麼模樣。
註: a603…這一串是16進制數字；16進制是以0-9，然後abcde分別代表11、12、13、14、15。

所以若要找nonce，唯一的辦法就是一個一個去試。當然符合0開頭的答案在這裏並不只有3，幾十、幾百、幾萬都有好多個數值算出來是0開頭的雜湊值。
但若果問題改一改成「請講出一個可以算到有5個0開頭的nonce」，那就要花點時間去試了。

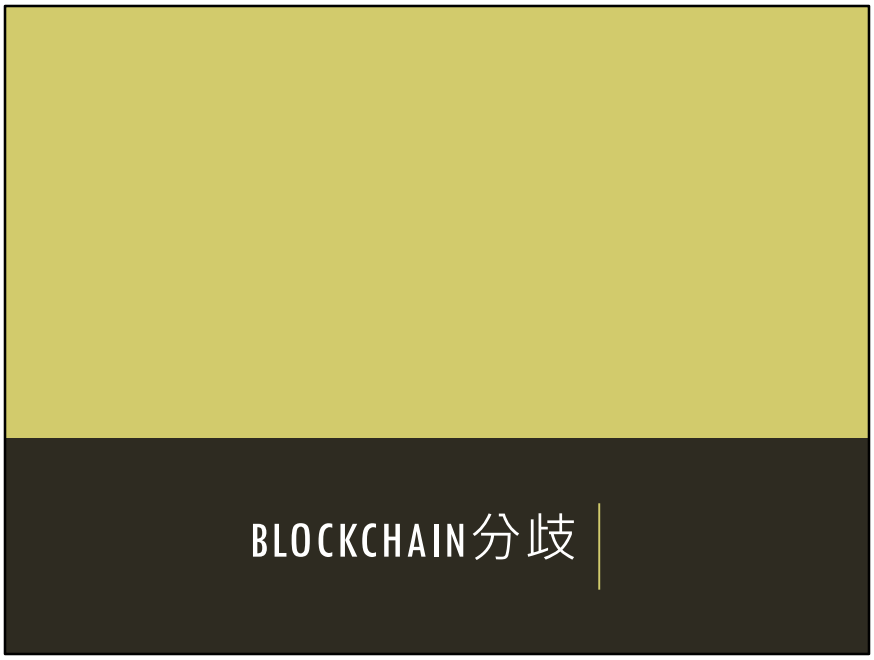


Q: 如果我黑了某一台挖礦電腦，而剛剛他又算出一個nonce，我把他的nonce偷了並先廣播出去，那我能把他那份獎金都搶掉嗎？
A: 不會。因為那個nonce只適用於他所編集的交易資料 – 當中包括那條「請將12.5BTC付進我口袋」這一段 – 的雜湊值
如果你要將「進我口袋」改成「進你口袋」，所需要的nonce根本不一樣。



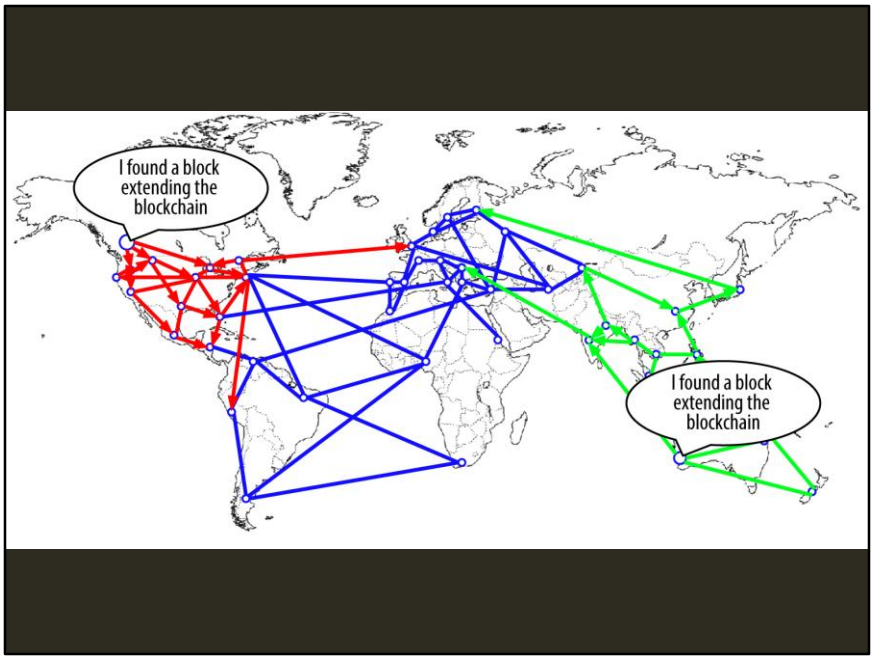
挖礦電腦在收到新的區塊訊息時，就會放棄手上正在挖的一塊。否則只是徒勞無功，因為其他節點根本不會再理會過期的區塊消失。

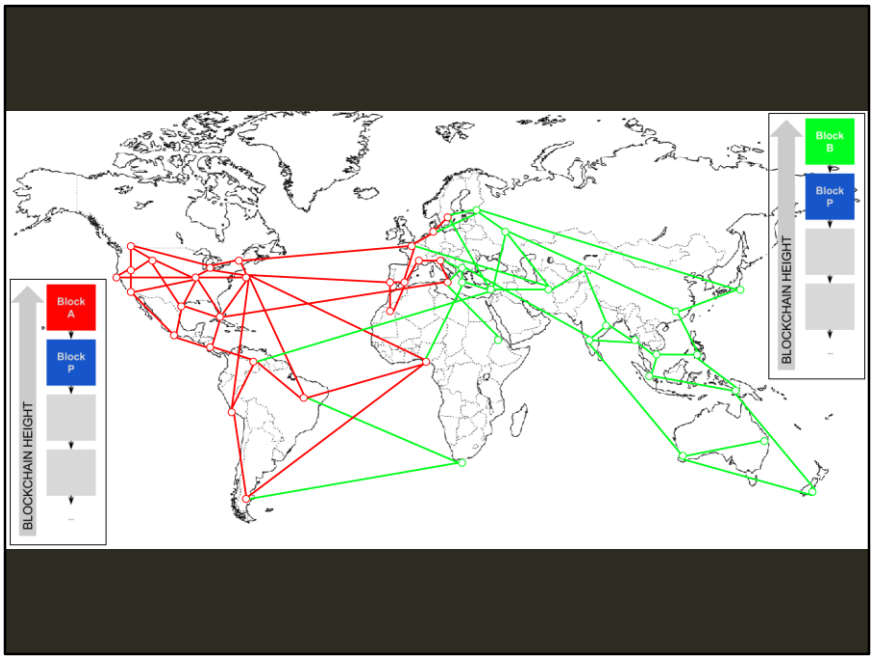
難度值 – 就係上幾頁提到每兩星期/2016個區塊調整一次，將難度控制於平均十分鐘挖出一個區塊。

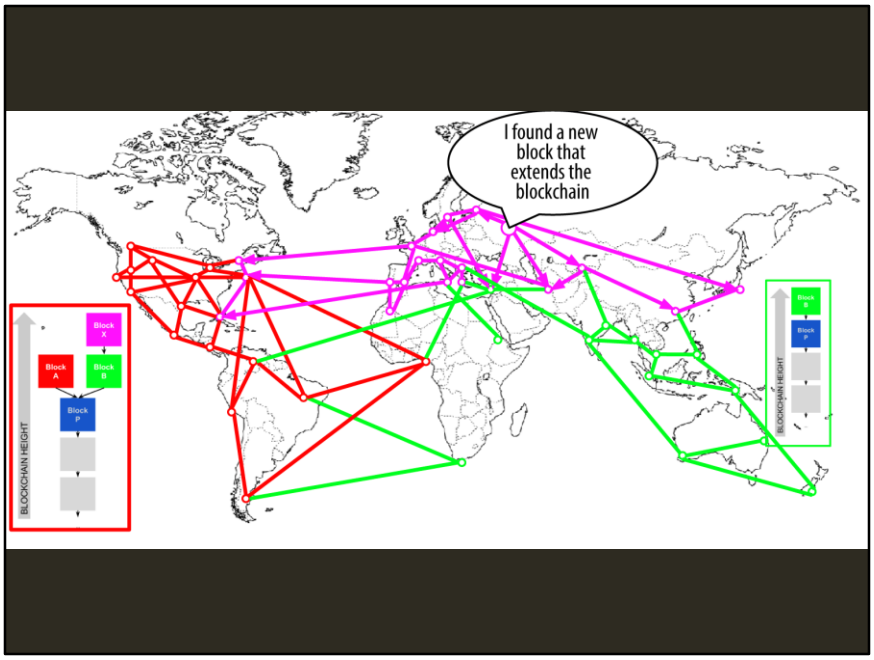


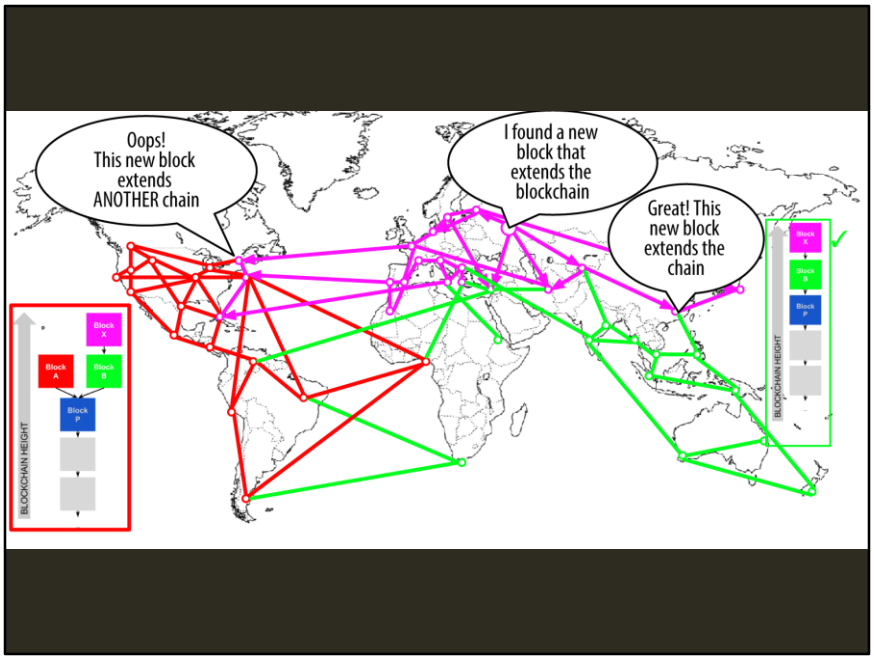
若然全世界有兩個方同時挖到新區塊會發生什麼事？消息同步還是有時間差的嘛


BLOCKCHAIN HEIGHT
Block P


I found a block extending the blockchain
I found a block extending the blockchain


Block A
Block P
BLOCKCHAIN HEIGHT
Block B
Block P
BLOCKCHAIN HEIGHT


I found a new block that extends the blockchain
BLOCKCHAIN HEIGHT
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block P
Block P



最終都會整合到一條鏈上，因為節點都是按規則運算，而且只會在最長的條鏈上挖。
上圖紅色的老區塊A就會消失，存在裏面的交易就算同沒有發生過一樣。

實際上，出現一層分歧的機率大約是一周一遇，但兩層就微乎其微。
如果一個交易是藏在3幾個區塊之下，基本上都無人能夠推翻其結果。

有一些交易，例如將BTC存入交易所，可能會要求等 3 個確認（三層深）才算數，這個純粹是雙方自定的協議 – 視乎大家能接受到的風險和時間，這與Bitcoin規則本身無關。

中本聰和接他棒的人是有組成一個「官方組織」去商討和制定Bitcoin技術，而且有一個開源的公版客戶端設計 (Reference Client)
(有點像Nvidia的Founder's Edition? XD)
那個公版是開源的，通訊協議也是公開有文檔當。致於要不要使用公版即是自由選擇，就像HTTP一樣，大家都可以用不同的瀏覽器瀏覽網頁。
有名的客戶端好像有兩三個，史上亦都發過某一版本有Bug而算不出Block。但只要>50%的運算力都傾向支持某一個規則，那個就是Bitcoin。

官方亦可以無恥地突然推一個新版本，改成挖一個Block得50000個BTC。
但是社群會不會跟著用？這個就不是單一組織能控制的事。
又或者最終會像Ethereum一樣，衍生出兩個貨幣來，因為兩套規則都各自有他的粉絲投放資源運行節點

Q1: 節點是伺服器(Server)嗎？
A1: 其實只要是電腦就可以，其實Server也是普通電腦而已。實際上可能是個Raspberry Pi、可能是跑Windows的、Linux的、也可能是寬頻路由器（就是故意不提Mac…噢…提了）

而只做規則驗証所需要的電費，比起挖礦的都低好多。(回到POW的原理)

舉例就好像用Bittorrent (BT)一樣，某君想下載某檔案自然就要跑一個BT App，其實亦即是一個BT節點。
越想守護Bitcoin規則的人，就越有誘因去用小小電力去跑一個節點，例如他可能係個商家、投資者、投機者…

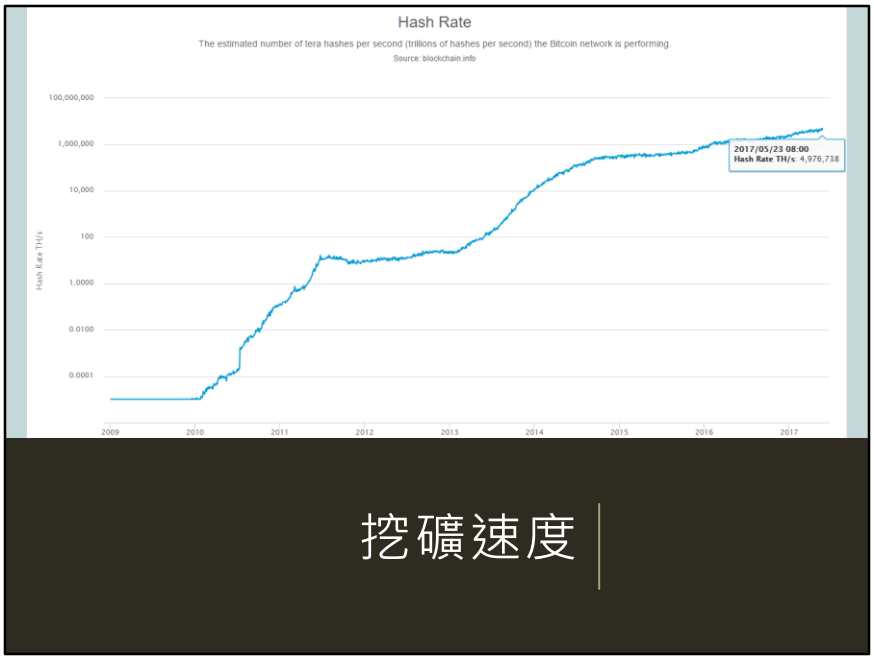
Q2: 出bug要hard fork的時候，可以直接更新客戶端？
A2: 其實係要大家去升級更新。有些客戶端可能有自動更新功能 (如同Windows Update般)，有些可能要手動去做。
情況如某天你用舊版的BT App發現須要更新才能下載別的，自自然然會去更新。
挖礦的人都不希望浪費能源挖出廢物，所以亦有誘因去隨大流升级。

Q3: 感覺就好像遊戲一樣，BTC就是裏面的貨幣
A3: 差不多啦，都只是一個數字 (其實銀行裏的又何嘗是？)。但就沒有營運商 - 不會突然公布「今天抽SSR機率改成X%」，而是以眾玩家的共識作準。

說了半天，到底怎樣才能拿到BTC？有三招：交易所買賣、挖、交易收款

交易所買賣

存入法幣，與買賣貴金屬、股票差不多少



自己一个挖基本上不可能中獎

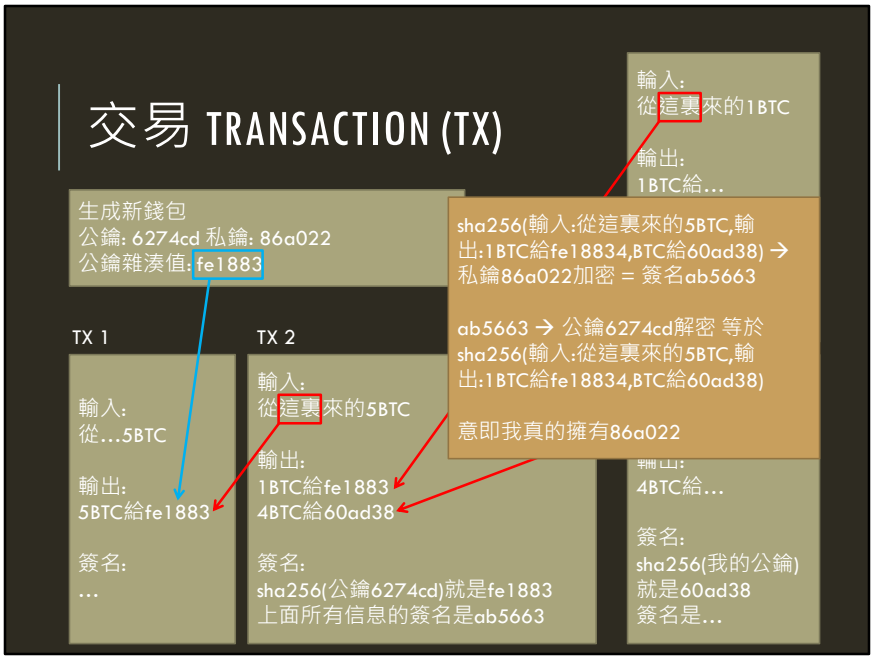
一台電腦的運算能力大概是每秒幾百K個hash上下。
今日(2017-05-23)參與整個Bitcoin挖礦的速度是4976738T個hash上下。
機率有多低自己算咯。
順帶一提:
1T=1000G
1G=1000M
1M=1000K
1K=1000

挖礦池
MINING POOL

大家一齊挖，誰挖到就拿出來，然後按返每部機嘅速度平分

第三就係有誰把BTC給你 (可能因為你賣了什麼给他？)
這裏要先說說公私金鑰的概念

和現實的公司章差唔多
其他人看見你在份文件上蓋了個公司章(如同簽名一樣)，就知道我手上真的有一個公司章(私鑰)，即使我從來都不需要把章的實物(私鑰)拿出來給人看。
通過數學保証，沒有人可以單單透過觀察蓋過章的文件，而雕一個一模一樣的章出來。



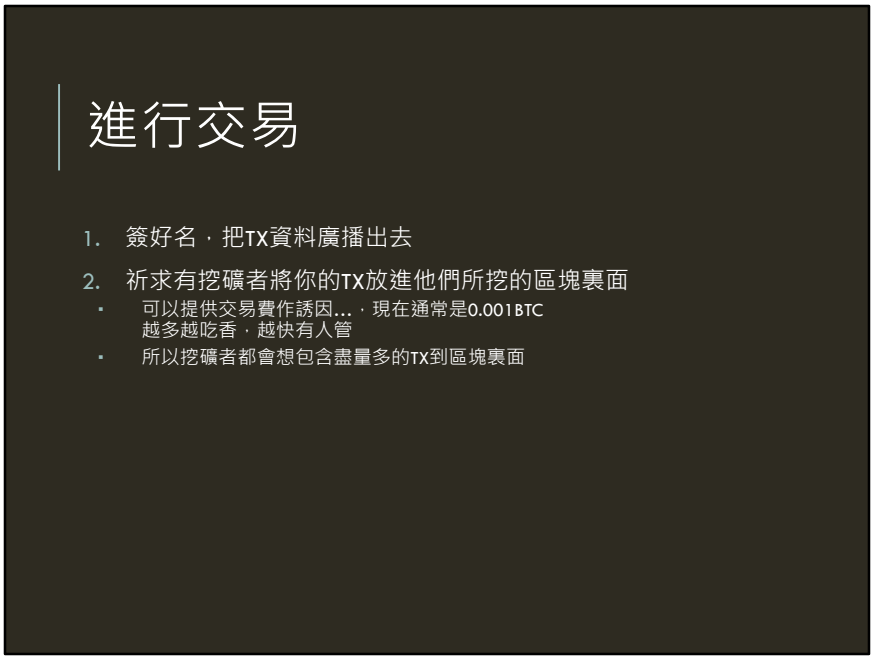
簡單版，先不提及腳本(Script)

生成新錢包，即是公私金鑰對，將公鑰的雜湊值(基本上即錢包地址)給想轉你BTC的人

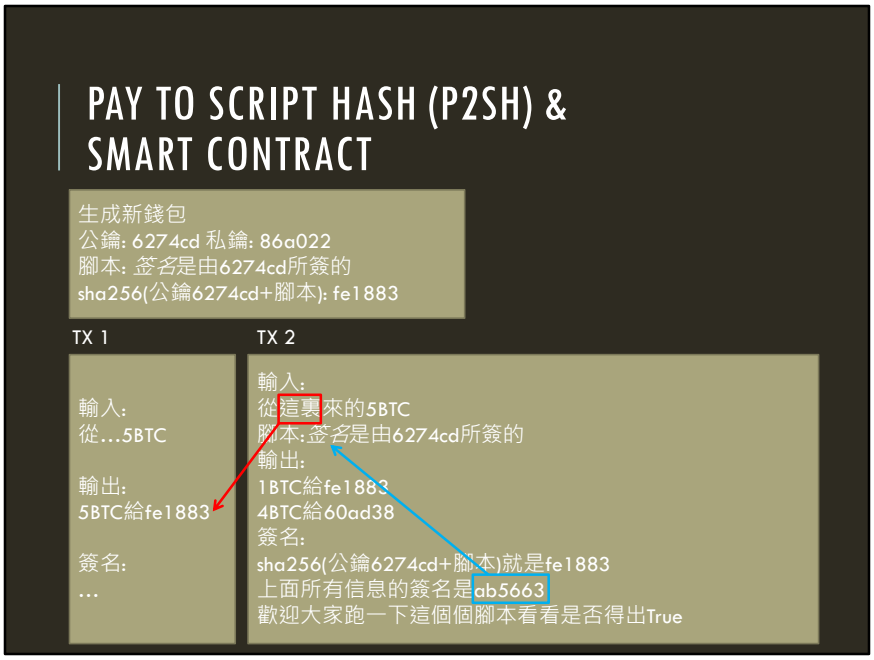
之後收到了BTC又怎樣花呢？（若不能花就不是金錢啦）
看上圖，其實就是一個TX跟住一個TX環環相扣，除了獎金是沒有上一個TX之外。

節點會驗証區塊裏面的TX是否符合規則，沒有問題才會納入Blockchain，例如：

- 公鑰的雜湊值和上個TX指定的錢包地址一樣，而且簽名正確
- 輸入總金額比輸出總金額小 (除了獎金交易)
- 還有剩下的是會給到礦嘅人



挖到一個包含你的TX的區塊出來，廣播出去又被廣泛接納的話，就會成為歷史的一部份

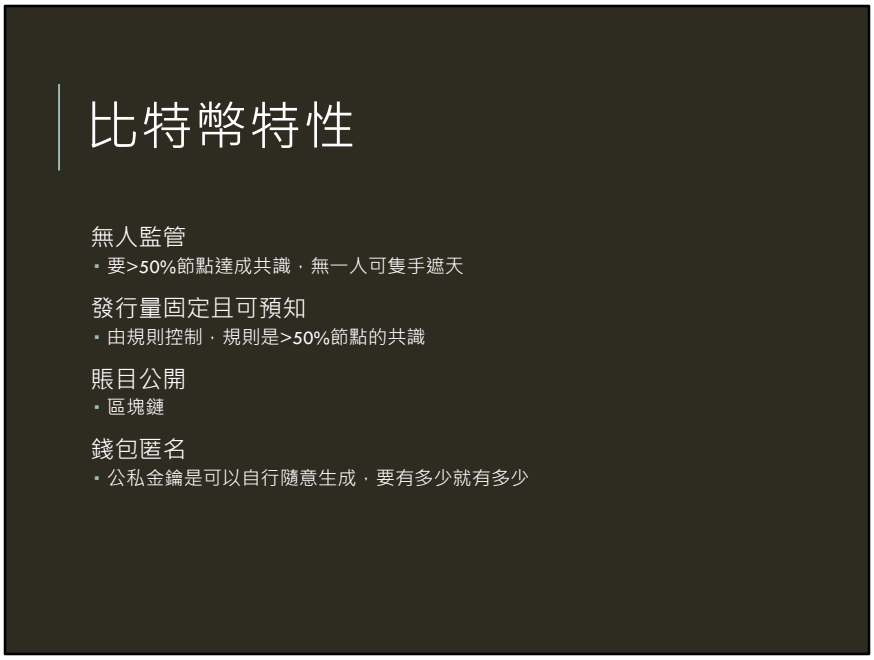


實際上一個交易資料是稍為複雜一點點，看上圖

腳本不一定是圖到那個。Bitcoin腳本是用佢一套特定的語言去寫成，例如腳本可以是

- 需要多個簽名才會True
- 直接return true亦可

這個腳本語言是故意設計成非Turing Complete嘅，免得有些頑皮的人...Halting Problem呀



回顧一下為什麼比特幣有這些特性

ALT-COIN (其他加密貨幣)

Litecoin (2011年)

- 採用scrypt而不是sha256作為pow
- 2.5分鐘一個block

還有不下數十種，各有不一樣的參數，但原理大同小異

Ethereum 以太坊

- 腳本語言是Turing Complete，使POW不是白白浪費電力而是做一些有義意的運算

投資、投機？
價格可跌可升…

法幣的歷史係由1971年開始，Bitcoin係2009年。未來兩種東西會怎樣發展，套句粵語「有早知無乞兒(乞丐)」
早期就曾經有人用幾萬個BTC買一塊Pizza。

Bitcoin與法幣的購買力終歸究底是什麼？兩樣都不可以吃進肚子裏，最終也只是「信」字一個。