

Saifedean Ammous 著

吳國慶 譯

# 比特幣 標準

中央銀行的去中心化替代方案  
The Bitcoin Standard



## 了解比特幣歷史、特性、用途與未來的基本指南

這是一本幫助您瞭解比特幣經濟，並透過歷史上曾經實踐金錢功能的多種技術，來了解比特幣如何作為這些可行技術的數位版本的書。本書並非廣告行為或是邀請大家來購買比特幣。正好相反，比特幣的價值可能會繼續波動，而且至少還需要一段時日，而且比特幣網路也可能因為可見或不可見的因素，導致成功或失敗。它在使用上也需要技術能力與面對風險，因而對許多人來說並不適合。所以本書並不提供投資建議，但會協助評估其網路與操作的經濟屬性，讓讀者能在決定是否投資之前，預先了解情況。

只有在對擁有和儲存比特幣的實際操作方面，進行過廣泛而深入的研究之後，您才應該考慮是否持有比特幣。由於比特幣市場價值的飆升，讓它看起來像是無腦式的投資，但仔細研究無數的網路駭入與駭客攻擊、詐騙及安全漏洞等讓人們失去比特幣的事件，對那些覺得比特幣可以提供穩定獲利的人，都是一種警告。

如果在閱讀本書後，認為值得擁有比特幣。你的首要投資不應該是購買比特幣，而是投資時間來了解如何安全的購買、儲存和擁有比特幣。比特幣具有這種相關知識無法委外的本質特點，任何對使用這個網路感興趣的人，都無法推托個人責任，這便是進入比特幣世界所需要進行的真正投資。



Saifedean Ammous 著

吳國慶 譯

# 比特幣 標準

中央銀行的去中心化替代方案  
The Bitcoin Standard



Saifedean Ammous 著

www.qitubk.com 奇兔電子書下載

吳國慶 譯

---

# 比特幣 標準

---

中央銀行的去中心化替代方案

The Bitcoin Standard



Authorized translation from the English language edition, entitled *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (9781119473862) by Saifedean Ammous, published by John Wiley & Sons, Inc. Copyright © 2018 by John Wiley & Sons, Inc.

All Rights Reserved. This translation published under license with the original publisher John Wiley & Sons, Inc.

CHINESE TRADITIONAL language edition published by GOTOP INFORMATION INC, Copyright © 2019.

獻給我的妻女，  
她們賦予我寫作的動力。

也謝謝中本聰，  
給我值得寫作的題材。

# 目 錄

## Contents

### **1 金錢 1**

---

### **2 原始貨幣 11**

---

### **3 貨幣金屬 17**

---

為何選擇黃金？ ..... 19

羅馬的黃金時代與沒落 ..... 25

拜占庭與拜占庭金幣 ..... 28

文藝復興時期 ..... 29

美好年代 ..... 34

### **4 政府的錢（法定貨幣） 41**

---

貨幣民族主義與自由世界的終結 ..... 43

兩次世界大戰之間的年代 ..... 48

第二次世界大戰與布雷頓森林體系 ..... 53

政府貨幣的軌跡紀錄 ..... 60

## **5 金錢與時間偏好 73**

---

貨幣通貨膨脹 .....	81
儲蓄和資本累積 .....	90
創新：「零到一」比「一到多」 .....	96
藝術的蓬勃發展 .....	99

## **6 資本主義的資訊系統 105**

---

資本市場社會主義 .....	109
商業週期和金融危機 .....	114
貿易的健全基礎 .....	127

## **7 健全貨幣與個人自由 133**

---

政府應該管理貨幣供應嗎？ .....	134
不健全貨幣與長期戰爭 .....	144
有限政府與全能政府的比較 .....	147
侵吞額 .....	153

## 8 數位貨幣

165

比特幣作為數位現金 .....	167
供應、價值和交易 .....	176
第八章附錄 .....	190

## 9 比特幣有什麼用途？

193

儲存價值 .....	193
個人主權 .....	200
國際化與線上結算 .....	205
全球計價單位 .....	212

## 10 比特幣的疑問

217

比特幣採礦是一種資源浪費嗎？ .....	217
失控：為何沒人可以改變比特幣 .....	222
反脆弱 .....	230
比特幣可以「擴容」嗎？ .....	232
比特幣是犯罪分子專屬嗎？ .....	238
如何殺死比特幣：初學者指南 .....	240
替代幣 .....	250
區塊鏈技術 .....	257

**A** 致謝 273

---

**B** 參考書目 275

---

# 關於作者

About the Author

Saifedean Ammous 是黎巴嫩美國大學的經濟學教授，以及哥倫比亞大學資本主義與社會中心成員，並擁有哥倫比亞大學永續發展博士學位。



# 序

## Foreword

納西姆・尼可拉斯・塔雷伯  
(Nassim Nicholas Taleb、黎巴嫩金融風險專家、  
《黑天鵝效應》一書作者)

**讓**我們從事情邏輯的開端講起。或者相反的，從事情結束的部分——「現代」開始談起。如同書寫的當下，我們正處在一個難以理解的領域，例如從宏觀經濟現實裡，目睹一場對抗某些專家階級的完整暴動。而且這些專家不單已不再是專家，他們甚至無法自知這個事實。美國聯邦儲備會前主席葛林斯班與伯南克，也只掌握到一部份的經驗現實，也就是我們發現的太晚：宏觀的資產負債表要比微觀的資產負債表走得更長久。這也正是為何我們必須更小心，到底要讓誰來制定中央的宏觀決策。

更糟的是所有中央銀行都是在相同模式下運作，形成養分貧瘠的單一思路。因為在複雜領域下，專業知識不會高度集中；而在有機狀態下，如同海耶克（F. A. Hayek、奧地利經濟學家、主張自由經濟）所證明，事情會以自動分散的方式進行，只不過海耶克使用的是「知識分散」的觀點。而現在看起來，我們似乎不必用到事情的「知識」部份就能運作良好，而且也不需要個人理性的部分，我們所需要的就是「架構」而已。

這並不是在要求所有參與者都有決策的部分主導能力，因為動機強烈的參與者，可以不成比例的扭曲決策方針（我研究過少數民族統治的不對稱性），這是在保障每個參與者都可以選擇是否要成為玩家。

然而在規模轉變下，卻產生了神奇的效果：理性市場並不需要個別交易者理性，事實上，他們在「零智能」下的運作良好，亦即良好設計下的「零智能群眾」，會比集權管理下的高智能人類群組表現得更好。

這也就是為何比特幣是個好主意，因為它填補了複雜系統的需求。並不只是因為它是加密貨幣，重點是在於無人擁有它，也就是沒有任何官方權威可以控制它的命運。它是由群眾，也就是使用者所共有。而且它現在已經有了多年的交易紀錄，足以為自己爭取權益。

對於其他競爭的新數位貨幣來說，他們必須要先擁有這類「海耶克式」的分散式資產才行。

比特幣是一種無政府貨幣嗎？可能有人會問：我們所擁有的金、銀、其他金屬以及其他貨幣，不也是沒有政府的嗎？這種說法並不正確。因為當你交易黃金時，可能交易的是港銀的黃金，最後會收到一紙存貨證明，然後你可能會把它帶到紐澤西州之類。銀行控制託管遊戲而政府控制銀行（或者應該客氣一點的說是銀行家與政府官員，緊密地結合在一起管理）。因此比特幣比起

黃金在交易上的更大優點是：結算並不需要特定託管人，政府並無法控制你腦子裡的那些密碼。

最後，比特幣將會渡過陣痛期。它可能會失敗，不過也很容易捲土重來，因為我們已經知道一切如何運作。就目前的狀態而言，它的交易過程可能並非很方便，還無法輕鬆地在你附近那家強調美德信號（virtue-signaling、一般指星巴克努力塑造的企業形象）的連鎖咖啡，購買一杯無咖啡因濃縮咖啡。雖然在目前拿比特幣來直接當作貨幣可能太過激進了，不過這確實是第一種有機的貨幣。

它的存在就像一種保險策略，可以用來提醒政府：國家體制所能控制的最後對象——貨幣，已經不再由他們獨佔。這點讓一般大眾在對抗歐威爾式的未來時，多了一份保障。

納西姆・尼可拉斯・雷伯  
寫於 2018 年 1 月 22 日

# 前言

## Prologue

2008年11月1日，一位署名為 Satoshi Nakamoto（中本聰）的電腦程式設計師，在密碼學郵寄清單發了一封電子郵件，聲稱他發明了一種「完全點對點式，不須第三方認證的新電子現金系統」<sup>註1</sup>。他複製了論文摘要來解釋這項設計，並且將連結放上網路。在本質上，比特幣為自己的原生貨幣提供了支付網路，並使用複雜的方法讓會員認證所有交易，而無需信任網路上的任何單一會員。此電子貨幣會以預定匯率發行，以酬謝耗費運算能力來計算交易區塊的用戶，等於是在為這種工作提供回報。相較之前發明數位貨幣的各種企圖而言，此項發明的最奇特之處，便在於只有它真正成功了。

雖然是聰明且精簡的設計，不過這樣古怪的實驗產品，並不太能吸引數位貨幣技客圈以外的人。比特幣在最初幾個月的情況真的是如此，全世界大概只有幾十個人加入比特幣社群，進行挖礦，並將挖得的比特幣寄給彼此，當成數位形式的收藏品。

---

註1 完整的電子郵件可在中本聰研究所（Satoshi Nakamoto Institute）的所有已知 Satoshi Nakamoto 著作檔案中找到，亦可參閱 [www.nakamotoinstitute.org](http://www.nakamotoinstitute.org) 上。

不過在 2009 年 10 月，一項網路交易<sup>註 2</sup>以 5.02 美元賣出 5,050 比特幣，其交易價格等於 1 美元兌換 1,006 比特幣，亦即登錄了比特幣的第一筆貨幣交易<sup>註 3</sup>。此項價格是經由計算產生 1 比特幣所需花費的電力價值而得。

用經濟學的角度來說，這個開創性的時刻，可以說是比特幣生命週期中最重要的時刻。比特幣從此不再只是一個程式設計師的邊緣社群裡所玩的數位遊戲，它開始成為市場上的有價貨物，代表任何人在任何地方都可以積極的為它估值。接著在 2010 年 5 月 22 日，有人付了 10,000 比特幣買了市價 25 美元的兩個披薩，這也是比特幣第一次做為交易的媒介，從市場貨物變成交易媒介，一共花了七個月的時間。

---

註 2 目前已停止運作的 New Liberty Standard（新自由標準）網站。

註 3 引自 Nathaniel Popper, *Digital Gold*（Harper 出版，2015 年）。

從那時開始，比特幣網路在會員與交易數量上逐步成長，加上處理能力的貢獻，它的貨幣價值飛速成長，在 2017 年 11 月<sup>註 4</sup>突破每比特幣 \$7,000 美元的行情。歷經八年，證明比特幣的發明不再只是一場線上遊戲，而是一項技術，可以透過市場考驗並應用在真實世界的許多用途上，其匯率圖表也經常出現在電視、報紙與網站上，跟著國際貨幣匯率一起出現。

我們最好把比特幣理解為一種分散式軟體，可以在貨幣轉移價值時，防止意外通貨膨脹的發生，而且無需透過第三方認證。換句話說，比特幣具有現代中央銀行的自動化功能，藉由程式編碼讓它們可被預測且幾乎無法改變，以便在成千上萬網路成員裡達成去中心化。亦即在沒有其他成員允許下，任何人都無法變更這些程式碼。這種作法讓比特幣成為第一個達成可信任的數位現金與數位硬幣的操作範例。雖然比特幣是數位時代的新發明，但它聲稱要解決的問題，也就是提供一種讓所有者可完全掌控，並盡可能長期保持其價值的貨幣形式，就如同人類社會自古以來所做的一樣。

本書藉由多年研究這項技術，以及研究它所能解決的經濟問題，來呈現這些問題的概念，並透過歷史觀點看人類社會以前是如何找出解決方案。不過我的結論可能會嚇到那些認為比特幣只

---

註 4 換句話說，在這 8 年間作為市場商品，從第一個價格 0.000994 美元上漲到寫作時的歷史最高價 7,888 美元，比特幣已經上漲了近八百萬倍，或者，更精確的數字是 799,513,944 %。

是投機者或推動者用來「賺快錢的騙局或詭計」的人。事實上，比特幣確實改良了以前的「保存價值」解決方案，而且它可以作為數位時代的「聲錢（sound money、指健全貨幣）」<sup>譯註</sup>的適用性，可能會讓反對者感到意外。

歷史可以讓我們預見將要發生之事，特別是當你仔細檢視歷史時；而時間則會告訴我們，本書所舉實際案例的適切性。因此，本書第一部分有其必要解釋「金錢」的作用與特性。

身為一位帶有工程背景的經濟學者，我通常會從「打算解決的問題」來瞭解一項技術，因為這樣可以將之從偶然事件、粉飾過或瑣碎的特性裡抽離出來，辨識出這項技術真正的功能本質。藉由瞭解金錢所打算解決的問題，便可能闡明為何金錢會被分為「聲錢」與「非聲錢」，並且可以套用概念架構來了解「如何」與「為何」各式各樣的商品如貝殼、琉璃珠、貴金屬與法幣（法定貨幣）可以具備金錢的功能性，同時也要了解「如何」與「為何」有些商品會失敗或成功，達成保存價值與交易的社會性目的。

本書的第二部分則透過歷史來探討個人、社會與整個世界所捲入的「聲錢」與「非聲錢」形式。「聲錢」亦即健全貨幣，可以讓人們進行長期思考，以便為未來進行儲蓄或投資。而從長期來

---

譯註 「聲錢（sound money）」是由有形商品如黃金所支持的健全貨幣；對比於「非聲錢（unsound money）」如「法定貨幣」，僅是由政府立法所支持的不健全貨幣。



看，儲蓄或投資便是資本累積與人類文明進步的關鍵。貨幣是經濟的訊息與衡量系統，健全貨幣可以讓交易、投資與創業行為在堅實的基礎上進行，而非健全貨幣則會讓這些行為變得混亂。健全貨幣也是自由社會的一項基本元素，可以提供堅固有效的壁壘來反抗專制政府。

本書的第三部分則會解釋比特幣網路的運作方式，以及它最明顯的經濟特色，並分析把比特幣作為一種健全貨幣形式的可行性，也會討論到一些比特幣並不適用的情況，然後解釋一些圍繞著比特幣常見的誤解與錯誤觀念。

本書的寫作動機在幫助讀者瞭解比特幣經濟，並透過歷史上曾經實踐金錢功能的多種技術，來了解比特幣如何作為這些可行技術的數位版本。本書並非廣告行為或是邀請大家來購買比特幣。正好相反，比特幣的價值可能會繼續波動，而且至少還需要一段時日，而且比特幣網路也可能因為可見或不可見的因素，導致成功或失敗。它在使用上也需要技術能力與面對風險，因而對許多人來說並不適合。所以本書並不提供投資建議，但會協助評估其網路與操作的經濟屬性，讓讀者能在決定是否投資之前，預先了解情況。

只有在對擁有和儲存比特幣的實際操作方面，進行過廣泛而深入的研究之後，你才應該考慮是否持有比特幣。由於比特幣市場價值的飆升，讓它看起來像是無腦式的投資，但仔細研究無數的網路駭入與駭客攻擊、詐騙及安全漏洞等讓人們失去比特幣的事件，對那些覺得比特幣可以提供穩定獲利的人，都是一種警告。

如果在閱讀本書後，認為值得擁有比特幣，你的首要投資不應該是購買比特幣，而是投資時間來了解如何安全的購買、儲存和擁有比特幣。比特幣具有這種相關知識無法委外的本質特點，任何對使用這個網路感興趣的人，都無法推托個人責任，這便是進入比特幣世界所需要進行的真正投資。



## 1

## 金錢

---

**比**特幣是具有金錢功能的最新科技，提高了數位時代的技術可行性，以解決所有人類存在現實的持續難題：如何不受時空限制來移動經濟價值。為了瞭解比特幣，首先必須瞭解金錢，而為了瞭解金錢，無可避免的必須先了解金錢的功能與歷史。

一般人交易價值最簡單的方式，便是與他人交換有價值的貨物。直接交易的過程好比以物易物，但這只能在小範圍裡的少許貨物與服務下進行。在假設人數不多，與世隔絕的小型經濟體內，並沒有太多關於特定化或交易的相關研究。而對個人來進行推敲，如此交換的可能都是最基本的生存需求物，並且是直接彼此交換的行為。「以物易物」一直存在人類社會中，延續至今日。不過這種方式相當不實際，而且通常會發生在限定情況下，例如經常是彼此高度熟識的情況裡才會發生。

而在更精細、更大型的經濟體下，個人的機會開始來臨，可以專門製作更多產品，並與更多人進行交易。這些交易對象跟他們本身並沒有

關聯，也就是如果持續對貨物、服務或喜好加以記錄，是非常不切實際的那種「陌生人」的交易。市場愈大，專門化與交易的機會便增加，不過在需求考量上的問題也會變得更大，因為你所想要的貨物提供者，並不一定想要你所能提供的貨物。

這個問題要比不同貨物的不同需求來得更複雜，因為這種問題要分成三個不同層面。

首先，在規模上並不會剛好相符：你想要的貨物並非等值於你手中的貨物，將這些貨物分割成較小的單位可能並不實際。你可以想像賣鞋的人想買房子，不可能因為一雙鞋的價值而只買到房子的一小部份，屋主也不可能想收下與房子等值的一大堆鞋子作為交換。其次，在時間框架下，也常缺乏價值剛好等同的機會：你想售出的貨物可能是易腐敗的農產品，而想買的貨物則是較耐久且價格較高，因此很難真的累積這些易腐敗的貨物，直到足夠跟耐久性貨物等值交易的時刻。例如你很難累積到足夠多的蘋果，一次性的拿去換一部汽車，因為在交易之前，可能大部分蘋果就會腐爛掉。第三，地點也缺乏剛好相等的可能性：你可能想在甲地賣房子，卻想在乙地買房子，而房子並無法搬移（正常情況下）。以上三種問題都讓「直接交易」變得非常不切實際，其結果就是人們需要求助於能夠呈現更多層面的交易，以便符合他們的經濟需求。

以物易物唯一可行的場合は透過「非直接交易」：你試著找出其他人想要的其他貨物，並且找到肯拿該貨物與你欲售貨物交換的人。這類中間商品便是交易的媒介，而由於任何貨物均可當作交易媒介，因此當經濟範圍與規模擴大時，為自己想交換貨物的交易方，持續尋找他想要的不同貨物供應商來交換，就會變成非常不切實際的作法，因為你可能要做成多筆不同交易，才能買到自己想要交換的貨物。

更為有效的解決方法很自然的出現，只要交易機會越大，便會比交易機會小的方案更具生產力：使用交易的單一媒介（或少量媒介），吸引大家以自己的貨物來交易。這種大家廣為接受的交易媒介便稱為「錢」。

金錢定義的典型功能便是作為「交易媒介」。換句話說，這是一種非消費（商品）購買的貨物，也與其他貨物（投資或資本型商品）的生產行為無關，但主要的用途是拿來交換其他貨物。而「投資」也就是為了產生收入以便交換其他的貨物，這點跟金錢也有三種不同層面：首先，投資會提供回報，而一般金錢交易並不提供；其次，投資總是與失敗風險相互關聯，金錢則有最小的交易風險；第三，投資的流通性比金錢來得小，若要動用通常需要一大筆交易費用。這點可以幫助我們了解為何人類一直有金錢需求的存在，而手上握有的投資，並無法完全取代金錢。人類的生活天生就帶著不確定性，也永遠無法確定自己到底會需要用到多少錢<sup>註1</sup>。

因此在常識與幾乎所有人類文明的古老智慧下，都會告訴我們應該把自己的部分財富，以金錢的價值形式儲存起來，因為這是持有財務最靈活的方式，可以在必要的時候讓持有者快速清算資產，而且比較起其他投資工具來說，這是風險最小的持有方式。而方便持有金錢的代價，則是來自放棄金錢可能帶來的消費，也放棄了可能因投資而帶來的回報。

就市場狀況下檢視人們的這類選擇，奧地利經濟學派之父以及經濟學邊際分析的創始人門格爾（Carl Menger），得到一個貨物可以如同貨幣在

---

註1 詳見 Ludwig von Mises（路德維希·馮·米塞斯）所著「*Human Action*（人類行為）」一書第250頁。關於未來的「不確定性」，便是持有貨幣的主要驅動元素。如果對未來可以確定的話，人們便會事先知道所有的收入與支出，並加以理想化的擬訂計劃，而不必保留任何現金。然而不確定性是生活裡必然的一部份，因此人們必須在手裡握著錢，以便在無法預知未來的情況下花錢。

市場上被廣泛採用的關鍵性理解，也就是「可銷售性」：貨物越容易依持有者所需在市場上販售，而且價格損失最低者。<sup>註2</sup>

並沒有什麼原則規定哪種商品可以當作金錢來使用。一般人想買什麼東西並非靠運氣，而是帶有目標的交換某種東西，因而可以在實質上使用金錢。由於不同人有不同的意見、選擇，因而延續了金錢的使用。從人類歷史來看，許多東西都曾被當作金錢的用途：黃金、白銀最明顯常見，但也有使用銅、貝殼、大石頭、鹽、牲畜、政府文件、貴重礦石，甚至在特定場所還用酒與煙來當錢。人類的選擇是主觀性的，也就是選什麼當錢並沒有「對」與「錯」，但這些選擇會產生不同的影響。

商品的相對流通性，可以依據其所帶來的「問題」解決能力加以評估，也就是針對之前所提過「缺乏需求巧合性」問題的三個面向：亦即跨規模（大小數量）、跨空間、跨時間。可以跨規模流通的貨物，就可以方便的分成小單位或群組成較大單位，讓貨物擁有者依想要的數量加以販售。而跨空間的流通性代表當人們旅行時，較方便運送該貨物或隨身攜帶，這也讓好的金錢媒介通常在每單位重量上，可以具有較高的價值。這兩種特性對各種可以當作錢的貨物來說，並不難辦到。但第三種要件：跨時間的流通性，則最具決定性。

貨物得以跨時間流通，跟它是否可在未來保有價值的能力有關，亦即可讓持有者將財富儲存於其中，也就是金錢的第二項功能：儲存價值。要能讓貨物跨時間流通，便須具有不會腐爛、腐蝕或其他類型被惡化的能力。我們大概可以說任何想以漁獲、蘋果或橘子作為長期儲存財富標的者，將得到痛苦的教訓，而且可能一時半刻還察覺不出這樣儲存財富應擔

---

註2 Carl Menger 所著「貨幣的起源（On the Origins of Money）」，經濟學報第二卷（1892）：239–255 頁，C. A. Foley 譯。



心之處。跨時間的物理完整性雖然是必需的，但卻是跨時間流通的非必要條件，因為貨物即使在物理條件上並未有所減損，其價值仍有可能大幅下跌。

為了保存貨物本身的價值，在貨主持有貨物期間，也不能發生貨物大量增加供應的情況。做為金錢運用的形式在歷史上的通性之一，便是會使用某種機制來限制貨物新單位的生產，以維持現有貨物單位的價值。生產新貨幣單位的相對難度，決定了貨幣的強度：難以增加供給的貨幣被稱為**強勢貨幣**（*hard money*、硬通貨），而供應量可以大幅增加的則是**寬鬆貨幣**（*easy money*、軟通貨）。

我們可以透過兩種貨物的不同供應量，來了解當成貨幣時的「硬度」：（1）**庫存**，亦即現有的供應量，包括過去生產的所有物品，減去已消耗或銷毀的所有物品；以及（2）**流量**，這是在下一個時段所將進行的額外生產。庫存與流量之間的比值，便可代表貨物作為金錢的「硬度」，以及它作為貨幣的角色是否適當。「庫存流量比」低的貨物，便是在人們將之作為儲存價值用途時，會大量的增加供應。這類貨物在被作為儲存價值的用途時，不太可能維持住它的價值。而「庫存流量比」高的貨物，其貨物比較可能在一段時間後仍維持其價值，也就是經歷時間考驗下，依舊能保持可銷售性<sup>註3</sup>。

若人們選擇具有高庫存流量比的硬通貨作為價值儲存時，他們購買來儲存的行為會增加貨物的需求，使其價格上漲，如此便會激勵生產者加速供應該貨物。但由於其流量相對於現有供應仍屬少量，即使新生產貨物大量增加，也不會顯著的壓抑其價格。另一方面，如果人們選擇以低庫存流量比的軟通貨來儲存財富時，其生產者便會創造大量的貨物而導致價格遽

---

註3 Antal Fekete, 「金子到哪去？（*Whither Gold?*）」（1997），1996 國際貨幣獎得主，Bank Lips 贊助。

降，讓貨物貶值，瞬間剝奪儲蓄者的財富，並且隨著時間推移摧毀貨物的可銷售性。

我喜歡把這種情況稱為「軟通貨陷阱」：任何被用來儲存價值的商品都會被增加供應。而任何容易被大量增加供應的商品，將會摧毀用它來儲存價值當做財富的那些人。

這個陷阱的必然結果便是任何成功作為貨幣的東西，都會有一些自然或人為的機制來限制商品進入市場的新流量，而且隨著時間經過仍保持其價值。因此，任何擔任貨幣角色的東西，其生產成本必須高昂，否則容易讓人產生賺錢的誘惑，因而會破壞儲戶的財富，讓想以這種媒介儲蓄的人打消念頭。

每當一種自然產生、技術性或政治發展而導致貨幣商品的新供應迅速增加時，商品便會失去其貨幣地位，並被其他具有高庫存流量比、也更為可靠的交換媒介所取代，這點我們會在下一章加以探討。貝殼被拿來當作錢，因為很難找到；散煙被當作監獄裡的錢，因為難以採購或生產。而作為國家貨幣時，只要供應增加的速率越低，貨幣便越可能被個人持有，並隨時間推移而能維持價值。

當現代技術讓貝殼進口與捕獲變得容易時，使用它們作為貨幣的人們，轉為使用金屬或紙幣，而當政府增加其貨幣供應時，公民便轉向持有外幣、黃金或其他更可靠的貨幣資產。二十世紀很遺憾的提供了大量這類悲慘案例，尤其是在發展中國家。存活時間最長的貨幣媒介，便是那些擁有相當可靠的限制供應增加機制的媒介，換句話說就是「硬通貨」。貨幣媒介之間的競爭始終存在，我們可以透過不同競爭對手在庫存流量比的技術影響，預知其競爭結果，這點將會在下一章進行論證。

雖然人們可以自由使用喜歡的任何商品作為交換媒介，但事實上隨時間演進，使用「硬錢」的人將獲益最多，因為其交易媒介的新流量微乎其微，價值甚少減損。而那些選擇「軟錢」的人，非常可能因為供應成長迅速而失去價值，從而減低了市場價格。無論透過前瞻性的理性計算或現實教訓的慘痛回顧，都可看出大部分的金錢和財富，將會集中在選擇最硬與最暢銷貨幣形式的人。

然而商品本身的「硬度」和「可銷售性」並不會在時間裡停滯。由於不同社會和時代的技術能力都有所差異，各種貨幣形式的「硬度」與「可銷售性」也隨之變化。事實上，選擇最佳貨幣的因素，取決於社會在塑造不同商品可銷售性的技術現實。因此，奧地利經濟學家在他們對於「聲錢（健全貨幣）」的定義裡，並非站在教條主義或客觀主義者的立場，來將它們定義為特定的貨物或商品。他們的定義是交易者在市場上自由選擇的任何一種貨幣，並非透過強制性的權威規定貨幣，同時貨幣的價值也需透過市場交易，而非由政府強制決定<sup>註4</sup>。自由市場貨幣競爭在產生可靠貨幣方面無情且有效，因為它只允許那些選對合適貨幣的人，能夠長期維持可觀的財富。政府沒有必要把最硬的錢強加給社會；社會在政府產生之前就會自行發現，任何政府想達成金錢效果的強制行為，都只會阻礙貨幣競爭的進程。

硬錢與軟錢對個人和社會的全部影響，遠超過單純的經濟損失或收益，這是本書的核心主題，我們會在後面的第5、6、7章詳加討論。而那些能夠以良好的儲存價值儲蓄財富的人，可能會比那些儲存價值不良的人，更懂得規劃未來。貨幣媒介的穩健性，亦即其隨時間保持價值的能

---

註4 Joseph Salerno 著，「聲錢與非聲錢（*Money: Sound and Unsound*）」，路德維希·馮·米塞斯研究所，2010年，第xiv至xv頁。

力，便是重視現在勝過未來的人或對長時間儲存有偏好的人，到底佔多數或者少數的決定性因素，而這也是本書裡的關鍵概念。

除了庫存流量比之外，貨幣媒介可銷售性的另一個重點便是「接受度」。接受該貨幣媒介的人越多，流通性就越高，買賣的價損也更可能減少。如同一般電腦網路協議所證明，在具有許多點對點交易的社交環境中，產生一些標準來支配交易是很正常的，因為加入交易網路的收益，會隨網路規模擴大而呈指數成長。因此，當數百個幾乎相同的網路創建和推廣後，Facebook 以及幾個社群媒體網路便佔據了市場的主導地位。

同樣的，任何發送電子郵件的設備，都必須使用 IMAP / POP3 協議來接收電子郵件，並使用 SMTP 協議發送電子郵件。雖然還有許多可以使用良好的協議被發明出來，但幾乎沒有人用，因為大家的郵件都是在 IMAP / POP3 和 SMTP 上，一旦用了其他協議，恐怕就會妨礙與所有人的電子郵件交流。同樣的，就錢的觀點看，不可避免的會有一個或數個商品成為主要交換媒介，因為財產「容易交換」的特性至關緊要。如前所述，交換媒介並非為了取得財產，而是為了它的可銷售性。

此外，廣為接受的交換媒介便可依其條件表達各種價格，如此便能發揮貨幣的第三個功能：記帳單位。在沒有公認交換媒介的經濟體中，每種商品必須按照各種可交換的商品來定價，導致產生大量的價格種類，難以計算。而在具有公認交換媒介的經濟體中，所有商品的所有價格均會以相同的記帳單位（該交換媒介）表示。在這種社會裡，金錢作為衡量人際價值的指標，獎勵生產者為他人貢獻價值，並向消費者表明需支付多少價值才能獲得他們想要的商品。只有以統一的交換媒介作為記帳單位，才能實現複雜的經濟計算，並進一步邁向更專業化的複雜任務、資本累積和擴大市場的可能性。市場經濟的運作取決於價格，而準確的價格則需取決於共同使用的交換媒介，這反映了不同商品的相對「稀有」性。若是寬鬆貨

幣，其不斷發行增加數量的能力，會阻礙它準確反映機會成本。貨幣發行數量上的每個意外變化，都會扭曲其作為衡量人際價值及經濟訊息管道的角色。

使用單一交易媒介，可使經濟規模成長到跟願意用它的人數一樣的大。而經濟規模越大，從交易和專業化所帶來的獲利機會就越大，也許更重要的是「生產結構」的週期，可以變得更長也更複雜。

生產者便可專門生產資本商品，也就是必須花更長時間才能生產出來的「終端型」消費商品，從而生產出更具產能且更優質的產品。在較原始的小型經濟體下，魚類的生產結構包括漁夫走到岸邊及徒手捕魚，整個過程從開始到結束需要幾個小時。而隨經濟發展，使用了更為複雜的工具與資本商品等，這些工具的產能大大延長了生產過程的持續時間，也提高了生產率。在現代世界裡，魚類被那些要花好幾年建造，而且可以運作數十年的高精密漁船捕獲。這些船能夠航行到小船無法抵達的海域，從而產出原本無法取得的漁獲。這些船也可以勇敢地抵禦惡劣天氣，並在嚴苛條件下繼續生產，而資本密集度較低的船隻在這種競爭下，只能毫無用處的停航。

隨著資本累積使這個過程變得更長，每單位勞動力的生產量能也越來越高，比起那些只具有基本工具且無資本累積的原始經濟體來說，前者可以生產出他們永遠無法實現的優質產品。若沒有金錢扮演交換媒介的角色來落實專業化、儲存價值以創造未來、鼓勵個人將資源用於投資而非消費、以及作為計算經濟損益的計算單位 ... 等，一切便不可能實現。

從貨幣演進史看，曾經有過多種不同商品扮演了金錢的角色。依據每個時代的技術能力差異，這些商品也都具有不同程度的貨幣硬度和穩健性。從貝殼到鹽、牛、銀、黃金和黃金支持的政府鈔票，直到最近幾乎都使用政府提供的法定貨幣等，每次技術的演進，都讓我們可以使用具有更

多優點的新形式貨幣，但同樣的，也會帶來新的陷阱。藉由檢視在歷史上作為金錢角色的工具與材料的歷程，就可以分辨出「好錢與壞錢」的各項特徵。唯有具備這樣的知識背景，才能進一步了解比特幣的功能以及它如何作為貨幣媒介的角色。

下一章將探討歷史上被作為金錢的各種工藝品與物品的歷史，包括雅浦島石幣、美洲的貝殼到非洲的玻璃珠，以及古代的牛和鹽等。

每種交換媒介都在某段期間發揮其作為貨幣的功能，並且擁有其人口可用的最佳庫存流量比，但在失去這項特性後便終止了。因此最重要的一點，便是從「如何」以及「為何」的角度，來理解貨幣未來的可能發展，以及比特幣將會扮演的角色。

第 3 章將轉而分析貨幣金屬，以及黃金如何成為世界主要貨幣金屬，影響整個十九世紀末的黃金標準時代。第 4 章分析了政府貨幣的轉移及其記錄。第 5、6、7 章則討論經濟和社會影響後的各種貨幣，第 8 章介紹了比特幣的發明及其貨幣特性。

## 2

## 原始貨幣

---

在我見過所有歷史上的貨幣形式裡，最類似於比特幣運作的貨幣，便是古代貨幣系統裡的雅浦島石幣（Rai stones on Yap Island），雅浦島目前隸屬於密克羅尼西亞聯邦。了解他們如何用石灰石雕刻的大圓形石頭作為金錢的用途，將有助於我們在第 8 章解釋比特幣的操作。而進一步了解雅浦島石幣如何失去其金錢角色的精彩故事，更是金錢一旦「變軟」就會失去貨幣地位的學習課題。

構成貨幣的石頭有各種尺寸，有些大到形成中間有孔以方便搬運的大圓盤，甚至可能重達 4 公噸。由於雅浦島上並無石灰岩，因此這些石幣並非島上的原生石材製成，而是從鄰近的帛琉或關島運來。這些石頭的美麗和稀有性，讓雅浦島民覺得渴望且珍貴。不過獲得這些石頭非常困難，因為要牽涉到艱苦的採石過程，還需用木筏和獨木舟加以運輸，有些石頭甚至需要動用上百人才能運抵。一旦石頭到達雅浦島後，便會被放在一個大家都可以看到的顯著位置。



擁有這種石頭的人可以用它來作為付款方式，而不必真的搬走石頭：交易的所有內容便是持有石頭者向所有村民宣布，該石頭的所有權已移轉至購買者。所有村民都會知道石頭的新擁有者是誰，他便可隨時再用此石頭來支付其他費用。而且實際上並沒有辦法偷走石頭，因為它的所有權是眾所周知的。

幾百年、甚至可能是幾千年以來，這種貨幣體系對雅浦島民來說運作良好。雖然這些石頭很難移動，但它們具有「跨越空間」的可銷售性，你可以在島上任何地方用它們進行支付，而不同尺寸的各種石幣也能提供不同規模的可銷售性，包括使用單一石頭的「局部」來進行支付的可能性。由於獲得新石頭的難度和成本相當高，因此讓幾世紀以來石幣的可銷售性得到了保障，在雅浦島上並不存在的石頭，想從帛琉採集與運送過來十分不易，因此雅浦島獲得新石頭的成成本非常高，也就意味著現有的石幣商品的供應，遠大於在一定時間內生產的任何新商品，讓它們可以很謹慎的被島民選擇做為一種付款方式。換句話說，石幣的庫存流量比非常高，無論大家多想要，都不易引進新石頭來增加供應。或者，至少到 1871 年，一位名叫大衛奧基夫（David O'Keefe）的愛爾蘭裔美國船長，在雅浦海岸遭遇船難並被當地人救起為止<sup>註 1</sup>。

奧基夫看到將島上椰子賣給椰子油生產商的獲利商機，但他無法僱請島民為他工作，因為這些當地人非常滿足於他們在熱帶天堂的美好生活，而且給他們任何外國形式的金錢也沒用。但奧基夫並不妥協，他搭船前往香港，買了一艘大船和炸藥開到帛琉，用炸藥和現代工具開採了幾塊大石頭後，揚帆前往雅浦島，向當地人獻上石頭作為椰子的貨款。

---

註 1 奧基夫的故事激起勞倫斯·克林曼和杰拉爾德·格林的寫作靈感，在 1952 年出版名為「奧基夫陛下（*His Majesty O'Keefe*）」的小說，並且在 1954 年被改編為好萊塢賣座電影，由伯特蘭卡斯特（Burt Lancaster）主演。

不過結果卻與奧基夫的預期相反，村民們並不熱衷於接收他的石頭，村長禁止村民為新石頭工作，並宣布奧基夫的石頭沒有價值，因為那些是「容易收集」的石頭。只有過去用當地人血汗採集的石頭，才能在雅浦島使用。不過其他村民並不同意，也真的為奧基夫提供了他所需要的椰子。如此造成島上的衝突，石幣作為金錢的功能也隨之喪失。如今島上的石幣比較像是作為儀式和文化的作用，而最常用的貨幣媒介也換成了目前政府的法定貨幣。

雖然奧基夫的故事具有高度象徵意義，但這只是預告了石頭的貨幣角色在現代工業文明入侵雅浦島後，將會難以避免地滅亡。隨著現代工具和工業能力的到來，石頭的生產花費一定會比以前便宜得多。也會有許多當地或外國的奧基夫，能為雅浦島提供更多的新石頭。現代技術會讓石幣的「庫存流量比」大幅下降：每年都可產出更多石幣，因此貶低了該島現有的庫存。對任何村民來說，使用這些石頭作為價值儲存變得越來越不明智，因而隨時間經過，石幣失去了可銷售性，也喪失了作為交換媒介的功能。

雖然細節或有不同，但庫存流量比下降的潛在動態，對於已經失去貨幣角色的各種貨幣都是相同的，例如本書撰寫之際的委內瑞拉玻利瓦幣暴跌亦是如此。

類似的故事還發生在西非幾世紀以來作為金錢功能的阿格雷珠（aggre beads），這些珠子在西非的來源並不完全清楚，有人認為它們是用隕石製成的，或是從埃及和腓尼基商人傳來的。唯一清楚的是在玻璃製造技術昂貴且不普遍的地區，相當珍貴，也因此讓它們具有較高的「庫存流量比」，具有經得起時間考驗的可銷售性。由於這些珠子小而珍貴，且可組成串珠、項鍊或手鐲，因而可有不同的交易規模；雖然珠子種類繁雜並非標準的交易單位，也不符合理想貨幣的定義，但由於容易移動的特性，遂讓阿格雷珠也具有跨越空間的銷售能力。

相較之下，這種玻璃珠在歐洲並不貴，而且沒有貨幣的功能，由於玻璃製造技術的精進，代表若玻璃珠被當作貨幣單位，生產者便會讓它們充斥市場——換句話說就是玻璃珠有「低庫存流量比」。

當歐洲探險家和貿易商在十六世紀訪問西非時，注意到這些珠子具有極高價值，因此開始從歐洲大量進口。接下來的過程便類似於奧基夫的故事，但由於珠子較小而人口規模更大，因此這是一個更慢、更隱蔽的過程，帶來了更大、更悲慘的後果。歐洲人肯定慢慢的買走了許多非洲寶貴的資源，因為他們帶回國的珠子少得可憐<sup>註2</sup>。歐洲人對非洲的入侵，慢慢的把阿格雷珠從硬錢變成了軟錢，破壞其可銷售性，並導致擁有這些珠子的非洲人，隨時間減損了購買力。這些輕易獲得珠子的歐洲人，轉移了財富而使非洲人變得貧窮。阿格雷珠後來也被稱為「奴隸珠」，因為它們在推動歐洲和北美人對非洲人的奴隸交易上，扮演了重要的角色。貨幣媒介價值的「一次性崩跌」是悲劇性的，但至少結束得很快，且其持有者可以用新的貨幣繼續開始交易、儲蓄和計算。但非洲這種貨幣價值隨時間緩慢流失，慢慢地將持有者的財富轉移給能以低成本生產該媒介的人，在本書的後半部分討論到政府貨幣的穩健性時，將會是值得記住的慘痛教訓。

貝殼是另一種貨幣媒介，從北美到非洲和亞洲廣泛應用於世界各地。從歷史記載看，最暢銷的貝殼通常是那些難以找到的貝殼，因為它們比容易找到的貝殼更有價值<sup>註3</sup>。

---

註2 為了將利潤極大化，歐洲人過去經常使用大量的琉璃珠壓艙，當然這也有助於船本身的航行穩定。

註3 Nick Szabo「賣出：貨幣的起源（*Shelling Out: The Origins of Money*）」，2002年，你可在<http://nakamotoinstitute.org/shelling-out/> 網址線上閱讀。

跟阿格雷珠一樣，美洲原住民和早期歐洲殖民者也廣泛使用了貝殼串珠（wampum shell、白色溝螺貝殼）：由於它們很難被找到，因此具有很高的庫存流量比，甚至可能是當時最耐用的商品。這些貝殼也與阿格雷珠一樣具有單位不統一的缺點，亦即其價格和比率，無法輕易的衡量或一致的表達出來，這點對經濟成長和專業化程度形成重大阻礙。

歐洲殖民者從 1636 年開始採用貝殼作為法定貨幣，但有越來越多的英國金、銀幣開始流入北美，由於其一致性較適合當做交換媒介，也可提供更好、更統一的價格面額，因而具有較高的可銷售性。此外，隨著更先進的船隻和技術被用於海上捕獲貝殼，因此它們的供應高度膨脹，導致其價值降低，並且隨著時間推移而喪失可銷售性。1661 年時，貝殼停止作為法定貨幣，無法繼續扮演貨幣的角色<sup>註 4</sup>。

這不僅是北美貝殼貨幣的命運；只要使用貝殼的社會獲得規格化的金屬貨幣時，他們就會加以採用，並從這樣的轉換中獲益。同時，工業文明到來後，以化石燃料為動力的船隻，更容易在海洋裡獲取貝殼，因而增加了生產流量並迅速降低其庫存流量比。

其他古老的金錢形式包括牛，營養價值珍貴，因而成為任何人可擁有的最珍貴的財產之一。而牛易於移動的特性，讓它也具備了跨空間銷售的能力。牛隻在今日依舊繼續扮演著貨幣的作用，許多社會仍將它們用於支付，尤其是當成嫁妝之用。然而體積龐大不易分割，代表牛隻較難解決跨規模分割銷售的問題，因此另一種形式的貨幣與牛隻並存，那就是鹽。鹽可以保存很長一段時間，也很容易分裝成任何需要的重量。

---

註 4 Ibid。

這些史實在英語中仍可見到，因為「金錢 (*pecuniary*)」這個詞來自 *pecus*，亦即拉丁語中的「牛」，而「薪水 (*salary*)」這個詞則源自 *sal*，也就是拉丁語中的「鹽」。<sup>註5</sup>

隨著技術的進步，尤其是冶金技術的發展，人類為這些舊交換媒介開發出更優越的貨幣形式，並開始快速的進行取代。這些金屬比起貝殼、石頭、珠子、牛與鹽，顯然是更好的交換媒介，因為它們可以製成一致性、具有高度價值的小單位，而且更容易四處移動。

將舊交換媒介封棺埋葬的另一根釘子，則來自大量使用碳氫化合物燃料的能量，顯著的提高了生產能力，並快速增加這些媒介的新供應（流量），亦即依賴生產難度來保護高「庫存流量比」的貨幣形式難以持續。現代燃料的動能可以輕鬆的開採石幣，也可以非常低的成本製造阿格雷珠，較大的船隻也能快速的收集貝殼。這些錢一旦失去硬度，其持有人便被大量的掠取財富，整體社會結構也因此崩潰。拒絕奧基夫便宜石幣的雅浦島酋長，了解大多數現代經濟學家都無法理解的東西：容易生產的貨幣根本就不值錢，而寬鬆貨幣並不會使社會更富裕；相反地，將所有得來不易的財富換取容易生產的東西，只會變得更加貧窮。

---

註5 Antal Fekete，「金子到哪去？ (*Whither Gold?*)」，1997年。1996國際貨幣獎得主，Bank Lips贊助。

## 3

## 貨幣金屬

---

隨著人類越來越精通生產商品的技術能力，對金屬和日用品的使用也逐漸成長，許多金屬開始大量生產，需求也變得夠大，讓這些金屬具有高度可銷售性，很適合用來作為貨幣媒介。這些金屬的高密度與高價值，比鹽或牛更容易移動，因此可以跨越空間大量暢銷。最初的金屬生產並不容易，很難快速增加供應而提供了跨越時間的良好銷售性。

由於金屬的耐久和物理特性，加上它們在地球上的相對蘊藏量有所不同，因此某些金屬會比其他金屬更有價值。鐵和銅由於相對高的蘊藏量與和抗鏽蝕的能力，可以大幅增加產量。新產品將使現有庫存相形見绌，因而破壞價值。但這些金屬的市場價值相對較低，可以適用於較小的交易。另一方面，貴金屬如銀和金更為耐用，也更不易腐蝕或破壞，因此可跨越時間增加可銷售性，並有助於作為未來的價值儲存。特別是黃金象徵的堅不可摧特性，可以代代相傳儲存價值，因而使我們能夠做更長期的規劃。

最初金屬是按重量進行買賣<sup>註1</sup>，但隨著時間與冶金技術的演進，已經可以把金屬製成均勻的錢幣，然後在上面標記重量。大家無需再花時間秤重或估價，金屬也因此更為暢銷。最被廣泛使用的三種金屬是金、銀和銅，最早的紀錄遠從希臘國王克羅伊斯（Croesus）的時代開始到二十世紀初，這種以錢幣作為主要貨幣形式的歷史，大約已經有 2500 年。金幣是跨越時間下最暢銷的商品，因為經歷時間演變都還能保值與防腐、抗鏽蝕。同時它們也是跨越空間的暢銷商品，因為體積重量小而方便運送。銀幣的優勢則是具有跨越規模暢銷的優點，因為與黃金相比，銀的每單位重量價值較低，可以方便地作為小額交易的交換媒介，銅幣則可用在價值最低的交易上。

透過將價值標準化為容易辨別的單位，錢幣便可推動大型市場的建立，增加全球專業化和貿易的範圍。雖然是當時技術上可行的最佳貨幣體系，但仍有兩個主要缺點：第一點是以兩三種金屬作為貨幣標準時，由於供需起伏的原因，其價值會隨時間波動而產生經濟方面的問題，也為這些錢幣的擁有者製造禍端。尤其是銀，因為產量增加和需求下降，銀幣的價值也會隨之下降。第二個更嚴重的缺點，便是政府與偽幣製造者常會做的，減少錢幣裡的貴金屬含量，也就是將部分購買力轉移給偽幣製造者或政府，而降低了金屬的價值。硬幣金屬含量減少，會減損貨幣的純度與穩健性。

然而到了十九世紀，隨著現代銀行業的發展和溝通方式的改進，人們可以使用由一般銀行和中央銀行金庫裡的黃金所支持的現鈔與支票進行交易。這就可以讓黃金支持的交易在任意大小規模上實現，減低對白銀作為次要貨幣角色的需求，並在黃金標準下獲取所有貨幣必需的可銷售性。

---

註1 Nick Szabo，「賣出：貨幣的起源（*Shelling Out: The Origins of Money.*）」，2002 年。你可在 <http://nakamotoinstitute.org/shelling-out/> 網址線上閱讀。

黃金標準藉由將地球上大部分經濟體與基於市場選擇的良好貨幣結合起來，因而產生了前所未有的全球資本累積與世界貿易。然而它的悲劇性缺陷便是將黃金集中在銀行和後來的中央銀行金庫後，銀行和政府便有機會以超過其持有的黃金數量，增加法定貨幣的供應量，讓貨幣貶值，同時也讓貨幣的部分價值，從其合法的持有人轉移到政府和銀行手中。

## 為何選擇黃金？

為了理解商品貨幣的出現，我們必須更仔細地回到在第 1 章介紹過的寬鬆貨幣陷阱，並且要先區分商品的市場需求（商品消費或自願持有商品的需求）以及貨幣需求（作為交換媒介和儲存價值的需求）。每當有人選擇某種商品作為價值儲存時，便是在以超出正常市場的需求來有效地增添此商品需求，因而導致商品價格上漲。舉例來說，各種工業用途的銅市場需求量約為每年 2000 萬噸，其價格約為每噸 5,000 美元，因此總市值約為 1000 億美元。請想像一下，如果有位億萬富翁決定把等值於 100 億美元的銅儲存起來，當他的銀行專員們四處試著採購全球銅礦年產量的 10% 時，必然會導致銅價的上漲。雖然一開始看起來像是億萬富翁自己的理財策略而已，但當他決定購買資產時，就已經會讓銅礦在完成購買之前大幅升值。當然，他也可能是因為這樣的升值，會導致更多人買更多銅作為儲蓄，讓銅價也因而上漲。

但即使有更多人加入這個將銅貨幣化的行列，我們所假設的這位痴迷於銅的億萬富翁，也將陷入困境。因為價格的上漲，讓銅成為全球工人和資本家都認為是利可圖的一門生意。而我們並無法確實測量地底下的銅礦蘊藏量，更別說還要採礦與提煉，因此事實上，銅的生產數量唯一的約束力，便是到底有多少勞動力和資本投入其中。更多的銅要靠更高的成本



來生產，於是價格和產出數量將繼續上升，直到滿足貨幣投資者的需求為止；我們假設額外增加 1000 萬噸的銅，每噸要 10,000 美元。而在某個時刻，貨幣需求必定會平息，某些銅持有者會想要釋出部分庫存來購買其他商品，因為畢竟這是他們購買銅的原因。

貨幣需求平息之後，在其他條件相同的情況下，銅市場將恢復其原有的供需狀況，也就是每年需求量 2000 萬噸，每噸售價 5,000 美元的銅。但當持有者開始出售累積的銅庫存時，便會大幅下跌低於此價格。億萬富翁也將在這個過程裡虧損；因為他當時推高了銅的價格，所以後來是以每噸超過 5000 美元的價格，購買了他的大部分庫存，但現在他的所有庫存價值低於每噸 5000 美元。後來加入的人甚至是以更高的價格購買，因此也將比億萬富翁本人損失更多。

這個模型適用於所有消耗品，例如銅、鋅、鎳、黃銅或石油，因為它們主要是作為消費與消耗用途，而非庫存之用。這些商品的全球庫存在任何時刻，大致都與新的年產量相同。新的供應也會持續生產，以供消費。如果儲蓄者決定將財富儲存在這種商品中，在價格上漲到足以吸納所有投資之前，儲蓄者們的財富只能買到商品全球供應量裡的一小部分，因為他們正在跟那些可以有效在行業裡運用這種商品的消費者相互競爭。而在商品生產者的收入增加後，他們便可投資以增加產量，於是商品價格再次崩跌，從而剝奪儲蓄者的財富。整個事件的淨效應便是做出錯誤決定的儲蓄者，把財富轉移給他們所購買商品的生產者了。

這便是對「市場泡沫」的剖析：需求增加會導致價格急遽上漲，因而更增加需求，也進一步抬高了價格，然後會帶動商品產量增加與供應增加，當然不可避免地導致價格下跌，等於懲罰了那些以高於市場價格購買的人。泡沫裡的資產「投資者」被掠奪、「生產者」則獲益。對於銅以及幾乎世界上的所有商品而言，這種波動在歷史記載裡大多如此，會一直透過

財富貶值與長期貧困來懲罰選擇把這些商品作為貨幣的人，然後商品便回歸其作為市場商品的本性，而非作為交換媒介。

任何可以良好儲存價值的東西，必須能擊敗這個陷阱：當人們以它作為價值儲存時，它必須可以升值，但它的生產者也必須受到限制，不可以增加太多供應量而使價格降低。這樣的資產才能獎勵那些將它當做價值儲存的人，而這些把它做為主要價值儲蓄的人，從長遠來看可以增加財富。因為選擇其他商品的人，若不把財富移轉過來複製此成功路徑，就會失去他們的財富。

就整個人類歷史上看，這場比賽顯然是由黃金獲勝，因為兩種獨特的物理特性，使黃金能與其他商品區隔開來，保有其貨幣角色：首先，黃金在化學上相當穩定，幾乎不能被銷毀。其次，黃金無法從其他材料中合成（儘管煉金術士們說可以），並且只能從原礦石中提煉，這點在地球上極為罕見。

黃金的化學穩定性，意味著幾乎所有人類開採出來的黃金，或多或少的仍被世界各地的人所擁有。人類以珠寶、金幣和金條的形式，累積了越來越多的黃金。這些黃金從未被消費過，也不會生鏽或消解掉。而無法從其他化合物裡提煉黃金，代表增加黃金供應的唯一途徑便是從地下開採黃金。這是一種昂貴、具有毒性、且無法確定會採到的過程。人類已開採黃金數千年，而其回報率不斷的下降，代表世界各地人民所持有的黃金儲備，累積自幾千年來的黃金生產，因此比每年的新產量要大上好幾個級數。過去七十年裡，從相對可靠的統計數據來看，黃金在年度存貨的成長率一直在 1.5% 左右，從未超過 2%（見圖 1<sup>註 2</sup>）。

---

註 2 資料來源：美國地質調查局。

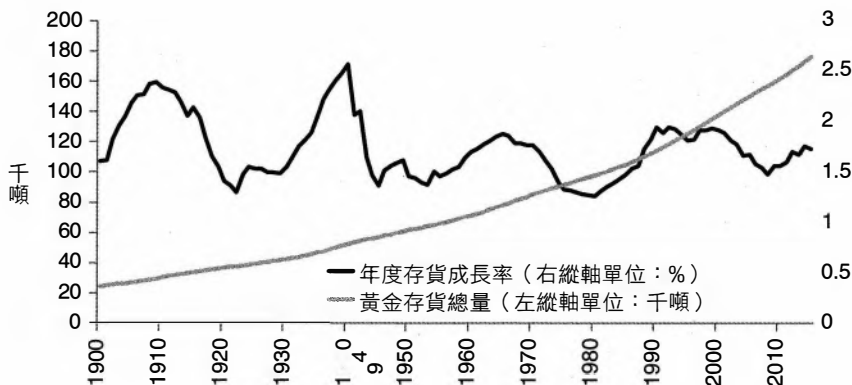


圖 1 全球黃金存貨與年度存貨成長率

為了解黃金與其他消費商品之間的差異，請想像一下對黃金作為價值儲存有大量需求時的影響，例如導致價格飆升且年產量增加一倍。這種情況對任何消費商品來說，產量增加一倍會使任何現有庫存相形見绌，從而導致價格崩跌並危及持有者的財富。然而對於黃金而言，這種導致年產量翻倍的價格飆升是微不足道的，因為產量增加 1.5% 而庫存增加就會變為每年 3%。新的生產節奏保持不變，庫存卻成長更快，因此新增加的增幅也微乎其微。實際上對於金礦業者來說，不太可能開採大量的黃金來大幅壓低價格。

只有白銀在這方面近似於黃金，其年供應成長率在歷史上約為 5-10%，目前大約上升至 20% 左右。會比黃金高有兩個因素：第一點是白銀會腐蝕，也會運用在工業上，亦即現有庫存相對於年產量而言，並不像黃金庫存相對於其年產量那麼大。其次，銀在地殼中的蘊藏量比黃金大，也更容易提煉。

由於具有第二高的庫存流量比，且每單位重量的價值低於黃金，因此幾千年來，白銀都是作為價值較小交易上的主要貨幣服務，因為將高價的黃金分成較小單位並不實用。以國際黃金標準支持的紙鈔，更能以任何規

模進行交易，白銀的貨幣角色也因此消失，本章稍後將會對此進行更詳細的討論。由於小型交易不再需要白銀，因此它很快就失去了貨幣角色，而成為工業用的金屬，與黃金價值相比也更下跌。白銀本來可以保持其第二名的貨幣地位，但隨著十九世紀的技術發展，讓支付本身可以不必真的移動貨幣單位，因此雖然在貨幣競爭中是第二名，但也等於是失敗。

這就解釋了為何白銀泡沫以前就發生過，如果再次發生還是會面臨破滅的命運：一旦大量的貨幣投資流入白銀，生產商可以大幅增加供應並使價格崩跌，讓儲存白銀者的財富也跟著下跌。在所有商品中最為人知的弱勢貨幣陷阱，便來自白銀本身。早在 70 年代末期，非常有錢的亨特家族兄弟決定重現白銀的貨幣化，開始大量購買白銀使其價格上漲。他們的理由是，隨著價格上漲，會有更多人想買白銀，然後價格便會更高，導致人們會更想用白銀進行支付。然而，無論亨特兄弟買了多少，他們的財富都無法與銀礦業者和白銀持有者持續向市場售出白銀的能力相提並論。最後，白銀的價格崩跌了，亨特兄弟損失了 10 多億美元，這可能是歷史上了解「庫存流量比」重要性最貴的一課，讓你學到並非所有閃閃發亮的東西都是黃金<sup>註3</sup>（見圖 2<sup>註4</sup>）。

也正是這種「始終如一」的低黃金供應率，讓它能維持在整個人類歷史裡，扮演貨幣角色的根本原因，由於各國中央銀行繼續持有大量黃金以保護其紙鈔貨幣，因此黃金得以在今日繼續扮演其角色。官方中央銀行黃金儲備約為 33,000 噸，約佔已開採黃金總量的六分之一。

---

註 3 「白銀狂熱後的鉅額帳單（Big Bill for a Bullion Binge）」，時代雜誌，1989 年 8 月 29 日。

註 4 資料來源：美國地質調查局黃金資料、世界白銀協會資料、BP 英國石油統計資料、作者收集自各種媒體來源的銅資料。

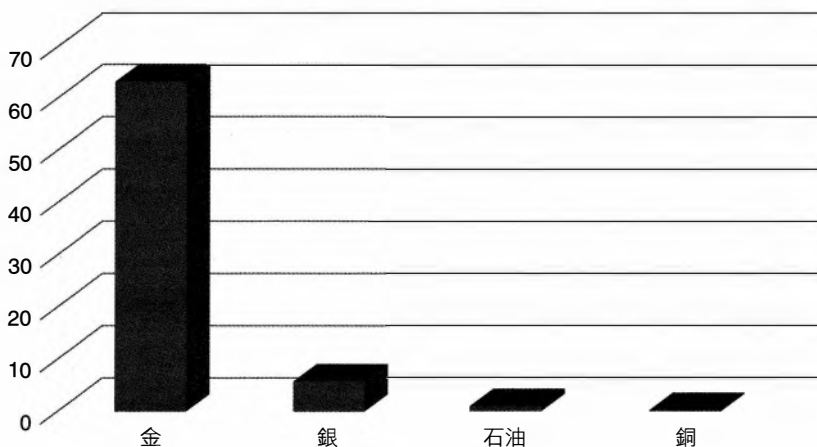


圖 2 現有庫存相對於每年生產量的倍數

黃金的高「庫存流量比」，讓它成為「供應價格」彈性最低的商品，因此黃金供應量所增加的百分比，會隨著黃金價格上揚而增加。由於世界各地人民現有的黃金供應量是累積數千年的產物，若價格上漲  $X\%$ ，雖然會導致新的採礦產量增加，但這些增加的量比起現有庫存，仍顯得微不足道。例如，2006 年黃金現貨價格上漲了 36%，若發生在其他商品上，應該會大量增加採礦產量來填補市場需求並降低價格。不過相反的，2006 年的黃金年產量為 2,370 噸，還比 2005 年減少 100 噸，到 2007 年又再減產了 10 噸。而 2005 年新增供應量為現有庫存的 1.67%，在 2006 年是現有庫存的 1.58%、2007 年則是 1.54%。即使價格上漲 35% 也不會導致新的黃金供應量明顯增加。根據美國地質調查局的數據，單年產量增加最高的是 1923 年的約 15%，而庫存增加幅度僅為 1.5% 左右。即使產量增加一倍，庫存可能也只會增加 3-4% 左右。全球「庫存」年增率最高的是 1940 年，當時庫存增加了約 2.6%。正常年度庫存成長率不會超過這個數字，而且自 1942 年以來從不曾超過 2%。

在金屬產量開始激增後，中國、印度和埃及等古代文明開始使用銅，然後用銀作為金錢，因為這兩者在當時較難製造，而且具有跨越時間空間的良好可銷售性。雖然黃金在這些文明裡備受推崇，但其稀有性便代表交易的可銷售性會受到限制。最早將黃金鑄造成一般的貿易用幣，是在現代文明發源地希臘的克羅伊斯國王統治時期。全球貿易的活躍，把黃金的吸引力散佈全球，讓金幣廣泛地傳播應用。自此人類歷史的每個轉折，便與貨幣的穩健性息息相關。人類文明在廣泛採用健全貨幣的時代與地區蓬勃發展，而不健全的貨幣則往往會帶來文明的衰落與社會的崩潰。

## 羅馬的黃金時代與沒落

迪納厄斯（denarius）是羅馬共和國時期交易用的銀幣，內含 3.9 克白銀。當時世界文明地區最有價值的錢是金幣，也更為普遍。羅馬共和國最後一位獨裁者凱撒大帝（Julius Caesar），創造了奧里烏斯（aureus）硬幣，約含 8 克的黃金，在歐洲和地中海廣為通用，等於在舊世界裡，增加了貿易與專業化的新範疇。即使有凱撒大帝暗殺事件的政治動盪，經濟依舊穩定了 75 年，共和國也在繼任者奧古斯都統治下，轉變成為羅馬帝國。一直持續到惡名昭彰的尼祿統治時期，他是第一個與羅馬「剪幣」陋習（修剪硬幣邊緣，便可在擁有相同幣值下，多出許多金銀原料）相關的皇帝，也就是皇帝徵收居民的硬幣，將它們鑄成純量較低的金幣或銀幣。

只要羅馬能夠持續征服擁有巨額財富的新土地，皇帝和士兵就可以享受這些戰利品。皇帝還可以強制降低糧食與其他主食的價格來收買人心，有時甚至會免費贈與。所以許多農民便不想再過農耕生活，離開鄉下搬到羅馬，因為可以免費過上更好的生活。日換星移，舊世界已沒有更多富饒土地可供征服，然而不斷成長的奢華生活與不停增加的軍隊，都需要新的

財源。而活在皇帝的慷慨與價格抑制下，不事生產的公民數量持續增加。西元 54-68 年在位的尼祿皇帝，終於找到解決問題的方法，而且是跟凱因斯在第一次世界大戰後，針對英美經濟問題的解決方法高度類似：亦即將貨幣貶值可立即降低工人的實質工資，減輕政府補貼主食的負擔，並可為政府其他經費提供更多資金。

奧里烏斯（aureus）銀幣的重量從 8 克減到 7.2 克，而銀的含量則從 3.9 減到 3.41 克。如此國家財政得到暫時的緩解，但已造成高度破壞性的惡性循環：民情憤怒、管制價格、硬幣貶值和價格上揚等，像可預測的四季嬗遞一樣，一個接一個來到<sup>註 5</sup>。

在卡拉卡拉統治時期（西元 211-217 年），金的含量減少到 6.5 克，在戴克里先統治（西元 284-305 年）下，進一步減少到 5.5 克，然後他推出了蘇勒德斯（solidus）的替代金幣，只含 4.5 克黃金。在戴克里先的監管下，發行的銀幣竟只有銀色的痕跡蓋住青銅，而銀色的部分會隨磨損迅速消失，因此最後迪納厄斯（denarius）也無法再作為銀幣使用。由於通貨膨脹在第三和第四世紀愈演愈烈，隨之而來的是皇帝為掩飾通貨膨脹的錯誤，下令對基本商品實行價格管制。由於市場力量試圖調高價格來回應貨幣的貶值，而控制價格會限制調高價格，讓生產商即使生產商品也無利可圖。所以經濟生產便停滯不前，直到有新的法令允許價格自由調漲為止。

隨著貨幣價值的下跌，羅馬帝國終結衰敗的漫長過程，形成了現代讀者可能已經很熟悉的週期：

剪幣會貶低奧里烏斯（aureus）銀幣的實際價值，增加貨幣供給則讓皇帝持續超支濫用，但最導致通貨膨脹和經濟危機的終極原因，其實是病

---

註 5 詳見 Schuettinger 與 Butler 合著，具高度娛樂性的《Forty Centuries of Wage and Price Controls》（四千年的工資與價格控制）一書。

急亂投醫的皇帝，試圖透過更多的剪幣作法來改善財政。Ferdinand Lips（費迪南德·利普斯）記錄此一過程，為現代讀者上了這堂課：

現代凱因斯主義經濟學家與當代投資者應當很感興趣，雖然羅馬皇帝們瘋狂地想要「管理」他們的經濟，但他們唯一成功的，就是讓事情變得更糟糕。價格與工資受到控制以及用法律規範貨幣，就像試圖阻擋潮汐一樣的不可行。暴動、腐敗、無法無天以及投機賭博的盲目狂熱，更像瘟疫一樣吞沒了帝國。由於金錢變得如此不可靠且狂貶，因此大宗商品的投機行為，將會變得比製作生產更具吸引力<sup>註6</sup>。

這些行為對羅馬帝國帶來毀滅性的長期影響。雖然一直到公元二世紀的羅馬，可能都還不算成熟的「自由市場資本主義」經濟，因為羅馬政府對經濟活動仍有許多限制，但是奧里烏斯（aureus）銀幣，依舊建立出當時人類歷史上最大的市場經濟，也成就了世界上規模最大、最具成效的勞動分工<sup>註7</sup>）。羅馬公民和主要城市，透過與帝國遙遠角落的貿易，獲得了基本的生活必需品。這點有助於解釋繁榮成長後，面臨勞動分工瓦解，帝國所遭受的毀滅性崩潰。稅收增加和通貨膨脹讓「控制價格」的作法行不通，城市居民開始逃往空無一物的田地，因為那裡至少有機會可以自給自足的生活，而且因為收入不足也不必繳稅。羅馬帝國錯綜複雜的文明殿堂，以及整個歐洲和地中海的大規模勞動分工，開始崩潰。這些勞工的後裔各自獨立，成為自給自足的農民，但不久後也變成生活在封建領主下的農奴。

---

註6 Ferdinand Lips，「黃金戰爭：從瑞士觀點看反對健全貨幣的鬥爭（*Gold Wars: The Battle Against Sound Money as Seen from a Swiss Perspective*）」，紐約：貨幣教育促進基金會，2001年。

註7 Ludwig von Mises，「人類行為：學者版（*Human Action: The Scholar's Edition*）」，路德維希·馮·米塞斯研究所，1998年。



## 拜占庭與拜占庭金幣

戴克里先（Diocletian）皇帝的名字，永遠會跟財政和貨幣計謀擺在一起，因為他的統治讓帝國陷入深淵。在他退位一年後，君士坦丁大帝接手管理帝國的責任，在經濟上採取負責的政策與改革來扭轉劣勢。君士坦丁是第一位基督教皇帝，他努力將蘇勒德斯（solidus）金幣維持在含金 4.5 克以上，禁絕剪幣或劣幣，接著在西元 312 年開始大量鑄造金幣。他也將政治中心東移，在歐亞交界處建立了君士坦丁堡，開啟了東羅馬帝國，然後便以蘇勒德斯金幣作為法定貨幣。雖然羅馬帝國持續在經濟、社會和文化上走下坡，也終於在西元 476 年滅絕，但拜占庭帝國（東羅馬帝國）則存在了 1123 年，蘇勒德斯金幣也成為人類歷史上服役時間最長的「聲錢」。

君士坦丁在保持蘇勒德斯金幣完整性方面的努力，使其成為世界上最容易辨識與最廣泛接受的貨幣，後來也被稱為「*bezant*」（拜占庭金幣）。當時的羅馬帝國在破產皇帝無力支付士兵酬勞下湮滅，貨幣當然也隨之崩潰。但此時的君士坦丁堡則在財政與貨幣方面茁壯成長，並延續繁榮了幾個世紀。雖然汪達爾人和西哥德人在羅馬橫衝直撞，但君士坦丁堡依舊繁榮，幾世紀以來未曾被入侵。不過跟羅馬一樣，君士坦丁堡的淪陷，也發生在統治者開始讓貨幣貶值之後，歷史學家普遍認為這個過程，開始於君士坦丁九世莫諾瑪洛斯統治時期（Monomachos, 1042-1055<sup>註8</sup>）。隨著貨幣貶值，財政、軍事、文化也隨之低落，帝國精神不再，危機增加且寸步難行，直到 1453 年被鄂圖曼人征服為止。

---

註8 David Luscombe 和 Jonathan Riley-Smith，「新劍橋中世紀歷史」：第 4 卷，*C.1024-1198*（劍橋大學出版社，2004 年），第 255 頁。

即使被貶值且所屬帝國崩潰的情況下，拜占庭金幣依舊透過其他形式的「聲錢」繼續流傳至今，甚至根本不是任何國家專屬的官方貨幣，這就是伊斯蘭第納爾（dinar）。它隨著伊斯蘭教在拜占庭的黃金時期崛起，這種第納爾在重量和大小方面，都類似於拜占庭金幣，因此在伊斯蘭教傳播的地區廣為通用。

奧米亞王朝第五代哈里發（最高統治者）阿卜杜勒 - 馬利克・本・馬爾萬（Abdul-Malik ibn Marwan），定義了伊斯蘭第納爾的重量和價值，並在西元 697 年印上伊斯蘭教的清真言（*shahada*）信條。奧米亞王朝淪陷後，雖然歷經其他幾個伊斯蘭國家，但第納爾幣仍繼續使用中，並在伊斯蘭地區以跟原先拜占庭金幣相同的重量和尺寸廣泛流通，被用於嫁妝、禮物和各種直到今日尚存的宗教與傳統習俗中。而跟羅馬人和拜占庭人不同之處，在於阿拉伯和穆斯林文明的崩潰，跟貨幣的崩潰並未相互關聯，因為他們在幾個世紀以來一直保持著貨幣的完整性。羅馬皇帝戴克里先西元 301 年首次鑄造的蘇勒德斯（*solidus*）金幣，雖然已經改名為拜占庭金幣或伊斯蘭第納爾，但在今日仍能繼續流傳。17 個世紀以來，世界上的多數人都使用了這種貨幣進行交易，即可證明黃金跨時間的可銷售性。

## 文藝復興時期

在羅馬帝國的經濟和軍事崩潰之後，封建主義成了組成社會的主要模式。健全貨幣的瓦解，也成為羅馬帝國前公民轉變成當地封建領主轄下農奴的關鍵。由於黃金都集中在封建領主手中，因此當時歐洲農民可用的主要貨幣形式改為紅銅與青銅幣。而這些金屬的工業生產越來越容易，供應量極易膨脹；冶金技術的進步，也讓它們很難做為儲蓄價值之用。相同情況的銀幣，通常也會因為普遍的貶值、詐騙或非標準化，很難具有跨越空間的可銷售性，因而限制了整個歐亞大陸之間的貿易範圍。

稅收與通貨膨脹摧毀了歐洲人民的財富和儲蓄。當新一代的歐洲人來到這個世界時，無法從先人繼承累積的財富，而且缺乏廣泛接受的健全貨幣標準，嚴重限制了貿易範圍，使城鄉與社會彼此脫離關聯，日益增加的狹隘主義，也讓一度繁榮和文明的社會，陷入了農奴制度、疾病、封閉思想與宗教迫害的黑暗時代。

雖然一般普遍認為是「城邦」的崛起讓歐洲脫離黑暗時代，進入文藝復興時期，「聲錢」在這股風潮的作用感覺並不明顯。因為在城邦制度下，大家可以享有工作、生產、貿易和繁榮的自由，但事實上有很大部分是因為城邦採用了健全貨幣標準的結果。一切都始於 1252 年的佛羅倫斯（Florence），當時這座城市鑄造了弗羅林（florin），這是自凱撒大帝的奧里烏斯（aureus）銀幣以來，歐洲第一個主要的聲錢。佛羅倫斯的崛起使其成為歐洲的商業中心，其弗羅林幣亦成為歐洲主要的交易媒介，讓它們的銀行業在整個歐洲蓬勃發展。

威尼斯最早跟隨了佛羅倫斯的腳步，在 1270 年鑄造了與弗羅林相同規格的達克特（ducat）幣。到了十四世紀末，有超過 150 個歐洲城市和城邦，鑄造了跟弗羅林相同規格的硬幣。讓所轄公民們可以有尊嚴和自由的累積財富與進行貿易，而且使用的是可以跨越時間空間，具有高度可銷售性的健全貨幣。也有分成小硬幣，更增添其散佈的能力。隨著歐洲農民的經濟解放，義大利城邦也迎來政治、科學、知識與文化繁榮，隨後並傳播到整個歐洲大陸。無論是在羅馬、君士坦丁堡、佛羅倫斯或威尼斯，歷史都一再證明健全的貨幣標準是人類繁榮的必要先決條件，沒有這種貨幣標準，社會就會處於野蠻和破壞的邊緣。

雖然引入弗羅林後，我們可以見證貨幣穩健性的演進，越來越多歐洲人可以採用黃金和白銀進行儲蓄與貿易，歐洲和世界市場也都能擴張規模，但實際情況並不完美。在許多時期裡，不同的君主會貶低其人民的貨幣，用來資助戰爭或奢侈的支出。由於它們是實體的使用，銀和金可以相

互補充：黃金本身的高庫存流量比，代表它是長期價值儲值與大額支付的理想方式，但銀的每單位重量的價值較低，很容易被分割成適合較小交易量和持續時間較短的數量。雖然這種安排有其優點，卻有一個主要缺點：黃金和白銀之間波動的匯率，會造成貿易和計算上的問題。儘管嘗試修復兩種貨幣的相對價格，但都以失敗告終，不過黃金的貨幣優勢即將勝出。

由於這些國家設定了兩種貨幣之間的匯率，因此會讓持有者考慮是否繼續持有或花掉它們。這種不方便的雙金屬貨幣制度，在歐洲和世界各地持續了幾個世紀，但是從鹽、牛和貝殼到金屬的轉變過程裡，這些無法阻擋的技術演進，為我們提供了解決方案。有兩種特殊的技術進步，讓歐洲和世界遠離實體硬幣，並加速消滅了白銀的貨幣角色：第一項技術是「電報」，最早在 1837 年開始商業應用；第二項則是不斷成長的「火車」網路，可以跨越歐洲運輸。有了這兩項技術創新，銀行便可相互聯絡，在必要時可以有效地「跨空間」付款，並從帳戶中扣款，而非以實體金錢進行付款。因此使用票據、支票和紙質收據作為貨幣媒介的應用逐漸增加，減少了實體金幣和銀幣的使用。

越來越多國家開始選擇以金庫裡的貴金屬所支持，並可立即贖回的紙幣，作為他們的貨幣標準。有些國家選擇的貴金屬是黃金，其他國家選擇的是白銀，這是一個產生巨大影響的決定。英國在 1717 年成為第一個採用現代黃金標準的國家，而且是在著名物理學家牛頓（Isaac Newton）的帶領下進行，因為他被任命為皇家鑄幣廠廠長。黃金標準在推動大英帝國全球貿易時，發揮了重要的作用。英國在 1914 年之前均能維持其黃金標準，但其中在 1797 年至 1821 年的拿破崙戰爭裡，黃金標準暫時被中止了。英國的經濟霸權與它的優勢貨幣標準，錯綜複雜的牽連在一起，其他歐洲國家也開始效法。拿破崙戰爭的結束，預告著歐洲黃金時代的開始，歐洲主要國家一個接一個開始採用黃金標準。越多國家正式採用黃金標準，市場上便有更多可交易的黃金，接著其他國家一起加入的誘因就會越大。

在這之後的一般民眾不僅不必分別攜帶金幣和銀幣，應付不同大小規模的交易，更可將自己的財富以黃金存入銀行，並使用收據、帳單和支票來支付任何規模的款項。擁有紙質收據的人可以自己付款；銀行貼現帳單並用於清算，支票可從發行銀行兌現等。這等於解決了黃金「跨規模」的可銷售性問題，也使黃金成為最佳的貨幣媒介，但前提是這些囤積人民黃金的銀行，不會增加紙鈔收據的發行供應量即可。

由於這些媒介是金庫裡的實體黃金所支持，並可使用任何數量或大小進行支付，因此不再需要白銀作為小額支付之用。白銀貨幣角色的喪鐘是由法國－普魯士戰事的結束所敲醒，當時德國從法國獲得了 2 億英鎊的賠償金，並用來換成黃金標準。在德國以黃金標準加入英、法、荷蘭、瑞士、比利時和其他國家後，貨幣的大鐘擺已經決定性的擺向支持黃金，因而導致世界各地仍在使用白銀的個人和國家，見證其購買力逐漸喪失，因此加強了轉向黃金標準的動力。印度也終於在 1898 年從白銀轉為黃金，中國和香港則在 1935 年，是世界上最後放棄白銀標準的經濟體。

只要黃金和白銀用於直接支付，都會具有貨幣角色，它們彼此的相對價格在很長一段時間內大致保持不變，也就是每盎司黃金可兌換 12 到 15 盎司左右的白銀，大約等同於它們在地殼裡的相對稀有性，以及採礦困難度和採礦成本的高低。但隨著受金屬支持的紙幣與金融工具越來越受歡迎，白銀的貨幣角色便失去了正當性，個人和國家都轉向持有黃金，導致白銀價格大幅下跌，並從此一蹶不振。二十世紀裡兩者之間的平均比值為 47：1，在 2017 年時為 75：1。雖然黃金仍可當做貨幣發揮作用，例如從中央銀行囤積的儲備黃金便可證明，但白銀可視為完全失去了貨幣角色（見圖 3<sup>註 9</sup>）。

---

註 9 資料來源：Lawrence H. Officer 和 Samuel H. Williamson，「從 1257 年到現在的黃金價格（The Price of Gold, 1257–Present）」，衡量價值（2017 年），參閱 <http://www.measuringworth.com/gold/>。

白銀的非貨幣化對當時使用它作為貨幣標準的國家，會產生明顯的負面影響。與歐洲國家的黃金基準相比，印度便面臨了盧比的持續貶值。

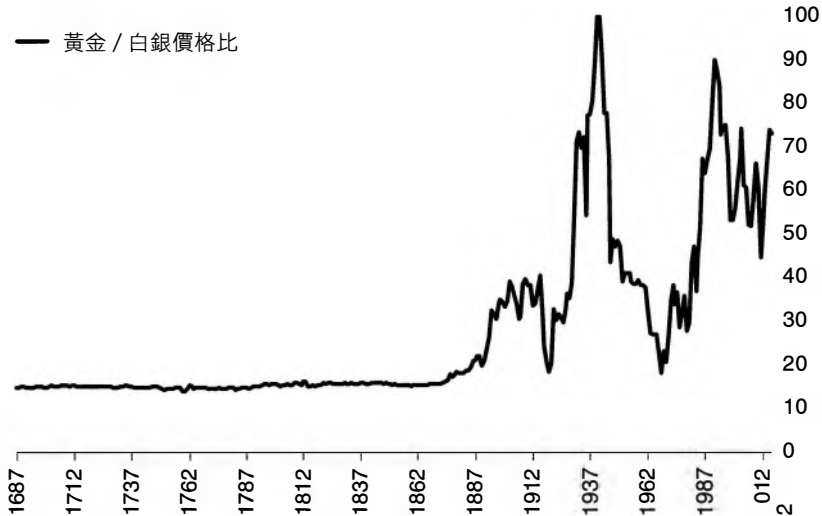


圖 3 每盎司黃金白銀價格比，1687–2017

這些歐洲國家讓英國殖民政府必須增加稅收來維持運作，導致英國殖民主義面臨不斷成長的動盪和怨恨。當印度終於在 1898 年將其盧比轉移為黃金支持的英鎊時，從法國－普魯士戰爭結束後的 27 年裡，支持盧比的白銀損失了 56% 的價值。而對直到 1935 年仍保持白銀標準的中國而言，其白銀（包含各種名稱與形式）在此期間則損失了 78% 的價值。

筆者認為，中國和印度的歷史，以及它們在二十世紀未能趕上西方的原因，跟這些國家使用流通性差的貨幣金屬，而造成財富與資本的大規模破壞密不可分。事實上白銀不適合當貨幣的情況，使得中國人和印第安人，處於類似西非人使用琉璃珠幣的情況：隨著歐洲人到來，國內的硬錢對外國人來說根本是弱勢貨幣，並且被外國人的硬錢驅逐與控制，在此期間，中國和印度境內的外國資本和資源也就越來越多。這是一場具有重大

意義的歷史教訓，任何認為只要拒用就不必瞭解比特幣的人，都該記住這一點。歷史說明了在面對其他持有更強勢貨幣的人，你無法把自己抽離即將發生的後果。

由於黃金掌握在日益集中的銀行手中，它們在時間、規模與地點上都得到了可銷售性，但卻在作為現金、在金融和政治當局簽發收據、結算支票與囤積黃金時，失去作為財富的能力。更可悲的是，黃金唯一能夠解決跨越規模、空間、時間可銷售性的方法，便是加以「集中化」，結果反而變成二十世紀經濟學家所強調，健全貨幣主要問題的犧牲品：也就是個人對貨幣的主權和對政府集中控制的抵制運動。因此我們可以理解為何 Menger 這樣的十九世紀「聲錢」經濟學家，對金錢穩健與否的理解，集中在市場利益的可銷售性。而二十世紀的「聲錢」經濟學家如米塞斯、海耶克、羅斯巴德和薩勒諾，則是集中在對金錢的分析，堅決抵制國家的控制。因為 20 世紀金錢的致命弱點，便是過度集中於政府手中，稍後我們會看到二十一世紀所發明的比特幣，其主要設計就是為了避免集中控制的情況。

## 美好年代

1871 年普法戰爭結束，隨之而來的是歐洲主要大國轉向相同的貨幣標準，也就是黃金，而造就了一段繁榮昌盛的時期。隨時間推移與回顧，讓這個時期的成就顯得更為驚人。十九世紀的情況可以作為一個很好的案例，尤其是十九世紀後半，更是世所見證的人類繁榮、創新和成就的最大時期，其中由黃金扮演的貨幣角色，便是最重要的關鍵。由於白銀與其他交易媒介逐漸式微，地球上多數人便都使用了相同的黃金貨幣標準，於是在電信和運輸的改善下，以前所未有的方式，促進了全球資本累積與全球貿易。

不同貨幣其實只是不同重量的實體黃金，國與國貨幣之間的匯率，變成是不同重量單位之間的簡單轉換而已，就像將英寸轉換為公分一樣的簡單。英鎊定義為 7.3 克黃金，法國法郎為 0.29 克黃金，德國馬克為 0.36 克黃金，這意味著它們之間的匯率必須固定為 1 英鎊等於 26.28 法國法郎與 24.02 德國馬克。跟公制與英制單位用來衡量基本長度的方式是一樣的，國家貨幣也只是衡量經濟價值的一種方式，並以大家都有儲藏的黃金價值來表示。有些國家的金幣因為是純金打造，所以在其他國家相當暢銷。每個國家的貨幣供應量並非透過具有博士學位的中央計劃委員會所制定，而是透過市場體系的自然運作所決定。人們可自由持有想要的金錢數量，也可以花錢購買在本地或國外生產的商品，因此實際的貨幣供應量並不容易估計。

貨幣的穩健性反映在世界各地的自由貿易中，但也許更重要的是在黃金標準下，多數先進社會所增加的儲蓄率，得以讓資本累積來資助工業化、城市化以及改良現代生活的技術提升等。（詳見表 1<sup>註 10</sup>）

表 1 黃金標準下的主要歐洲經濟時期

貨幣	黃金標準期間	年
法國法郎	1814-1914	100 年
荷蘭盾	1816-1914	98 年
英鎊	1821-1914	93 年
瑞士法郎	1850-1936	86 年
比利時法郎	1832-1914	82 年
瑞典克朗	1873-1931	58 年
德國馬克	1875-1914	39 年
義大利里拉	1883-1914	31 年

註 10 資料來源：Lips，2001 年。



到 1900 年時，大約有 50 個國家正式使用黃金標準，包括所有工業化國家；而沒有達成官方黃金標準的國家，仍然也會使用金幣作為主要的交易媒介。許多最重要的技術、醫學、經濟和藝術的人類成就，都是在黃金標準時代所發明。這或許可以解釋為何此一時期，會被稱為「美好年代（*la belle époque*）」或整個歐洲的「美麗時代（*beautiful era*）」<sup>11</sup>。英國人見證了「不列顛治世」的巔峰時期，大英帝國擴張版圖，而且沒有大規模的軍事衝突。在 1899 年，當美國作家內莉·布利（Nellie Bly）在 72 天內展開環遊世界的破紀錄之旅時，她隨身攜帶的是英國金幣和英格蘭銀行券<sup>註 11</sup>，因為內莉可以在所到之處，只用同一種形式的錢來環遊世界。

這個時代在美國被稱為「鍍金時代（*Gilded Age*）」<sup>12</sup>。美國內戰後於 1879 年恢復黃金標準，經濟也蓬勃發展，但曾經被一陣子的「貨幣狂熱」所打斷，事實上那也是白銀作為貨幣的最後一次慘痛教訓，我們會在第 6 章加以詳談。大致是因為當時的財政部強制將白銀作為貨幣來套利，導致貨幣供應量大幅增加，而想把國庫券和白銀換成黃金的人，通通跑到銀行擠兌，結果便造成 1893 年經濟衰退，事件過後，美國經濟成長也才有機會復甦。

世界上多數國家都使用某種穩健的貨幣單位，從來沒有一個時期是如此的資本累積、跨全球貿易、政府受合宜限制以及全球生活水準的轉變。當時西方經濟不僅更加自由，社會本身也更加自由。政府裡很少有專門「細部管理」人民生活的官僚機構，正如米塞斯所說：

---

註 11 Nellie Bly，「環遊世界七十二天（*Around the World in Seventy-Two Days*）」，紐約：畫報週刊，1890 年。

黃金標準是資本主義時代的世界標準，增進了政治和經濟雙方面的福利、自由與民主。在自由貿易商的眼中，黃金標準的主要優勢，在於它確實是國際貿易、國際貨幣和資本市場交易所需的國際標準。同時也是西方工業主義和西方資本家，可以把西方文明帶到地表最偏遠地區所需的交易媒介。然後在各地摧毀陳年偏見與迷信的束縛，散播新生命的種子與全新的安康生活、放縱心靈，創造前所未有的財富。它也為西方自由主義帶來了前所未有的進步，並已準備好將所有的國家，團結在一個自由國度的聯盟中，讓所有國家得以和平共處、相互合作。

因此我們可以很容易的理解，為何人們會將「黃金標準」視為所有歷史變革裡，最偉大與最有益的象徵。<sup>註 12</sup>

然而這個美好的世界在多災多難的 1914 年崩潰了，這一年不光是第一次世界大戰爆發，世界主要經濟體也脫離了黃金標準，也是使用不健全的「政府貨幣」來取代黃金的一年。只有在第一次世界大戰期間維持中立的瑞士和瑞典，才能在 1930 年代維持了黃金本位。此後由政府控制金錢的時代，開始在全球蔓延，帶來了徹底的災難性後果。

雖然十九世紀的黃金標準，可以說是世界上最理想的「聲錢」，但它仍有某些缺陷。首先，政府和銀行總是發行超出其儲備黃金總量的交換媒介。其次，許多國家的儲備裡不僅使用黃金，還包括其他國家的貨幣。身為當時世界超級大國的英國，已經可以從英鎊被世界各地作為「儲備貨幣」而獲益，造成英國銀行的黃金儲備，只佔全部貨幣供應量的一小部分

---

註 12 路德維希·馮·米塞斯，「人類行動（*Human Action*）」，第 472-473 頁。

而已。而國際貿易的成長，需要依賴全世界大量資金的結算，因此英格蘭銀行的紙幣在當時許多人的心目中，變得「和黃金一樣好」。雖然黃金是非常健全的「硬錢」，但用於中央銀行之間的支付結算時，這些貨幣名義上可以兌換成黃金，但實際上貨幣比起黃金更容易被生產出來。

這兩個缺點代表黃金標準也可能很脆弱，尤其是在某些執行黃金標準的國家，遇上大量民眾想把紙幣換成黃金的時候。這兩個黃金標準致命缺陷問題的核心，在於使用實體黃金的結算過程相當繁瑣、昂貴且不安全，因此實體黃金必須集中儲備在少數幾個地方，例如一般銀行和中央銀行，讓它們很容易被政府掌控。

由於以實體黃金支付和結算的交易筆數，佔所有支付交易的比例幾乎是無限小，因此持有黃金的銀行和中央銀行，便可透過並未完全由實體黃金支援的貨幣，進行交易與結算。結算網路因此變得非常具有價值，擁有結算網路者的「信用」可以被有效的貨幣化。而當經營銀行可以具有這種創造貨幣的能力時，政府自然傾向透過中央銀行來接管銀行業。因為這樣的誘惑相當強烈，而且當政府控制這類無形的金融財富後，不僅可以讓反對人士保持沉默，而且可以透過金融宣傳來灌輸錯誤的概念。黃金本身並沒有機制可以限制當權者的操縱，同時也必須依賴與信任政府不會濫用黃金標準，還要信任一般人民也一直對政府的做法維持警惕。

在人口普遍受過高等教育且了解不健全貨幣的危險時，一切似乎是可行的。但隨著每一代人都表現出「有錢便自覺聰明」的情況<sup>註 13</sup>，高明騙子與宮廷弄臣型經濟學家的魔笛聲，將證明多數人無力抵抗，只有少數知識淵博的經濟學家和歷史學家，正在進行一場艱苦的戰鬥，說服人們亂搞

---

註 13 詳見約翰·格魯布，「帝國的命運與尋覓生存之道（*The Fate of Empires and Search for Survival*）」。

「貨幣供應」並不能為人民產生財富，而允許主權國家可以操縱貨幣發行量，只會導致政府更能控制每個人的生活。文明的人類生活必須依賴於健全貨幣，才能為貿易和資本累積，奠定堅實的基礎。

黃金「集中化」很容易被自己的敵人奪走貨幣的角色，而且歷史上黃金有太多的敵人，這點米塞斯自己也很清楚：

民族主義者正在打擊黃金標準，因為他們希望將自己的國家從世界市場上抽離，並盡可能的讓國家自給自足即可。干涉主義者政權與壓力團體，也一起打擊黃金標準，因為他們認為這是在操縱商品價格和工資比例的努力過程裡，遇上的最大障礙。但是最熱衷於攻擊黃金的人，就是那些想要「擴張信用」的人。對他們來說，信用擴張是解決所有經濟問題的靈丹妙藥<sup>註14</sup>。

黃金標準可以否決政治領域裡，加印現金帶來的「增加購買力」的想法。若要人們廣為接受黃金標準，便需認清「不能透過印鈔票來使所有人都更有錢」的事實。對黃金標準的深惡痛絕，來自認為無所不能的政府，認為可以「透過少量紙張創造財富」的迷信…。政府急於摧毀黃金標準，因為它們荒謬的認為「信用擴張」是降低利率和改善貿易平衡的適當手段…。人們反對黃金標準，則是因為想用國家的「自給自足」，來取代自由貿易、和平戰爭與極權主義政府所支配的自由等<sup>註15</sup>。

二十世紀剛開始時，各國政府透過發明基於黃金標準成立的現代中央銀行，將公民的黃金置於其控制之下。第一次世界大戰開始時，這些黃金儲備的集中化，使各國政府可以將貨幣供應量擴增到黃金儲備的範圍外，

---

註14 路德維希·馮·米塞斯，「人類行動（*Human Action*）」，第473頁。

註15 路德維希·馮·米塞斯，「人類行動（*Human Action*）」，第474頁。

從而降低了貨幣價值。然後這些中央銀行持續沒收並累積更多黃金，直到 1960 年代，以美元當做全球貨幣標準的趨勢開始成形。雖然一般認為黃金是在 1971 年被完全「非貨幣化」，但中央銀行繼續維持大量黃金儲備，並且在過去十年恢復購買黃金之前，非常緩慢地處置黃金儲備。即使中央銀行一再宣布要終止黃金的貨幣角色，但他們維持黃金儲備的行動也更為積極。從貨幣競爭的角度來看，維持黃金儲備是非常理性的決定。保留外國政府的寬鬆貨幣做為儲備，只會導致本國貨幣的價值與儲備貨幣一起貶值，而且儲備貨幣的獲利是由該國儲備貨幣的發行人獲得，而非本國中央銀行可以累積。

此外，如果中央銀行出售所有黃金儲備的話（估計約佔全球黃金存貨的 20%），最可能的影響是本來因工業與美學用途而備受推崇的黃金，在價格差不多的情況下很快被大眾收購，中央銀行也將沒有任何黃金儲備。弱勢的政府貨幣與強勢黃金之間的貨幣競爭後，終究會產生一個贏家。即使在政府貨幣的世界裡，政府也無法取消黃金的貨幣角色，因為黃金的價值無庸置疑（詳見圖 4<sup>註 16</sup>）。



圖 4 中央銀行官方黃金儲備，單位為噸

註 16 資料來源：世界黃金協會儲備統計。參閱 <https://www.gold.org/data/gold-reserves>。

## 政府的錢（法定貨幣）

---

**第**一次世界大戰是「自由市場選擇貨幣媒介」時代的終結，也是政府貨幣時代的開始。雖然黃金繼續支撐全球貨幣體系至今，然而政府的法令、決策和貨幣政策比起任何個人觀點，都更能塑造出世界的貨幣現實。

政府貨幣的通用名稱是法定貨幣（*fiat money*），來自拉丁語中的法令、命令或授權。本章一開始，便需了解政府貨幣的兩個重要事實。首先，即使同樣都由政府管理，但「可以兌換黃金的錢」和「不可贖回的政府貨幣」之間，存在極大的差異。在黃金標準下，貨幣就是黃金，政府只承擔由黃金儲備所支持，鑄造標準單位金幣或印刷紙鈔的「責任」。政府並未控制經濟中的黃金供應，人們可以隨時用紙鈔兌換為實體黃金，並在彼此交易時使用其他形狀或形式的黃金，例如金條和外國硬幣等。另一方面，不可贖回的政府貨幣如政府公債或紙鈔，被拿來當作貨幣時，政府便能在認為合適的情況下增加供應。若有人使用其他形式的貨幣進行交易，或試圖創造更多的政府貨幣，便會面臨「違法」而被處罰的風險。

第二個同時也是經常被忽視的事實，便是法定貨幣與名稱上面所暗示的「法令」特性恰恰相反，因為法定貨幣不能只透過政府命令流通；它們最初都可以用黃金或白銀來兌換，或可以把貨幣兌換回黃金或白銀。只有把可兌換性轉換成可銷售性的貨幣形式，才能讓政府的紙鈔獲得可銷售性。政府可以頒布法令要求人們用紙鈔進行支付，但政府無法將這種可銷售性直接強加於紙鈔上，這些紙鈔必須可以換回黃金、白銀才行。直到現在，所有的政府中央銀行都維持儲備以支持其本國貨幣的價值。多數國家的儲備裡也都保留了一些黃金，而沒有黃金儲備的國家則會以其他國家的法定貨幣形式保留儲備，因為這些外國貨幣也是由黃金儲備所支持，亦即沒有任何法定貨幣可以不帶任何形式的儲備支持而流通。這個重大誤解與國家貨幣理論中心原則恰好相反，亦即並非政府將黃金定為貨幣；相反的，政府只有透過持有黃金，才能讓大眾完全接受其貨幣。

最古老的法定貨幣實例是「交子」（*jiaozi*，與餃子諧音），這是十世紀時中國宋朝發行的紙幣。最初，交子是黃金或白銀的收據，但隨後政府控制其發行並暫停兌換，然後一直加印交子直到貨幣價值崩潰為止。元朝在 1260 年也發行了法定貨幣，名為「交」（*chao*、交鈔），並大量供應而遠遠超出了貴金屬支持的量，其災難性後果可想而知。隨著貨幣價值的崩潰，人們陷入赤貧之中，許多農民只好將孩子賣為奴隸還債。

因此政府貨幣會類似於第 2 章討論的原始貨幣形式，或是黃金以外的商品。這些非黃金的商品因為與自己的庫存量相比，供應量可以迅速被大量增加，導致快速喪失其可銷售性，也破壞購買力並造成持有者的貧困情況。

這些法定貨幣跟黃金有所不同，由於之前討論過的金屬基本化學性質之故，黃金的供應無法快速增加。政府要求用此貨幣來支付稅收，雖然可以保證這些貨幣的壽命更長，但只有政府能夠防止貨幣供應的快速擴張，才有可能保證貨幣不會迅速貶值。當我們比較不同國家的貨幣時，就會發現最廣泛使用的主要國家貨幣，其年度供應成長率低於可銷售性較低的次要貨幣。

## 貨幣民族主義與自由世界的終結

米塞斯在上一章結尾引文中，點名提到「聲錢」有許多敵人。戰勝黃金標準的時刻始於1914年中歐的一場小戰爭，但人類歷史上的這些貨幣敵人，卻在第一次世界大戰中，如雪片般到處飛來。當然在戰爭剛開始時，沒有人想到它會持續那麼久，並造成這麼多傷亡。舉例來說，英國報紙稱它為八月銀行假日戰爭（譯註：歐洲部分地區將國定假日稱為銀行假日），認為它將會是一次英國軍隊輕易獲勝的夏季旅遊。當時大家覺得這應該只是一場有限的地區性衝突。而且在整個歐洲幾十年來的相對和平後，新一代的歐洲人尚未意識到發動戰爭的可能後果。時至今日，歷史學家們仍未能提供令人信服的戰略或地緣政治的解釋，來說明為何奧匈帝國與塞爾維亞分離主義分子之間的衝突，會引發一場世界大戰，奪走了數百萬人的性命並徹底改變世界版圖。

仔細回顧時，你將發現第一次世界大戰與以前有限戰爭之間的主要區別，既非因為地緣政治也不是戰略，而是一場「貨幣之戰」。當政府使用黃金標準時，可以直接控制大型金庫，而人民使用這些可贖回黃金的紙幣。但在戰事激烈的情況下，政府可以輕易發行更多紙幣，而且會比向公民「徵稅」來得更為容易。因此在戰爭開始幾週後，所有主要交戰方都暫停了黃金兌換，快速取消黃金標準，並且讓人民改為使用法定貨幣標準。這些法定貨幣便是政府所發行，不可兌換黃金的紙張。

簡單停止黃金的可贖回性之後，政府在戰爭可做的努力，便不再只侷限於國庫裡所擁有的資金，而是擴展為整體人民的財富。只要政府能夠印出更多的錢，並讓其公民與外國人都能接受這些錢，便可以持續為戰爭提供資金。若是在之前的貨幣體系下，黃金是掌握在人民手中的貨幣，政府只有自己的國庫以及為戰爭提供資金的稅收或發行債券，才能用來負擔戰



爭經費。如此一來，戰爭的規模便會有所限制，這也是二十世紀之前，世界各地可以經歷相對長期和平的重要核心。

如果歐洲國家仍處於黃金標準下，或者歐洲人民可以自己掌控黃金，讓政府只能尋求稅收而非靠通貨膨脹資助戰事，歷史便可能會有所不同，世界大戰也很可能在衝突後的幾個月內便結束，因為其中一方耗盡了戰爭經費，並且面臨人民不想放棄財富來供應捍衛政權存亡的人。但隨著黃金標準的中止，資金用盡也還不能結束戰爭；因為一個主權政府必定會透過通貨膨脹，徵收人民累積的財富。

歐洲國家的貨幣貶值，使得血腥的僵局持續了四年，而且沒有任何解決方案或任何進展。這些國家的人民並非無感，因為前線士兵毫無理由的冒著生命危險，而且這種戰爭通常只是那些彼此是家人或姻親的君主，其無限的虛榮和野心所造成。代表這場戰爭毫無意義的最具體事蹟，便是在 1914 年聖誕節前夕，法國、英國和德國士兵都停止戰鬥、放下武器，越過戰線相互寒暄交談。許多德國士兵曾在英國工作、會說英語，而且大多數士兵都喜歡踢足球，也臨時組團辦了多場即興賽事<sup>註1</sup>。

這場休戰暴露出令人震驚的事實，這些士兵彼此無冤無仇，並沒有從這場戰爭裡獲得任何好處，也看不出任何繼續打下去的理由。這些國家最好的競爭場合應該是在足球場上，這是更普遍更受歡迎的比賽，也可以更和平的發展族群與國家的關係。

戰爭持續了四年，幾乎沒有任何進展。直到美國在 1917 年介入戰爭，參與一方並在金錢耗費上擊敗另一方，投入了敵人無法比擬的大量資源來扭轉戰爭。雖然所有政府都在利用通貨膨脹來資助自己的戰爭機器，

---

註 1 馬爾科姆·布朗和雪莉·西頓，「聖誕節休戰：西部戰線 1914 年 12 月（*Christmas Truce: The Western Front December 1914*）」，倫敦 Pan Macmillan 出版，2014 年。

但德國與奧匈帝國在 1918 年開始出現貨幣價值嚴重下降，讓戰敗無可避免。將交戰雙方貨幣的匯率與當時仍處於黃金標準下的瑞士法郎相比，能有效評估每種貨幣貶值的情形，如圖 5<sup>註 2</sup> 所示。

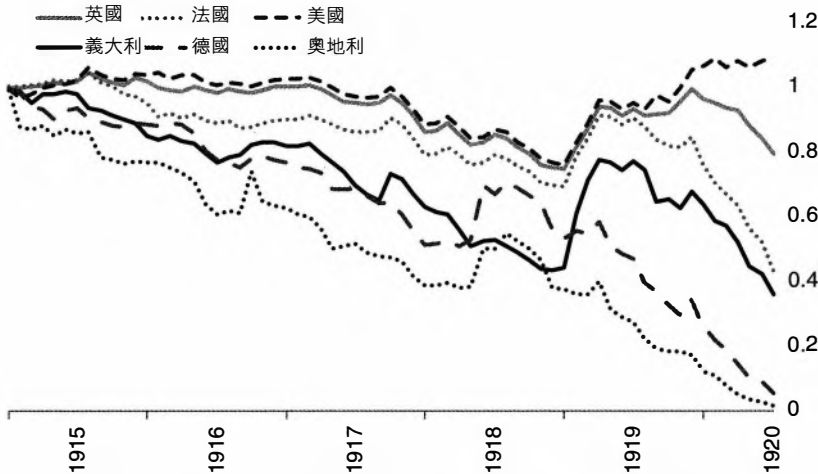


圖 5 第一次世界大戰期間，主要國家兌換瑞士法郎匯率（1914 年 6 月 = 1）

塵埃落定後，所有主要歐洲大國的貨幣價值都在下跌。

表 2 第一次世界大戰期間各國貨幣對瑞士法郎貶值的情形

國家	第一次世界大戰貨幣貶值
USA	3.44%
UK	6.63%
FRA	9.04%
ITA	22.3%

註 2 資料來源：George Hall，「第一次世界大戰期間的匯率和傷亡人數（Exchange Rates and Casualties During the First World War）」，貨幣經濟期刊。

國家	第一次世界大戰貨幣貶值
GER	48.9%
AUS	68.9%

敗戰的德國與奧地利，其 1918 年 11 月的平均貨幣價值，下降到原先 1913 年的 51% 和 31% 的價值。義大利的貨幣下降為原先的 77%，而法國的貨幣僅下降到原值的 91%，英國為 93%，美元仍維持原有價值的 96%<sup>註 3</sup>（見表 2<sup>註 4</sup>）。

戰爭所帶來的地理變化，完全不值得如此的大屠殺，因為多數國家獲得或失去了邊界的土地，也沒有勝利者可以宣稱佔領了值得犧牲的大片土地。奧匈帝國分裂成較小的國家，但依舊由自己的人民統治，而非戰爭的贏家取得。戰爭主要的變化在於消滅了許多歐洲君主制度，並以共和政權取代。無論這樣的轉變是否更好，戰爭都已對這些國家造成了毀壞與荒蕪。

隨著中央銀行贖回黃金，以及主要經濟體在國際上暫停或嚴格限制黃金的流通，政府仍可維持貨幣在戰前與黃金互換的價值，即便是在黃金漲價的情況下也可以。而隨著戰爭結束，圍繞黃金標準的國際貨幣體系，便不再具有其功能性。

註 3 我很好奇德國和奧地利跟瑞士如此接近，加上這些人口之間的密切關係，可能會導致更多德國和奧地利人用他們的貨幣兌換瑞士法郎，加速這些貨幣的崩跌，從而延伸了政府的經濟資源，並在第一次世界大戰的結果中，扮演了決定性的角色。但我從來沒看到過任何關於這個問題的研究，若各位親愛的讀者曾經看過的話，請不吝通知我。

註 4 從 1914 年 7 月到 1918 年 11 月。資料來源：George Hall，「第一次世界大戰期間的匯率和傷亡人數（Exchange Rates and Casualties During the First World War）」，貨幣經濟期刊。

此時這些國家都已脫離黃金標準，必須認真面對是否應重回黃金標準的大難題，如果回復的話，該如何重新評估貨幣與黃金交換比例呢。他們現有的貨幣存量對黃金存量的公平市場估值，將會令人厭惡的承認貨幣所面對的「貶值」。而恢復舊的匯率將導致公民改為要求持有黃金，而非無處不在的紙鈔收據，這也將會導致黃金流向具有較公平價位的外國。

此種困境將資金從市場中奪走，並轉變為政治控制的經濟決策。原先是以市場自由參與所決定的最暢銷商品，來作為貨幣交易媒介，同時也當作價值、供應與利率之用，現在卻變成由國家政府集中規劃，亦即海耶克在精彩的同名書中所稱「貨幣民族主義」的貨幣體系：

「貨幣民族主義」指的是一個國家在世界貨幣供應中的份額，不應由決定不同的地區或行政區的那種原則和機制，來決定應該擁有多少相對數量的貨幣。一個真正的國際貨幣體系，將會是一個整個世界擁有同質的貨幣體系，例如我們可以在不同的國家取得貨幣，而且該貨幣在各地之間的流通，是由所有個人意志的行動，所產生的結果<sup>註5</sup>。

黃金很難再回歸成為世界性的同質貨幣，各國中央銀行的獨佔地位和對黃金所有權的限制，迫使人們使用國家政府的貨幣。引入網路原生的比特幣，可以突破國家疆界與政府控制範圍，提供一個新國際貨幣系統出現的可能性，這點將在第9章詳細分析。

---

註5 弗里德里希·海耶克，「貨幣民族主義和國際穩定（*Monetary Nationalism and International Stability*）」，Fairfield、NJ：Augustus Kelley 出版，1989 [1937]。

## 兩次世界大戰之間的年代

在國際黃金標準下，貨幣在國家之間自由流動以換取貨物，不同貨幣之間的匯率，只是不同重量黃金之間的轉換。而在貨幣民族主義下，每個國家的貨幣供應量，以及貨幣之間的匯率，是透過國際會議與協議來訂定。在凡爾賽條約施加的大量賠償下，德國遭受重大的通貨膨脹，而且還試圖也用通貨膨脹來進行償還。英國面對的重大問題則在試圖維持黃金標準，但兌換比率高估了英鎊並低估了黃金，因此從其海岸不斷流出黃金到法美兩國。

貨幣民族主義世紀的第一個主要條約是 1922 年的熱那亞條約。根據該條約內容，美元和英鎊在其他國家的儲備中，被視為類似於黃金的儲備貨幣。此舉是英國希望透過讓其他國家大量購買英鎊作為儲備，來減輕高估英鎊的問題。世界主要大國宣示脫離穩固的黃金標準，迎向通貨膨脹主義以解決經濟問題。這種做法的瘋狂之處在於，這些政府想要進行通貨膨脹，又希望能維持貨幣價格接近戰前的黃金標準。人們會用數字來尋求安全：如果每個人的貨幣都貶值的話，資本也就無處可藏。但這種方式無法奏效，因此黃金持續從英國流向美國和法國。

英國黃金的流失是個鮮為人知但後果極為嚴重的故事，Liaquat Ahamed 的《金融之王》（*Lords of Finance*）一書鎖定了這件事，並且仔細探究涉及的人、事、地點等，但他採用了凱因斯主義對此問題的理解，而將整個事件的責任歸咎於黃金標準。儘管進行了廣泛的研究，但 Ahamed 並未理解到問題不在黃金標準，而是在第一次世界大戰後的政府，想要回歸第一次世界大戰前的黃金本位。如果他們向人民承認打仗所造成貨幣貶值的程度，並以新的兌換率重新將貨幣與黃金連動，那麼雖然可能會暫時出現經濟衰退，但後來的經濟便能恢復健全貨幣的「聲錢」基準。

對此事件較好的處理方式與瞭解其可怕的後果，可以參考 Murray Rothbard 的《美國大蕭條》（*America's Great Depression*）。由於英國的黃金儲備正大量從海岸流向價值更高的地方，英格蘭銀行行長 Sir Montagu Norman 過於依賴法國、德國和美國同行增加貨幣供應量使紙幣貶值，希望這個方法可以阻止黃金繼續流出英國。雖然法國與德國的銀行家並不合作，但紐約聯邦儲備委員會主席 Benjamin Strong 在整個 1920 年代進行了通貨膨脹貨幣政策。如此或許真的在一定程度上，成功減少了黃金從英國流出，但其更重大的影響是在美國的房市與股市造成更大的泡沫。美國聯邦儲備銀行的通貨膨脹政策在 1928 年底結束，此時美國經濟雖已成熟，但因通貨膨脹現象造成的停滯，導致不可避免的經濟崩潰。隨之而來的便是 1929 年的股市崩盤，而且美國政府的反應措施，更使這一切成為現代歷史上最長的經濟蕭條。

關於「大蕭條」的常見說法，多半是認定胡佛總統選擇在經濟衰退時按兵不動，因為他對自由市場恢復能力的錯誤信任，以及他堅守黃金標準所導致。而當他被繼任取代後，羅斯福總統活躍了政府扮演的角色，並且暫停黃金標準，才讓美國經濟復甦。溫和一點的說，上述這些理論實屬無稽之談。因為胡佛不僅增加政府在公共工程項目上的開支來應付大蕭條，而且也倚仗美國聯邦儲備銀行來擴張信用，並使他的政策著重在工資普遍下降的情況下，盡量提高工資水平。此外，他還制定了價格管控措施，以使產品（尤其是農產品）的價格保持在高水平，接近在蕭條前被視為公平、正確的價位。此後美國和全球所有主要經濟體，都開始實施貿易保護政策，這點讓整個世界的經濟情況變得更糟。<sup>註 6</sup>

---

註 6 你可在 Murray Rothbard 的「美國大蕭條（*America's Great Depression*）」裡，找到對胡佛干預政策的詳細內容。

仔細從歷史書中閱讀，便會發現一個鮮為人知的事實，也就是在 1932 年的美國大選中，胡佛從一個「高度干預」的財政基礎上執政，羅斯福則在財政和貨幣責任平台上行政。美國人實地投票反對胡佛的政策，但是當羅斯福上台後，他發現和影響胡佛的利益一起行動會更方便。因此，胡佛的干預政策被放大為後來眾所周知的「羅斯福新政（The New Deal）」。其中相當重要的一點，便是要瞭解這項「新政」裡，並沒有什麼獨特或新鮮的政策，其實只是胡佛高度干預政策的「放大版」。

從經濟學的前瞻性來理解便可清楚顯示，價格控制總是會適得其反，造成過剩與短缺。1930 年代美國經濟所面臨的問題，跟「固定工資」及「價格控制」密切關聯。工資設定得太高會造成失業率太高，在某個時刻甚至達到 25% 的失業率，而價格控制則造成各種商品的短缺與過剩。一些農產品甚至被燒毀以維持高價格，造成人們挨餓、渴求工作的瘋狂局面，而生產者卻無法僱用他們，因為負擔不起工資。這些生產者有時還必須燒掉一些作物，以維持它們的高價。所有的作法都是為了維持在 1929 年之前繁榮水平時的價格，並維持美元與黃金相比仍保有其價值的錯覺。1920 年代的通貨膨脹導致房市和股市出現大量資產泡沫，造成工資和價格的人為上漲。在資產泡沫破滅之後，市場價格透過美元價值下跌（與黃金相比），以及實際工資與價格的下降，來尋求重新調整。被誤導的中央規劃人員們，頑固的想要阻止美元、工資和價格被高估，因為三者同時發生可能引發經濟癱瘓，導致人們拋售美元換取黃金，以及大規模失業與生產失敗等。

當然只要擁有健全的貨幣，這些情況便不會發生；而只有過度放大貨幣供應，才會冒出這些問題。然而即使在通貨膨脹發生之後，若能以市場決定的價格將美元以黃金的價值重新估算，並且讓工資和價格自由調整，整體情況便不會如此難堪。

這個時代的政府經濟學家認為，錯誤並不在通貨膨脹，而是在限制政府通貨膨脹的黃金標準。為了解開黃金標準的束縛，羅斯福總統頒布了一

項行政命令，禁止私人擁有黃金，強迫美國人民以每盎司 20.67 美元的價格將黃金賣給美國財政部。由於人民被奪走了可靠的黃金，被迫以美元交易。羅斯福隨後還將國際市場上的美元，從每盎司黃金兌換 20.67 美元升值至每盎司兌換 35 美元，實質讓美元貶值了 41%（與黃金相比）。這是多年的通貨膨脹現象的必然事實，也就是從 1914 年美國聯邦儲備銀行成立，到資助美國進入第二次世界大戰的經費的期間。

這是放棄健全貨幣，以政府發行的法幣來取而代之，因而把世界主要經濟體，轉變為中央規劃與政府指導下的失敗案例。由於政府控制金錢，因此他們控制著多數經濟、政治、文化和教育活動。雖然凱因斯從未學過或專業的研究過經濟學，但他把握住強權政府的時代精神，帶給政客們想要聽到的決定性內容。

幾個世紀以來，世界各地學術研究所獲得的經濟知識基礎瞬成泡影，因為那些時間珍貴的政治家和極權主義政府，以結論最簡便的新信念來取而代之：經濟狀況可以透過總支出的槓桿來決定，任何失業率上升或產業放緩，並沒有生產結構上的根本原因所導致，也不是中央規劃者扭曲了市場；而是全部歸咎於支出短缺，其補救措施就是貨幣貶值與增加政府支出。儲蓄會減少支出，而由於支出是最重要的因素，所以政府必須竭盡所能阻止公民儲蓄。然後進口會導致工人失業，因此必須增加國內商品消費的支出。政府喜歡這個說法，凱因斯自己也知道這一點。他的書於 1937 年在納粹高峰的時代被翻譯成德文，而他在德國版的簡介中寫道：

「總產量理論」是以下這本書的重點，但比起生產理論與特定產品分配所採用自由競爭和大量放任的狀況來說，會更適合極權主義國家的狀況。<sup>註 7</sup>

---

註 7 引自 Henry Hazlitt，「新經濟學的失敗（*The Failure of the New Economics*）」、277 頁。



世界尚未復原，但凱因斯風暴已經崛起。大學研究失去獨立性，徒然成為政府統治機構的一部分。「學院經濟」不再是一門專注於理解人類在經濟蕭條下，該如何選擇以改善現況的知識學科。相反的，它變成政府的分支部門，用來指導這些政策制定者，採取最佳的政策來管理人民的經濟活動。政府「對經濟進行管理」變成必要的概念，也成為所有現代經濟教育的必然起點，正如我們從現代經濟學教科書中可以看出，政府扮演的角色變成與上帝在宗教經文裡的作用相同：全在、全知、全能的力量，只需分辨問題再圓滿的解決即可。政府不會受到「機會成本」概念的影響，而且政府對經濟活動的干預，很少被認定有負面的結果，如果真的遇到問題，反而會促使政府進行更多的干預。

將「經濟自由」視為經濟繁榮基礎的古典自由主義傳統，很快的被丟在一旁，因為偽裝成經濟學家的政府宣傳者，把因政府控制所導致與加劇的大蕭條，誤導為對自由市場的反駁。古典自由主義者變成 1930 年代各國政治上的敵人；他們在俄羅斯、義大利、德國和奧地利等國被謀殺或驅逐。但很幸運的，在美國和英國只受到了學術上的迫害。這些偉大的學者在這些國家，委身為中等官僚與差勁的統計學家職位，每個大學的經濟系裡，都充滿了「學院經濟」的科學主義與不確定性。

目前政府認定的經濟學課程，仍在歸咎大蕭條時期的黃金標準。而在 1870 年至 1914 年間，四十多年所形成不間斷的全球成長和繁榮的相同黃金標準，卻在 1930 年代突然停止運作，因為黃金標準會限制政府擴大貨幣供應來對抗蕭條的作法，使這些經濟學家無法解釋毫無意義的凱因斯主義，到底與動物本能有何差異？

這些經濟學家似乎都沒有注意到，如果問題確實是來自黃金標準，那麼暫停之後就應該開始復甦。但結果完全相反，在停止黃金標準之後花了十多年的時間才恢復成長。對貨幣與經濟有基本認識的人來說，其結論顯

而易見，造成 1929 年大崩潰（Great Crash）的原因是在第一次世界大戰後的幾年裡，改變了黃金標準，而加劇大蕭條的原因則是由政府控制，以及胡佛與羅斯福時代的經濟社會化所造成。黃金標準的暫停與戰時的鉅額支出，並未對大蕭條有任何緩解的作用。

隨著世界主要經濟體脫離黃金標準，全球貿易很快就會在動盪不安的法定貨幣海岸遇上船難。沒有任何標準可支援國際價格機制，政府也越來越被國家主義與孤立主義影響，操縱貨幣變成了貿易政策的工具，於是各國倚賴貶值貨幣來為出口商提供優勢。更多貿易限制被各國建立，經濟民族主義也成為可預見災難性後果的時代精神。40 年前在普遍互信的黃金標準下交易而繁榮的國家，現在卻彼此存在著巨大的貨幣與貿易壁壘，喧囂的民粹主義領導人將所有的失敗歸咎於其他國家，不斷上升的仇恨民族主義潮流，很快的實現了 Otto Mallery 的預言：「如果士兵不會跨越國界，商品自己會；除非放棄貿易壁壘，否則炸彈將從天而降。」<sup>註 8</sup>

## 第二次世界大戰與布雷頓森林體系

炸彈確實從天而降，在此之前還有無數難以想像的謀殺與恐怖形式。

由政府指導經濟下所建立的戰爭機器，遠比世界任何國家所見過的都更為先進。這一切要歸咎於最危險荒謬的凱因斯主義謬論的普及，也就是他們認為政府在軍事方面努力支出，將有助於復甦經濟的觀念。在凱因斯主義天真的經濟學中，認為所有的支出都是支出，因此這些支出來自個人

---

註 8 Otto Mallery, 「經濟聯盟和持久和平 (*Economic Union and Durable Peace*)」, Harper and Brothers 出版, 1943 年, 第 10 頁。

照顧家庭或來自政府謀殺外國人都沒關係：一切都算在總需求內，也都能降低失業率！而隨著越來越多的人在大蕭條期間挨餓，所有主要政權都慷慨的花錢武裝自己，其結果便是又回到三十年前那種毫無意義的破壞。

對於凱因斯主義經濟學家來說，戰爭是導致經濟復甦的原因，若僅透過政府官僚收集的統計數據來看待生活，那麼這種荒謬的概念確實可以站得住腳。隨著政府戰爭支出與徵兵員額的增加，總支出飆升而失業率急劇下降，因此參與第二次世界大戰的所有國家都能因為參與戰爭而復甦。然而任何未受凱因斯主義經濟學影響的人，都知道在第二次世界大戰期間，即使在那些像美國一樣未在領土上戰爭的國家，也無法想像被描述成「經濟復甦」的國家。在死亡和破壞之外，交戰國的大量資本和勞動力資源貢獻給戰爭，其國內生產便會嚴重短缺，因而導致資源配給與價格控制。以美國來說，建造新房子與修復現有房屋均被禁止<sup>註9</sup>。而更明顯的是，無論讓士兵攜帶武器的「總支出」是多少，都無法爭辯那些佔交戰國人口一大部分的戰鬥與前線「死亡士兵」，已經不能享有任何形式的經濟復甦。

在凱因斯主義的「總需求理論」被當作經濟狀況的決定因素時，最具破壞性的一次打擊，發生在第二次世界大戰過後，尤其是在美國。

一系列因素導致政府大幅減少開支，讓當時的凱因斯主義經濟學家認為戰後的前景堪憂：因為軍事敵對狀態的結束，將大量減少政府的軍費支出。民粹主義的消失以及由溫和且非偶像型的杜魯門取代羅斯福，對抗由共和黨控制的國會，除了造成政治僵局，也阻礙「新政」法規的更新。凱因斯主義經濟學家把這些因素擺在一起分析，指出即將發生的災難，正如幾乎是戰後經濟教科書主要編寫者的 Paul Samuelson 在 1943 年所寫的：

---

註9 Robert Higgs, 「第二次世界大戰和凱因斯主義的勝利 (World War II and the Triumph of Keynesianism)」, 2001 年, 獨立研究所研究文章。參閱 <http://www.independent.org/publications/article.asp?id=317>。

從上次戰爭結束的經驗裡，所得出的最後結論終究不可避免——戰爭是否會在未來 6 個月內突然結束，我們是否又會毫無計畫地以最快的速度，結束我們對戰爭的努力，遣散部隊、取消價格控制，並從天文數字般的赤字，甚至是 30 年代的鉅額赤字，迎來任何經濟體所不曾面臨過，失業與工業混亂的最大時期<sup>註 10</sup>。

然而第二次世界大戰的結束和新政的解體，代表美國政府在 1944 年到 1948 年之間，削減了驚人的 75% 開銷，還取消了大部分的價格控制。然而在這些年裡，美國經濟卻出現了非比尋常的繁榮。戰爭所動員的約 1000 萬人回到家中，而且幾乎無縫地加入了勞動力市場。隨著經濟生產的蓬勃發展，跟凱因斯主義的所有預言完全相反，也完全否決了「支出是經濟決定因素」的荒謬觀念。一旦從 1929 年崩潰以來首次減少政府中央規劃，並允許價格自由調整後，市場就會自動扮演經濟活動協調機制的角色，將賣方和買方配對，激勵生產消費者需求的貨物，並彌補工人們付出的努力。

然而情況遠非完美，因為世界仍然脫離黃金標準，導致貨幣供應始終存在扭曲，這將持續讓世界經濟一再陷入危機。

大家都知道歷史是由勝利者所撰寫，但在政府法幣的時代，勝利者還可以決定貨幣制度。美國召集各國盟友代表，前往新罕布夏州的布雷頓森林，討論制定新的全球貿易體系。歷史上對建立這種系統的人物並不友好，英國方面的代表是凱因斯（John Maynard Keynes），他的經濟教義在戰後數十年裡，將會在現實的海岸上擱淺，而美國的代表懷特（Harry

---

註 10 Seymour Harris, 「戰後經濟問題（Postwar Economic Problems）」一書裡的 Paul Samuelson 「戰後充分就業（Full Employment after the War）」，紐約，McGraw-Hill 出版，1943 年。

Dexter White），後來則被揭發是與蘇聯政權接觸多年的共產主義者<sup>註 11</sup>。在爭取中央計劃全球貨幣秩序的戰鬥中，懷特以一項計劃取勝，甚至可以讓凱因斯跟他比較起來不再像是精神失常的人。這項計畫也就是讓美國成為全球貨幣體系的中心，美元可用來作為其他中央銀行用的全球性儲備貨幣，他們的貨幣可按固定匯率兌換成美元，而美元本身亦按固定匯率轉換為黃金。為促進此一貨幣體系，美國應該從其他國家的中央銀行取得黃金。

雖然美國人民仍被禁止持有黃金，但美國政府承諾以固定利率，用美元向其他國家的中央銀行贖回黃金，開啟了所謂的黃金交易窗口。從理論上講，全球貨幣體系仍然算是以黃金為基礎，如果美國政府不過度供應超出其黃金儲備的美元來維持可兌換性，而且其他國家也不將他們的貨幣供應量超過國內的美元儲備，那麼貨幣體系確實有機會可以接近第一次世界

---

註 11 在國會面前調查和作證後，懷特兩次心臟病發作，並因服藥過量而死亡，被判定可能為自殺。這個故事比較可靠的觀點可以參考 Benn Steil 的「布雷頓森林之戰（*The Battle of Bretton Woods*）」，亦即從懷特是蘇聯間諜的觀點來看。儘管比較不討喜，但這種解讀可當作更細膩的觀點。美國進步人士（American progressives）和俄國共產黨人之間的聯繫始於 1917 年的俄羅斯政變，正如英美歷史學家 Antony Sutton 所描述，其中還包括了美國向布爾什維克黨提供大量資金，以求廢除俄羅斯君主制的努力。威爾遜主義美國進步人士曾支持國際聯盟以及後來的聯合國，他們尋求建立一個全球民主進步「技術官僚管理」下的世界政府，並尋求支持此一目標的國際力量共同合作，罷黜那些不肯配合世界秩序的反動君主。因此，美國的利益在促進布爾什維克與協助他們掌權方面，發揮了主導作用。尤其是透過革命期間待在紐約的托洛斯基（Leon Trotsky），為俄國同志提供資金和武器。雖然托洛斯基是一個願意與美國利益合作的國際社會主義者，但他並不打算在俄羅斯奪權，而是想讓史達林接替列寧，走向更狹隘的方向，並優先考慮國內的社會主義而非全球合作。從那時起，美國進步人士與俄羅斯的利益相互關聯，試圖動搖俄羅斯重新與美國進步人士的利益合作，但計畫並未成功。因此，我們可以更理解懷特不應只被稱為共產主義間諜，而是作為一個尋求與俄國布爾什維克合作一項偉大計劃的美國進步人士，以便尋求戰後經濟的秩序。

大戰前的黃金標準。當然這件事並未成真，事實上，匯率是變動的，而且貨幣供應量還讓政府可以改變這些匯率而變成「根本不固定」。<sup>註 12</sup>

為了管理這項全球金融體系所希望的固定匯率，並解決任何潛在無法固定匯率的根本問題，布雷頓森林會議因此建立了國際貨幣基金組織（IMF），以作為全球中央銀行之間的國際協調機制，並達成匯率與資金流動的穩定目標。事實上，布雷頓森林會議是試圖透過中央規劃，來完成十九世紀國際黃金標準「自發性實現」的目標。在經典的黃金標準下，貨幣的單位是黃金，而資本和貨物在國家之間自由流動，自發地調整物流而不需要中央的控制或指導，也永遠不會導致國際收支平衡的危機：因為無論金錢或貨物跨境流動多少，都由其擁有者自行決定，不會出現宏觀經濟上的問題。

然而，在布雷頓森林體系中，政府由凱因斯主義經濟學家主導，他們將激進的財政和貨幣政策，視為政府政策上自然與重要的組成部分。而持續的管理貨幣和財政，自然會導致本國貨幣價值的波動，從而導致貿易和資本流動上的不平衡。當一個國家的貨幣貶值時，其產品對外國人來說變得更便宜，導致更多貨物離開該國，而貨幣持有人則會尋求購買外幣，以保護自己免受貨幣貶值所影響。

由於貨幣貶值通常伴隨著人為的低利率，資本會尋求移出該國，到能獲得更好回報的國家，卻也因此加劇貨幣的貶值速度。另一方面，當其鄰國貶值時，那些維持貨幣較優的國家將面臨資本流入，導致其貨幣進一步升值。因此貶值將播下更多貨幣貶值的種子，而貨幣升值則會導致更多的升值，相互為兩國政府帶來問題。而黃金標準不存在這樣的問題，所以兩

---

註 12 美國國務院，「第一卷」、「聯合國貨幣與金融會議論文集：新罕布什爾州布雷頓森林（*Proceedings and Documents of the United Nations Monetary and Financial Conference*）」，Bretton Woods, New Hampshire, 1944 年 7 月 1 日至 22 日。

國的貨幣價值是恆定的，也由於它是黃金，因此貨物和資本的變動並不會影響貨幣的價值。

黃金標準的自動調整機制，可以提供一個衡量所有經濟活動的恆定量尺，而浮動貨幣則讓世界經濟變得不平衡。國際貨幣基金組織的作用是在世界各國政府之間，進行不可能的平衡行動，並試圖在這一混亂中找到某種形式的穩定或均衡，並將匯率保持在預定數值的範圍內，但貿易和資本流動也一直變化並改變匯率中。倘若全球經濟沒有一個穩定的計價單位，那麼這個任務就像是想用一個每次使用時都有不同長度的彈性捲尺一樣，完全無法用來建造房子。

在布雷頓森林建立了世界銀行與國際貨幣基金組織之後，美國及其盟國希望建立另一個國際金融組織，專門用來負責安排貿易政策。此項建立國際貿易組織的初步嘗試失敗，因為美國國會拒絕批准該條款，不過在1948年出現了取代方案，亦即關稅暨貿易總協定（GATT）。關稅暨貿易總協定旨在幫助國際貨幣基金組織，完成「平衡預算和貿易」這項不可能的任務，以確保金融穩定。換句話說，就是用來集中規劃全球貿易、財政和貨幣政策以保持平衡，彷彿這樣的事情是可能辦到的。

布雷頓森林體系有個相當重要但經常被忽視的問題，亦即大多數成員國已經將大量黃金儲備轉移到美國，並以每盎司 35 美元的價格收取美元。

合理的說法是美元將成為全球貿易貨幣，各國中央銀行將透過美元進行交易與結算，可以省卻黃金實際流動的必要性。從本質上來說，這個系統類似於將整個世界經濟當作單一國家運行的黃金標準，由美國聯邦儲備銀行作為世界的中央銀行，世界上所有的中央銀行則當作區域銀行。而最主要的差別在於黃金標準下的貨幣紀律，幾乎完全消失在這個世界上，而且無法有效控制所有中央銀行擴張其貨幣供應，因為沒有任何國民可以將

政府貨幣換回黃金。只有政府才能用美元從美國贖回他們的黃金，事實證明這比預期的情況來得更為複雜。因為目前外國中央銀行以每盎司 35 美元收購的黃金，其市值超過 1,200 美元。

貨幣擴張主義成為新的全球基準，該制度與黃金之間的脆弱聯繫，證明它無力阻止全球貨幣狂墜，也無法阻止影響多數國家的持續性國際收支平衡危機。然而美國被放在一個非常重要的位置，雖然超出範圍，但有點像是當年羅馬帝國掠奪並放大多數舊世界所使用的貨幣供應量。當美元分佈在世界各地，中央銀行必須將其作為儲備以便互相交易，美國政府可以因擴大美元供應而獲取大量金錢，也沒有理由擔心會出現國際收支逆差。法國經濟學家 Jacques Reuff 創造了「無淚的赤字」這一短語，描述了美國獲得的新經濟現實，它可以從世界上購買任何想要的東西，並透過擴大整個世界都使用的美元發行量來為其融資。

第二次世界大戰結束後的前幾年裡，相關的財政限制很快就讓位給「只要通貨膨脹就可以買到免費午餐」這種政治上無法抗拒的誘惑，戰爭與福利國家更是如此。在第二次世界大戰期間興盛的軍事工業發展，成為艾森豪威爾總統所稱的軍事 / 工業綜合體，也就是一個巨大的工業集團，強大到足以要求政府提供更多資金，並推動美國外交政策走向無窮無盡的一系列昂貴衝突，沒有理性上的最終目的，也完全沒有明確的目標。

凱因斯主義好戰激進派學說，聲稱這種戰事花費對經濟有利，因此使得數百萬人的生命，更容易被美國選民所吞噬。

然而這種戰爭機器對美國人民來說也會覺得更加美味可口，因為它來自同樣的政治家，以各種形態和形式來加強政府福利。從大社會（The Great Society）計畫到負擔得起的住房、教育與醫療保健，法定貨幣讓美國選民忽視經濟法則，並且認為免費午餐或永遠有折扣的午餐，是有可能發生的。由



於缺乏黃金的可兌換性，也可以將通貨膨脹的成本分散到世界其他地區，因此唯一獲勝的政治方案便包含利用通貨膨脹來增加政府支出，且戰後每位總統任期裡，都可以見到政府支出與國債的成長，以及美元購買力的喪失等。在法幣可為政府提供資金的情況下，不同政黨之間的政治差異消失了，因為政治不再包含利益權衡，每位候選人都可從中獲益。

## 政府貨幣的軌跡紀錄

黃金微弱的可兌換性，是美國政府通貨膨脹主義裡的一個惱人細節，它呈現出兩種症狀：第一，全球黃金市場總是透過更高的金價，反映出通貨膨脹的現實。過去是由建立倫敦黃金總庫（London Gold Pool）來解決，該黃金總庫試圖透過減少政府持有的部分黃金儲備，賣到市場來降低黃金價格。這種方法可以暫時解決問題，但在 1968 年時，美元與黃金相比不得不重新估值，以面對多年來的通貨膨脹。第二個問題則是某些國家想從美國運回其黃金儲備，因為他們開始面臨紙幣購買力的下降。法國總統戴高樂甚至派遣一支法國艦隊到紐約，用來運回法國的黃金。但當德國人也打算運回他們的黃金時，美國決定自己已經受夠了。由於黃金儲備越來越低，因此尼克森總統在 1971 年 8 月 15 日宣布，停止外國美元兌換黃金，讓黃金價格在市場上自由浮動，不再與美元掛鉤。

事實上，美國違背了美元依固定匯率贖回黃金的承諾。國際貨幣基金組織負責維持的世界貨幣之間的固定匯率，現在已經放鬆，並由貨物和資本的跨境流動，以及日益複雜的外匯市場來做決定。

擺脫了黃金贖回藉口的最終限制後，美國政府以前所未有的規模擴大了貨幣政策，讓美元的購買力大幅下降而導致商品價格全面上漲。美國政

府與經濟學家，指責導致價格上漲的所有事物與所有人，但唯一逃過指責的卻是導致價格上漲的主要原因，也就是美元供應的增加。多數其他國家的貨幣表現更差，因為它們既是通貨膨脹的美元所支持下的受害者，同時也要面對發行貨幣的該國中央銀行所造成的通貨膨脹。

尼克森總統的這項舉動，完成了從第一次世界大戰時開始的完整進程，也就是將世界經濟從全球黃金標準，轉變為基於幾種政府發行貨幣的標準。對於一個日益全球化以及在交通與電信上進步的世界而言，自由波動的匯率構成了霍普（Hoppe）稱之為「局部易貨交易系統」<sup>註13</sup>。從在沙子上虛擬線條「另一邊」生活的人購買東西，需要使用一種以上的交易媒介，並且重新喚起之前提過的那種「缺乏需求巧合」的古老問題。因為賣方不想要買方持有的貨幣，所以買方必須先購買另一種貨幣，導致產生「轉換貨幣」的成本。隨著運輸和電信的進步，持續促成全球經濟的一體化，這些缺乏效率的成本也不斷增加。外匯市場的日交易量為 5 兆美元，純粹是由於缺乏單一的全球同質性國際貨幣，造成這種效率低下的結果。

雖然大多數政府都有自己發行的貨幣，但美國政府生產的是「支持其他政府貨幣」的主要儲備貨幣。

這是人類歷史上首次出現整個地球都使用政府貨幣來運作，雖然此種方式在多數學術圈裡被認為是正常和無庸置疑的，但這類主要貨幣形式的可靠程度仍值得探究。

理論上我們可以創造一種人為的稀有資產，然後賦予其貨幣角色。在放棄黃金標準之後，世界各國政府都這樣做了，比特幣的創造者也是如此，但結果卻截然不同。在法定貨幣與黃金之間的連結切斷之後，紙幣的

---

註 13 Hans-Hermann Hoppe, 「政府法幣如何可行？（How Is Fiat Money Possible?）」，  
奧地利經濟學評論，第 7 卷第 2 期，1994 年。

供應成長率高於黃金，因此其價值與黃金相比大幅下跌。美國在 1971 年貨幣供應的 M2（廣義貨幣供應量）總量約為 6000 億美元，現在則超過 12 兆美元，年均成長率為 6.7%。相對來看，1971 年 1 盎司黃金價值為 35 美元，現在的價值則超過 1,200 美元。

觀察政府貨幣的軌跡記錄，描繪隨時間變化下不同貨幣的庫存流量比綜合圖表。便可發現已開發國家相對穩定和強勢的貨幣，通常只會有個位數的成長率，但會具有較高的變異性，包括通貨緊縮衰退期間的供應收縮等<sup>註 14</sup>。而開發中國家的貨幣經常面對供應成長率接近庫存量比率，導致災難性的「超通貨膨脹（hyperinflation）」和持有該貨幣者的財富遭到破壞。世界銀行提供了 1960 年至 2015 年間，167 個國家廣義貨幣成長的數據，這些國家的年平均數據繪製在圖 6 中。雖然所有國家和所有年份的數據並非完整，但平均起來每個國家的貨幣供應成長率為每年 32.16%。

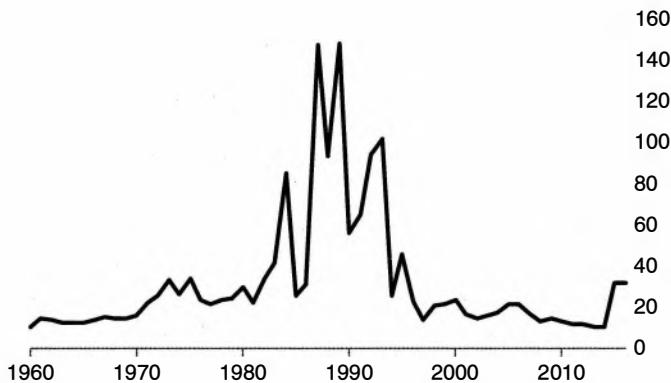


圖 6 1960 年至 2015 年間，167 種貨幣的廣義貨幣年均成長率

註 14 這是政府貨幣的一個很重要但常被低估的特徵。由於銀行在發放貸款時會製造貨幣，償還貸款或借款人破產會導致貨幣供應量減少。增加或減少貨幣供應量，要依據各國政府和中央銀行的決定。

32.16%的數字不包括幾個「超通貨膨脹」的年份，在這些年份裡貨幣被完全摧毀並以新貨幣取代，因此這項分析的結果，並不能明確告訴我們哪些貨幣表現最差，因為某些最重要的數據無法比較。

如果觀察一下「貨幣供應平均成長率最高的國家」表格所顯示出的這些國家名單，他們在追蹤紀錄期間裡，都有過幾次廣為公開的通貨膨脹事件。表 3<sup>註 15</sup> 顯示了貨幣供應量年均成長率最高的十個國家。

**表 3** 1960 – 2015 年間，年度廣義貨幣供應成長率最高的十個國家

國家	平均值
尼加拉瓜	480.24
剛果民主共和國	410.92
安哥拉	293.79
巴西	266.57
秘魯	198.00
玻利維亞	184.28
阿根廷	148.17
烏克蘭	133.84
亞塞拜然	109.25
亞美尼亞	100.67

在「超通貨膨脹」期間，開發中國家的國民出售本國貨幣，並且購買耐用品、各種商品、黃金和外幣等。

註 15 資料來源：世界銀行。

國際儲備貨幣如美元、歐元、日元和瑞士法郎，在世界上大部分地區都可買到，即使黑市也可以買到，滿足全球對儲存價值的大量需求。當你檢查貨幣供應成長率時，原因就變得很明顯，因為這些貨幣的供應成長率，相對來說較低。由於它們是全球多數人選擇使用的主要價值儲存，因此有必要將其供應成長率與較不穩定的貨幣，分開進行檢查。表 4 列出目前外匯市場上十種流通量最大的貨幣，以及 1960～2015 年和 1990～2015 年期間的年度廣義貨幣供應量成長率<sup>註 16</sup>。1960 年至 2015 年期間，十種最具國際流通性貨幣的平均值為 11.13%，而在 1990 年至 2015 年期間僅為 7.79%。這表示全球最受歡迎且銷售量最高的貨幣，近幾十年來的庫存流量比率高於其他貨幣，如同本書分析所預測的結果。

表 4 全球十大貨幣的廣義貨幣供應量年均成長率

國家 / 地區	年度貨幣供應成長率	
	1960-2015	1990-2015
美國	7.42	5.45
歐元區（19 個國家）		5.55
日本	10.27	1.91
英國	11.30	7.28
澳大利亞	10.67	9.11
加拿大	11.92	10.41
瑞士	6.50	4.88
中國	21.82	20.56
瑞典	7.94	6.00
紐西蘭	12.30	6.78

註 16 資料來源：所有國家使用世界銀行資料，歐元區使用 OECD.Stat 資料。

在國家貨幣浮動時代開始的 1970～1980 年間，是大多數國家經歷高通貨膨脹的時期。在 1990 年後情況好轉，平均貨幣供應成長率逐漸下降。經合組織（OECD）數據顯示，經合組織國家在 1990 年至 2015 年期間，年度廣義貨幣供應成長率平均為 7.17%。

我們可以看到世界主要國家貨幣的供應量，通常以可預測的低百分比成長。已開發國家比起開發中國家，有較緩慢的貨幣供應成長速度，開發中國家在近代歷史上，出現多次商品價格快速上漲與超通貨膨脹的情況。已開發國家的廣義貨幣成長率通常在 2%至 8%之間，平均約為 5%，也很少攀升至兩位數或下降至負值。而發展中國家的成長率則較不穩定，成長率可能會達到兩位數，有時甚至是三位數、四位數或下降為負值，反映出這些國家和貨幣的金融不穩定性較高（圖 7<sup>註 17</sup>）。

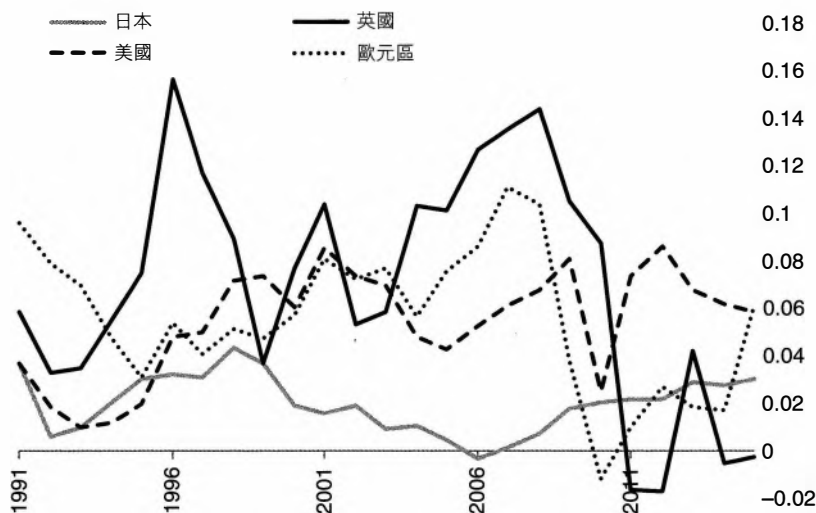


圖 7 日本、英國、美國和歐元區的年度廣義貨幣成長率

註 17 資料來源：OECD.Stat。

每年只有 5% 的成長可能聽起來不多，但它可以在 15 年內使一個國家的貨幣供應量翻倍。這就是白銀在黃金貨幣競爭中失利的原因，黃金的供應成長率較低，代表購買力所受的影響較為和緩。

「超通貨膨脹」是一種政府貨幣獨有的經濟災難。從來沒有一個超通貨膨脹的例子會發生在以黃金或白銀標準運行下的經濟體，即使像貝殼和飾珠這類人為製品，也是隨時間過程失去其貨幣角色，而且通常是慢慢失去，貨幣的替代品也會慢慢接管其付款的購買力。但由於政府貨幣的生產成本趨近於零，因此整個社會很有可能僅在幾個月甚至幾週的時間內，看到自己的所有儲蓄以貨幣的形式憑空消失。

超通貨膨脹比起人們喪失大量經濟價值來說，反而是危害更深的一種現象，因為它會讓幾世紀甚至幾千年所建立起來的社會經濟生產結構，更徹底的崩潰。而隨著貨幣的崩潰，除了基本求生以外，其他關於交易、生產或從事任何事情都變得不可能。由於消費者、生產者和工人們無法互相以狂貶的貨幣進行支付，幾世紀以來社會發展的生產與貿易結構崩潰，人們認為理所當然的一些商品也會開始消失，累積的資本也會被摧毀並拋售以資助消費。首先是奢侈品的消失，但很快的就會遵循生存基本要素，也就是人類一直退化回野蠻狀態，必須自生自滅，努力確保最基本的生存需求。如此隨著個人生活品質顯著衰退，絕望開始轉變為憤怒，想要尋找代罪羔羊。此時最會煽動群眾與掌握機會的政治家，便可利用這種情況激起人民的憤怒而贏得權力。最活生生的例子便是 1920 年代威瑪共和國的通貨膨脹，不僅導致世界上最先進繁榮經濟體的破壞與崩潰，還助長希特勒的崛起。

即使教科書說「由政府管理貨幣供應帶來許多優點」是正確的，但世界任何地方的超通貨膨脹危害，將遠遠超過由政府管理貨幣的優點，政府貨幣開始的這個世紀，帶來了遠比任何一個災難事件都更為嚴重的後果。

在 Steve Hanke 與 Charles Bushnell 的研究內容撰寫之際，委內瑞拉便經歷了這種諷刺所比喻的真實事件，遭受貨幣崩毀的蹂躪，但其實這種事件從第一次世界大戰結束以來，已經發生過 56 次。Hanke 和 Bushnell 將超通貨膨脹定義為「在一個月內價格上漲超過 50%」。他們已驗證了歷史上 57 次超通貨膨脹事件<sup>註 18</sup>，其中只有一次發生在貨幣民族主義時代之前，也就是 1795 年的法國通貨膨脹——密西西比泡沫，這也是因為政府貨幣所造成，而且是由現代政府貨幣名譽之父 John Law 所設計。

政府提供貨幣的問題在於貨幣健全與否，完全取決於負責的人如何控制不讓供應膨脹的能力。只有政治方面的限制才能提供貨幣的「硬度」，因此並沒有物理、經濟或自然方面的條件，可以限制政府只能生產多少貨幣。牛隻、銀、金和貝殼都需要認真努力的生產，不可能在短時間內大量出現，但政府貨幣卻只需要政府的一紙命令即可。不斷增加供應代表貨幣會持續貶值，剝奪持有者的財富，使那些印刷貨幣的人與最早收到貨幣的人受益<sup>註 19</sup>。歷史已經證明，政府會難以避免的屈服於膨脹貨幣供應量的「誘惑」。無論理由是因為徹底貪污或「國家緊急情況」，甚至是通貨膨脹經濟學派造成的干擾，政府總是會找到理由與方法來印更多的錢，擴大政府權力並減少貨幣持有者的財富。這與銅生產商人開採更多銅以應對銅的貨幣需求一樣；獎勵貨幣產品的生產者，但懲罰了那些將銅當作儲蓄價值的人。

---

註 18 Steve Hanke 與 Charles Bushnell，「委內瑞拉登上記錄：Hanke-Krus 世界超通貨膨脹表第 57 筆記錄（Venezuela Enters the Record Book: The 57th Entry in the Hanke-Krus World Hyperinflation Table）」，應用經濟學研究，第 69 期（2016 年 12 月）。

註 19 愛爾蘭裔法國經濟學家 Richard Cantillon 在十八世紀的解釋之後，這種現象便被稱為「坎蒂隆效應」（Cantillon Effect）。根據 Cantillon 的說法，貨幣供應擴張的受益者是最先收到新貨幣的人，他們能在因自己所造成的物價上漲之前花錢。而從他們那裡收到貨幣的人，會先面臨一點物價上漲。隨著錢花得更多，物價持續上揚，一直到較後面才收到貨幣的人，必須承受實際的購買力下降。這就是為何通貨膨脹會傷害最貧困的人口，而幫助了現代經濟富有者的最佳解釋。從中受益最多的人是能獲得最多政府信貸的人，而受傷最多的則是那些領固定收入或最低工資的人。



若一種貨幣可靠的證明其供應量不會擴大，便能立刻獲得顯著的貨幣價值。2003 年當美國入侵伊拉克時，空中轟炸摧毀了伊拉克中央銀行，也摧毀伊拉克政府印製伊拉克第納爾的能力。由於沒有中央銀行來印製第納爾，因此伊拉克人對其貨幣更加信任，導致第納爾一夜之間大幅升值<sup>註 20</sup>。類似的故事也發生在索馬利亞先令上，因為他們的中央銀行也被摧毀了<sup>註 21</sup>。在明顯變得稀有而非易於貶值的情況，人們才會更想得到政府貨幣。

有幾種原因讓政府貨幣成為這個時代的主要金錢形式。首先，政府會要求稅收以該政府貨幣支付，也就是說一般人只能接受，這使得政府貨幣在可銷售性方面具有優勢。其次，政府對銀行系統的控制和監管意味著銀行只能用政府批准的貨幣開立帳戶與進行交易，從而使政府貨幣的可銷售程度高於其他任何潛在競爭對手。第三，許多國家的貨幣法規中，明定了使用其他形式的貨幣進行支付是違法的。第四，所有政府貨幣仍由黃金儲備所支持，或是由黃金儲備支持的貨幣所支持。根據世界黃金協會（World Gold Council）的數據顯示，各國中央銀行目前的儲備黃金約為 33,000 噸。由於許多政府沒收了人民與銀行的黃金，並迫使大家使用政府發行的貨幣，因此各國中央銀行的黃金儲備量，在二十世紀初期迅速上升。在 1960 年代後期，由於布雷頓森林體系在貨幣供應增加的壓力下日趨窘迫，因此各國政府開始卸下部分黃金儲備。但在 2008 年趨勢開始逆轉，中央銀行重新回購黃金，全球黃金供應量也增加。諷刺的是，在政府貨幣時代，政府本身擁有的官方儲備黃金，比 1871~1914 年的國際黃金標準還多。

---

註 20 「美元還是第納爾？（Dollar or Dinar?）」、米塞斯日報，參閱 <https://mises.org/library/dollar-or-dinar>。

註 21 J. P. Koning, 「孤兒貨幣：索馬利亞先令的奇怪案例（Orphaned Currency: Odd Case of Somali Shillings）」參閱 <https://jpkoning.blogspot.ca/2013/03/orphaned-currency-odd-case-of-somali.html?m=1>。

黃金顯然沒有失去其貨幣角色；仍然是債務的唯一終結者，是唯一一種自身價值不需依賴他人，也沒有交易對手風險的主要全球資產。然而其貨幣角色僅限於中央銀行，個人則被規定必須使用政府貨幣。

中央銀行大量的黃金儲備，可以作為在黃金市場上售出或租賃的緊急供應，以防止黃金價格在需求增加時上漲，保護政府貨幣的壟斷作用。正如葛林斯潘曾經解釋：「若金價上漲，中央銀行隨時準備以更多的數量租賃出黃金<sup>註 22</sup>」（參考圖 4<sup>註 23</sup>）。

而隨技術發展允許形式更複雜的貨幣，包括易於攜帶的紙鈔等，也帶來了新的可銷售性問題，亦即賣方在沒有第三方對貨幣可能進行的限制干預下，賣掉自己貨幣的能力。這點並非商品貨幣本身存在的問題，因為它的市場價值來自「市場」，並且無法由第三方記錄其交易：牛、鹽、黃金和白銀都有販售的市場與買家。但由於政府將貨幣發行作為商品的代價可忽略不計，因此發行貨幣的政府可能會損害貨幣的可銷售性，甚至宣稱它不再適合作為法定貨幣。2016 年 11 月 8 日的印度便發生了這類事件，因為印度人一覺醒來，聽到政府突然說要暫停 500 和 1000 盧比的法定貨幣身分，轉眼之間，高度暢銷的貨幣就失去它的價值，而且必須排很長的隊伍到銀行進行交換。

隨著越來越多的人開始減少對現金的依賴，更多的人將資金投入政府監管的銀行，使其更容易被沒收或進行資產控制。事實上，這些程序通常發生在經濟危機期間，也就是當時個人最需要這些貨幣的時候，這也是政府發行的貨幣在可銷售性的主要障礙。

---

註 22 「對金融衍生品的監管。」美國眾議院「銀行和金融服務委員會主席」葛林斯潘的證詞。1998 年 7 月 24 日。

註 23 資料來源：世界黃金協會儲備統計。參閱 <https://www.gold.org/data/goldreserves>。

政府對貨幣的控制，已經把貨幣從生產價值的回報，變成了對政府官員服從的回報。如果政府不肯接受的話，任何以政府貨幣來累積財富都很不切實際，因為政府可以從壟斷控制的銀行中沒收你的資金，或放大貨幣發行量以貶值持有人的財富，並將貨幣獎勵給最忠誠的人，徵收重稅並懲罰逃稅的人，甚至還可以取消帳單等。

在奧地利經濟學家 Menger 的時代，確定什麼是「最佳貨幣」的標準，圍繞著了解可銷售性與市場選擇的貨幣。而在二十世紀裡，政府對貨幣的控制，代表一個新的、非常重要的標準被加入可銷售性中，亦即根據其持有人的意願，而非由其他人所控制，這就是貨幣的可銷售性。將這些標準結合起來，便可完全理解「健全貨幣」這個術語的意義：也就是市場所自由選擇的貨幣，完全由個人所能掌控，並且是在自由市場而非從任何其他第三方手上，合法取得的貨幣。

雖然 Mises（米賽斯）在他的時代支持黃金作為貨幣的「堅定捍衛者」角色，但他明白這種貨幣角色並非黃金所固有或內在的東西。身為奧地利傳統經濟學的院長之一，Mises 很清楚價值必須存在於人類意識上，因為金屬和物質並沒有內建的東西可以賦予它們貨幣的角色。而對於 Mises 來說，黃金的貨幣地位是由於它滿足了作為「聲錢」的條件，如他所說：

「聲錢」的原則有兩方面，正面的部分是同意市場選擇作為常用的交易媒介，負面的部分則在於阻礙政府干預貨幣體系的傾向<sup>註24</sup>。

---

註 24 Ludwig von Mises, 「金錢與信用理論 (*The Theory of Money and Credit*)」, 第二版, 紐約州哈德遜歐文頓鎮: 經濟教育基金會, 1971 年, 第 414-416 頁。

根據 Mises 的說法，聲錢是市場自由選擇下的貨幣，仍可由其持有者控制，不會被插手管理或強制干預。

只要錢是由持有者以外的某人所能控制，無論控制它的人是誰，總會強烈的想透過通貨膨脹或沒收手段，來竊取貨幣的價值，並作為在眾多持有人身上實現「政治目標」的工具。事實上這種方式可以很有效的從生產者手中獲取財富，並交給那些專門控制貨幣而不實際生產社會價值的人，就像歐洲商人透過在第 2 章中所提到的廉價珠子充斥其市場，以掠奪非洲社會一樣。當這種財富的途徑仍然開放時，任何社會都沒有繁榮的機會，而且代價就是被那些尋求富裕生活途徑的人，把社會變得貧窮。換個角度講，健全的貨幣可以讓大家保有價值，對任何人來說都是通往繁榮社會的唯一途徑，可以讓社會的整體努力，集中在生產、合作、資本累積與貿易上。

二十世紀可說是不健全貨幣與國家無所不能的世紀，由於政府拒絕把貨幣交由市場選擇，並將政府發行的紙幣以暴力威脅強加給人民。隨時間推移，政府也就能夠控制越來越大的國民收入佔比，支出和赤字也持續增加，貨幣不斷貶值，因此離健全貨幣便越來越遠。而政府持續干涉生活的各個層面，也就越能控制教育系統，並利用教育在人們的腦海中植入「經濟學規則不適用於政府」的念頭，並說這種規則會使他們的花費越來越多。凱因斯以這種鬆動貨幣的作法，在現代大學傳授的觀念便是：政府支出只有收益，而非成本。畢竟，政府總是可以印鈔票，因此不會對其支出產生任何實際限制，也就可以用來實現選民希望政府達成的任何目標。

對於那些崇尚政府權力並享受極權控制的人，例如二十世紀裡的許多極權主義和進行大規模謀殺的政權而言，這種貨幣的安排就如同上天賜予的禮物。但對於那些重視人類自由、和平與合作的人來說，經濟改革的機會逐漸消退，而政治進步的前景，也讓回歸貨幣理性成為幻夢的這種情況，真是令人沮喪的一刻。

正如海耶克所說：

在把貨幣發言權從政府手中奪回之前，我不相信人們能有機會再獲得「好錢」，也就是說，既然無法暴力地從政府手中奪權，我們所能做的便只有利用狡猾迂迴的方式，引進一些「他們無法阻止的東西」<sup>註 25</sup>。

這場 1984 年的演講裡，海耶克的先見之明現在聽起來十分傑出，因為當時這種「他們無法阻止的東西」的實際形式還不明朗。在他說出這些話後的三十年間，以及在整個世紀裡，政府不斷擦掉黃金標準作為健全貨幣的痕跡後，世界各地的人們終於開始有了機會，以市場和政府以外自由選擇新形式的錢，進行儲蓄和交易。在醞釀初期，比特幣似乎就己能滿足米賽斯和海耶克的所有要求：一個高銷售性的自由市場選擇，並且可以抵制政府的干預。

---

註 25 摘自 1984 年與弗萊堡大學的 James U. Blanchard 進行的訪談影片。

## 5

## 金錢與時間偏好

---

**貨**幣健全與否，是以自由市場選擇的可銷售性來決定，因為它可以跨越時間保持其價值，亦可以跨越空間有效的延續價值，同時還可以被劃分成不同大小的規模來進行交易。貨幣的供給不能由強制的權威機構操縱，強迫作為其他的用途。從前面的討論以及奧地利經濟學家所提供的貨幣經濟學原理來看，健全貨幣的重要性可以解釋成三個主要原因：第一，它保護了貨幣跨越時間的價值，激勵人們更仔細的思考未來，降低他們在短期時間上的需求偏好。而降低時間偏好更可累積價值，啟發人類文明進步，促使人類合作、繁榮與安居樂業。第二，健全貨幣可以讓貿易有穩定的基礎計價單位，促成更大的市場，不受到政府控制和脅迫，自由貿易更能帶來和平與繁榮。

此外，計價單位對各種形式的經濟計算與規劃都不可或缺，而不健全的貨幣會使經濟計算變得不可靠，也成為經濟衰退與經濟危機的根本原因。最後，健全貨幣是個人免於專制與壓迫的必要條件，因為極權國家創造貨幣的能力，給了政府不正當的權力，而這種權力本質上會吸引最不值得、也最不道德的人，努力去攫取權力的韁繩。

健全的貨幣是決定個人「時間偏好」的主要因素，這是個人在做決策時，一個相當重要且被廣泛忽略的觀點。時間偏好是指個人比較重視現在或比較重視未來，因為人類不會永遠活著，在任何時刻都有可能突然死亡，而使未來變得不確定。而由於消費是生存所必需，人們總是比較重視現在的消費，而非未來的消費，因為缺乏現在的消費，未來便可能永遠不會到來。換句話說，時間偏好對所有人來說都是正值；因此與現在相比，對未來的偏好總是會打點折扣。

更進一步來看，由於我們可以利用時間和資源來生產更多商品，人類的理性總會偏向於現在多於未來，想擁有更確定數量的資源，用來生產更多商品。而對於願意延遲一年才獲得商品的人來說，便需可以在未來獲得更多的商品才行。誘惑個人願意延後獲得商品所需增加的商品數量，便是決定時間偏好的主要原因。所有理性的個體都有「非零」（或正或負）的時間偏好，但時間偏好會因人而異。

動物的時間偏好遠高於人類，因為它們的作用是滿足直接的本能衝動，很難有「未來」的概念。不過有些動物能夠建造未來可以使用的巢穴或家園，因此這些動物的時間偏好，便低於僅求滿足飢餓和侵略等直接需求的動物。人類具有較低的时间偏好，因此能夠遏制我們的本能和動物衝動，並能思考對未來更有利的事情，然後採理性行動而非衝動。若可以產生更優質的商品時，人類便可選擇生產更長時間才能完成的商品，而不會把所有時間都花在生產「即時」的消費需求上。

隨著人類減少時間偏好，便可開發在「更長時間範圍」內才能完成的任務，來滿足更多的遠程需求，並可開發出生產未來商品而非生產立即消費商品的心態，換句話說，可以創造出「資本商品」。

動物和人類都會打獵，但人類與動物有別之處在於肯花時間開發狩獵工具。有些動物可能會隨機使用工具來捕獵其他動物，但它們沒有能力擁

有這些工具，維持長期的使用。只有透過較低的時間偏好，人類才能決定花時間遠離狩獵，並將這段時間用於建造不能吃的長矛或釣竿，讓他可以更有效的捕獵。這就是投資的本質：人們把立即滿足延後，將時間與資源投入資本商品的生產，進行更複雜或技術更先進的生產，並延伸應用到更長的時間範圍。這種選擇「延遲滿足」以便在較長時間內從事風險生產的唯一原因，在於這些較長的過程，將會達成更多產量以及更優質的產品。換句話說，投資可以提高生產者的生產力。

經濟學家 Hans-Hermann Hoppe 解釋：一旦人類的時間偏好下降到足以讓任何儲蓄、資本或耐用消費品形成時，隨著時間經過，時間偏好會進一步下降，也就形成人類「文明過程」的開始。<sup>註1</sup>

花時間製作釣竿的漁民，每小時能捕到的魚獲會比用徒手捕魚的漁民多。但建造釣竿的唯一方法，便是將最初的工作時間用於無法產出食用魚的工作，亦即把時間花在生產釣竿上。這是一個「不確定」的過程，因為釣竿可能不好用，漁夫可能完全浪費時間而沒有收穫。投資不僅需要延遲滿足，還可能帶來失敗的風險，這就表示投資只會在期待有獎勵的情況下進行。個人的時間偏好越低，就越可能參與投資，延遲滿足並累積資本。

資本累積越多，勞動的生產率越高，生產的時間範圍也會越長。

為了更生動的描述這種差異，請假設有兩個人相互之間的比較。這兩人都赤手空拳從零開始，但兩人有不同的時間偏好：例如假設是哈利比琳達有更高的時間偏好。哈利選擇只用手抓魚，每天需要花大約 8 個小時捕到足夠的魚來養活自己。另一方面，琳達具有較低的時間偏好，每天只花 6 個小時捕魚，然後每天食用較少量的魚，並花兩個小時來製作釣竿。

---

註1 Hans-Hermann Hoppe, 「民主：失敗的神 (*Democracy: The God That Failed*)」, 第 6 頁。



一週過去了，琳達成功製作出一根工作用的釣竿。在第二週，她用釣竿在相同的八小時內，捕獲哈利漁獲量的兩倍。琳達對釣竿的時間投資，讓她可以每天只工作四小時，就吃到跟哈利相同數量的魚，而由於她的時間偏好較低，因此她不滿足於自己目前的成就，相反的，除了花四小時捕到哈利在八小時才能捕獲的魚之外，又花另外四個小時更進一步的累積資本，例如建造自己的漁船。一個月後，琳達擁有一根釣竿和一艘船，讓她可以更深入大海，捕到哈利從未見過的魚。琳達的生產力不僅只是在每小時提高；她所捕獲的魚也跟哈利有所不同，也能捕到更好的魚。現在她只需要一個小時的捕魚時間，就能確保一天食用所需的漁獲量，因此她將剩下的時間用於更多的資本累積，例如建造更好更大的釣竿、漁網和船，進一步提高生產力並提高她的生活品質。

如果哈利與他的後代，繼續依照同樣的時間偏好來工作和消費的話，後代們將繼續過著跟他一樣的生活，具有跟他一樣的消費和生產力。而如果琳達和她的後代繼續享有同樣較低的时间偏好，便可不斷提高生活品質，增加資本存量，並以更高的生產力水平從事勞動，完成必須花費更長時間才能製造的商品。在現實生活裡，跟琳達後代相同的例子，便是當今世界上最大的拖網漁船 *Annelies Ilena* 號的擁有者。這艘強大的捕魚機器在 2000 年完成之前，花費數十年的時間來構思、設計和建造，它也能繼續運行數十年，為低時間偏好的投資者，提供花了這麼多年建造過程的資本回報。

琳達的後代在生產魚的過程方面，已經變得既漫長又複雜，可能需要花數十年的時間才能完成，而哈利的後代每天仍要花八個小時來完成捕魚。像琳達後代的生產力遠高於哈利後代的這種差異，才是值得參與更長生產過程的主要原因。

時間偏好重要性的關鍵證明，來自 1960 年代後期著名的史丹佛棉花糖實驗<sup>註 2</sup>。心理學家 Walter Mischel 把小孩留在一個放了棉花糖或餅乾的房間裡，然後告訴孩子們想吃的話，可以直接吃掉沒關係，不過他會在 15 分鐘內回來，屆時如果糖果沒被吃掉，便會給他們第二顆糖果作為獎勵。換句話說，孩子們可以選擇立即滿足於一顆糖果，或者延後滿足而收到兩顆糖果。這是一種測試兒童時間偏好的簡單方法：時間偏好較低的學生可以等待第二顆糖果，而時間偏好較高的學生則無法等待。數十年後，Mischel 追蹤調查這些人，發現與當年的棉花糖測試對照下，低時間偏好的孩子長大後，很明顯的具有較好的學業成績、較高的 SAT 分數、較低的體重與較少藥物成癮的情形。

身為一位經濟學教授，我會在自己教授的每門課程裡，仔細講解棉花糖實驗。因為我認為這是在經濟學上，可以教給學生最重要的一課，但我也很訝異在各大學的經濟學課程裡，幾乎完全忽略這一課，甚至許多學院派經濟學家，完全不熟悉時間偏好及其重要性。

雖然微觀經濟學關注的是個人之間的交易，宏觀經濟學則考量政府在經濟作用裡的角色，但事實上對任何個人幸福最重要的經濟決策，是來自他們對於未來所做的時間考量。

每個人每天都會跟其他人進行某些經濟交易，但他們會跟未來的自己，進行更多的交易。這些交易的例子很多：例如決定省錢而非花錢；決定投資學習以獲得未來就業的技能，而非尋求低薪的直接就業；購買功能性和價格合理的汽車，而非為名貴的汽車負債；加班工作而不是和朋友出

---

註 2 Walter Mischel、Ebbe B. Ebbesen 與 Antonette Raskoff Zeiss，「延後滿足的認知與注意機制（Cognitive and Attentional Mechanisms in Delay of Gratification）」，人格與社會心理學雜誌，第 21 卷，第 2 期（1972 年）：第 204-218 頁。

去聚會；或者，我最喜歡在課堂上舉的例子：決定每週都研讀每學期的課程內容，而非在期末考前一晚臨時抱佛腳。

在上述每個例子裡，都沒有人強迫你作決定，而且這些選擇下的後果，無論成敗，主要的受益者或輸家都是個人本身。決定個人生活選擇的主要因素是時間偏好，雖然時間偏好和自我控制因人而異，但整體而言，在決策的各個方面都可以找到強烈的關聯性。我們應該牢記清楚的事實：一個人在生活裡的命運，大部分取決於他與未來自我之間的這些交易。儘管他想把自己的失敗怪罪給別人，或者將成功歸功於他人，但他跟自己一起進行的這些交易，可能會比任何外部環境或條件更為重要。無論時間偏好較低的人如何受到現實情況考驗，都可能會找到一種方法來讓未來的自我保持優先，直到目標實現為止。無論用多少未來財富來吸引具有較高時間偏好的人，他可能也會找到方法繼續破壞和欺騙未來的自己，例如那些戰勝一切困難與不利環境的人，或者那些擁有豐富技術與才能的人，他們的故事也可能形成鮮明的對比，儘管這些故事讓他們獲得了豐厚回報，但較高的時間偏好仍會讓他們浪費所有才能，未替自己帶來持久的利益。例如許多專業運動員和演藝人員，雖然賺到大量的錢，但也常在死後身無分文，因為他們的高時間偏好戰勝了未來的自己。另一方面，許多沒有特殊才能的普通人勤奮工作，為實現經濟保障而存錢並做長期投資，讓孩子未來的生活可以過得更好。

只有透過降低時間偏好，個人才能開始欣賞長期投資的美好，並開始優先考慮未來的收穫。

當一個社會裡給孩子的遺產比自己從父母那裡得到的更多時，便可稱為文明社會：因為生活逐漸改善，生命的目的也在於讓下一代生活變得更好。隨著社會資本水平不斷提高，生產力隨之增加，生活品質也跟著提高。社會的基本需求獲得保障，也可遠離危險環境，因此人們不會只追求

物質幸福或辛苦工作，而可以將注意力轉向生活裡更深的層面。他們經營家庭與社會關係；從事文化、藝術與文學項目；並尋求為社會與世界提供持續的貢獻。文明的重點不是在累積更多的資本；而是在資本累積後，可以讓你實現什麼，當基本需求可以滿足、最迫切的危險也可以避免時，便可追求生活意義更高的繁榮與自由。

個人的時間偏好由許多因素決定<sup>註3</sup>。自己與財產的安全，可說是最重要的因素之一。生活在衝突和犯罪地區的人，喪命的機率大增，因此可能會對未來的期望值打折，導致比生活在和平社會的人有更高的時間偏好。財產安全也是影響個人時間偏好的另一個主要因素：經常被政府或小偷剝奪個人財產的社會，當然會有更高的時間偏好，因為這種行為會讓個人優先考慮將資源用於即時滿足，而非投資於隨時可能會被剝奪的財產。稅率也會對時間偏好產生不利的影響：稅收越高，個人可保留的收入便越少；這也導致個人在稅收範圍內的工作機會減少，對未來的儲蓄當然也變少，因為稅收負擔比起消費，更容易降低儲蓄，尤其對於低收入者來說，大部分的消費都是基本生活所需。

而跟我們的討論最相關的時間偏好影響因素，便是預期貨幣的未來價值。

在人們可以隨意選擇貨幣的自由市場下，最可能會選擇的是「跨越時間」仍能維持價值的貨幣形式。貨幣越能維持價值，就越能激勵人們延遲消費，進而將資源投入未來的生產，形成資本累積以改善生活水準。同時

---

註3 讀者可以參考 Hoppe 的「民主：失敗的神 (*Democracy: The God That Failed*)」第1章裡對這些因素的精彩討論。更多的基礎和技術討論則可在 Murray Rothbard 的「人、經濟和國家 (*Man, Economy, and State*)」第6章、Mises「人類行為 (*Human Action*)」的第18、19章以及 Eugen von Böhm-Bawerk 的「資本與利益 (*Capital and Interest*)」中找到。

也會讓人們在其他方面，例如生活裡「非經濟」的部分，具有較低的時間偏好。而當經濟決策可以朝向「未來」發展時，各種決策很自然的都會隨之朝向未來。人與人之間會變得更和平與合作，並了解合作比起衝突的短暫獲利來說，才是更有價值的長期戰略。因此人們也會培養出強烈的道德感，優先考慮可以為自己及子女帶來最佳長期結果的道德選擇。而且比較會長遠考慮的人，比較不需要欺騙、撒謊或偷竊，因為這種動作的獎勵在短期內可能不錯，但從長遠看，比較可能帶來毀滅性的負面影響。

貨幣購買力的下降，有點類似於徵稅或強制徵收的形式，即使表面上的價值不變，仍會降低貨幣的實際價值。在現代經濟裡，政府發行貨幣與人為降低利率有密切關聯，這也是現代經濟學家的理想目的，因為降低利率可以促進借貸和投資。但這種操縱資本價格的效果，是在人為降低儲戶、投資者以及借款人支付的利率。這種過程的自然含義是減少儲蓄並鼓勵借貸。在這段期間，個人將會花掉更多的收入，並且向未來預支更多的錢。如此一來，不僅對他們在財務決策裡的時間偏好產生影響；也很可能影響生活中的一切。

長遠來看，從保有或提升價值的貨幣轉向會損失價值的貨幣，將會是一場相當重大的轉變：社會整體的儲蓄減少，累積的資本也變少，甚至開始消耗原先的資本。工人的生產率保持不變或者下降，即使神奇的透過印刷更多貶值紙幣來增加名義上的工資，但實質的工資仍會停滯不前。隨著人們開始增加消費和減少儲蓄，他們會在所有的決策中變得更加面對現實，因而導致道德上的瑕疵，甚至提高參與衝突、破壞、自我毀滅行為的可能性。

這有助於解釋為何文明在健全貨幣體系下興盛，但在貨幣體系貶值時就會瓦解，就像羅馬人、拜占庭人和現代歐洲社會一樣。十九世紀文明與二十世紀文明的對比，可以從「遠離健全貨幣」與所有隨之產生的問題背景中，加以理解。

## 貨幣通貨膨脹

整個歷史都見證了一個簡單的事實，那就是任何想到創造某種貨幣媒介的人，都會嘗試建立此貨幣媒介，因為參與這種做法的誘惑力實在太強了。然而創造貨幣媒介並非對社會有所貢獻的舉動，因為任何規模的經濟體都會有已經足夠的金錢。越能在製作生產上有所限制的貨幣媒介，便越能作為交換媒介與穩定的價值儲存。跟其他商品不同的是，貨幣作為交換媒介時，其價值儲存和會計單位的功能，與貨幣數量的多寡是背道而馳的。貨幣的重要性在於其購買力，而非數量多寡，因此任何數量的貨幣都足以履行貨幣功能，只要它可以在規模上被分割與組合，來滿足持有者的交易和儲存需求。任何數量的經濟交易，都可透過任何規模的貨幣供應來支持，前提是只要這些單位夠用也可拆成更小單位即可。

理論上理想的貨幣會是一種「供應固定」的貨幣，亦即沒有人可以生產更多貨幣。在這樣的社會裡獲得金錢唯一不犯罪的方式，便是為他人創造有價值的東西，然後向他們換得貨幣。當每個人都想獲得更多的錢，便會更努力工作並生產更多價值，從而改善每個人的物質幸福，然後再使人們累積更多的錢並提高生產力。只要能防止他人增加貨幣供應，這種錢便可用來作為價值儲存；而當儲存的財富不會隨著時間經過而貶值時，便會鼓勵儲蓄，並讓大家對未來有更多的考量。隨著財富和生產力不斷增加、關注未來的能力提高，人們便會開始降低他們的時間偏好，專注於改善生活中「非物質」層面，包括精神、社會與文化方面的努力。

然而事實證明，不可能出現一種無法創造出更多數量的貨幣形式。無論選擇何種交換媒介，都會因升值而導致更多人試圖生產更多交換媒介。歷史上最好的貨幣形式，便是能使新的貨幣供應與現有庫存量相比，變動最小的貨幣，以便讓創造新貨幣無利可圖才行。例如黃金作為貨幣堅不可

摧，因為它是一種庫存量自開採以來一直成長的金屬。由於金礦開採已持續數千年，煉金術方面也未有大規模的商業可行性，因此新開採的黃金供應仍只佔現有黃金庫存的一小部分。

這種性質便是為何黃金已成為「聲錢」的代名詞：因為物理和化學上的「鐵則」，讓黃金供應得到保障，亦即永遠不會大量的增加。儘管人類一再嘗試，但幾世紀以來仍未能產生比黃金更健全的貨幣形式，這就是為何它一直是歷史上大多數人類文明所使用的主要貨幣工具。即使世界已經轉變為以政府貨幣作為價值儲存、交換媒介與會計單位，政府本身仍會儲備大量的黃金，並且佔了世界黃金總供應量的極大比例。

凱因斯抱怨說，黃金開採是一項相當浪費的活動，不僅消耗大量資源，也沒有為真實的財富增加任何東西。雖然他的批評確實帶有關鍵的真實性，亦即增加貨幣媒介供應，並不會增加使用該貨幣的社會總財富，不過他忽略了黃金作為貨幣的角色，是因為比起其他金屬來說，黃金是種只能吸引少數人和資本資源來勘探與開採的金屬。因此即使金價飆升，黃金的供應增加數量也一樣不會變多。而由於黃金較為罕見難找，因此開採黃金當成貨幣的利潤，將遠低於開採其他任何可能作為貨幣角色的金屬，導致挖掘黃金的人力時間和資源也會最少。若是任何其他的金屬被當作貨幣媒介時，每當社會的時間偏好下降，越來越多人購買金屬用來儲存時，便會提高該種金屬的價格，為生產更多該種金屬帶來龐大的利潤。

由於這種非黃金的金屬一定較容易腐蝕，因此新的產量將會比現有庫存的百分比（相對於黃金）大得多（如之前銅的範例所示），因而價格降低並使持有者的儲蓄貶值。在這樣的社會中，儲蓄者的財富很快就會被偷走，利益會轉移給那些開採金屬，且讓該金屬產量遠遠超出經濟用途的人。這種社會裡也很少發生儲蓄或有用的生產，因為大家接著就會對生產貨幣媒介的獲利痴迷，社會將越來越腐敗，然後被更富有生產力的社會取

代和征服，因為別的社會裡的人會有更好的事情可以做，不必貪圖生產更多的貨幣媒介。

貨幣持續競爭下，會使個人和社會處於不利地位，因為這些人將儲蓄投資於黃金以外的金屬，也因此獎勵了那些將儲蓄投入黃金的人，因為黃金生產無法輕易擴增，也因為它會讓人們將努力導引到生產貨幣以外的東西，產出更多有用的商品與服務。這點有助於解釋為何阿拉伯學者 Ibn Khaldun 認為「黃金探勘和採礦」是繼綁架勒索贖金者後，「最不受尊敬的職業」<sup>註 4</sup>。愚蠢的凱因斯譴責黃金作為貨幣的行為，因為他認為黃金開採太過浪費，但實際上黃金在所有可能當作貨幣用的金屬來說，反而是最不會浪費的。不過凱因斯的「解決方案」更是愚蠢，因為他替黃金提出一個「法定貨幣」標準，然後將更多的人力時間、勞動力與資源，用來確保貨幣的供應與從中獲利。在黃金作為貨幣媒介的歷史中，從來沒有僱用像今天的中央銀行行員那麼多的礦工與工人。而且所有相關的銀行和企業，都可透過與貨幣印刷機緊密連結而獲利，這點將在第 7 章裡加以討論。

當新供應與現有供應相比微不足道時，貨幣的市場價值，便取決於人們願意持有該貨幣以及願意用它來消費的意願。這些因素會隨時期不同而有所差異，因為個人的意願，將取決於願意擁有大量貨幣或願意擁有較少貨幣的不同時期。

但整體而言，它們對「整個社會」來說會略有不同，因為貨幣是市場上邊際效用最小的商品。而「邊際效用遞減規律」正是經濟學的基本定律之一，亦即它在獲得更多其他商品後，都會降低每個額外單位的邊際效用。貨幣的存在並非為了自身的利益，而是為了可以與其他商品進行交易，因此它的效用會比任何其他商品減少得慢一些，因為它一定可以換成任何其他商

---

註 4 Ibn Khaldun, *Al-Muqaddima*。



品。隨著個人持有的房屋、汽車、電視、蘋果產品或鑽石的增加，他們對每個額外單位的邊際估值便會下降，因而導致對累積更多商品的意願減少。但是擁有更多的貨幣並不會像這些商品一樣，因為持有更多的貨幣，代表持有者可以很方便的將貨幣兌換成心裡最重視的下一個商品。貨幣的邊際效用實際上確實有在下降沒錯，因為對於每日收入為 1 美元的人而言，增加額外 1 美元的收入，絕對會比每日收入為 1,000 美元的人，感覺得到的更多。但貨幣的邊際效用下降速度，一定會遠低於任何其他商品，因為它的效用下降是著眼於「想要的商品」，而非「特定的好商品」。

持有貨幣的邊際效用緩慢下降，代表對貨幣的邊際需求不會發生顯著變化。將它與幾乎穩定的供應相結合後，在商品和服務方面，便能產生相對穩定的市場價值。這意味著貨幣不太可能顯著升值或貶值，而使其成為一項雖然不太會賺錢的長期投資，但卻是一種良好的價值儲蓄。人們對投資通常會期望有顯著的升值潛力，但通常也會伴隨著重大損失或折舊風險的機會，因此投資等於是承擔風險的獎勵，但健全的貨幣會有最小的風險，也不太能提供任何獎勵。

因此整體而言，貨幣需求可能只會隨著時間偏好的變化而改變。當人們普遍降低時間偏好後，會有更多人想要持有貨幣，導致它的市場價值與其他商品與服務相比有所提升，進而獎勵了貨幣持有者。另一方面，一個演變成較高時間偏好的社會，會傾向於減少持有的貨幣，逐漸降低其市場邊際價值。無論是哪一種情況下，持有貨幣仍然是整體風險最小且最有價值的資產，這點便是貨幣需求的根本原因。

這項分析有助於解釋黃金在數年、數十年甚至數百年內，保持價值的卓越能力。若以黃金克數來衡量羅馬帝國的農產品價格，便會顯示出它們與今日的價格，具有明顯的相似程度。檢查戴克里先（Diocletian）的西元

301 年價格法令<sup>註5</sup>，並將黃金價格轉換為等值的現代美元後，我們發現一磅牛肉價格約為 4.5 美元，而一品脫啤酒價格約為 2 美元，一品脫高級葡萄酒價格為 13 美元左右，一般葡萄酒價格則為 9 美元，一品脫的橄欖油約 20 美元等。比較某些特定行業的工資數據，也出現類似的模式。不過指出這些個別數據雖然具有代表性，但並不能作為問題的最終答案。

Roy Jastram 對目前可用的最長持續數據，進行了黃金購買力的系統研究<sup>註6</sup>。觀察從 1560 年至 1976 年的英國數據，分析黃金在商品方面的購買力變化後，Jastram 發現黃金在前 140 年的購買力下降，但從 1700 年至 1914 年則保持相對的穩定，然後英國才脫離了黃金標準。在這兩個多世紀以來，英國主要使用黃金作為貨幣，其購買力保持相對穩定，批發商品的價格也是如此。而在第一次世界大戰之後，英國取消了黃金標準，黃金的購買力因而增加，各項商品的批發價格指數也隨之增加（見圖 8<sup>註7</sup>）。

我們必須了解貨幣媒介在價值上保持完全恆定，在理論上是不可能也無法確定的。隨著新技術引進了可以替代舊貨的新商品，加上不同貨物的供需條件會隨時間產生變化，因此貨幣所能購買的商品和服務也會隨著時間而變化。貨幣單位的主要功能之一是作為經濟商品的會計單位，而商品價值會不斷變化，因此我們不可能精確的衡量貨幣商品的價格，只是在很長的一段統計期間裡，用類似於 Jastram 的研究，來表明黃金作為交換媒介時，會比其他形式的錢，更能保持價值的整體趨勢。

---

註 5 R. Kent, 「戴克里先最高價格法令 (The Edict of Diocletian Fixing Maximum Prices)」, 賓夕法尼亞大學法律評論, 第 69 冊 (1920 年): 第 35 頁。

註 6 Roy Jastram, 「黃金常數: 英國和美國經驗 1560-2007 (The Golden Constant: The English and American Experience 1560-2007)」, 英國 Cheltenham: Edward Elgar, 2009 年。

註 7 資料來源: Jastram, 「黃金常數 (The Golden Constant)」。

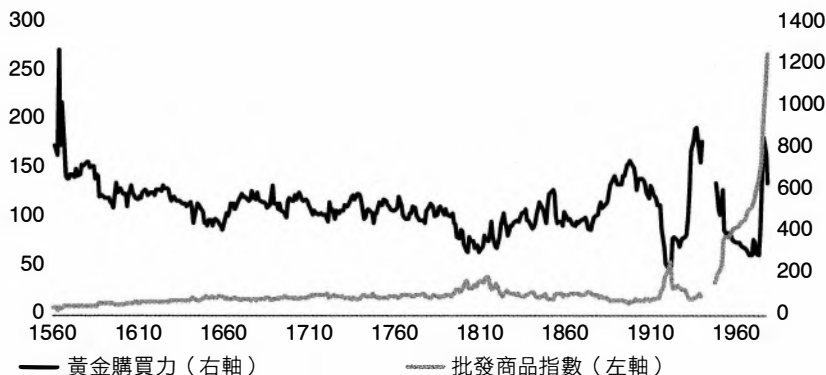


圖 8 英格蘭黃金購買力和批發商品指數，1560-1976

來自美國的最新數據顯示，集中觀察過去兩個世紀，經濟成長速度快於 Jastram 數據所涵蓋的時期，說明了黃金的商品價值有所增加，其價格以美元計價為大幅上漲。這是黃金與最健全貨幣完全一致的時刻。所有商品的供應量都比黃金更容易增加。因此隨著時間推移，這些商品的供應將比黃金更充足，導致黃金的購買力隨之上升。如圖 9 所見<sup>註 8</sup>，只要與黃金連動，美元對商品的價值也會上漲，但當與黃金的關係被切斷時，美元的價值就會大幅下跌，就像美國南北戰爭期間狂印鈔票，以及 1934 年美元貶值和沒收公民黃金後的時期一樣。

1931 年至 1971 年期間，貨幣在名義上與黃金掛鉤，但其實只是透過政府的各種安排，允許在神秘難解的條件下以紙幣換取黃金。此一時期政府貨幣和黃金的價值以及政策的變化，都相當不穩定。

註 8 資料來源：美國的歷史統計數據，E 52-63 和 E 23-3 系列。請參閱 <https://fred.stlouisfed.org>。



圖 9 黃金和美元商品價格，以對數表示，1792-2016

對於黃金和政府貨幣之間的比較，觀察從 1971 年到現代的這一時期更為有用。在此一時期，自由浮動的國家貨幣在市場上交易，而中央銀行的任務則是保證其購買力（見圖 10<sup>註 9</sup>）。

即使是表現最好，最穩定的政府貨幣與黃金相比，其價值仍大幅下降，當它們都與黃金脫鉤後，目前的價值約為 1971 年價值的 2-3%。但這並不代表黃金的市場價值上漲，而比較像是法定貨幣價值的下降。在比較商品和服務價格與政府貨幣和黃金價值時，我們發現以政府貨幣來看商品價格顯著上漲，但以黃金來看商品價格則相對穩定。

註 9 資料來源：美國聯邦儲備銀行統計數據。請參閱 <https://fred.stlouisfed.org>。黃金價格數據則來自世界黃金協會 [www.gold.org](http://www.gold.org)。



圖 10 主要貨幣金價，1971-2017

例如，作為現代工業社會主要商品之一的每桶石油價格，自 1971 年以來在黃金計價方面一直相對穩定，而在政府貨幣方面卻增加了幾個級數（見圖 11<sup>註 10</sup>）。

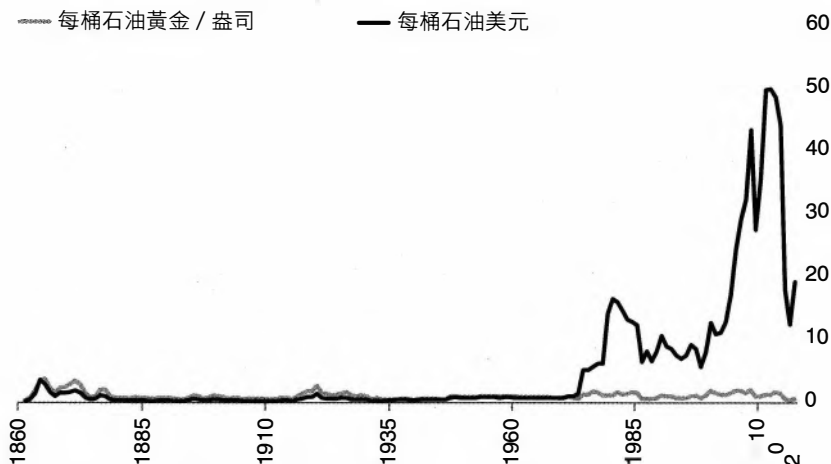


圖 11 石油價格 / 美元與石油價格 / 每盎司黃金，1861-2017，1971 年價格開始分歧

註 10 資料來源：BP 統計評估和世界黃金協會。

穩健貨幣的供應量不能輕易擴大，因此價值會比寬鬆貨幣穩定，因為基本上它並不會彈性供應。社會對貨幣的需求，則會隨時間偏好不同而有些微變化。

另一方面，由於生產商能夠大幅改變「軟錢」的生產數量，因此隨著貨幣數量的變化以及作為價值儲存的可靠性忽升忽降，持有者的需求也將產生大幅波動。

價值的相對穩定性，不光可以讓持有者的儲蓄維持相對的購買力，對於保持貨幣單位作為計價單位的完整性來說，更為重要。當供需變化較小，貨幣價值可穩定預測時，便可像黃金一樣，當作其他商品與服務價格變化的可靠信號。

另一方面就政府貨幣而言，貨幣供應量是透過中央銀行和商業銀行的供應增加而增加，並透過通貨緊縮的經濟衰退與破產來減少。由於人們對貨幣價值的期望與中央銀行的政策，導致對貨幣的需求變得更加不可預測。這種高度不穩定的組合，也導致政府貨幣在較長期間內無法預測價值。中央銀行確保價格穩定的使命，便是透過各種工具不斷管理貨幣供應，以期確保價格穩定，因而使得許多主要貨幣在短期間內，與黃金相比下的波動較小。但從長遠來看，政府貨幣供應的不斷增加與黃金穩定緩慢的增加相比，都讓黃金的價值顯得更能預測。

自由市場所選擇的健全貨幣，正是因為它可以隨著時間推移而保持價值，自然比起政府強制規定的不健全貨幣，有更好的穩定性。如果政府貨幣可以當作良好的會計單位與價值儲存單位，就不需要制訂貨幣法來強制執行，世界各國政府也不需沒收大量黃金，並將黃金持續存放在中央銀行儲備。而只要中央銀行繼續持有黃金，甚至開始增加儲備，便可證明從長期來看，它們對本國貨幣的信心，會隨著紙幣價值的持續探底，而讓黃金成為不可避免的貨幣角色。

## 儲蓄和資本累積

貨幣價值下降造成的關鍵問題，便是它會對未來的儲蓄產生負面影響。時間偏好是普遍積極的：亦即在考慮選擇今天或將來擁有同一種商品時，任何理智的人都希望今天就擁有它。因此只有增加未來的回報，人們才會考慮延遲滿足。健全貨幣是會隨著時間經過而略微增值的貨幣，這表示繼續持有健全貨幣很可能會提高購買力。而由中央銀行控制的不健全貨幣，其明確的任務是繼續維持通貨膨脹，因此無法對持有貨幣者提供持有的獎勵，讓他們更有可能去花錢或借錢。

在投資的方面，穩健的貨幣可以創造一個經濟環境，產生正向的回報以利於投資者，因為其貨幣單位可以保住價值，如果遇上無法升值的情況，也可用來強化投資的動力。從另一方面看，由於不穩定的貨幣只有在「回報高於貨幣的貶值率」才可升值，因而鼓勵了高回報但高風險的投資與支出。此外，由於貨幣供應的增加意味著利率降低，因此儲蓄和投資的動力也會減少，變相鼓勵了借貸行為。

這項 46 年的不健全貨幣實驗記錄，證實了此一結論。已開發國家的儲蓄率一直在下降，降至非常低的水平，而個人、市府與國家債務已激增到過去難以想像的程度（見圖 12<sup>註 11</sup>）。

只有瑞士在 1934 年之前一直維持官方的黃金標準，並且在 1990 年代初期之前，繼續以大量黃金儲備支持其貨幣，因而繼續維持著高儲蓄率，成為西方文明世界裡「低時間偏好」的最後堡壘，儲蓄率甚至達到兩位數，而其他西方經濟體的儲蓄率，已經暴跌到個位數甚至負儲蓄率。

註 11 資料來源：OECD 經合組織統計數據。

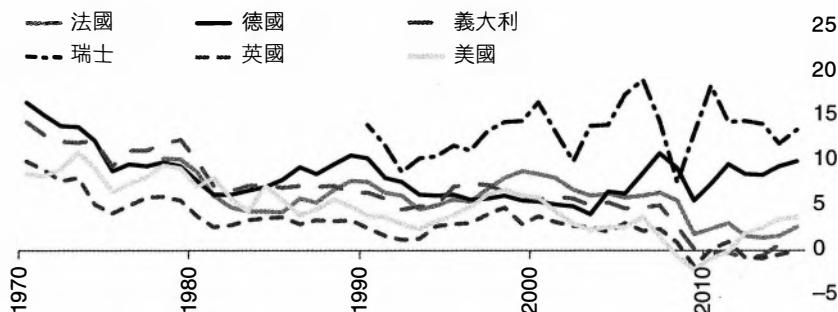


圖 12 1970-2016 年主要經濟體的國民儲蓄率百分比，單位%

七大已開發經濟體<sup>註 12</sup>的平均儲蓄率，在 1970 年為 12.66%，但在 2015 年下降至 3.39%，下降近四分之三。

在西方世界儲蓄率急劇下降的同時，債務仍在繼續增加。西方家庭平均負債超過年收入的 100%，而各級政府和家庭的債務負擔總額，超過國內生產毛額（GDP）數倍，也產生了重大影響。當凱因斯主義經濟學家向民眾保證「債務有利於經濟成長、儲蓄將導致經濟衰退」時，這些數字便被正常化。凱因斯主義經濟思想中最普遍的幻想之一，就是國債「無關緊要，因為這是我們自己欠自己的債務」。只有凱因斯的「高時間偏好」門徒，才無法理解這個「我們自己」是什麼意思。它不光等於字面上的負債，而是分成幾代人的負債：也就是目前這些都屬於「犧牲未來、不計後果」的消費。更糟的是，這句話後面通常會接著出現「情緒勒索」的說法：例如「如果不借錢投資未來，我們就無法改變現狀」。

許多人都在假裝這是奇蹟般的現代發明，認為這是凱因斯的出色見解，也就是「支出是最重要的，確保高消費，債務便可繼續延長下去，也

註 12 此七大已開發經濟體為美國、日本、德國、英國、法國、義大利與加拿大。



就不必儲蓄了」。事實上，這項政策並不是新發明，頹廢的羅馬皇帝在國勢衰敗期間也採用此一政策，現在不過是改用在政府發行的紙幣上。

紙幣比起舊的金屬貨幣而言，其實可以更平和、更不露痕跡的加以管理，但其結果是一樣的。

二十世紀對炫耀性消費的狂熱，跟健全貨幣被破壞，以及凱因斯主義「高時間偏好」思想的爆發，脫離不了關係，因為他們把「貶抑儲蓄、神化消費」，當成了經濟繁榮的關鍵。減少儲蓄的結果便反映在增加支出上，利率經常被降低，又使銀行能發行比以往更多的信貸，貸款已不再受限於投資，而是轉移到消費行為上。信用卡和消費貸款允許個人為了消費而借錢，甚至不必假裝自己是在對未來進行投資。凱因斯經濟學對現代經濟無知的深度，看起來確實非常諷刺，因為他們認為「資本主義」是基於儲蓄資本累積的經濟體系，也就是釋放「炫耀性消費」的元凶，這點剛好與資本累積完全背道而行。因為資本主義是人們放棄時間偏好，延遲即時滿足，並投資於未來所發生的事情。而債務驅動的大眾炫耀性消費，同樣也是資本主義的正常組成部分，就像窒息是呼吸過程裡正常的一部份。

這也有助於解釋凱因斯經濟學的主要誤解之一：也就是認為透過儲蓄來延遲當前的消費，會讓工人失業並導致經濟生產停滯不前。凱因斯認為任何時刻的支出水平，都是經濟狀況最重要的決定因素，因為在沒研究過經濟學的情況下，他對資本理論一無所知，也不了解「就業」不只是最終產品，亦可生產「資本產品」，也就是在未來所生產的最終產品。凱因斯靠家裡可觀的財富過活，不必工作，對儲蓄或資本累積以及它們對經濟成長的重要性並不了解。因此，凱因斯會在消費支出下降和儲蓄增加的同時，觀察到經濟衰退，而假設增加儲蓄與減少消費，會跟經濟衰退有一定的因果關係。

如果凱因斯曾經學習過資本理論的基礎，就能了解消費減少是對「商業週期循環」的自然反應，是接在貨幣供應擴張之後所引起（我們將在第

6 章加以討論)。他也將能理解經濟成長得以開始的唯一原因，便是延遲滿足加上儲蓄與投資，這些行為都會延長生產週期，並以更好的生產方式提高生產率，從而提升生活水準。他也能夠意識到自己之所以會出生在一個富裕社會中的富裕家庭，唯一的原因，便是他的祖先花了幾個世紀累積資本，延遲滿足並投資於未來而獲得。但是，就像帝國衰敗期間的羅馬皇帝一樣，凱因斯永遠無法理解建立富裕所需要的工作和犧牲，反而相信「高消費」才是繁榮的主因，而非繁榮所產生的結果。

債務與儲蓄完全相反，如果說儲蓄創造了資本累積和文明進步的可能性，那麼債務便是倒過來，減少幾代人的資本存量、降低生產率並且降低生活水準。無論是房貸、社會保險合約或政府公債，都要靠更高的稅收與債務貨幣化的繼續融資，當代人可能是自羅馬帝國滅亡以來（或至少自工業革命以來），西方世界的第一代，以「比父母更少」的資本存量進入社會。這一代人不會目睹他們的儲蓄累積或提高資本存量，而是必須努力償還隨債務日益成長的利息，更拼命的為自己幾乎無法享受的福利計劃提供資金，還要支付更高的稅收，而且幾乎無法為晚年的生活進行儲蓄。

從健全貨幣到貶值貨幣的轉變，會導致幾代人累積的財富被浪費在一兩代內的炫耀性消費上，而使舉債成為資助主要支出的新方法。在 100 年前，大多數人都會用自己的勞力或累積的儲蓄，支付房屋、教育或婚姻費用。這種觀念對今天的人們來說似乎很荒謬，即使有錢人也不會只生活在自己的經濟能力範圍內，而是會利用他們的財富來獲得更多的貸款，為大宗消費提供資金。這種作法可以持續一段時間，但我們不能把這點持續性誤認成永久性，因為這是對社會的資本存量進行系統性消費，就像把要作為種子用的穀物吃掉一樣。

當貨幣被國有化時，便會置於政治家的控制之下，他們在幾年任期時間內經營，然後努力再被選上。這種過程很容易導致短期決策，同時政客也會濫用貨幣來為後續的競選活動提供資金，犧牲後代的利益。正如 H. L.

Mencken 所說：「每次選舉都像是把贓物當成高級品來拍賣」<sup>註 13</sup>。在一個貨幣自由與健全的社會中，個人必須以會影響到家庭資本的「長遠目光」來作各種決定。雖然有些人可能會做出不負責任的決定，傷害到後代的福祉，但那些想做出負責任決定的人，仍有權選擇自己的決定。一旦貨幣國有化，這種決定就會變得越來越難，因為中央政府對貨幣供應的控制，無可避免的破壞了儲蓄的動機，同時也增加借貸的動機。無論一個人多麼謹慎，他的孩子仍將目睹家庭的儲蓄會失去價值，也必須繳稅來支付政府所造成的通貨膨脹費用。

隨著各代繼承的遺產減少，更降低了家庭作為「整體」的力量。而政府沒有限制的支票簿，也能增強控制與塑造人們生活的能力，使政府在個人生活各方面，發揮越來越重要的作用。本來家庭可為個人提供資金的能力，已經被國家的慷慨所削弱，也導致維持家庭的能力下降。

在傳統社會裡，個人會意識到自己將來需要孩子的支持，因此他們會在自己健康的年輕時期，開始建立家庭，並為孩子投資最好的生活環境。但如果長期投資在整體上看起來前景不佳，當貨幣貶值時，不僅儲蓄沒有好處，投資的利潤也會降低。此外，隨著政治家透過貨幣印刷機的魔力，向人們推銷永恆幸福與退休福利的謊言時，更會使人們覺得對家庭的投資，變得越來越沒有價值。因此隨時間經過，建立一個家庭的動機逐漸下降，越來越多的人最後孤老以終。

配偶不太可能投入必要的情感、道德和金融投資來使家庭關係成長，因此可能會造成更多的婚姻破裂，而僅存下來的家庭也只會生更少的孩子。這種慢慢普遍的「現代家庭關係崩潰」現象，要從不健全貨幣導致的

---

註 13 H. L. Mencken 和 Malcolm Moos（編輯），「廢話狂歡節（*A Carnival of Buncombe*）」、巴爾的摩：約翰霍普金斯出版社，1956 年，第 325 頁。

結果來談，因為它會使國家介入家庭幾千年來所發揮的重要作用，並減少家庭成員投資長期關係的動機。

以政府的慷慨來代替家庭關係，對家庭裡的個人而言，仍然是場失敗的交易。許多研究顯示，生活滿意度大幅取決於與伴侶和孩子所建立的長期親密家庭關係<sup>註14</sup>。還有許多研究表明在家庭破裂後，抑鬱症和心理疾病的發病機率會隨時間推移而上升，尤其是在女性方面<sup>註15</sup>，而家庭破裂也正是抑鬱症和心理疾病的主要原因。

當政府透過從未對長期投資有任何興趣的凱因斯，教導如此的經濟教義而造成家庭崩潰，當然不可能只是巧合。凱因斯從小生長在富裕家庭，幾代人累積了大量資金，讓他成為一個放蕩的享樂主義者。他最大的成年生活花費在戀童癖，包括在地中海造訪兒童妓院<sup>註16</sup>等。維多利亞時期的英國，是個具有強烈道德感、低人際衝突與穩定家庭的「低時間偏好」社會，而凱因斯恰好屬於反傳統的一代，所以他將這些傳統視為必須擊敗的壓抑機制。

要了解凱因斯的經濟學，就必須了解他逐漸相信可以靠自己的意志，見到社會裡具有塑造出來的那種「道德感」。

---

註14 George Vaillant，「經驗的勝利：哈佛大學學生大調查（*Triumphs of Experience: The Men of the Harvard Grant Study*）」，馬薩諸塞州劍橋市：哈佛大學出版社，2012年。

註15 Betsy Stevenson 和 Justin Wolfers，「女性幸福下降的悖論（*The Paradox of Declining Female Happiness*）」，美國經濟期刊：經濟政策，第1卷，第2期，2009年，第190-225頁。

註16 詳見 Michael Holroyd，「立頓斯特雷奇：新傳（*Lytton Strachey: The New Biography*）」，第1卷，第80頁，其中凱因斯寄給在布魯姆斯伯里集團裡的朋友 Lytton Strachey 的一封信，建議他們去參觀突尼斯這個「床和男孩都很便宜」的地方。另見 David Felix 的「凱因斯：關鍵人生（*Keynes: A Critical Life*）」第112頁，引用來自凱因斯的一封信件內容告訴朋友，「我要去埃及... 剛剛得知『床和男孩』都已準備好了」。在另一封信裡他還建議 Strachey 去突尼斯和西西里島「如果你想去那些男孩裸體跳舞的地方」。

## 創新：「零到一」比「一到多」

我們可以從儲蓄的水準與社會投資的項目類型，看出「健全貨幣」對時間偏好和未來走向的影響。就像 19 世紀晚期的世界一樣，在健全貨幣制度下，個人較可能願意從事長期的投資，並有大量資金可用於資助那些很花時間的項目。因此，人類歷史上一些最重要的創新，都誕生於十九世紀末的黃金時代。

在這些開創性的工作裡，Bunch 和 Hellemans 在「科學和技術史」裡，記載了科學和技術史上最重要的 8,583 項創新與發明的清單。物理學家 Jonathan Huebner<sup>註 17</sup> 分析了這些事件，以及它們發生的年份與當年全球人口的關係，並計算了自黑暗時代以來，每年人均事件的發生率。Huebner 發現，儘管創新總數在二十世紀有所上升，但人均創新數量在十九世紀達到頂峰。

仔細研究 1914 年以前世界的創新，便可為 Huebner 的數據提供支持。亦即我們可以毫不誇張的說：現代世界是在第一次世界大戰前的黃金標準年代發明的，二十世紀只是在精煉、改良、優化、簡約與推廣十九世紀的發明而已。

二十世紀進步的奇蹟，讓人們很容易忘記實際的發明——亦即改變世界的創新——幾乎都發生在黃金時代。

---

註 17 Jonathan Huebner，「全球創新可能下滑的趨勢——技術預測和社會變革（A Possible Declining Trend for Worldwide Innovation）」，*Technological Forecasting and Social Change*，第 72 卷（2005 年：第 980-986 頁。

在 Peter Thiel 的暢銷書《從零到一》中，他藉由製作新技術的第一個成功範例，來討論這些「創造新世界的夢想家」對這個世界的影響。

正如他所說，一項技術從「零到一」成功案例的轉變，是發明裡最難和最重要的一步，而從「一到多」的轉變，則是一個擴展、營銷與優化的問題。一般迷戀「進步」概念的人，可能很難接受這樣的事實：在 1914 年之前的健全貨幣世界，便是零到一的世界，而 1914 年後的政府生產貨幣的世界，則是從一到多的世界。從一到多的轉變並無不妥，但它確實為我們提供大量的思路泉源，可以用來思考為何在現代貨幣體系下，沒有更多「零到一」的變革發生。

現代生活使用的大多數技術，都是在黃金標準下的十九世紀所發明的，並以逐漸成長的資本累積來資助發明，也就是儲蓄者將財富以健全貨幣累積，而且這些儲蓄並不會快速貶值。以下就是黃金時期重要創新的摘要：

- 冷熱自來水、室內廁所、各種管道、中央暖氣：

這些發明對今天生活在文明社會裡的任何人來說，感覺都是理所當然，但這卻是大多數人「生與死」的區別。因為它們是消除全球多數傳染病的主要功臣，也幫助了城市地區的成長，減少出現疾病的危害。

- 電力、內燃機、大量生產：

現代工業社會圍繞著「碳氫化合物能源」的利用成長而建立，如果沒有這種能源，現代文明的任何產物都不可能出現，這些能源和工業的基礎技術，便是在十九世紀發明。

- 汽車、飛機、地鐵、電梯：

感謝「美好年代」時期讓城市街道上不再充滿馬糞，也給了我們環遊世界的能力。汽車是 Karl Benz 於 1885 年發明，1904 年則有萊特兄弟發明飛機，Charles Pearson 在 1843 年建造地鐵，Elisha Otis 則在 1852 年發明電梯。

- 心臟手術、器官移植、闌尾切除術、嬰兒保育箱、放射治療、麻醉劑、阿司匹林、血型與輸血、維生素、心電圖、聽診器：

外科手術和現代醫學也歸功於「美好年代」時期。現代衛生設備以及引進可靠的碳氫化合物能源，讓醫生能夠改變治療病患的方式，而非使用幾個世紀以來適得其反的錯誤做法。

- 石油衍生化學品、不銹鋼、氮基肥料：

讓現代生活成為可能的工業產物與材料，都源自「美好年代」時期的變革創新，這些創新產生了大規模的工業與農民生產。塑膠跟塑料製作的一切商品，都是石油衍生化學品的產物。

- 電話、電報、錄音、彩色攝影、電影：

雖然我們將現代視為大量通訊的時代，但實際上在二十世紀所取得的成就，大部分都是改良自十九世紀的創新。史上第一台電腦是巴貝奇電腦，由 Charles Babbage 於 1833 年設計，但在 1888 年由他的兒子亨利完成。我們甚至可以說，網際網路與上面所包含的內容，都是 1843 年在電信發明時的錦上添花，但確實包含了核心的要素。電報從根本上改變了人類社會，讓通信可以不需要信件或郵差的實際運輸。那也是電信界的「零到一」時刻，隨後到來的一切都是「一到多」的改進。

## 藝術的蓬勃發展

健全的貨幣對人類繁榮的貢獻，不只限於科學技術的進步，也可在藝術世界裡親眼目睹。

佛羅倫斯與威尼斯藝術家是文藝復興時期的領導者，這點並非巧合，因為這兩個城市是歐洲最先採用健全貨幣的城市。巴洛克、新古典主義、浪漫主義、寫實主義與後印象等學派，都是由富有的顧客所資助，這些顧客持有健全的貨幣，具有極低的時間偏好，肯耐心等待數年甚至數十年才能完成並流傳千古的傑作。歐洲教堂的驚人穹頂，由無數的建築師與藝術家如布魯內萊斯基和米開朗基羅，經過幾十年的靈感雕琢與裝飾而完成，這些都是由時間偏好極低的顧客才能提供資助。而讓這些資助者們留下深刻印象的唯一方法，便是製作可以流芳百世的藝術品，使他們美名流傳，成為偉大藝術家的偉大作品擁有者與贊助者。這就是為何佛羅倫斯的麥第奇家族對藝術的贊助，可能會比他們在銀行和金融方面的創新，更為世人所知，而這些較不為人所知的創新，甚至可能對後代來說更為重要。

同樣地，巴哈、莫扎特、貝多芬，還有文藝復興、古典與浪漫時期作曲家的音樂作品，都會讓現代音樂感到羞愧。因為那些人那種僅僅花幾分鐘錄下如動物般的噪音，就從音樂工作室裡大量賣出，向人類出售最低微的本能而獲利。黃金時代的音樂不僅觸動人類的靈魂交流，也喚醒人們聯想到比生活瑣事更為昇華的呼喚，但今日的噪音音樂則訴求人類最基本的動物本能，透過讓人沉迷於立即感官享受，來忘卻生活現實，不關心長期的結果或更深刻的內容。資助巴哈的布蘭登堡協奏曲是一筆很「硬」的錢，而資助 Miley Cyrus 的扭腰擺臀則是很「輕軟」的不健全貨幣。



在健全貨幣和低時間偏好的時代裡，藝術家致力於完善他們的工藝，長遠考量以製作有價值的作品。花多年時間學習工作所需的複雜細節和技術，追求完美並發展出超越常人的能力，令贊助者與一般大眾感到驚喜。如果是未經多年努力研究技藝的人，便沒有機會被稱為藝術家。真正的藝術家並不會高傲的向大眾敘述藝術是什麼，或是解釋只花一天製作的爛作品有多麼的深奧。

巴哈從未宣稱自己是個天才，或告訴大家他的音樂為何比別人更好；相反的，他把時間都花在改善自己的技藝。米開朗基羅花了四年的時間，吊掛在西斯廷教堂的天花板上工作一整天，每天只吃一點東西，把大部分時間都拿來畫出他的傑作。甚至還寫了一首詩來描述這場苦難<sup>註 18</sup>：

住在這個窩裡，讓我得了甲狀腺肥大  
像來自倫巴第滯流河裡的貓，  
或其他地方所發生的情況一樣——  
讓我的肚子靠近了下巴：  
我的鬍子指向天空；我的後頸往下，  
固定在脊椎上：我的胸骨明顯的  
像豎琴一樣生長：豐美的繡飾  
從刷子滴落，或厚或薄的塗抹在我的臉上。  
腰部像槓桿一樣擠壓我的肚子：  
屁股像個馬墊在承受我的重量；  
我的腳沒方向的來回徘徊；

---

註 18 John Addington Symonds, 「米開朗基羅的十四行詩 (*The Sonnets of Michael Angelo Buonarroti*)」(倫敦: Smith Elder & Co. 出版, 1904 年)。

在前面，我的皮膚變得鬆散與拉長；在後面，  
彎著身體讓它們變得又緊又繃；  
橫向的我像張敘利亞弓的使勁：  
我知道，這看起來虛假古怪，  
一定是擠著腦袋和眼睛的結果；  
因為生病可以讓瞄準的槍彎曲。  
來吧，喬瓦尼，試試吧  
救救我垂死的形象與名氣；  
因為我吃的是過錯、畫的是羞愧啊。

只有經過幾十年如此細緻和專注的努力，這些天才才能成功的製作出這些偉大傑作，讓他們的名字永久化為本身技藝的代表。在貨幣不健全的時代裡，沒有藝術家可以像米開朗基羅或巴哈這樣低時間偏好的努力工作，讓自己正確精進技藝或花大量的時間讓作品完美。只要漫步在現代藝廊裡，便可看到大量生產的展示作品裡，所需要用到的努力或才能，甚至不會多過無聊的 6 歲兒童的發揮。

現代藝術家不再以工藝與長時間練習吸引觀眾，而是以自負、衝擊性、憤怒與存在焦慮的方式，吸引觀眾欣賞他們的藝術，而且通常還加上一點政治理想的偽裝，例如天真的馬克思主義變種，而假扮成有深度的樣子。若要舉出現代「藝術」真的好在哪裡的話，應該就是它們看起來很聰明，以開玩笑或惡作劇的那種小聰明。多數現代藝術的生產或製作過程裡，都沒有完美或令人欽佩的元素存在，因為它是大量的由懶惰沒才華的假文人，在幾小時內拼貼製作出來，這些人幾乎不花時間去練習工藝。因此只有依賴廉價的自負、淫穢和衝擊感，才能引起人們對現代藝術這位「沒穿衣服的國王」進行關注，也只有長期自命不凡，侮辱他人不理解自己的作品，才可能賦予作品的價值。

當政府法幣取代健全貨幣之後，低時間偏好與品味高尚的顧客，便被政府官僚取代，然而他們的藝術品味，就跟那些政治上的議程一樣低劣。如此一來，美感與長久流傳都不再重要，重點變成要為那些只會政治空談，或為那些能控制大型畫廊和博物館資金來源的官僚，留下深刻印象。這些畫廊和博物館在政府重點保護下，變成了藝術品味與藝術教育標準的壟斷者。藝術家和捐贈者之間的自由競爭，現在被不負責任的官僚機構，以中央的藝術規劃加以取代，因此我們可以預見即將發生的災難性後果。一般自由市場裡，得獎者應該是被大家認定提供最佳商品的人，當政府可以決定誰是贏家和輸家時，那些在生活裡沒有其他成就，只好跑去當官僚的人，就會變成品味與美感的仲裁者。原先藝術上的成就，是由那些透過好幾代智慧和低時間偏好，成功獲得財富的人所決定，現在則變為在政治與官僚系統下「混得最好」的人所決定。只要對這類人稍加認識，便足以向任何人解釋為何當代藝術會變成龐然巨獸的原因。

在他們不斷滋養、成長的控制領域中，幾乎所有現代政府都投入預算，資助各種媒介的藝術和藝術家。但隨時間推移，還出現了一些奇怪且難以置信的現象，例如政府為了政治目的而暗中干預藝術的離奇故事。

雖然蘇聯資助和指導共產主義「藝術」以實現政治與宣傳目的，但最近的報導還揭露了中央情報局，竟然資助與推動當時不受歡迎的抽象表現主義藝術家如 Mark Rothko 與 Jackson Pollock 的作品，在歐洲巡迴展覽，以作為美國人在政治上的藝術反擊<sup>註19</sup>。這一切只有在貨幣不健全的情況下，才會出現這種藝術災難。也就是世界上最大的兩個經濟、軍事和政治巨頭，選出來積極推動與資助那些毫無品味的藝術垃圾。兩國情報單位主

---

註 19 參見 Frances Stonor Saunders，「文化冷戰：中央情報局和藝術與文學的世界（*The Cultural Cold War: The CIA and the World of Arts and Letters*）」，新出版，2000 年，ISBN 1-56584-596-X。

事者低劣的藝術品味，確實剛好夠讓他們在華盛頓和莫斯科的間諜組織與官僚機構找到工作。

由於 Medicis 家族的品味，已經被類似加州車輛管理局工人的藝術品味所取代，結果整個當代藝術界便形成一個充滿視覺厭惡的垃圾藝術世界，那些懶散無才的假藝術家，只花幾分鐘即可快速換來支票，捏造一點關於作品象徵的荒謬故事，便能欺騙世界上的藝術品追求者。這種做法，實在跟那些像歹徒般徹底墮落的假藝術家無異。Mark Rothko 的「藝術」只花幾個小時就製作出來了，但一樣賣給容易上當的收藏家。他們的收藏等於是數百萬不健全的貨幣，而且顯然還把現代藝術收藏，當成這個時代最賺錢的「快速致富」騙局。而這類現代藝術家並不需要任何才能、工作或者努力，只要板著臉和擺著自負的態度，不耐煩的向暴發戶們講解為何在畫布上潑潑的油彩，並不只是醜陋毫無思想的潑潑油彩，只因為這些暴發戶們不能理解這些「無法解釋」的藝術作品，然後很容易就能換來一筆大錢。

令人震驚的不只是現代藝術界，類似 Rothko 這類假藝術家的侵門踏戶；事實上能與過去偉大作品相比的傑作也消失了。你很難不注意到，今天世界各地少有類似西斯廷教堂這類偉大藝術的創作；也很少有傑出作品可跟達文西、拉斐爾、林布蘭、卡拉瓦喬或維梅爾的偉大畫作相比擬。更令人驚訝的是，照說靠著現代技術與工業化的進步，應該要比黃金時代更容易實現這類偉大藝術創作才對。

西斯廷教堂會讓參觀者肅然起敬。對其內容、工法與歷史的任何進一步詮釋，都可以把大家的敬畏，轉化為其中所蘊含的思想、工藝與努力上的深度欣賞。在 Rothko 這類假藝術家成名之前，即使是最細心的藝術評論家，也會直接無視的路過 Rothko 的畫作，甚至完全沒看到它，更別提會買下來帶回家了。唯有透過一群爛評論家，花費無數的時間宣傳這些作品，

才會讓畫廊與有野心的暴發戶，開始假裝這些作品有更深層次的意義，然後花費現代的不健全貨幣加以購買。

多年來這些假裝有深層意義的故事，在現代藝術博物館中留下了各種隨機作品，只有現代藝術愛好者才會吹捧他們，也說明了這個時代藝術品味的空洞。但是，這些人對於現代藝術的價值，或許沒有比世界各地藝術展覽的「清潔工」，更加合適的讚揚了。因為他們表現出令人欽佩的洞察力與對工作的奉獻精神，一再地將昂貴的現代藝術作品，丟進他們所屬的垃圾桶中。在這個時代最具代表性的「藝術家」如 Damien Hirst、Gustav Metzger、Tracey Emin 和義大利雙人組 Sara Goldschmied 和 Eleonora Chiara，都得到了展場清潔工仔細的評論，因為他們扔到垃圾桶的東西，遠比花費數百萬美元的不安暴發戶們更加的挑剔。

另一件足以忽略這些無價值塗鴉的事，便是政府竟然資助這種尷尬的情況，而且還認為是值得的。畢竟沒有人可以透過無能且上班打盹的車輛管理局員工般的行為，來批評美國這樣的國家，因為他們可以藉由這些倒霉的收藏家客戶來消除沮喪。也許我們不應該以政府工作人員的工作內容，來判斷這個時代，只因這些工作人員聽命將成堆廢紙板的無聊故事，當成了藝術成就。但即便如此，我們也很難找到能跟過去的成就相提並論的作品。在《從黎明到頹廢》一書中，對現代「民主」文化的辛辣批判裡，Jacques Barzun 得出了結論：「20 世紀貢獻和創造的所有內容，都是透過分析或批評以及模仿和謔仿的改進」。Barzun 的書引起這個時代裡許多人的共鳴，因為它包含大量令人沮喪的事實：

一旦你能克服「進步是必然的」這種固有偏見，就會面臨到這樣的結論：我們這一代人在文化和精緻度方面，確實比不上我們的先人。就像戴克里先統治下的羅馬一樣，必須靠通貨膨脹為生，在羅馬競技場的野蠻場面上消費和買醉，這些當然比不上凱撒時代偉大的羅馬人，因為他們必須清醒努力的工作來賺取金幣。

## 6

# 資本主義的資訊系統

---

「失業潮的原因並非資本主義，而是因為政府不讓企業有權使用健全貨幣。」

—海耶克

**貨**幣作為交換媒介時，必須讓經濟參與者可以進行經濟規劃與計算。當經濟生產從非常原始的規模開始發展之後，一般人很難在不固定的參考框架下，比較不同對象的相互價值，而有辦法做出製造生產、消費與貿易決策。因此這種計價單位的特性，便是貨幣作為交換媒介和價值儲存以外的第三種功能。為理解這種計價特性對經濟體系的重要，我們做了一般聰明人在尋求經濟問題解答時所做的事：向過去的奧地利經濟學家們求助。

海耶克的「在社會中使用知識（*The Use of Knowledge in Society*）」，可說是有史以來最重要的經濟論文之一。不像一些高度理論化、無足輕重或深奧難解的現代學術研究一樣，這 11 頁內容在出版 70 年後，都

還繼續被廣泛的閱讀，也持續對全球許多人的生活和事業產生影響。當然也許比不上它對網際網路上最重要的網站之一「維基百科」的影響那樣重要，因為「維基百科」也是人類歷史上最大的單一知識體系。它的創始人 Jimmy Wales 表示，在拜讀了海耶克這篇論文以及對知識的解釋之後，讓他興起了建立「維基百科」的想法。

海耶克對這個問題的解釋，和當時流行的基本看法並不相同，他認為經濟問題不僅是分配資源和生產的問題，更精確地說，是使用任何個人或群體所缺乏的「知識」，來分配資源和產品的問題。生產條件的經濟知識、生產要素的相對可用性和豐富程度、個人偏好等，均非整個群體能夠完全了解的客觀知識。相反的，經濟條件的知識，在本質上是由相關人士「個人的決定」來分配。每個人的思想都被用於學習和理解跟他們本身相關的經濟訊息，高度智慧和勤奮的人會花費幾十年的時間，學習他們所在行業的經濟現實，以便在單一產品的生產過程中，達到權威的地位。不可思議的是，所有這些需要由每個人執行的「個人決策」，都可透過將所有訊息匯總到「某位個人」腦中，來替每個人進行經濟上的計算。但也並非瘋狂的追求，想把所有知識集中到某個決策者手中。

在自由市場經濟體系裡，「價格」是知識，也是傳遞訊息的信號。每個決策者只能透過檢查相關貨物的價格，來做出自己的個人決定。因此這些貨物的價格，精煉自所有市場條件和現實，然後轉化為其個人的一個「可操作變量」。反過來說，每個「個人的決定」將會在塑造價格方面發揮作用，任何中央機構都無法將形成價格的所有訊息隱瞞或取代其功能。

為了解海耶克的觀點，請想像以下的情況。假設某個國家的基礎設施被地震嚴重破壞時，而這個國家是世界上某商品的主要生產國，例如 2010 年的智利大地震，智利是世界上最大的銅生產國。當地震襲擊一個擁有大

量銅礦的地區時，它對這些礦區以及出口銅礦的港口造成破壞。因此供應到世界市場的銅減少了，立刻導致銅價上漲 6.2%<sup>註 1</sup>。世界上任何與銅市場相關的人，當然都會受到影響，但他們並不需要知道關於地震、智利和市場條件的任何事情，才決定如何採取行動。因為價格上漲這件事本身，便包含他們必須知道的所有相關資訊。很快的，所有需要銅的公司現在都必須減少銅的需求量，延遲不是迫切需要的採購，並盡可能尋找銅的替代品。另一方面，價格上漲會使世界各地生產銅的所有公司，現在都想生產更多的銅，以便在價格上漲的時機獲利。

隨著價格的上漲，全世界銅行業的每個人，都想採取行動來減輕地震的負面影響：因此其他地區的銅礦生產者會提高供應量，各地需要銅的消費者則會降低需求。如此一來，地震所造成的短缺嚴重程度便會下降，而價格上漲帶來的額外收入，也有利於幫助礦區重建基礎設施。幾天之內，銅的價格便恢復了正常。當全球市場變得更加一體化也更大時，這種個別商品中斷的影響力正越變越小，因為建立商品市場的人，可以善用生產深度與流通性，經歷最短的中斷期便能迅速平復。

而為了了解「價格是傳播知識方法」的威力，請再想像一下，地震發生的前一天，整個全球的銅工業不是一個市場機制，而是由特別的專門機構所控制，如此便代表生產是在「沒有參考價格」的情況下進行分配。這種機構要如何應付地震呢？在全球各地眾多的銅生產商中，該如何決定哪些生產商要增加產量，以及增加多少？如果是在價格體系裡，每個公司自己的管理階層都會查看銅價與生產相關的所有價格，以便找到最有效的產量解答。許多

---

註 1 Ben Rooney, 「智利地震後的銅罷工 (Copper Strikes After Chile Quake)」, *CNN Money* (2010 年 3 月 1 日)。參閱 <http://money.cnn.com/2010/03/01/markets/copper/>。



專業人士在同一家公司工作了幾十年，可以在價格的協助下得出答案。他們對自己公司的了解，遠遠超過中央的規劃，因為中央機構在決定時，沒有市場價格可供參考。此外，如果沒有價格來讓消費者透露出他們的偏好，那麼中央規劃者便無法決定哪些銅行業，應該減少使用量。

無論這些機構收集了多少客觀數據和知識，都沒有辦法了解個人在執行決策時所包含的全部分散知識，包括自己的偏好和對物品的價值判定等。因此，價格不僅僅是讓資本家獲利的工具；也是經濟生產的訊息系統，可以跨國際的傳播經濟知識，並協調複雜的生產過程。任何試圖免除自由市場價格的經濟體系，都會導致經濟活動徹底崩潰，並使人類社會回歸原始狀態。

價格也是讓市場經濟得以發生貿易和進入專業化的唯一機制。若沒有價格，人類就無法從一些非常原始的小生產規模，進化到分工與專業化而獲利。貿易可以讓生產者將自己比較具優勢的商品專業化，例如用相對較低的成本生產優勢商品，進而提高自己的生活水準。只有以共同的交換媒介來表達準確的價格，人們才有可能確定自己的商品為優勢，並專注加強此一優勢。由價格訊息所領導的專業化，將可帶領生產者透過邊做邊學，以及為生產累積特定資本，進一步提高這些產品的生產效率。事實上，即使沒有相對成本的既有差異，專業化也會讓每個生產者累積與生產相關的資本，進而提高其邊際生產力，使他們能夠降低生產的邊際成本，並與那些為其他商品專業化而累積資本的人，相互進行貿易。

## 資本市場社會主義

雖然多數人都能了解「價格體系」對分工的重要性，但很少人會了解它在資本累積和分配所發揮的關鍵作用，因此我們必須轉向 Mises 的作品尋求解釋。在 1922 年 Mises 的《社會主義》一書中，他解釋了社會主義制度必定失敗的經典原因，並非社會主義只存在「動機」問題的普遍觀點（也就是如果大家都能得到同樣的獎勵，誰還願意工作呢？）因為你不工作的話通常會受到政府謀殺或監禁等懲罰，因此不管過程有多麼血腥，社會主義可說成功的克服了「工作動機」的問題。一個世紀以來，全世界約有 1 億人被社會主義政權所謀殺<sup>註2</sup>，這種懲罰顯然不是理論上而已，因此其「工作動機」可能還強過資本主義制度。所以社會主義的失敗，一定不只是「激勵」的問題而已，Mises 便是第一個能夠準確解釋為何社會主義會失敗的人，即便社會主義當時已透過創造「新社會主義者」，成功克服了「激勵」的問題。

Mises 揭露了社會主義的致命缺陷：如果沒有自由市場出現的價格機制，社會主義就會在經濟計算中失敗，最重要的是在資本品的分配中失敗<sup>註3</sup>。如我們之前所討論過的，資本生產涉及到越來越複雜的生產方法，生產時間範圍也拉長，而且還會產生大量無法消費的中間產品，這些先生產出來的中間產物，要在未來參與完成消費商品的最終生產。複雜的生產結構，只能從每個資本的生產者和消費者，彼此良好且複雜的買進賣出個

註 2 Stephane Courtois、Nicolas Werth、Karel Bartosek、Andrzej Paczkowski、Jean-Louis Panne 和 Jean-Louis Margolin，「共產主義黑皮書：犯罪、恐怖、鎮壓（*The Black Book of Communism: Crimes, Terror, Repression*）」，哈佛大學出版社，1997 年。

註 3 Ludwig von Mises，「社會主義：經濟社會學分析（*Socialism: An Economic and Sociological Analysis*）」，Ludwig von Mises 研究所，Auburn，AL，2008 年（1922 年）。

人計算網路中產生<sup>註4</sup>。最有效的分配，便是讓價格機制來決定，也就是透過最需要此資本商品的用戶，為它們喊出最高的價格。

資本商品的供給與需求，來自生產者和消費者的互動，以及他們不斷做出的決定。

在社會主義制度下，政府擁有並且能夠控制生產工具，讓它變成整個經濟裡所有資本商品的唯一買家與賣家。這種集中化扼殺了市場的實際運作，以致無法根據價格做出合理決策。而沒有個別買家可以競標資本商品價格的資本市場，整體資本或個人資本商品就無法制定價格。而如果沒有資本商品的價格來反映相對的供給和需求，就不會有合理的方法來確定資本如何利用最為有效，也沒有合理的方法來決定每種資本商品的生產量。在政府擁有鋼鐵廠的世界裡，所有在生產消費品和資本商品過程中會使用到鋼鐵的工廠，他們在鋼鐵或用鋼鐵生產的產品上，都無法看到價格。因此也無法得知哪種鋼材最重要或最有價值。如此一來，政府該如何確定是否將數量有限的鋼材，用來製造汽車或火車？因為政府同時還擁有汽車和火車工廠，而且會透過強制命令向市民分配他們可擁有的汽車或火車數量？如果沒有市民的價格體系來決定火車和汽車之間的關係，就無法知道鋼材的最佳分配為何，也無法知道實際上最需要鋼鐵的地方。若用問卷來調查市民意願，更會是一項毫無意義的工作，因為沒有價格便無法決定選擇所涉及的實際機會成本。沒有價格的調查，可能會發現每個人都想擁有自己的法拉利，但當你必須付錢的時候，很少人還想選擇法拉利。中央計劃者永遠不會知道每個人的偏好，因此也無法以最能滿足個人需求的方式分配資源。

---

註 4 凱因斯經濟學存在許多問題，但最荒謬的是完全沒有任何關於資本生產結構「如何運作」的概念。

此外，當經濟生產過程裡的所有資料都為政府所擁有時，在缺乏價格機制下，無法協調出適當的資本商品生產數量，來讓所有工廠都能運作。「稀缺」是所有經濟學的起點，我們不可能為所有商品生產無限量的供應；因此必須進行權衡、分配資本、土地和勞動力，除了生產鋼鐵外，很可能還要同時考量生產更多銅所需的代價。

在自由市場裡，一旦工廠開始搶購銅和鋼，便會在市場裡創造了稀有性與升值能力，抬升的價格，會讓這些銅與鋼的製造商，競相搶購製造它們的原料資源。而對於火車、汽車、銅、鋼鐵、勞動力、資本土地偏好和機會成本網路各方面，中央規劃者完全無法了解。因為沒有價格，就無法計算如何分配這些資源，生產出最優質的產品，結果就是生產方面的完全崩潰。

然而這些只是計算上的問題，只涉及到靜態市場生產的現有商品。但當我們察覺到人類的相關事物沒有純粹靜態的東西時，整個問題就會更加明顯，因為人類會一直尋求方法來改善經濟狀況、生產新產品並尋找更多更好的生產方法。人類對於修補、改進和創新的不斷努力，為社會主義帶來了最棘手的問題。即使中央規劃體系可以成功管理靜態的經濟，但對於變化的調適或允許創業的方面，便無能為力了。社會主義制度如何計算並不存在的技術和創新呢？如果沒有跡象得知產品是否能用，又該如何為這些產品分配生產要素？

「那些把創業和管理混淆在一起的人，閉起眼睛不肯面對經濟問題…因為資本主義制度並不是資本管理體制；而是企業家體制。」

—Ludwig von Mises<sup>註5</sup>

---

註5 Ludwig von Mises，「人類行為（*Human Action*）」，第703-704頁。

這種說法的目的，並不是用來反對社會主義經濟體制，經歷過上個世紀社會主義體制最後嘗試的每個社會體，在遭受災難、血腥與全面失敗後，應該不會再有任何理智的成年人，想把這種體制當真。我們的重點應該是放在釐清兩種體制在分配資本與生產決策上的差異：到底該用價格或由中央規劃來做分配與生產的決定？雖然世界上多數國家，都沒有負責直接分配資本貨物的中央規劃委員會，但每個國家都會有一個中央計劃委員會，用來處理最重要的市場，也就是資本市場。

自由市場可以解釋為「買賣雙方依據自己訂定的條款自由交易」，而且可以自由進出市場：沒有第三方會限制賣方或買方進入市場，也沒有第三方會補貼無法在市場上交易的買家和賣家。然而目前世界上卻沒有任何一個國家，具有帶著這些特徵的純粹資本市場。

現代經濟中的資本市場裡，還包含了可借貸資金市場。當生產結構變得更加複雜且長期時，生產者不再需要投入自己的儲蓄，反而是透過各種機構，把銀行裡的儲蓄借給專門從事生產的企業。其中必須的貸款利率，來自貸款貸出價格與借款人為獲得貸款所支付價格的利差計算而得。

在可借貸資金的自由市場中，其資金供應量會與其他供應曲線一樣，隨著利率一起上升。換句話說，利率越高，大家會越想儲蓄，資金供應量上升，並向企業家或企業提供這些儲蓄。另一方面，貸款需求與利率成反比，也就是利率越高，企業家和企業便會減少借貸，利率也因而再度降低。

資本自由市場的利率是正向的，因為人們積極的時間偏好，代表除非將來能夠獲得更多資金，否則大家都想把錢握在手上。而一個社會若擁有大量低時間偏好的個人，便可能會擁有大量的儲蓄，而讓利率走低，並為企業投資提供充足的資金，為以後帶來顯著的經濟成長。隨著整體社會提高時間偏好，人們不太願意儲蓄，利率便會升高，生產者也較難找到借貸

資本。生活在和平且擁有安全財產權和高度經濟自由的社會，可能會有較低的時間偏好，因為它們為個人提供一種強烈動機，增加其對未來的期望值。另一位奧地利經濟學家 Eugen von Böhm-Bawerk 甚至認為，一個國家的利率反映其文化水平：人民的智慧與道德力量越高，便有越多的儲蓄，利率也會越低。

但由於現代中央銀行的發明，且持續干預著最關鍵的市場，讓資本市場並未在當今任何現代經濟中，發揮利率原先的作用。因為中央銀行會透過各種貨幣工具，決定利率以及供應多少貸款金額，而且會透過控制銀行系統來加以運作<sup>註 6</sup>。

對現代金融體系的一個基本事實，就是銀行只要借錢出去就會創造出貨幣。在類似於現今世界各地的局部儲備銀行系統中，銀行不僅可以把客戶的儲蓄出借，還可以把客戶的活期存款出借。換句話說，雖然存款人可以隨時提回自己的錢，但這些錢有很大部分已作為貸款發給了借款人。除了向借款人提供資金，也同時可讓存款人提回資金，讓銀行有效地創造了新的資金，而導致貨幣供應增加。如此便可建立貨幣供應量與利率的基本關係：當利率下降時，貸款增加導致貨幣增加，貨幣供應量也增加。從另一方面看，利率上升則會導致貸款減少與貨幣供應量減少，或至少會降低其成長率。

---

註 6 中央銀行所使用的主要工具包括：設定聯邦基準利率、設定所需儲備率、參與公開市場操作以及決定貸款資格標準。在任何初級的宏觀經濟學教科書中，都可以找到這些工具操作機制的詳細說明。總結如下：中央銀行可以透過以下方式實施貨幣擴張政策：（1）降低利率、刺激貸款並增加貨幣供應；（2）降低存款準備率，允許銀行增加貸款，增加貨幣供應；（3）購買國債或金融資產，這也可增加貨幣供應；以及（4）放寬貸款資格標準，允許銀行增加貸款，因而增加貨幣供應。反轉這些步驟便能進行貨幣緊縮政策，讓貨幣供應量減少，或至少降低貨幣供應量的成長率。

## 商業週期和金融危機

在資本自由市場中，可貸資金的供應多寡，由決定依照利率來放貸的市場參與者所制訂，而在擁有中央銀行和局部儲備銀行的經濟體中，這些可貸資金的供應，便是由政客、銀行家、電視專家、有時甚至是軍事將領所影響下的經濟學家委員會來管控。

任何熟悉經濟學的人，都該了解控制價格的明顯危機。若政府決定訂立蘋果的價格並阻止變動，其結果不是造成蘋果短缺就是過剩，無論生產過剩或生產不足，都會給社會造成巨大損失。在資本市場裡發生類似的事情時，影響會更具破壞性，因為資本參與了每種經濟商品的生產，所以會影響到經濟的每個層面。

我們必須先了解可貸資金與實際資本品之間的區別。在擁有健全貨幣的自由市場經濟中，儲蓄者必須延遲消費以節省開支來儲蓄，而存進銀行作為儲蓄的錢，是來自延後本來的滿足所取消的錢，以便可以在未來獲得更多滿足。最後確切的儲蓄金額，便成為提供給生產者可貸資金的實際數目。資本商品的可用性與消費的減少密不可分：實際的物質資源、勞動力、土地和資本商品，將從本來作為最終消費品的用途，轉變為生產資本商品。例如在最後端工作的人，被指示離開汽車銷售的工作崗位，轉職到汽車工廠工作；如此一來，傳說裡的玉米種子便可被種入地下，而不是被吃掉。

稀缺性是所有經濟學的基本出發點，其最重要的含義便是一切都有「機會成本」的概念。而在資本市場中，資本的機會成本便是放棄消費，消費的機會成本便是放棄資本投資。利率正是用於這種關係的價格：當人們有更多投資上的需求，利率便會上升，激勵更多儲蓄者將更多的錢拿來儲蓄。當利率下降時，便可激勵投資者進行更多投資，而且會投資在要花

更長時間才能完成的先進技術生產方法。因此較低的利率，可以讓更長期與更高產能的生產方法參與生產：社會也會從魚竿進步到用柴油動力大船來捕魚。

隨著經濟發展越來越複雜後，雖然實體資本與可貸資金市場之間的聯繫，在現實裡並未改變，但它確實在人們的腦海中變得更混淆了。擁有中央銀行的現代經濟，便建立在忽視這種基本權衡的基礎上，並假設了銀行可以用新的資金為投資提供後盾，消費者也不必放棄消費。因此儲蓄和可貸資金之間的聯繫被切斷，甚至在經濟學教科書裡也不再教授<sup>註7</sup>，更別說忽視它以後，已經造成的災難性後果。

由於中央銀行管理貨幣供應和利率，造成儲蓄和可貸資金之間，難以避免的存在著差異。中央銀行通常會試圖刺激經濟成長與投資以及增加消費，因此它們傾向於增加貨幣供應量並降低利率，導致可貸資金數量大過了儲蓄的金額。在這些人為的低利率環境下，企業願意承擔更多「債務」來投資生產項目，而非由儲蓄者為這些投資提供資金。換句話說，延遲消費的價值會小於借入資本的價值。而如果沒有足夠的消費延遲，就不會有足夠的資本，土地和勞力資源便會在生產的最初階段，從消費品轉向更高階的資本商品。畢竟天下沒有白吃的午餐，如果消費者的儲蓄減少，投資者的資金就會減少。創造新的紙張或增加紙上的數字來克服儲蓄不足的問題，並無法神奇的增加整個社會的實體資本存量；反而只會讓目前已存在的貨幣貶值並扭曲市場價格。

---

註7 在教高年級學生「一個假設的資本自由市場」課程時，我覺得非常有趣，因為可以觀察他們臉上的反應。當他們將資本自由市場如何運作的簡潔邏輯，跟假科學的凱因斯主義中央計劃理論相互比較，就會讓他們在「貨幣理論」課堂上，直接學會什麼叫做「不幸」。



這種資金短缺不會立即出現，因為銀行和中央銀行可以為借款人「發行」足夠的資金，畢竟這是使用不健全貨幣最方便之處。如果是在健全貨幣的經濟體下，便不可能發生這種對資本價格進行操縱的情況：因為一旦人為降低了利率，銀行裡的儲蓄金額短缺，便會反映出借款人可貸資本減少，導致利率上升，貸款需求減少，儲蓄供應提高，一直到兩者可以相符為止。

不健全貨幣使得這種操縱變成可能，但當然時間會很短，因為政府無法一直隱瞞事實。人為的低利率與多印出來的紙鈔，欺騙了生產者參與「超出實際可用資本資源」的生產過程。在沒有實際延遲消費的支持下，這些多餘出來的資金，一開始會讓更多生產者借入資金，並認為這些錢可以讓他們購買生產過程所需的資本商品。但隨著越來越多的生產者，一起競標比預期更少的資本商品和資源時，當然就會讓生產過程所需的原料型資本商品價格上漲，導致許多資本投資同時崩潰。這就是政府操縱計謀曝光的一刻，因為這些資本投資，面對新資本商品價格上漲時，會變得無利可圖；這些項目就是 Mises 所說的「錯誤投資」，也就是資本市場被扭曲才會進行的投資，一旦資本錯誤配置暴露後，生產過程便無法完成。中央銀行對資本市場的干預，會讓更多這類型的錯誤投資持續發生，因為價格扭曲導致了投資者計算錯誤，但中央銀行的干預並不能增加實際可用資本的數量，所以這些額外的投資項目並未完成，也成了不必要的資金浪費。而且停掉這些項目以後，還會導致整個經濟體的失業率上升。而這種過度擴張的企業同時失敗的情況，就是經濟上所謂的「經濟衰退」。

只有了解資本的結構與認知操縱利率會破壞資本累積，才能理解經濟衰退的原因和商業週期的波動擺盪。「商業週期」是操縱利率、扭曲資本市場的自然結果，因為投資者以為從銀行貸到了不健全貨幣，就可擁有更多的資本。但跟凱因斯主義的「動物神話」相反的是，商業週期並非由標榜「動物精神」所引起的神秘現象，商業週期之所以被忽視的原因，就是

因為中央銀行家們，妄想操縱經濟復甦<sup>註8</sup>。經濟邏輯很清楚的告訴我們，「操縱利率」的必然結果就是經濟衰退，同樣的，「訂定價格上限」必然會造成物資短缺。

我們可以從 Mises 的作品中借用一個類比<sup>註9</sup>，稍做修飾來加以說明：請想像一個社會的資本存量為建築的磚塊，而作為「承包商」的中央銀行負責用磚塊蓋房子。蓋一棟房子需要 10,000 塊磚，開發商正在尋找有能力建造 100 棟房子的承包商，也就是總共需要 100 萬塊磚。但有一位渴望贏得標案的凱因斯主義承包商意識到：如果他能提交一份合約，承諾建造 120 棟房子而且只需用 80 萬塊磚，他的得標機會就會增加。但這就像操縱利率一樣：增加資本需求又減少資本的供應。因為事實上，完成 120 棟房屋需要 120 萬塊磚，但現在只有 80 萬塊磚可用。80 萬塊磚可以開始建造 120 棟房子，但並不足以完成這些房子。由於凱因斯主義的工程奇蹟，開發商非常高興看到多出 20% 的房子，而且還只花了 80% 的成本，因此他用省下的 20% 成本，為自己買了一艘新遊艇。

不過這場騙局無法持久，因為很明顯的房子最後無法完工，建商也必須停工。承包商不僅沒有交付 120 棟房子，甚至也交不出任何一棟房子。而且留給開發商 120 棟半成屋，只能算是沒屋頂的一大堆磚塊而已。承包商的詭計減少了開發商所要花的錢，導致建造的房屋數量少於正確的價格信號。如果是和誠實的承包商簽約，開發商就會擁有 100 棟房子。跟扭曲數字的凱因斯主義承包商合作，只要資本被分配到一個沒有事實依據的計劃時，開發商就是在繼續浪費他的資本。如果開發商有點意識到這個錯

---

註 8 奧地利資本理論中，並不缺乏解釋衰退的說法，這些都是 20 世紀初期貨幣轉變的重新論證。所以你甚至不需閱讀關於凱因斯主義或流行心理學理論最新的現代反駁論述。只要閱讀海耶克在 1933 年的「貨幣理論和貿易週期」，或者 Rothbard 在 1963 年的「美國大蕭條」，便已足夠。

註 9 Ludwig von Mises，「人類行為（*Human Action*）」，第 560 頁。

誤，那麼一開始浪費在 120 棟房子上的資本可能不多，新的承包商還可以拿剩下的磚塊來蓋出 80 棟房子。如果開發商在資本耗盡之前仍然搞不清現實狀況，那麼他只會擁有 120 棟未完工的房子，這些房子也毫無價值，因為沒人願意住在沒有屋頂的房子裡。

當中央銀行透過銀行借貸來供應更多貨幣，並操縱利率讓它低於市場清算價格時，就會立即減少社會可用的儲蓄量，同時也會增加借款人的需求量，進而讓這些借入的資本投向無法完成的項目。所以貨幣形式越不健全，中央銀行越容易操縱利率，商業週期的盈虧也就越嚴重。貨幣歷史證明，當貨幣供應受到操縱時，商業週期和經濟衰退的嚴重程度要比不受操縱時來得更糟糕。

雖然多數人認為社會主義者的「社會」已成為過去，市場體系也由資本主義經濟所帶領，但現實狀況是資本主義制度若缺乏資本自由市場，就會無法運作。因為資本價格是透過供需關係產生，資本家的決定是由準確的價格信號所驅動，中央銀行干預資本市場，便是所有經濟衰退的根源，也讓大多數政治家、記者、學者與左派人士，責怪資本主義造成了危機。也只有透過中央規劃的貨幣供應，才會造成資本市場價格機制被破壞，導致經濟的大幅衰退。

每當政府開始走上貨幣供應膨脹的道路時，其負面後果難以避免。如果中央銀行停止通貨膨脹，利率上升，隨之而來的便是經濟衰退，因為許多已啟動的項目都將被視為無利可圖而放棄，接著便會暴露出資源和資本的配置失當。而若中央銀行無限期的繼續通貨膨脹，就會不斷增加錯誤分配的規模、浪費更多資本，使難以避免的經濟衰退更加嚴重。所以面對凱因斯怪人所強加的「免費午餐」，我們無可避免的要付出沉重的代價。

「老虎（通貨膨脹）跟在我們後面：到底會持續多久呢？一旦老虎被放開，我們就會被吃掉；然而，如果我們拼命堅持，但老虎也跑得越來越快，我們依舊會失敗！我很慶幸不會親眼看到最後的結果。」

—海耶克<sup>註10</sup>

中央銀行對貨幣供應的計劃既不可取也不可行。這等於是讓最誇大自負的人來管理經濟，讓一個經濟體裡最重要的市場，活在少數人的指揮下。這些人對市場經濟的現實一無所知，甚至還相信他們可以自行規劃一個大型、抽象與緊急的市場，就像資本市場一樣。想像一下如果中央銀行可以「預防」、「打擊」或「管理」經濟衰退，那不就跟「把放火狂和縱火犯找來當消防隊」，一樣的天真幻想與誤入歧途？

健全貨幣的相對穩定，是因為它來自於市場的選擇，因此可以透過不同的價格與個人的決策來經營自由市場。而不健全的貨幣供應是由中央所規劃，無法出現準確的價格信號，因為它在本質上就已受到控制。透過幾個世紀的價格控制後，中央計劃者試圖找到不合理的「最佳價格」來實現他們想要的目標，但無濟於事<sup>註11</sup>。價格控制必定失敗的原因，並非中央計劃者無法選到合適的價格，而是因為「指定」任意價格後，本來的正常市場參與者因為消費與生產決定，所將調整出來的市場價格無法出現，因而造成了「必然的」短缺或盈餘。同樣的，信貸市場的中央計劃也必定失敗，因為它也破壞了「市場的價格發現機制」，無法為市場參與者提供準確的信號和激勵來管理消費和生產。

---

註10 弗里德里希·海耶克，「老虎跟在你後面（*A Tiger by the Tail*）」，p126。

註11 「四千年的價格和工資控制：如何不對抗通貨膨脹（*Forty Centuries of Price and Wage Controls: How Not to Fight Inflation*）」，強烈推薦的歷史記錄，描述歷史上的價格控制所造成的悲慘又令人生畏的災難後果，Robert Schuettinger 和 Eamonn Butler 著。

正如奧地利商業週期理論所解釋的，資本市場中央計劃所採取的失敗形式是「繁榮與蕭條的週期」。難怪這種功能障礙似的興衰週期，被視為市場經濟的正常組成，因為在現代經濟學家心目中，能控制利率的中央銀行，才是現代市場經濟的正常組成吧。就此方面而言，中央銀行的過去記錄，跟沒有中央計劃與控制貨幣供應的時期相比來說，非常糟糕。美國聯邦儲備委員會成立於1914年，必須為1920～1921年的儲備急劇萎縮負責，然後又遇上1929年的大蕭條，影響也延續到1945年底。從那時候開始，「經濟蕭條」成為經濟上的常規與痛苦，每隔幾年就會重複出現，也讓政府更有理由對經濟的影響進行干預。

瑞士經濟的命運，可以當作「健全貨幣」確實較好的一個例子。瑞士是健全貨幣的最後堡壘，一直維持著貨幣與黃金之間的連動，直到國家命運乖違，決定放棄全球貨幣中立地位，並在1992年加入國際貨幣基金組織。在此之前，瑞士的失業率趨近為零，幾乎從未超過1%。而在他們加入國際貨幣基金組織之後，組織規則直接阻止政府將其貨幣價值與黃金連動，因此瑞士經濟也開始體驗凱因斯主義「滑稽貨幣」的樂趣，失業率在幾年內便上升到5%，然後就很少低於2%以下（見圖13<sup>註12</sup>）。

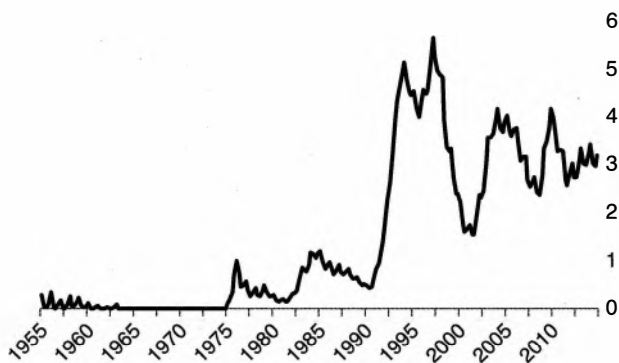


圖 13 瑞士的失業率百分比

註 12 資料來源：美國聯邦儲備銀行經濟數據，詳見 <https://fred.stlouisfed.org>。

在我們把經濟蕭條與黃金標準的時期相互比較時，必須先記住 19 世紀時，歐洲和美國的黃金標準已經不是最完美的健全貨幣形式，因為它帶有幾個缺陷。其中最嚴重的便是銀行和政府經常將貨幣與信貸供應量，擴大到黃金儲備之外，導致了二十世紀常見的繁榮和蕭條輪替（雖然現在的幅度可能小一點）。

知道這樣的背景才可以更清楚的了解，現代貨幣史並不像凱因斯主義氾濫以來學校教科書裡教的那種。一般認為 Milton Friedman 與 Anna Schwartz 的《美國貨幣史》（*The Monetary History of the United States*）是貨幣主義思想的創始文本，也是美國貨幣史上最權威的作品。這是一本 888 頁的厚書，令人驚訝的匯集著難以數計的事實、細節、統計數據與分析工具，但卻沒讓不幸的讀者理解一個關鍵問題，也就是金融危機和經濟衰退的原因。

Friedman 與 Schwartz 這本書的根本缺陷，可以說是現代學術研究的典型範例：用嚴謹取代邏輯的一場「精心練習」。該書有條不紊的「避免」質疑一個多世紀以來，影響美國經濟的金融危機原因，反而用令人印象深刻的研究數據、事實、瑣事和枝微末節來淹沒讀者。

這本書的核心觀點在於「經濟衰退」是由於政府速度不夠快，沒有儘快透過增加貨幣供應、重新擴大銀行業，來迅速處理金融危機、銀行擠兌以及通貨緊縮的問題。也就是典型的 Friedman 自由主義者們，會將經濟問題歸咎於政府的處理方式，但這種有缺陷的推理，反而會鼓勵政府增加干預以作為解決方案。因此這本書的明顯錯誤，在於作者從未討論過背後的真正原因，到底是什麼原因才導致這些金融危機、銀行擠兌與貨幣供應緊縮？正如我們從奧地利商業週期理論的敘述裡所見，經濟衰退的唯一原因便是從擴大貨幣供應開始所造成的通貨膨脹。由於不了解真正原因，所以 Friedman 與 Schwartz 完全無負擔的推薦了自己認為的原因當作處方：也

就是政府必須在經濟衰退的第一個跡象出現時，積極介入銀行體系，瞬間進行資本重組以增加流通性。現在你應該可以開始明白，為何現代經濟學家討厭理解「邏輯因果」關係；因為這樣會拆穿所有解決方案的假面具。

Friedman 與 Schwartz 在 1867 年開始寫這本書，因此，在他們分析 1873 年經濟衰退的原因時，便完全忽略了美國政府印刷美元來支持內戰的這件「小事」，這才是當時經濟衰退的最終原因啊。整本書裡都一直在上演這種分析模式。

Friedman 與 Schwartz 幾乎沒有在書中討論 1893 年經濟衰退的原因，只略微提到會推動白銀是因為黃金不足以滿足經濟上的貨幣需求，然後就用那年經濟衰退的瑣事來擠滿讀者視線。他們並未提到 1890 年美國國會批准的「謝爾曼白銀購買法案」，該法案要求美國財政部用新發行的國庫券來購買大量白銀。由於當時白銀在全球範圍內幾乎已完全被貨幣化，持有白銀或國債券的人試圖換取黃金，導致財政部黃金儲備的大量流失。事實上，財政部透過增加貨幣供應來假裝白銀仍然是貨幣，引發了錯誤的貨幣擴張主義。這些行為讓美國國債貶值而造成金融泡沫，並在黃金提領增加後崩潰。任何記載該時期的史書，都可對那些粗略理解貨幣理論的人說個清楚，然而 Friedman 與 Schwartz 竟然刻意避免提及這些事。

這本書對 1920 年經濟衰退的處理上，忽略了美國為資助第一次世界大戰必須進行的大規模貨幣擴張。儘管在書裡的分析中未曾提及，但書裡的數據<sup>註 13</sup>依舊告訴我們，從 1914 年 6 月至 1920 年 5 月期間，貨幣存量增加了 115%。此一成長只有 26% 是由於黃金持有量增加，亦即其餘增加部分是由政府、銀行與美國聯邦儲備銀行所推動。這就是 1920 年經濟蕭條的主要原因，但書裡並沒有提到。

---

註 13 見 Friedman 與 Schwartz 的書，在第 206 頁的表 10。

最令人好奇的是，他們為何完全忽視 1920～1921 年經濟蕭條復甦時，經濟學家 Benjamin Anderson 所稱的「最後自然回復充分就業」，稅收和政府支出減少，工資可自由調整，因此在不到一年的時間裡迅速恢復充分就業<sup>註 14</sup>。1920 年的蕭條是美國歷史上出口緊縮最快的一次（從 1920 年 9 月到 1921 年 7 月的 10 個月內下降了 9%），復甦的也最快。

在其他蕭條時期，隨著凱因斯主義者和貨幣主義者注入流通性、增加貨幣供應量與增加政府支出等手段，經濟復甦也變得越來越慢。

雖然每個人都試圖吸取大蕭條的教訓，但主流經濟學教科書從未提及 1920 年的經濟蕭條，也從未試圖了解為何這種蕭條如此迅速復甦<sup>註 15</sup>。當時的總統沃倫哈丁有著對自由市場的堅定承諾，拒絕聽取干預主義經濟學家的呼籲。因此這些不良投資被清算，其中使用的勞動力和資本很快就被重新分配給新的投資。由於沒有政府干預一開始造成的經濟扭曲，因此失業很快就恢復到正常的水準。這是 Friedman 與 Schwartz 推薦內容的明顯對立面，所以在他們的書裡當然也沒有提到。

說到這本書裡最著名的一章（也是大家唯一可能讀過的內容）便是第 7 章，整章內容主要便是在講大蕭條。該章從 1929 年 10 月的股市崩盤之後談起（前一章結束在 1921 年）。整個 1921 年至 1929 年 10 月期間，包含大蕭條的任何原因都跳過了，其重要性竟然比不上本書 888 頁裡的任何一頁。

註 14 Murray Rothbard，「美國大蕭條（*America's Great Depression*）」，第 5 版，第 186 頁。

註 15 在 James Grant 的書「被遺忘的衰退：1921 年，自我解決的崩潰（*The Forgotten Depression: 1921: The Crash That Cured Itself*）」裡，有對這場經濟蕭條的詳細解讀（Simon & Schuster 出版，2014 年）。



簡單地說，Friedman 與 Schwartz 提到價格水準在整個 1920 年代的上升並不快，因而得出「這段時間並非通貨膨脹」的結論，同時也認為經濟蕭條的原因不可能是通貨膨脹。但事實上 1920 年代經濟成長非常快，所以導致價格下跌。而由於美國聯邦儲備銀行試圖協助英格蘭銀行，阻止黃金從英國海岸流出，導致了貨幣膨脹。而這整個事件又因為是英國銀行貨幣膨脹，而非工資向下調整所造成的原因。貨幣供應增加和經濟快速成長的淨效應，應該是價格水平不會大幅上漲，但資產價格（主要是住房和股票）則會大幅上漲；然而貨幣供應增加並沒有轉化為消費者物品價格的上漲，因為這主要是被美國聯邦儲備銀行用來刺激股市與房市。而在 1921 年至 1929 年期間，貨幣供應量增加了 68.1%，黃金庫存僅增加 15%<sup>註 16</sup>。亦即美元庫存的增加超過了黃金庫存，這也就是大蕭條的根本原因。

值得一提的是貨幣主義者之父 Irving Fisher，曾在 1920 年代致力於「價格水平的科學管理」。Fisher 想像當美國擴大貨幣供應量時，大量收集的數據與科學管理，可以讓他控制貨幣供應和資產價格的成長，以確保價格水平保持穩定。1929 年 10 月 16 日，Fisher 驕傲地在「紐約時報」宣布股票已到達「恆久的高點」<sup>註 17</sup>。結果股票市場從 1929 年 10 月 24 日開始崩盤，隨著大蕭條逐漸加深，直到 1950 年代中期，Fisher 過世幾年後，股市才終於來到他在 1929 年所說「恆久的高點」。毫無疑問的，Milton Friedman 後來便尊稱 Irving Fisher 是美國曾出現過最偉大的經濟學家。

這場崩盤是由於 1920 年代的貨幣擴張所造成的，在股市中產生了巨大虛幻的財富泡沫。一旦貨幣擴張變慢時，泡沫就會破掉。而一旦經濟泡沫破裂之後，便意味著通貨緊縮旋風出現，讓所有泡沫裡的虛幻財富通通

---

註 16 Murray Rothbard，「美國大蕭條（*America's Great Depression*）」。

註 17 「Fisher 認為股票到達恆久的高點」，*紐約時報*，1929 年 10 月 16 日，第 8 頁。

消失。隨著財富的消失，開業中的銀行必須努力履行義務，如此便暴露了只擁有局部儲備的銀行系統問題，簡直就是一場等待發生的災難。有鑑於此，雖然無法完全保證企業和股票市場的損失，但也應該由聯邦來保護人民的存款。不過事實上讓銀行獨力承擔，允許進行清算並讓價格下跌，才是唯一的解決方案。這種解決方案雖然會帶來痛苦的經濟衰退，但這是一開始讓貨幣擴張所造成的結果！

若想嘗試加入更多促進流通性的措施來避免經濟衰退，只會讓一開始造成的危機更加的病入膏肓。

貨幣擴張創造了虛幻的財富，也錯誤的分配了資源，因此這種財富必須消失，市場才能透過適當價格機制來恢復正常運作。正是有了虛幻的財富才會導致崩潰，要將這種虛幻的財富回歸原處只得重新疊好紙牌屋，以便為另一場更大更強的崩潰做好準備。

由於忽略在 1929 年之前累積的貨幣膨脹與股市崩盤有關，因此 Friedman 與 Schwartz 只認為是美國聯邦儲備銀行對崩潰的反應，導致經濟陷入大蕭條。他們認為，如果美國聯邦儲備銀行開放貨幣政策，讓銀行體系增加流通性，那麼股市的損失對整體經濟來說是無關緊要的，也不會發生大蕭條。事實上，美國聯邦儲備銀行在應對這場危機時是擴張性的，此一事實在大量數據裡被忽略了。雖然美國聯邦儲備銀行的確試圖減輕行業的流通性短缺，但它無法阻止崩潰。這並不是因為缺乏決心，而是因為經濟範圍內錯誤分配資本投資的崩潰，以及在第 4 章中討論過的「嚴重干預」政策所導致。

在這項大型作業裡，有三個重要的問題仍然沒有得到解決，也剛好可以揭露其邏輯的一個明顯漏洞。第一個重要問題是為何不比較 1920 年與 1929 年的經濟蕭條？儘管美國聯邦儲備銀行沒有使用作者推薦的方式進行

干預，但 1920 年的衰退並未持續很久。第二個問題是為何美國在十九世紀還沒有中央銀行的時期，從未遭受過金融危機？而當國會指示財政部像中央銀行的做法在內戰時多印鈔票，以及 1890 年白銀貨幣化時，才發生了金融危機？第三個同時也是最有說服力的問題，就是美國為何在經濟持續成長最長的時期之一，也就是 1873 年至 1890 年這段期間，沒有發生任何金融危機？更何況當時根本沒有中央銀行，貨幣供應受到限制，價格水平也持續下降？然而 Friedman 與 Schwartz 只稍微提到這個時期，指出儘管價格水平下降但經濟成長令人印象深刻，卻沒有用心評論價格水平下降的情況，到底如何發生。

正如 Rothbard 所解釋，市場經濟運作下，並沒有任何內在因素會造成持續的失業問題。在自由市場正常運作時，可以看到許多人失業或辭去工作，許多公司也因各種緣故破產或關閉，但這些失業大致將會由市場裡的新工作或新業務加以填補，因此在任何時刻都只有少到幾乎可忽略的人是自願失業的，就像 19 世紀黃金標準未被濫用時的情況一樣，瑞士在 1992 年之前也是這種情況。只有當中央銀行操縱貨幣供應和利率時，整個經濟範圍的大規模失敗才可能同時發生，因而導致整個企業界大規模的裁員浪潮，同時也造成本身技術無法輕易轉移到其他領域的工人，大量失業<sup>註 18</sup>。正如海耶克所說：「失業潮的起因不是資本主義，而是政府不讓企業使用健全貨幣。」<sup>註 19</sup>

---

註 18 見 Murray Rothbard，「經濟蕭條：成因與解決（*Economic Depressions: Their Cause and Cure*）」，2009 年。

註 19 弗里德里希·海耶克，「貨幣國家化（*Denationalization of Money*）」，1976 年。

## 貿易的健全基礎

在健全貨幣的世界裡，貨物和資本在不同國家之間流動，幾乎就像在同一個國家的不同地區間流動一樣：根據合法商人想要的互信互利原則進行交易。不論是使用凱撒大帝的 aureus 金幣，或是十七世紀阿姆斯特丹銀行的黃金標準，或者根據十九世紀的黃金標準，藉由實際將貨物從一個地方運到另一個地方，便是最重要的貿易保障。關稅和貿易壁壘幾乎都不存在，如果有的話，也只不過是用來支付過境費用或港口管理維護費用而已。

但在貨幣不健全的時代，例如歐洲淪為封建主義，或現代世界陷入貨幣民族主義的時代裡，貿易不再是交易者的權利，而是開始成為國家的重要問題，需要封建領主的監督或是政府對交易個人宣示領地主權等。在二十世紀裡，貿易本身便如此荒謬的完成了轉變，「自由貿易」一詞變成兩個人之間的「跨境」貿易，並根據各自政府商定的條件，而非商人彼此的條件進行交易！

在 1914 年多數政府暫停並限制使用紙幣兌換黃金，放棄了黃金標準以後，便開始了海耶克所稱的「貨幣民族主義」時期，亦即貨幣的價值不再是固定的黃金單位。黃金是具有最高庫存流量比的商品，因此在供應上的價格彈性也最低，讓黃金價格較易預測也相對穩定。然而相反的，政府貨幣的價值會隨貨幣和財經政策而變，也會因國際貿易而波動。降低利率或增加貨幣供應都會讓貨幣貶值，也會讓政府大花中央銀行提供給政府的貸款。當這兩個因素名義上都由政府「管理」時，他們至少可以自欺欺人地認為真的可以用管理來實現穩定。第三個因素則是所有國民與許多外國人行為的複雜綜合結果。亦即當一個國家的出口成長大於進口時（貿易順差），其國家貨幣將在國際外匯市場上升值；而當進口成長大於出口時（貿易逆差），其國家貨幣將會貶值。政策制定者可能不會將這點作為不應再

操縱貨幣價值的警示，也不會讓人們自由地使用波動性最小的商品作為貨幣，而是會開始對全球貿易的最小細節進行微觀的管理。

貨幣的價值，應該是衡量和計劃所有經濟活動的計價單位。然而從市場上波動性最小商品的價值，轉變成為透過政府貨幣的三種政策工具：貨幣、財政和貿易政策的總和，才能決定貨幣的價值。當然其中最不可預測的因素，就是個人對這些政策工具的反應。

用政府決策來指定價格的計價單位，就像政府試圖用決策來指定個人或建築物高度的測量單位。你可以想像當所有工程項目的測量，必須依據每天由中央測量單位發布的不同長度單位來測量，將發生多麼混亂的情形嗎？

這種測量單位的改變，可能只會影響到瘋子的虛榮心吧，因為把量尺縮短，就可以讓某個人本來面積為 200 平方公尺的房子，測量後真的變成 400 平方公尺，但這仍是同一棟房子啊！所有重新定義的測量單位，都將破壞工程師正確建造或維護房屋的能力。同樣地，貨幣貶值可讓一個國家在名義上變得更為富裕，或增加出口的表面價值，但它並不會真的讓這個國家更繁榮。

現代經濟學以「不可能的三位一體」來表達現代中央銀行管理者的困境：任何政府都無法成功實現「固定匯率、自由資本流動和獨立貨幣政策」這三個目標。如果要有固定匯率和自由資本流動，政府就不能制訂自己的貨幣政策，因為改變利率會導致資本流入或流出，讓匯率變得無法控制。我們也知道有多少現代經濟學家，希望透過貨幣政策來管理經濟。而想要擁有獨立的貨幣政策和固定匯率，只能透過限制資本流動來實現，這也是 1946 年至 1971 年期間，各國普遍存在的情況。但即使如此也無法持續限制下去，因為貨物減緩流動時，會以匯率的方式改變這種不平衡。亦即當一些國家出口過多，另一些國家進口過多時，便會導致政治談判以

重新調整匯率。由於每個國家政府都試圖追求自己的利益，並盡一切努力來做到這點，因此在國際組織裡想要敲定談判結果是不理性的。在 1971 年後，世界各國主要轉向於擁有獨立的貨幣政策與自由資本流動，但讓貨幣之間存在「浮動匯率」。

這種安排的優勢，讓凱因斯主義經濟學家可以用自己喜歡的工具來「管理」經濟，也能讓國際金融機構和資本家持續感到開心。對大型金融機構來說也是一大福音，因為這些金融機構每天產生價值數兆美元的外匯市場，交易大量的各國貨幣與期貨。但這種安排可能不會為所有人帶來好處，尤其是對那些真正為社會提供價值商品的生產企業。

在高度全球化下，外匯匯率取決於為數眾多的國內與國際變量，經營生產商品的企業突然必須面對前所未有的挑戰。一家成功的公司可能會在多個國家都有進出口業務，每次買賣行為都必須考量相關國家之間的外匯。在這個世界上，業務競爭激烈的公司，可能只是在匯率變化上就蒙受高額損失，甚至可能都還不是來自自己國家貨幣本身的匯損。如果該公司主要供應國的國家貨幣價值上升時，公司的投入成本也會上升，直到足以破壞該公司的盈利能力。而當主要出口市場的貨幣價值下降，也會發生相同的情況。一家花幾十年經營頗具競爭優勢的公司，也可能會在 15 分鐘裡，因為遇上無法預測的外匯波動而退出市場。這種情況通常會被歸咎於「自由貿易」的結果，經濟學家和政治家同樣也會拿它當藉口，進而實施受國民歡迎但深具破壞性的貿易保護主義政策。

由於自由資本流動和自由貿易，建立在浮動匯率陷阱的不安基礎上，因此國家企業與專業人士裡，會有更高比例的人關心匯率的變動。每個企業都需投入資源和人力，研究這個無法控制的重要問題。越來越多的人開始思考中央銀行、國家政府和貨幣流動的行為。這種精心設計的中央規劃以及隨之而來的經濟儀式，終究會妨礙經濟活動。

關於現代世界經濟最令人驚訝的事實之一，可能就是經濟生產活動與外匯市場規模的比較。根據國際結算銀行<sup>註 20</sup>估計，2016 年 4 月外匯市場規模為每天 5.1 兆美元，每年約為 1,860 兆美元。而根據世界銀行的估計，2016 年全球所有國家的國內生產總值合計只有大約 75 兆美元。這表示外匯市場規模大約是整個地球所有經濟生產的 25 倍<sup>註 21</sup>，請記住很重要的一點，外匯並不是一種生產的過程，這也就是為何一般 GDP 統計數據不會納入它的數據；因為將一種貨幣轉移到另一種貨幣並不會創造經濟價值；它只是為了交換不同國家的不同貨幣，所需付出的龐大代價。經濟學家 Hans-Hermann Hoppe 稱之為在國與國之間的「全球局部換貨交易系統」<sup>註 22</sup>，正在削弱全球貿易的獲利能力，並立下較高的交易成本限制，以試圖改善獲利結果。整個世界不僅浪費大量資本和勞動力試圖克服這些藩籬，各地企業與個人也經常因匯率波動的陷阱，造成經濟誤判而蒙受重大損失。

在自由的貨幣市場中，個人會選擇自己想要使用的貨幣，其結果就是他們會選擇「庫存流量比」較為可靠的貨幣。隨著需求和供應的變化，這類貨幣的波動最小，因此也會成為全球所渴望的交換媒介，讓一切經濟計算都可倚仗進行，成為跨越時間空間的共同計量單位。商品的可銷售性越高，就越適合這個角色。羅馬 aureus、拜占庭 solidus 或美元等，雖然都有缺點，但也都是在限定範圍下的好例子。

---

註 20 國際結算銀行（2016 年），中央銀行三年期調查，2016 年 4 月的外匯交易額。

註 21 更多相關訊息，請參閱 George Gilder 的「金錢醜聞：為何華爾街復甦，但經濟從來沒有復甦（*The Scandal of Money: Why Wall Street Recovers but the Economy Never Does*）」，華盛頓，D.C. Regnery 出版，2016 年。

註 22 Hans-Hermann Hoppe，「法幣為何可行？（How Is Fiat Money Possible?）」，奧地利經濟學評論，第 7 卷，第 2 期（1994 年）。

與此最接近的健全貨幣時代，是在國際黃金標準建立之後幾年裡的黃金，雖然如此，在當時的某些國家和社會裡，也仍在使用白銀或其他原始形式的貨幣。

現代生活裡的另一個驚人事實，就是 1900 年時的企業家是以任何國際貨幣價格進行計算，不必考慮任何匯率波動，也就是真的可以制定「全球性」的經濟計劃。而在一個世紀之後，相同的企業家若想制定跨國經濟計劃時，便會面臨一系列高度不穩定的匯率，讓他覺得自己好像走進了達利的超現實畫作裡。任何理智的分析師只要看到這堆爛攤子，應該都會得出結論，也就是最好將貨幣價值再次與黃金連動，來擺脫這種雜耍的行為。只要政府取消對貨幣政策控制的需求，解決不可能達成的三位一體，重新獲得自由的資本流動與自由貿易即可。如此便能立即創造穩定的經濟，並可釋放大量資金和資源，用來生產有價值的商品和服務，而不需猜測複雜的匯率波動。

然而不幸的是，負責目前貨幣體系的人比較希望繼續維持下去，因此他們傾向於找到管理貨幣的方法，並尋找更有創意的方式來詆毀與駁斥黃金標準。這點我們完全可以理解，因為這個工作讓政府可以用印刷機來獎勵這些負責的官僚。

浮動匯率與凱因斯主義意識形態的結合，為我們的世界帶來了全然的現代「貨幣戰爭」現象：由於凱因斯主義分析認為增加出口可以讓 GDP 增加，而 GDP 是經濟福祉的聖杯，因此在凱因斯主義者的心目中，促進出口的任何事情都是好事。由於貨幣貶值會使出口更便宜，任何面臨經濟遲緩的國家，都可透過將貨幣貶值與增加出口，來提高 GDP 和就業率。

這種世界觀非常不妥，因為降低貨幣價值並無法提高行業的實質競爭力。相反的，它只能為出口創造一次性的折扣，等於為外國人提供比本地人更便宜的價格，使當地人變窮而補貼了外國人。



它還會讓所有資產對外國人而言都變得更便宜，等於用折扣價格讓他們進入該國收購土地、資本和資源。在自由經濟秩序中，外國人購買本地資產並無問題，但在凱因斯主義經濟秩序中，外國人會積極獲得補貼，以折扣價來買遍整個國家。此外，我們也可從經濟史上看到，戰後最成功的經濟體如德國、日本和瑞士，隨著貨幣持續升值，出口量反而大幅增加。他們不需要經常貶值來讓出口成長；他們發展的是競爭優勢，讓產品獲得全球性的需求，結果反過來，跟貿易夥伴相比是自己的貨幣升值，也增加了國民的財富。而從他們那裡進口商品的國家，認為自己的國家可以透過簡單的貶值貨幣來增加出口，結果便會適得其反。因為他們只是在允許外國人以折扣價格來購買，因而摧毀了人民的財富。在戰後時期看到貨幣貶值最多的國家，同時也都是承受經濟停滯與衰退最多的國家，這點實非巧合。

貶值不僅無法讓國家通向繁榮，還有一個讓它無法運作的最簡單原因，那就是如果它起了作用，而且所有國家都試過這種做法，那麼各國貨幣都會貶值，就不會有哪個國家比其他國家更具優勢。這個原因可以讓我們了解全球經濟的現況，大多數政府都試圖以貶值貨幣來增加出口，也都抱怨對方在貨幣上的「不平等」操縱。事實上，每個國家都在使公民變得更窮，以增加出口並提高國內生產總值，也都會抱怨其他國家的相同行為。這種經濟上的無知，跟說這些話的虛偽政治家、經濟學家們恰好相互呼應。於是召開國際經濟峰會，各國領導人試圖透過談判來找出相互可接受的貨幣貶值程度，讓貨幣價值變成地緣政治的重要議題。

如果世界各國可以將全球的計價單位與價值衡量標準，建立在健全的全球貨幣體系基礎時，這些談判都是不需要的。

只要讓全球的生產者與消費者，可以準確評估成本和收益，將經濟利潤與政府政策隔開。亦即將貨幣供應問題從政府與經濟宣傳者手中釋放出來，健全貨幣將會讓每個人對社會有所貢獻，而不是藉由愚蠢的貨幣操縱來尋求致富。

## 7

# 健全貨幣與個人自由

---

「政府相信 .... 若必須在不受歡迎的稅收和非常受歡迎的支出之間做出選擇，那麼沒有別的出路，一切只能靠通貨膨脹，這也是為何我們會脫離黃金標準的原因。」

—*Ludwig von Mises*<sup>註 1</sup>

在健全的貨幣體制下，政府必須使用我們無法想像的方式進行運作：亦即他們必須在財政上「負責」（這點實在讓二十世紀政經新聞持續薰陶下的我們，難以習慣）。因為中央銀行不能增加貨幣供應以償還政府債務，政府預算也必須遵守每個健康經濟體所需負擔的財務責任規範（也就是貨幣民族主義想要廢除而國家教育試圖混淆的責任）。

---

註 1 Bettina Bien Greaves 「*Ludwig von Mises* 的貨幣與通貨膨脹：幾個講座合輯（*Ludwig von Mises on Money and Inflation: A Synthesis of Several Lectures*）」，第 32 頁。

對於活在現代的我們來說，歷經二十世紀無所不能的政府宣傳後，通常很難想像「個人自由和責任」可以取代政府威權的世界。然而在人類最偉大的進步和自由時期下的世界便是如此：政府被限制在保護國家邊界、私有財產和個人自由的範圍內，讓個人有極大程度的自由，自己決定選擇收益或負擔成本。所以接著我們要先仔細研究「貨幣供應」，是否真的需要由政府管理，然後再來談實際發生的後果。

## 政府應該管理貨幣供應嗎？

「政府必須管理貨幣供應」的想法，根本就是個現代騙局。對所有主流經濟學派和政黨來說，無疑都是種最初的「假設」，沒有任何現實證據的支持，而且每次管理貨幣供應的嘗試都會以經濟災難告終。貨幣供應管理是個「偽裝成解決方案」的問題；情感上的願望經常勝過了理性的堅持，因為這些政治宣傳裡的免費午餐，都會讓容易上當的選民願意買單。它的作用就像一種高度成癮性與破壞性的藥物，例如冰毒或糖：剛開始時又美又嗨，讓人擁有「無敵」的感覺，但只要藥效消退，其失望是毀滅性的，會讓受害者渴望更多藥物。這時便需做出艱難的抉擇：停止上癮的戒斷效果或者再注射一次，把結算日再往後延一天，然後承受更嚴重的長期傷害？

對於凱因斯主義和馬克思主義經濟學家，以及國家貨幣理論的其他支持者來說，錢指的就是「國家」所定的貨幣，因此國家決定做什麼，就會大量印錢來花在實現國家的目標上。經濟研究的目的當然也變成決定「如何最快、最大量的供應貨幣」以及「要達到什麼目標」。

但在民族國家發明之前，黃金已經被當成貨幣用了幾千年，這個事實本身就足以駁斥這種國家貨幣理論的說法。而且中央銀行目前都還持有

大量黃金儲備，也都在累積更多的黃金儲備，就可以證明即使沒有政府強制要求使用黃金，它也一直維持著貨幣性質。但無論國家貨幣理論的支持者，對於這些事實有什麼歷史方面的狡辯說法，他們的理論在過去十年裡，都已眼睜睜地被比特幣的持續成功與成長所淹沒。雖然沒有任何國家授權將比特幣當成貨幣，但比特幣因為可靠的銷售性，已經取得了貨幣的地位，所獲得的價值也已超越許多國家的貨幣<sup>註2</sup>。

目前各國政府認同的主流經濟思想學派有兩種：凱因斯主義者和貨幣主義者。雖然這兩種學派有著截然不同的操作方法與分析架構，也正進行著激烈的學術鬥爭，並互相指責對方不關心窮人、孩子、環境、不平等或其他流行詞彙等等，但他們都同意兩個毫無疑問的事實：首先，政府必須擴大貨幣供應量；其次，兩種學派都應該獲得更多的政府補助，以便持續研究真正重要的「大問題」，讓他們可以找到更有創意的方法來實現真理。

我們必須先了解這兩種思想流派的不同理論基礎，理解他們如何得出相同的錯誤結論。凱因斯是一位失敗的投資者和統計學家，也從沒學過經濟學，但因為他跟英國的統治階級的關係緊密，讓他在自己最有名的著作《就業、貨幣和利息通論》（*The General Theory of Employment, Money, and Interest*）裡，雖然寫的根本是令人尷尬的胡說八道，卻也能立刻被提升為「宏觀經濟學基本真理」的現況。而他的理論始於（毫無事實根據的）假設，也就是決定經濟狀況的最重要指標，便是整個社會的「總支出水平」。

---

註2 John Matonis，「比特幣消滅了『國家貨幣理論』（Bitcoin Obliterates “The State Theory of Money”）」，富比士雜誌（2013年4月2日）。參閱 <http://www.forbes.com/sites/jonmatonis/2013/04/03/bitcoin-obliterates-the-state-theory-of-money/#6b93e45f4b6d>。

當社會集體花費多的時候，這些支出會激勵生產者創造更多產品，並僱用更多工人，達到充分就業的平衡。如果支出增加太多，超出生產者的能力而無法跟上，便會導致通貨膨脹和整體物價上漲。另一方面，當社會支出增加太少時，生產者減少生產，解僱工人與失業增加，導致了經濟衰退。

因此凱因斯的經濟衰退是由「總支出水平的急劇下降」所造成，但他並不擅長掌握這些因果關係和邏輯解釋的概念，所以他從沒打算解釋為何支出水平會突然下降，反而只是創造另一個著名的愚蠢無意義言論，來省下解釋的麻煩，因為他竟然把突然下降歸咎於「動物精神（animal spirits）」疲乏。到目前為止，沒有人確切知道這些動物的精神是什麼，或為何它們會突然疲乏，但一切只說明了由國家資助的「家庭手工業」經濟學家，連嘗試解釋或找到相關實際數據的工作都沒做。這種精神上的解釋對於學術生涯來說非常有用，但對真正試圖了解商業週期的任何人來說，都沒有價值。因為坦白說，「大眾心理學」並不能代替資本理論<sup>註3</sup>。

由於不必找出經濟衰退的原因，所以凱因斯可以愉快地推銷他的解決方案。每當經濟衰退或失業率上升，原因就直接歸納成「總支出水平」下降，解決方案便是政府刺激支出，藉以增加產量，減少失業。而刺激總支出有三種方法：增加貨幣供應、增加政府支出或減少稅收。凱因斯主義者通常不贊成減稅，因為這是效率較低的作法，一般人通常也不會把被減掉的所有稅金都花掉，其中一部分的錢可能會被拿去儲蓄。而凱因斯絕不喜歡儲蓄，因為儲蓄就會減少支出，減少支出對經濟復甦來說，是最糟糕的一件事。

---

註3 在資本理論中，也沒有人可以取代奧地利資本理論，如同 Böhm-Bawerk、Mises、Hayek、Rothbard、Huerta de Soto、Salerno 等人所闡述。

所以政府的作用變成是透過增加消費或印更多鈔票，來提高社會整體的時間偏好。由於在經濟衰退期間很難加稅，因此「增加政府支出」就靠貨幣供應量的增加。這就是凱因斯主義的聖杯：只要在經濟上沒達到充分就業時，「增加貨幣供應」就能解決這個問題。大家也不必擔心通貨膨脹，因為凱因斯也「告訴（毫無根據的假設）」我們，通貨膨脹只會發生在支出過高的時候，而失業率過高就表示支出太低了。雖然增加貨幣供應量從長遠來看可能會有後果，但我們不必擔心長期後果，因為凱因斯又告訴我們：「到那個時候，大家都已經死了」<sup>註4</sup>。這也就是凱因斯最著名的防禦策略，那種高時間偏好下的任性不負責任聲明。

凱因斯主義對經濟的看法，當然與現實完全不同。如果凱因斯的通貨膨脹模型有任何道理的話，我們就可以推論不會有任何國家「同時」經歷高通貨膨脹與高失業率的情況。但實際上這已經發生了很多次，最明顯的例子就是 1970 年代的美國，儘管凱因斯主義經濟學家保證不會如此，儘管整個美國從尼克森總統到「自由市場」經濟學家 Milton Friedman 也都秉持這種認為「不可能發生」的態度，並且說「我們現在都是凱因斯主義者」。但為了消除失業，政府採取措施讓通貨膨脹增加，而隨著通貨膨脹的飆升，失業率卻是繼續上升，直接破滅了這種用前者換得後者的交易理論說法。在任何理智的社會中，凱因斯的思想都應該從經濟學教科書裡刪除，僅限使用在「學術喜劇」領域，但在政府對學術界緊密控制的社會裡，這些教科書將會繼續傳播更合理的凱因斯主義教條，以便讓政府印出

---

註 4 J. M. Keynes, 「貨幣改革法案 (*A Tract on Monetary Reform*)」(1923 年), 第 3 章, 第 80 頁。值得一提的是當代凱因斯主義者, 拒絕將這一引文解釋為凱因斯關注現在而犧牲了未來。相反地, 像 Simon Taylor 這樣的凱因斯主義者認為, 這代表凱因斯優先解決失業問題, 而非先擔心通貨膨脹的遠程威脅。可惜這種辯護只會使凱因斯的現代門徒與他一樣短視, 完全忽略了基本現實, 也就是因為通貨膨脹政策才會導致失業率大增。請參閱「『到那個時候, 大家都已經死了』的真正含義」, 可參閱 <http://www.simontaylorsblog.com/2013/05/05/the-true-meaning-of-in-the-long-run-we-are-all-dead/>。

更多的錢。如此便可在比喻上和實際上都有能力印錢，讓任何政府都能藉此增加權力，而所有政府也都在尋找這種能夠讓自己具有更大權力的理論說法。

在這個時代裡，政府認同的另一個經濟思想主要學派就是「貨幣主義學派」，其學派知識之父便是 Milton Friedman。這些貨幣主義者就像是凱因斯主義者的可憐被虐妻子：他們在那裡提供一個弱小、淡化的自由市場論證的「稻草人論證（曲解原意而為自己立論）」版本，創造一種思辯氣氛的幻覺，並且持續全面反駁，以防止好奇的知識分子認真思考自由市場的問題。跟凱因斯主義者相比，貨幣主義經濟學家實際上並不多，但因為這種彷彿對等的辯論，給了他們許多表達想法的空間。貨幣主義者在基本上跟凱因斯主義者一樣，認同凱因斯主義模型的基本假設，但他們利用一些精細複雜的數學謬論，解釋關於模型的一些例外結論，這些例外也讓他們敢建議政府在宏觀經濟裡略為減少作用，但也讓他們立刻被當成無情的邪惡資本主義敗類，因為他們不關心窮人。

貨幣主義者普遍「反對」凱因斯主義增加支出來降低失業率的努力（就是指從長遠看來，引發通貨膨脹可以降低失業率）。相反的，貨幣主義者更傾向於利用「減稅」來刺激經濟。因為他們認為自由市場在分配資源上，的確會比政府增加支出來得更好。雖然對於減稅與支出的爭論愈演愈烈，但現實情況是這兩項政策都會導致政府赤字增加，因而只能透過將債務貨幣化來籌集財源，因此實際上是在增加貨幣供應量。然而，貨幣主義者的思想核心是政府迫切需要防止貨幣供應崩潰與（或）物價下跌，他們認為這是所有經濟問題的根源。「物價下跌」或者說是貨幣主義者和凱因斯主義者所稱的「通貨緊縮」，將會造成人們進行儲蓄並減少開支，因而讓失業率上升，導致經濟衰退。所以貨幣主義者最擔心的，就是「通貨緊縮」會伴隨著銀行業資產負債表的崩潰，由於這種令人厭惡的因果關係，所以中央銀行必須盡一切可能，確保通貨緊縮不會發生。

對於為何貨幣主義者如此害怕通貨緊縮的典型反應，請參閱美聯儲前主席伯南克 2002 年發表的談話，題目為「通貨緊縮：確保『它』不會在這裡發生」<sup>註 5</sup>。

這兩種思想學派的貢獻總和，便是全世界大學的宏觀經濟學課程所達成的共識：中央銀行應該用可控制的速度來擴大貨幣供應，鼓勵人們花更多的錢，讓失業率保持降低。如果中央銀行緊縮貨幣供應，或者無法充分擴大貨幣供應量，就會出現通貨緊縮的漩渦，阻礙人們花錢，損害就業而導致經濟衰退<sup>註 6</sup>，這就是整場辯論的本質。然而多數主流經濟學家與教科書甚至沒有考慮「是否真的應該增加貨幣供應量」的問題，就先假設增加是已給定的條件，來討論中央銀行如何管理這種成長並決定其利率。目前普遍流行的凱因斯信條就是「消費與支出」的信條，以便滿足眼前的立即需求。透過不斷擴大貨幣供應量，央行的貨幣政策讓儲蓄和投資的吸引力降低，因而鼓勵人們增加消費、減少儲蓄和投資。這種做法的真正影響在於「炫耀性消費」的普遍現象，人們在生活上會購買超出本身需求的大量垃圾商品。當這種亂花錢的替代方案，碰到你的儲蓄會隨時間增加而貶值時，你可能也會想要在儲蓄失去價值之前，好好享受消費。財務決策會反映出人們的個性，在生活的各個層面也都會產生高度的時間偏好：貨幣貶值導致儲蓄減少、借貸增加，經濟生產、藝術和文化方面的短視近利，以及也許最具破壞性的便是土壤中的營養耗盡，導致食物裡的營養素不斷減少。

諷刺的是這兩種思想流派繼承了經濟學的經典傳統，也匯集了世界各地數百年的學術精華。

---

註 5 「州長伯南克在國家經濟學家俱樂部之前的談話」，華盛頓特區，2002 年 11 月 21 日，「通貨緊縮：確保『它』不會在這裡發生」。

註 6 詳見 Campbell McConnell、Stanley Brue 和 Sean Flynn，經濟學（紐約：McGraw-Hill 出版，2009 年），第 535 頁。



為了紀念第一次世界大戰前，黃金時代下奧地利的最後一代偉大經濟學家，現在通常將他們稱為「奧地利學派」。此學派借鑒了古典蘇格蘭、法國、西班牙、阿拉伯和古希臘經濟學家的作品，闡明他們對經濟學的理解。跟凱因斯主義與貨幣主義者對嚴謹數值分析和數學詭辯的僵滯有所不同，奧地利學派專注於以因果關係的方式建立對現象的理解，並從邏輯上推斷出真理的含義。

奧地利學派在貨幣理論上，認為貨幣是市場裡最具價值的商品以及最暢銷的資產，也就是持有者可以在最好的條件下，以最有利的方式出售的一種資產<sup>註7</sup>。可以保持價值的資產優於會失去價值的資產，那些想要選擇交換媒介的儲蓄者，便會傾向於隨著時間的推移而仍保持價值的資產，來作為儲蓄用的貨幣資產。透過交易網路的效應後，代表最後只會剩下一種或幾種資產，可以作為交換媒介之用。對於 Mises 來說，因為政府會被誘惑，想貶值儲蓄者投資所累積的財富，因此「政府無法控制」是貨幣穩健的必要條件。

如第 8 章所述，由於比特幣的總供給量已設置了「上限」，所以中本聰顯然沒有受到標準宏觀經濟學教科書的影響，而是更受到奧地利學派的影響。後者認為貨幣數量本身無關緊要，任何貨幣供應量都足以營運任何規模的經濟，因為貨幣單位可以無限拆分，它只是貨幣在實際商品與服務方面的購買力，而不應該是數量。正如 Ludwig von Mises 所說<sup>註8</sup>：

---

註 7 Carl Menger，「貨幣的起源（On the Origins of Money）」，1892 年。

註 8 Ludwig von Mises，「人類的行動（Human Action）」，1949 年，第 421 頁。

貨幣提供的服務，在於其購買的能力，沒有人會希望持有一定數量或一定重量的錢；而是希望他的錢具有一定數量的「購買力」。由於市場的運作傾向於確定貨幣在供需高點購買力的最終狀態，因為購買力一致，因此不可能會有過多或不足的貨幣。無論總金額大或小，每個個人和群體都能充分享受間接交換和使用貨幣所帶來的好處…即使改變貨幣供應，貨幣所提供的服務既不會增加也不會減損…整個經濟體中可用的貨幣數量一定足夠，以確保該貨幣能讓所有人做到想完成的事。

Murray Rothbard 與 Mises 持相同觀點<sup>註9</sup>：

一個貨幣穩定供應的世界，將類似於十八和十九世紀的大部分時期，其特點是工業革命的成功綻放，不僅資本投資與貨物供應增加，貨物價格與生產成本也都下降了。

根據奧地利的觀點，如果貨幣供應是固定的，那麼經濟成長將導致實際商品和服務的價格下降，因而可以讓人們在未來用他們的錢，購買越來越多的商品和服務。這樣的世界正如同凱因斯主義者所擔心的，確實會阻礙立即性的消費，也會鼓勵大家儲蓄和投資，以便在未來可能產生更多的消費。對於一個沉浸在「高時間偏好」的思想流派來說，我們可以理解凱因斯無法了解現在增加的儲蓄對目前消費的影響，會由過去增加的儲蓄所導致的支出增加而抵銷。因為一個不斷延遲消費的社會，將會比低儲蓄社會有更多的消費，由於低時間偏好的社會投資會更多，可以為社會成員創造更多的收入。即使他們的收入有極大比例用於儲蓄，低時間偏好的社會，最後也將擁有更高的消費水準，以及更大的資本存量。

---

註9 Murray Rothbard, 「奧地利貨幣理論」, 現代奧地利經濟學基礎 (1976年): 160 C184。

如果社會是之前說過「棉花糖實驗」中的一個小女孩，凱因斯主義經濟學就像在改變實驗，讓願意等待的小女孩只得到半個而不是兩個棉花糖來懲罰她，也讓自我控制和低時間偏好的概念適得其反。放縱直接的快樂比較像是經濟上的行為，最後將反映在文化和整個社會上。另一方面，奧地利學派透過傳播健全貨幣，瞭解大自然為人類所提供的現實考量判斷，若小女孩願意等待，就可獲得更多獎勵，因此從長遠來看她會更快樂，鼓勵她延遲滿足以增加未來的快樂。

當貨幣價值升值時，人們可能會在消費方面多加猶豫，以便替未來省下更多錢。而炫耀性消費、購物療癒的文化，讓你總是想把家裡的「廉價」塑膠垃圾，汰換成「更新、更華麗的」塑膠垃圾，這種消費方式如果換成是在一個貨幣會隨時間經過而升值的社會，應該無法佔有一席之地。因為這樣的世界會使人們產生較低的时间偏好，他們的貨幣決策會讓他們把行動方向定位於未來，讓他們越來越重視未來。因此，我們可以見到這樣的社會不僅讓人們有更多的儲蓄與投資，也會在道德、藝術與文化上迎向長遠的未來。

價值升值的貨幣可以激勵儲蓄，因為他們知道儲蓄在未來會有更多的購買力。因此它會鼓勵延遲消費，變成較低的时间偏好。從另一方面看，價值貶值的貨幣，會讓大家不斷尋找能夠超越通貨膨脹的回報，因此必然會帶來有風險的回報，導致風險項目的投資增加。當投資者的風險增加，損失也會增加。所以貨幣具有穩定價值的社會，通常會發展出低時間偏好，人們較可能學會儲蓄與思考未來；而具有高通貨膨脹和貨幣貶值的社會將產生高時間偏好，人們會忽視儲蓄的重要性，集中精力沈溺在即時享受中。

此外，貨幣升值的經濟體，比較可能投資具有「社會實際回報」的項目，而較不投資讓「貨幣升值」的項目，也就是預期會增加「社會資本存

量」的項目，較有機會獲得贊助。相較之下，貨幣貶值的經濟體會激勵個人投資於可以讓「貨幣貶值」提供正回報的項目，但不投資「社會實際回報」的項目。

這種打敗通貨膨脹但未增加「社會實際回報」的項目，會逐漸減少社會的資本存量，但對投資者來說仍然是理性的選擇，因為貨幣貶值會比減少資本的速度來得更快。這些投資就是 Ludwig von Mises 所說的「無利可圖」項目或投資，只有在通貨膨脹和人為低利率期間才有利可圖，一旦通貨膨脹率下降和利率上升，其無利可圖的事實便會浮現，成為繁榮與蕭條週期裡的「蕭條」時期。正如 Mises 所說：「繁榮會因投資稀有的生產要素而浪費，並且因為過度消費而減少可用的資本存量；也就是這種幸福是透過以後的貧困來支撐的」<sup>註 10</sup>。

這個觀點有助於解釋為何奧地利學派經濟學家，更傾向於把黃金當成貨幣，而凱因斯主流經濟學家，則支持政府發行可彈性調節的貨幣，以便可以在政府的要求下擴大。對凱因斯主義者來說，全世界的中央銀行都使用法定貨幣的這個事實，可以證明法定貨幣具有優越性。但在另一方面，對於奧地利學者而言，政府必須透過強制禁止黃金作為貨幣，並以法定貨幣支付的事實，也可以證明法定貨幣的劣勢，無法在自由市場取得成功。這也是商業週期會分為繁榮與蕭條的根本原因，雖然凱因斯主義經濟學家除了提出「動物精神」之外，沒有解釋過為何會發生經濟衰退，但奧地利學派經濟學家，已經發展出唯一解釋商業週期的連貫理論：奧地利經濟週期理論<sup>註 11</sup>。

---

註 10 Ludwig von Mises，「人類的行動（*Human Action*）」，1949 年，第 575 頁。

註 11 參見 Murray N. Rothbard，「經濟蕭條：原因和治療（*Economic Depressions: Their Cause and Cure*）」，Ludwig von Mises 研究所，2009 年。

## 不健全貨幣與長期戰爭

正如第 4 章討論的貨幣歷史所述，中央銀行控制的貨幣時代跟人類史上第一次世界大戰的開始，並非巧合。其中有三個根本原因，推動了不健全貨幣與戰爭之間的關係。

首先，不健全貨幣本身就是國與國間的貿易障礙，因為它在各國之間扭曲了貨幣價值，使貿易交流成為政治問題，在政府和人民之間形成了仇恨與敵意。其次，政府可以印鈔票，因此可以繼續掙扎，例如戰爭本來在貨幣耗盡時便應停止，現在則要等到完全摧毀貨幣的價值才會停下來。如果使用穩健的貨幣，政府的戰爭努力會被能徵得的稅賦所限制。如果不是健全貨幣，便只會受到貨幣摧毀前「可以印出多少鈔票」的限制，因此可以輕易地攫取人民的財富。第三，使用健全貨幣的個人，會產生較低的時間偏好，讓他們更會考慮合作而非衝突，如第 5 章所述。

個人可以交易的市場範圍越大、在生產中的專業化程度越高，能從貿易裡獲得的收益就越大。相同的勞動力，在 10 個人的原始經濟社會裡，將遠低於在 1000 或 1,000,000 人的較大市場所能消費的物質生活標準。生活在自由貿易社會中的現代個人，可以在高度專業化的工作裡每天工作幾個小時，再用賺來的錢，從全球任何一個生產者那裡，以最低的成本和最好的品質，購買她想要的商品。若要充分了解從你所能得到的貿易收益，請想像在一個「自給自足」的生活型態裡過日子的情況。對每個人來說，「基本生存」將成為一項非常艱鉅的任務，因為我們的大量時間會花在低效率與無成果的工作上，以得到基本的生存條件。

金錢是讓貿易發生作用的媒介，也是貿易得以擴展到個人關係小社群範圍以外的唯一工具。為了使價格機制發揮作用，便需與交易對象共同以健全貨幣形式計價。使用共同貨幣的區域越大，該區域內的貿易情況就會越容易也越能擴大。人民之間的貿易，便可透過讓彼此繁榮的交易獲利來創造和平共處。倘若區域內使用不同類型的不健全貨幣時，貿易就會變得更加複雜，因為價格會隨著貨幣價值不同而變化，使貿易的條件變得不可預測，並使規劃跨境經濟活動經常得到反效果。

由於傾向關注未來，因此具有「低時間偏好」的個體，會比「只重視當下」的個體，更不願意參與衝突。衝突在本質上具有破壞性，因此在多數情況下，聰明且願意計畫未來的人，都明白暴力衝突沒有贏家。因為比起一開始就「不參與」衝突而言，就算最後獲勝也可能損失更多。文明社會的運作前提是人們尊重彼此意志，如果有衝突，就會嘗試和平解決。如果找不到友好的解決方案，人們更可能是會分道揚鑣、相互錯開，而非繼續鼓譟或持續衝突。這點有助於解釋為何繁榮的文明社會，通常不會有太多的犯罪、暴力或衝突。

從國家層面來談，使用健全貨幣的國家更可能保持和平，或者對彼此之間的衝突有所限制，因為健全貨幣對政府軍事行動的籌資能力，構成了實際限制。在十九世紀的歐洲，想要互相爭鬥的國王，必須對轄下的人民徵稅，以便為軍隊提供資金。從長遠來看，這樣的戰略對防守的國王比對進攻的一方有利，因為防禦性的軍事行動會比進攻有更大優勢。防禦者在自己的土地戰鬥，靠近人民和補給線，把軍隊集中在防禦上的君主，會發現他的人民願意納稅以保護自己免受外國侵略者迫害。但征戰外國以滿足自己的君主，可能會面臨來自人民的怨恨，而且在別人的土地上作戰耗費更大。

這有助於解釋為何二十世紀是有史以來最致命的一個世紀。2005 年「聯合國人類發展報告」<sup>註 12</sup> 分析了過去五個世紀衝突所造成的死亡，發現二十世紀是最致命的時代。即使歐洲主要國家在黃金標準時代相互開戰，並以專業軍隊在戰場上作戰，戰事通常也無法持續太久。19 世紀歐洲的重大戰爭是 1870 年至 1871 年的普法戰爭，持續 9 個月，15 萬人陣亡，大約是第二次世界大戰中，平均每週的死亡統計數字（由二十世紀政府的不健全貨幣所資助）。由於黃金標準限制他們必須從稅收取得戰爭經費，因此歐洲各國政府必須在戰爭前籌措軍費，盡可能有效率的花錢整軍經武，並努力嘗試贏得決定性的勝仗。一旦其中一方戰事受挫，想靠加稅來重新武裝軍隊、扭轉局勢的話，就會變成一場後勤和經濟上的失敗，因此最好的做法是嘗試和平談判以減少損失。十九世紀最致命的戰爭是拿破崙戰爭，這是黃金標準在整個歐洲大陸正式實行之前的戰爭，也是法國大革命對通貨膨脹的愚蠢實驗後所進行的戰爭（見表 5<sup>註 13</sup>）。

表 5 過去五個世紀的衝突死亡人數

衝突持續期間的死亡人數			
期間	衝突死亡人數 (百萬)	該世紀中葉世界人口 (百萬)	衝突死亡人數占世界 人口比例(%)
16 世紀	1.6	493.3	0.32
17 世紀	6.1	579.1	1.05
18 世紀	7.0	757.4	0.92
19 世紀	19.4	1,172.9	1.65
20 世紀	109.7	2,519.5	4.35

註 12 「2005 年人類發展報告 (Human Development Report 2005)」，紐約：聯合國開發計劃署，2005 年。

註 13 資料來源：聯合國開發計劃署的「人類發展報告」(2005 年)。

在戰爭開始時，所有發達國家裡的大公司，都把戰爭當成一門生意來做，因此要靠戰爭延續下去才能繼續經營。他們的收入完全仰賴政府支出，並把公司命脈完全維繫在戰爭延續所需要的更多軍事開銷上。

美國的國防支出幾乎等於地球上其他國家的國防支出總和，這些大公司在美國政府持續參與的各項軍事行動上都擁有既得利益。因此這點比起任何策略、文化、意識形態或安全行動，都更能解釋為何美國介入世界上許多地區的衝突，而且這些衝突不會對一般美國人的生活產生任何影響。只有當貨幣不健全時，這些公司才能發展到如此巨大的規模，甚至可以影響新聞界、學術界和智庫來持續鼓勵參與更多戰爭。

## 有限政府與全能政府的比較

在 Jacques Barzun 的《從黎明到頹廢》一書裡提到的五個世紀西方文明史裡，認為第一次世界大戰的結束，是西方開始頹廢、衰敗和滅亡的關鍵轉折點。正是在這場戰爭之後，西方文明遇上了 Barzun 所說的「重大轉折」，即放任主義取代了自由主義，冒充者聲稱這只是強化而已，但實際結果卻完全相反<sup>註 14</sup>。

自由主義的成就原則是「最好的政府是管的最少的政府」；但現在對所有西方國家來說，政治智慧已經把這種自由（liberty），重新轉變為放任（liberality），這種轉變讓自由二字陷入混亂。

---

註 14 Jacques Barzun，「從黎明到頹廢（*From Dawn to Decadence*）」。



儘管自由主義認為政府的角色是允許個人生活在自由中，享受其行為所帶來的利益並承擔後果。但放任主義是一種更為激進的觀念，亦即政府的角色是在人民沉迷於自己的所有願望時，為發生的後果保護個人。因此在社會、經濟和政治上，政府的角色被轉變為實現願望的精靈，人們只需投票支持它想實現的目標即可。

法國歷史學家 Élie Halévy，將「暴政時代」定義為從 1914 年第一次世界大戰開始。當時世界主要大國轉向經濟和知識的「國有化」，把生產資料國有化，並轉向社會組織的工會主義和集團主義模式，同時也壓制與國家利益相衝突的意見，以及在他稱之為在「狂熱組織」裡散播的民族主義<sup>註 15</sup>。

這種古典的自由主義政府概念，只有在一個擁有穩健貨幣的世界才有可能，因為這種世界可以限制政府的威權與逾權。只要政府要向人民徵稅來維持運作，就必須把政府運作限制在人民可忍受的範圍。政府支出必須保持在稅收限度內，以維持預算平衡。亦即在穩健的貨幣社會裡，政府依賴人民的同意，才能為政府運作提供資金。政府每項新政策，都必須以預計的稅收或出售長期政府債券來支付，因此人民可以準確衡量此策略的真實成本，並可很方便的將政策獲得的好處進行比較。尋求合法國防與基礎設施項目經費的政府，使用計算稅收與債券收入時，人民很容易看到眼前政策是否有利。如果政府提高稅收來資助君主的奢侈生活，便會引起大規模民怨，危及統治的合法性，讓國家變得不穩定。政府的稅賦與徵收越重的話，人民就越可能抗拒納稅，收稅的成本也將大幅上升。無論透過選票或子彈，反對政府者便會用行動來取代政府。

---

註 15 Élie Halévy 和 May Wallas，「暴政時代（The Age of Tyrannies）」，經濟學刊，新系列，第 8 卷，第 29 期（1941 年 2 月）：第 77-93 頁。

健全貨幣可以讓政府行為具有一定的誠實和透明度，以便將統治限制在人民所希望和容忍的範圍內。它也會讓整個社會對行動的成本和收益進行公正的計算，任何組織、個人也將負擔維持生活所需的經濟責任：先生產，再消費。

從另一個角度看，不健全貨幣會讓政府把錢花在實現「大眾目標」上，收買忠誠度和歡迎度，且不必讓人民看到帳單。因為政府只是增加貨幣供應來資助自己制定的輕率計劃，這種計劃的真正成本，要到貨幣供應量太多的通貨膨脹導致物價上漲時，才由未來世代面對。被貶低的貨幣價值，也很容易歸咎給其他因素，政府通常會怪罪給外國人、銀行家、當地少數民族、前政府或甚至未來政府…等等的邪惡陰謀。不健全貨幣是政府手中的危險工具，尤其是現代民主政府必須面臨不斷的「連任」壓力，選民也比較不喜歡那些「提早規劃成本與收益」的候選人；而更喜歡「承諾免費午餐，將債務歸咎給前任政府或邪惡陰謀」之類的候選人。當人們試圖超越經濟規則，並藉由投票來獲得免費午餐時，民主就會變成一場妄想。當免費午餐的帳單來臨，也就是必須面對通貨膨脹和經濟衰退時，人們就會被這些惡棍候選人操縱，對那些代罪羔羊發脾氣。

不健全的貨幣，是大多數選民與那些不幸在大學研究過「現代宏觀經濟學」的人，共有的「當代妄想」核心：政府的行為沒有機會成本，因此政府可以用無所不能的魔杖，創造出自己想要的現實，無論是減少貧窮、強化道德、醫療保健、教育、基礎設施，改善其他國家的政治和經濟制度、或凌駕任何重要商品的供需規則等。多數現代人民都生活在這類妄想的夢境中，完全不必考量實際成本。因而實現這些目標所需要的只是「政治意願」、「強有力的領導」，以及「沒有發現貪腐」即可。不健全貨幣已從你頭腦裡思考公共事務的區塊裡，刪除了權衡與機會成本的概念。並會讓普通市民最後才發出驚呼之聲：原來你所想要的好東西，都不可能被你喜歡的政客或他的對手「憑空召喚」出來。這些日常生活裡的好東西，都

需要真實的人提供，他們必須一早起床，花幾天甚至幾年的時間，準備你所想要的東西，而不是把這些時間花來生產他們自己比較喜歡的其他商品。雖然不會有政治家靠「承認」這種現實來當選，但投票箱也無法逆轉這些人花掉的時間。無論何時，只要政府決定提供一些不能增加經濟產值的東西；都只是在證明對經濟生產進行集中規劃，將會產生可預期的不良後果<sup>註16</sup>。

對於暴君、專制政權與非法政府來說，不健全的貨幣是一種福音，讓他們可以增加貨幣供應，先資助自己的企業，避開實際的成本和收益，並讓人民在見證財富與購買力消失時，自行面對後果。歷史上充滿了實證，說明當政府擁有無端憑空產生貨幣的權力時，都會拒絕把這種特權還給人民。

每當我們提到歷史上最可怕的暴君，就會發現他們都經營著政府發行的貨幣制度，一再的膨脹貨幣以資助政府運作，這點絕非巧合。列寧、史達林、毛澤東、希特勒、羅瑞斯比爾（法）、波布（柬）、墨索里尼、金正日及其他許多惡名昭彰的政治慣犯，都有個很好的理由，因為他們都在政府發行不健全貨幣的時期統治，可以任意印刷鈔票來資助他們的集體屠殺、極權主義和狂妄自大。而在同樣的社會下，如果政府使用健全貨幣體系，且花錢之前必須先徵稅時，就不太可能會出現這類罪犯。這些政治怪物們，便沒有機會廢除健全貨幣，來資助他們的大規模謀殺。因為對健全貨幣的破壞，發生在更早之前，所用的是關於兒童、教育、工人解放和民族優越感的精彩故事。只要健全貨幣被摧毀，這些政治慣犯便很容易接管權力，增加不健全貨幣的供應量，然後控制所有的社會資源。

---

註 16 Murray Rothbard, 「社會主義的終結和經濟計算爭論 (The End of Socialism and the Calculation Debate Revisited)」, 奧地利經濟學評論, 第 5 卷, 第 2 期 (1991 年)。

不健全貨幣使政府的權力幾乎無所限制，給人民帶來巨大影響，被迫讓政治成為他們的生活中心，並將社會大部分的精力和資源重新定向到「誰來統治」與「如何統治」的零和遊戲。另一方面，健全貨幣會讓政府的形式影響有限。不論民主、共和或君主制，都會受到健全的貨幣約束，使大多數人在個人生活裡，享有較大的自由。

而在蘇維埃經濟或資本主義經濟裡，政府「運行」或「管理」經濟以實現經濟目標的概念，被認為是較好且必要的。因此這裡可以再回到凱因斯的觀點，了解他所提出「經濟制度的動機」，也是人類在過去幾十年中不得不與之對抗的概念。在他的一篇較少人知道的論文「自由放任的終結（*The End of Laissez-Faire*）」中，凱因斯提出他認為政府在社會中的作用，也表達了他對人們所期望的自由主義和個人主義的反對立場，但他也提出反對社會主義的理由：

十九世紀的國家社會主義源自 Jeremy Bentham、自由競爭等等，但在某些方面更清晰，某些方面則更為混亂，這點其實跟十九世紀個人主義背後的哲學意義相同。兩者都同樣把重點放在自由上，一邊是為了避免對現有自由的限制，一邊則是想破壞自然的或取得的壟斷情況，因此它們是對同一種知識氛圍的不同反應而已。

所以凱因斯對社會主義的疑問，在於其最終目標是「增加個人自由」。對於凱因斯來說，最終目標不該是關注「個人自由」這樣微不足道的問題，而應該是關注政府依需求來「控制經濟」的各個層面。他說明政府應扮演要角的三大主場域分別是：第一，「中央機構應刻意控制貨幣和信貸」，這點為現代中央銀行奠定了基礎。第二點與前者相關聯：凱因斯認為政府的作用應該是決定「整個社會整體儲蓄的規模，並將這些儲蓄以境外投資的形式，配合目前投資市場機構的判斷，在最具國家生產力的管道中分配儲蓄。我不認為這些問題應該像目前一樣，完全變成留給個人判斷或

私人獲利的機會。」最後，凱因斯相信，政府的角色是設計「一個無論人口多寡都合用的國家政策。無論是對大於、小於或等於目前的人口來說，都是最有利的政策。完成這項政策後，必須採取措施將其付諸實行。倘若整個社會必須優先關注原有成員，而非同時也關注少數的未來成員時，政策可能就較晚實行<sup>註17</sup>」。

換句話說，在凱因斯主義的「國家觀念」裡，所有廣泛被中央銀行家信奉的現代中央銀行學說，以及塑造全世界絕大多數經濟學教科書，都是來自某地某人，希望政府能夠指導人民生活上的兩個重要部分：第一，控制貨幣、信貸、儲蓄和投資決策，亦即資本配置的極權主義集中，以及自由個體企業的破壞，使個人從基本生存以上完全依賴政府。其次，控制人口數量和質量，也就是優生學。凱因斯與社會主義者不同的是，他並沒有尋求對個人做這種程度的控制，或者認為從長遠來看，是在增加人民的自由。凱因斯是在他認為合適的情況下，建立一個更加宏大的社會願景。雖然社會主義者至少會假裝為了利益而奴役他人，以便在未來解放他。凱因斯做的反而等於是希望政府為了自己的利益，將奴役人民作為最終目的。這可能有助於解釋為何 Murray Rothbard 說：「關於馬克思只有一件好事，至少他不是凱因斯主義者<sup>註18</sup>」。

雖然這樣的概念可能會吸引到象牙塔的理想主義者，他們會想像最後能帶來正面的結果，但事實上這樣會破壞經濟生產所需要的市場機制。而且在這種體系下，貨幣無法作為生產訊息系統，反而像是作為政府「效忠計畫」的工具。

---

註 17 J. M. 凱因斯，「自由放任的終結（The End of Laissez-Faire）」，勸說論文集（*Essays in Persuasion*）。第 272-295 頁。

註 18 Murray Rothbard，「與 Murray Rothbard 對談（A Conversation with Murray Rothbard）」，奧地利經濟通訊，第 11 卷，第 2 期（1990 年夏季）。

## 侵吞額

第3章解釋得到了貨幣角色的商品，如何激勵人們生產更多該商品。而容易大量生產的貨幣引來更多經濟資源，也吸引人類致力於生產該商品的時間。由於貨幣的目的不應該是為了本身價值，而應該是為了換取其他商品和服務，因此貨幣最重要的關鍵是它的購買力，而非它的絕對數量。任何增加貨幣供應的活動都不具社會效益，這也就是為何在自由市場中，任何承擔貨幣角色的商品，都會具有較可靠的高庫存流量比：亦即與目前現有總供應量相比，新貨幣供應量佔比極小。如此得以盡可能確保不會有太多的社會勞動力跟資本資源，被用來生產更多的貨幣，而是用來努力生產更有用的商品和服務，它們的絕對數量不該比貨幣本身來得更為重要。黃金成為全球領先的貨幣標準，因為其新產量始終只占現存供應量的一小部分，使開採黃金成為高度不確定和無利可圖的業務，因而會讓更多世界上的資本與勞動力，轉向非貨幣商品的生產。

對於凱因斯和弗里曼而言，擺脫黃金標準的主要吸引力之一，便是減少開採黃金，轉換為政府發行的紙幣，因為其生產成本遠低於黃金開採成本。但他們並未瞭解黃金的生產資源不易增加，其他貨幣商品的供應量反而很容易擴大這件事；他們也嚴重低估了社會的實際成本，亦即不健全貨幣的供應可以依政府的意願而擴大，而政府的意願很容易受到民主和特殊利益政治的影響。真正的成本不在於運行印刷機的直接成本，而是來自所有經濟活動的影響，因為生產資源很容易會去追逐新政府發行的貨幣，而不肯把資源花在從事經濟生產。

通貨膨脹信貸的建立，可以從經濟學家 John Kenneth Galbraith<sup>註 19</sup> 在他討論大蕭條時期的書裡，稱之為「侵吞額 (bezzle)」的泛社會範例來加以瞭解。隨著 1920 年代的信貸擴張飆升，企業資金氾濫，讓人很容易以各種方式貪污這些錢。但只要信用不斷擴增，資金被奪取的受害人，也可能會忘記這些罪行，因為受害者和強盜都認為自己很有錢，所以整個社會也都會產生「財富增加」的錯覺。中央銀行創造出來的信貸，為那些對社會無益的項目提供資金，並讓它們繼續在「非生產性」活動上消耗資源，導致繁榮假象無法長期持續。

如果是在健全貨幣體系中，任何存活下來的企業，都是透過提供社會價值而能為產品提供更高收益，並非因為企業投入生產的成本高低導致盈虧。一項業務能夠具有生產機會，多半是因為它把特定市場價格的投入「資源」，轉化為具有較高市場價格的「產出」。因此任何生產價值低於投入價值的公司都將關門，而該公司釋出的資源，便可被其他具有更高生產力的公司使用，經濟學家 Joseph Schumpeter 稱此為「創造性破壞」。如果沒有真正損失的風險，自由市場就沒有利潤可言，每個人都必須在這場遊戲做出投資決定：失敗是可能的，而且代價高昂。然而政府發行的不健全貨幣卻阻止了這種「自然淘汰」的過程，讓非生產性企業雖然不死，但也非真正活著，殭屍或吸血鬼般的「經濟等價物」，會利用存活的與較具生產性公司的資源，來生產價值低於生產商品所需資源的東西。如此便創造了一種新的社會階層，其存在是藉由與其他人不同的規則，他們的遊戲裡沒有真正的投資，而且產品也不必經過市場測試，完全不必擔心這種行為的後果。這類新的「階級制度」存在於政府資金所支持的每個經濟部門中。

---

註 19 John Kenneth Galbraith, 「1929 大崩潰 (*The Great Crash 1929*)」, 波士頓, Ma: Houghton Mifflin Harcourt 出版, 1997 年, 第 133 頁。

我們很難準確估計出在整個現代世界經濟裡，只追求政府印鈔，而不真正生產對社會有用商品和服務的情況，到底會占整體經濟活動的多少百分比。但我們可以看看哪些公司和部門在自由市場的考驗裡成功存活下來，哪些公司完全是靠政府的慷慨（無論是財政還是貨幣），才能生存下去。

更容易檢測「殭屍公司」的創造法則是財政支持。任何獲得政府直接支持的公司，或向公共部門出售產品而活著的絕大多數公司，都是成功的殭屍公司。如果這些公司對社會有用的話，一般人就會願意出錢購買這些公司的產品。但他們並無法靠民眾自願購買而生存，代表這些公司是一種社會的負擔，而不是社會的生產資產。

但危害更大的殭屍公司創造法，是透過低利信貸，而非政府直接購買產品。由於政府的法定貨幣已慢慢侵蝕社會的儲蓄能力，因此資本投資不再來自儲蓄者，而是來自政府創造出來的「債務」，也讓現有的資產減值。在健全貨幣的社會裡，一個人儲蓄的越多就越能累積資本，也就越能投資，這表示資本所有者比較容易變成時間偏好較低的人。但當資本是來自政府創造的信貸時，這些資本分配者便不再放眼未來，而是去找各種官僚機構成員攀關係套交情。

在健全貨幣下的自由市場，資本所有者選擇將資本分配給他們認為最有效的投資，並可以利用投資銀行來管理這種分配過程。這種過程會獎勵那些成功服務客戶的公司，並且找到它們的伯樂投資者，但也會懲罰判斷錯誤的公司。然而，在政府法定貨幣體系中，中央銀行實際上負責整個信貸的分配過程。它控制和監督分配資本的銀行，設定貸款資格標準，並試圖以數學方式來量化風險，忽略了現實世界風險的根本運作方式<sup>註 20</sup>。因

---

註 20 如果你因為某些因素還沒搞懂的話，應該閱讀塔雷伯（Nassim Nicholas Taleb）的著作：《隨機騙局、黑天鵝效應、反脆弱與不對稱陷阱》等。



此自由市場的檢驗停滯，因為中央銀行的信貸方向，可以完全否定獲利或損失的經濟現實。

在法定貨幣的世界裡，獲得中央銀行的貨幣源頭，比起服務客戶更重要。能夠獲得低利信貸營運的公司，將會比無法得到低利信貸的競爭對手，有更能持久營運的優勢。市場成功的標準越來越跟能否得到低利率資金有關，而跟能否為社會提供良好的服務則失去關聯。

這種簡單的現象解釋了現代經濟現實的大部分內容，例如出現許多大量賺錢，但對任何人都沒有任何價值的行業。政府機構就是最好的例子，他們因官僚無能所獲得的全球共同聲譽，只能解釋為這是一群完全脫離經濟現實，只有分配「侵吞額」資金功能的人。政府機構本應經歷「服務人民」的市場考驗難題，現在則是球員兼裁判的測試自己的所有失敗，然後結論是「需要更多的資金」。無論無能、疏忽或失敗的程度如何，政府機構和員工都很少會面臨真正的後果。即使政府機構存在的理由被消滅了，這些機構也會繼續運作，並為自己找出更多的職務與責任。例如黎巴嫩在國內火車退役、連軌道也廢棄幾十年後，仍然擁有一個火車管理局的情況<sup>註 21</sup>。

在全球化的世界裡，「侵吞額」不只存在於國家政府組織裡，也已發展成為國際性的政府組織。這種時間和體力的耗費，聞名全球，除了組織裡受僱的人以外，地球上的任何人都都不可能獲益。這些組織的所在地，遠離了資助他們的納稅人，面臨的審查甚至比國家政府組織更隨便，因此不僅運作不可靠，在預算、工作期限與工作責任上也更鬆散。

---

註 21 有關此主題的更多相關資訊，請參閱 James M. Buchanan 和 Gordon Tullock 的「同意的微積分：憲法民主的邏輯基礎（*The Calculus of Consent: Logical Foundations of Constitutional Democracy*）」（1962 年）。

學術界是另一個很好的例子，學生支付高額費用進入大學，尋求教授指導，但這些教授只花很少的時間和精力對學生進行教學與指導，而把大部分時間都集中在發佈一些令人難以理解的研究，以獲得政府補助並登上學術企業殿堂。在自由市場中，學者必須透過教學或寫出人們可以實際閱讀與受益的東西來貢獻價值。但一般人很少有機會閱讀學術論文，那是一種每個學科的一小群學者，彼此同意對方，執行「集體思維」的認同標準，然後把政治動機上的結論，偽裝成嚴謹的學術論文。

戰後時期最受歡迎和最具影響力的經濟學教科書，是由諾貝爾獎得獎者 Paul Samuelson 所撰寫。我們在第 4 章看到了 Samuelson 預測第二次世界大戰結束後，即將面臨世界歷史上最嚴重的經濟衰退，結果迎來的反而是美國歷史上最大的繁榮之一。接下來更誇張了：Samuelson 所寫的戰後最受歡迎的經濟學教科書《經濟學：介紹性分析》(*Economics: An Introductory Analysis*)，六十年來已銷售數百萬冊<sup>註 22</sup>。Levy 和 Peart<sup>註 23</sup>對不同版本的 Samuelson 教科書進行研究，發現他多次提出「蘇聯經濟模式」更有利於經濟成長，並在 1961 年的第四版，預測蘇聯經濟將在 1984 ~ 1997 年的某個時刻超越美國。而這些關於蘇聯超越美國的預測，隨著作者信心增加而繼續出現在第七版到 1980 年的第十一版中，只有對何時會超越的估計有所不同。

直到 1989 年第十三版出現在大學生書桌上時，蘇聯已開始解體，Samuelson 與當時的合著者 William Nordhaus 還在書上寫著：「蘇聯經濟

---

註 22 Mark Skousen，「保羅·薩繆爾森經濟學的堅持 (The Perseverance of Paul Samuelson's Economics)」，*經濟展望*期刊，第 11 卷，第 2 期 (1997 年)：第 137-152 頁。

註 23 David Levy 和 Sandra Peart，「蘇聯成長與美國教科書：來自內在的過去 (Soviet Growth and American Textbooks: An Endogenous Past)」，*經濟行為與組織雜誌*，第 78 卷，第 1-2 期 (2011 年 4 月)：第 110-125 頁。

證明了這一點，與許多懷疑論者早先認為的相反，社會主義指揮下的經濟體，可以發揮作用甚至茁壯成長…」<sup>註 24</sup>。

相同的觀點也不僅限於這本教科書，Levy 和 Peart 說明這種見解在第二受歡迎的 McConnell 經濟學教科書《原則，政策和問題》（*Economics: Principles, Policies and Problems*）以及其他幾本經濟學教科書裡都很常見。任何戰後在美國大學校園裡學習經濟學的學生（包含大多數世界各地的學生），都學到了蘇聯模式是組織經濟活動更有效的方式。即使在蘇聯崩潰和徹底失敗之後，同樣的大學還在繼續教授相同的教科書，新版本只是刪除了關於蘇聯成功的宏偉宣言而已，從不質疑書中其他經濟世界觀和方法論工具。這種明顯錯誤的教科書到底是如何繼續教下去的？為何凱因斯主義世界觀在過去七十年裡，雖然不斷被「現實」殘酷的拆穿（不管是第二次世界大戰後的繁榮、七十年代的停滯型通貨膨脹、蘇聯的崩潰解體等），都還能在大學裡繼續教下去？目前的凱因斯經濟學院院長 Paul Krugman，甚至還寫過「外星人入侵」對經濟的良好影響，因為它會迫使政府花錢和動員資源。<sup>註 25</sup>

在自由市場經濟體系中，應該不會有自重自愛的大學，會想教學生這些顯然是錯誤和荒謬的課程內容，而是會努力用最好的知識來幫助學生。但在一個完全被政府資金腐蝕的學術體系下，課程的決定與現實脫節，完全透過政府資助的政治性議程來決定。而政府通常熱愛凱因斯主義經濟學，就像他們在 1930 年代喜歡它的理由一樣：為獲得權力與金錢，提供更多的詭辯和理由。

---

註 24 Mark Skousen，「保羅·薩繆爾森經濟學的堅持（The Perseverance of Paul Samuelson's Economics）」，經濟展望期刊，第 11 卷，第 2 期（1997 年）：第 137-152 頁。

註 25 Paul Krugman，「長期停滯、煤礦、泡沫和勞倫斯·薩默斯（Secular Stagnation, Coalmines, Bubbles, and Larry Summers）」，紐約時報，2003 年 11 月 16 日。

在現代學術界的許多領域和學科裡，都可以繼續這類討論，因此相同的模式也一再重複出現：來自政府機構的資金，會由一群具有基本偏見的志同道合學者所壟斷，你無法「貢獻」改進現實世界生產效能的有用學問，來獲得這個學術體系下的工作或資金，而是必須幫腔推進「贊助者」的政治性議題。像這樣資金只有一個來源，就會消除自由市場「開放想法」的可能性。學術討論走向越來越吹毛求疵的細節，在這種像兄弟吵架裡的各方人士，最後總會同意要有「更多資金」來繼續研究這些重要的學術分歧。這些學術界的爭論幾乎與現實世界完全無關，除了那些為了升職必須撰寫論文的人以外，幾乎沒人讀過學術期刊的文章。但就算這種政府資助對任何人都沒有實質幫助，「侵吞額」事件依舊會不斷產生，因為幾乎沒有任何機制可用來減少這種學術資助。

在貨幣健全的社會裡，銀行業是非常重要且富有成效的工作，銀行家在經濟繁榮中扮演兩個非常關鍵的作用：保護作為存款的資產，以及調整配合「投資者與投資機會之間」的還款期和風險承受能力。工作做得好，銀行家便可分得自己的利潤，如果失敗就沒有獲利。因此只有成功的銀行家和銀行才能繼續工作，失敗者會被淘汰出局。在一個貨幣穩健的社會中，如果銀行失敗也不必擔心資金流通性的問題，因為所有銀行都持有投資者與存款人的存款，並有配合還款期限的投資項目。換句話說，流通性不佳與破產之間沒有區別，也沒有任何「系統性風險」讓任何銀行有「太大而不能倒閉」的藉口。因為失敗的銀行是其股東和貸款方的問題，並不會影響到社會上其他人。

然而在不健全貨幣下，可能就會出現「還款期限不匹配」的情形，僅有局部準備金的銀行只能算是金流的分支，因此銀行很容易出現資金流動危機或擠兌的情形。如果還款期限不匹配或只有局部準備金的銀行，遇到投資者和存款人同時要求提領存款的特殊情況時，便很容易出現流通性危機。要使這種「借方貸方到期日不匹配」得以安全的唯一方法，便是在銀

行即將破產的情況下，投資人隨時可以準備貸款給銀行<sup>註26</sup>。在貨幣健全的社會裡，中央銀行必須對未參與的所有人徵稅，以便貸款給銀行度過難關。但在貨幣不健全的社會中，中央銀行便會印出新的貨幣供應量，用它來支持銀行的流通性問題。因此，不健全貨幣會讓流通性與償付能力有所區隔：銀行本來應該根據其資產淨值來償付解決，但面臨資金流通性問題的緊急情況，當然無法在特定期間內履行其財務義務。由於存款人和貸方尋求將存款從銀行取出，因此便在缺乏流通性的情況下引發擠兌。更糟糕的是，一家銀行缺乏流通性，可能會導致與該銀行打交道的其他銀行也開始缺乏流通性，從而產生「系統性風險」問題。當然如果中央銀行在這種情況下，承諾提供資金流通性，便無需擔心流通性危機，也可避免銀行擠兌的情況，並使整體銀行系統安全。

如果沒有中央銀行使用彈性的貨幣供應來拯救這些銀行，局部準備金銀行或更普遍的到期日不匹配情況，可能會繼續下去而引發金融危機。但這種中央銀行會拯救一般銀行的做法，也為這些銀行帶來了「道德風險」的大問題。因為中央銀行會拯救他們以避免系統性危機，所以這些銀行現在可以承擔更大更多的風險。我們可以看到銀行業發展成一種既沒有風險，又能讓銀行家獲利的行業，然後將無回報的高風險性，轉嫁給一般人。

因此銀行業是目前看來唯一成長的行業，而且好像也不會面臨破產。由於經營銀行所涉及的系統性風險之故，銀行的任何失敗都被視為資金流動的系統性問題，因而會得到央行的支持做後盾。很少有其他私營企業可以享有如此高貴的特權，將「私營部門的最高盈利率」與「公共部門的保護」相結合。這種結合使銀行家的工作與公家機構的官僚具有「一樣的」

---

註 26 有關此聲明的正式模型，請參閱 D.W. Diamond 和 P. H. Dybvig，「銀行擠兌、存款保險和流通性（Bank Runs, Deposit Insurance, and Liquidity）」、政治經濟學雜誌，第 91 卷，第 3 期（1983 年）：第 401-419 頁。

創造性和生產力，但又比多數其他工作更能獲得價值。因此，隨著美國經濟變得越來越「金融化」，金融業也不斷成長。自 1999 年廢除「格拉斯－斯蒂格爾法案（Glass-Steagall Act）」以來，存款和投資銀行業務的分離限制已被取消，因此有 FDIC 存款擔保的存款銀行，現在也可以從事投資，FDIC 擔保可以保護他們免受投資損失的風險。而擁有損失擔保的投資者，等於有了可自由選擇且有效的「印鈔執照」。在有利可圖的投資下，他們不僅可以獲得所有收益，萬一損失的話還可以由社會共同買單。任何擁有這種擔保的人，都可以透過簡單的借款和投資來賺取大量資金。而這種「賺錢可得到利潤，損失則有人承擔」的情況，會造成更多資本和勞動力資源被吸引到金融業，因為它是世界上最接近免費午餐的東西。

經濟學家 Thomas Philippon<sup>註 27</sup>發表了在過去 150 年裡，金融部門的規模佔 GDP 百分比的研究結果。在第一次世界大戰之前幾年，此一比例不到 3%，之後急速上升，但在大蕭條時期下滑，而在第二次世界大戰結束後，幾乎以銳不可擋的方式成長。有趣的是，目前的大學生恰好印證了這一點，因為有很高的比例打算從事金融業，而非工程、醫學或其他更具生產力的行業。

原先隨著電信業的發展，應該可以預期會有更多的金融工作可以透過自動化、機械式的方法來完成，所以行業規模將會隨時間經過而變小。然而實際上金融業卻是繼續成長，不是因為任何基本需求，而是因為政府保護它免受損失，讓它得以茁壯成長。

在金融業中，「侵吞額」的情況可能最為明顯，但也不止發生在金融業裡。規模較大的公司比起規模小的公司，長期來說會較有競爭優勢。原先在

---

註 27 Thomas Philippon 和 Ariell Reshef。「現代金融發展的國際視角（An International Look at the Growth of Modern Finance）」，經濟展望期刊，第 27 卷，第 2 期（2013 年）：第 73-96 頁。

資本投資由儲蓄資助的社會裡，資本是由具有較低時間偏好的人所擁有，並且會根據他們對市場成功可能性的評估進行資本分配，判斷正確時得到獎勵，錯誤時則承擔損失。但由於貨幣不健全，因此資本儲蓄被摧毀，資本改成來自銀行信貸的膨脹，其分配是由中央銀行及其他銀行成員所決定。這些分配並非來自具有最低時間偏好、會做最佳市場預測也會做最謹慎決定的社會成員。反而改成來自政府官僚的決定，而他們的動機是盡可能地放貸，而非正確的放貸，因為即使判斷錯誤，他們也會受到明顯保護。

集中規劃的信貸分配與任何類型的中央計劃一樣，它讓官僚們勾選檢查項目、填寫文件，確保滿足老闆的要求，而失去銀行工作的基本目的。銀行家的洞察力和審查投資價值的努力，變成勾滿央行貸款需求的小方框。而確保集中信貸的一個主要優勢是規模，貸款數目較大的貸款人，在比較上似乎風險較小。因為公司越大，其成功的獲利模式就越可預測，如果失敗的話其能提供的抵押品也越大，讓銀行官員根據央行標準貸款時的安全感陡然提升。雖然許多行業可以從規模經濟中受益，但集中信貸則突出了以「規模」超越自由市場的超級優勢。任何可以向銀行借到更多資金但卻不知該怎麼辦的行業，都是很好的範例，因為這種情況不可能發生在以「儲蓄融資」的健全貨幣世界裡。

公司規模越大，越容易獲得低利貸款，因此跟小型獨立生產商相比具有更大優勢。若是在一個貸款來自「儲蓄」的社會中，一間小型的家庭式餐廳與一家快餐業巨頭，會站在平等的基礎上，競爭同樣的客戶與融資：客戶和投資者可以在兩個行業之間自由選擇分配的資金。大型快餐業的「規模經濟」優點，會被拿來跟小餐館廚師顧客間的「個人關注和客戶關係」相互較量，然後透過市場測試來決定優劣。但在中央銀行分配信貸的世界裡，較大的公司可以較低利率獲得資金，較小的競爭對手則無法獲

得<sup>註 28</sup>。這點也有助於解釋為何大型食品生產商，會在全球如此廣泛分佈的情況，因為較低的貸款利率讓他們可以獲得更高的利潤。除了中央銀行為大規模生產者所提供的巨大利益外，如此平淡無奇、大規模生產「垃圾食品」的勝利，真的令人難以理解。

在一個幾乎所有公司都透過中央銀行信貸擴張融資的世界中，由於注入了「侵吞額」類固醇，因此沒有簡單的方法可以辨別哪些行業是真正的成長，不過有些掩飾不了的徵兆可以用來判斷，例如任何會「抱怨他們的混蛋老闆」的行業，可能都是侵吞額事業的一部分。因為老闆可能真的擔當得起混蛋的說法，並活在侵吞額的虛假經濟現實中。一家為社會提供「較高價值服務」的高效率公司，其成功取決於客戶的滿意度；工人因為完成自己的重要任務而獲得獎勵，那些對工人不好的老闆，要不就是讓工人跑到競爭對手處，要不就是很快毀了自己的業務。

而在一家不為社會服務的非生產性企業中，只靠官僚主義的慷慨而生存，沒有任何有意義的標準可以獎勵或懲罰工人。由於如此慷慨的定期薪水且缺乏實際的生產，讓「侵吞額」從外表上看起來真的很誘人。如果說經濟學教了我們什麼重要的課程，應該就是「天底下沒有白吃的午餐」這件事。對這些毫無生產能力的人員分配資金，將會吸引許多想要從事這

---

註 28 信貸發行的集中化可被視為政府干預「寇斯定理（Coase's Law）」的運作，這是寇斯在其論文「公司的本質（The Nature of the Firm）」，經濟學刊，第 4 卷，第 16 期（1937 年），第 386-405 頁中所描述。根據寇斯的說法，公司存在的原因是個人承包任務的成本可能更高，因為涉及交易成本，例如搜尋資訊、議價、訂合約和執行的成本太高。因此只要公司能夠從內部開展的工作活動中獲益，並超過成本更高的外部承包時，該公司就會成長。而在貨幣貶值和中央分配信貸的世界裡，「完成融資」是規模成長的主要成本優勢，大公司擁有更多的資本貨物和抵押品，因此可以降低銀行的貸款條件，因此企業的成長動機，便不會專注於消費者的喜好上。反過來看，在資本自由市場中，企業必須更為依賴營收存活，並在自由市場上獲得信貸，必須以最有利、最適合消費者喜好的規模從事生產。



類工作的人，因此使得「及時且有尊嚴的完成工作」的成本提高，因為不論招聘、解僱、晉升和懲罰，都是由一層一層的官僚體系自行決定。如果沒有任何工作對公司有價值，每個員工便都可有可無，因而任何人維持工作的方法，就是協助證明他自己的上一層長官是有價值的，因此這些公司的工作變成了「辦公室政治」的全職遊戲。這種工作只會吸引那些喜歡掌握權力的淺薄物質主義者，為了薪水而多年忍受虐待的人，自己也希望能夠對其他人施加這種虐待。難怪從事這些工作的人經常沮喪，需要持續的藥物和心理治療來維持身體運作的基本功能。這種辦公室政治環境在人們身上所造成的精神破壞，並不值得花費「侵吞額」裡的錢。不過雖然這些組織不必承擔真正的責任，但毫無生產力的另一面便是新當選的官員上任後，很可能在幾週內就讓他們失去工作。所以對這些組織裡工作的人來說，是個更為悲慘的命運，因為他們通常沒有任何可以轉移到其他工作跑道的有用技能。

唯一可以解決這些悲慘命運的方法就是健全貨幣，因為它可以改變那些在「勾選方框」和「虐待狂老闆」下辛苦工作者的觀念，使「市場規則」成為任何人收入的唯一仲裁者。如果你發現自己在這類行業裡辛苦工作，工作壓力完全取決於老闆開心與否，而不是生產有價值的東西。你對這個現實不滿，也因為知道這個世界不該如此而感到寬慰或害怕，別擔心，你的工作不會永遠持續下去，因為政府的印刷機無法永遠運作下去。所以請繼續閱讀本書，因為健全貨幣的好處，可以為你帶來「擁有全新機會」的世界。

## 8

## 數位貨幣

---

從 1950 年代發明的第一台完全可編寫程式電腦開始，全球電信革命已越來越進入人類生活的物質層面，並為目前為止的各種古老問題，提供了工程技術上的解決方案。雖然銀行和新創公司使用電腦和網路技術來進行支付與保存交易記錄，但這些成功的創新並未提供新的貨幣形式，那些試圖提供新貨幣形式的創新都失敗了。而比特幣代表了貨幣問題上的第一個「真正的」數位解決方案，我們在比特幣上找到「可銷售性、穩健性和主權」等問題的潛在解決方案。比特幣在過去 9 年裡幾乎完勝，如果在接下來的 90 年裡繼續這樣運作，它將成為貨幣問題上，一個令人信服的解決方案，為個人提供抵抗意外通貨膨脹的貨幣主權，並可跨越空間、規模和時間而具有高度可銷售性。如果比特幣繼續這樣運作下去，那些以前被人類用來當作金錢的技術，例如貝殼、鹽、牛、貴金屬與政府紙鈔等，看起來就會像在我們的世界裡出現奇怪的時空錯亂，就像現代電腦旁邊擺著古代算盤一樣。

我們可以看到冶金技術引入後，以比串珠、貝殼和其他文物更好的方式，解決了貨幣形式的問題；而普通硬幣的出現，也讓金幣和銀幣比起不規則金屬塊，更適合作為優質的貨幣形式。我們也進一步看到以黃金支持的銀行，讓黃金作為全球貨幣標準的主導地位，並造成白銀的非貨幣化。從集中黃金的必要性來看，有黃金支持的政府貨幣會以更大的規模而暢銷，不過隨之而來的政府擴大貨幣供應和強制掌控，終於破壞了貨幣的穩健性和主權性。這一路走來的技術進步和現實情況，都塑造了人們所採用的貨幣標準，也對經濟和社會的影響相當大。選擇健全貨幣標準的團體與個人，例如凱撒大帝時代下的羅馬人、君士坦丁領導下的拜占庭人或黃金標準下的歐洲人，都獲益匪淺。而那些有著不健全貨幣或技術落後貨幣的人，例如奧基夫抵達時的雅浦島人，使用琉璃串珠的西非人，或十九世紀白銀標準下的中國人，均付出了沉重的代價。

比特幣代表一種對於貨幣問題的「新技術」解決方案，誕生自數位時代，利用了過去幾十年研發的幾項技術創新，並在多次嘗試生產數位貨幣的基礎上，提供了在它被發明之前，大家幾乎無法想像的能力。為方便理解個中原因，我們會將重點關注在比特幣的貨幣特性，以及它成立以來在網路上的經濟表現。如同討論黃金標準的書，不會討論黃金的化學性質一樣，本章也不會太仔細研究比特幣網路運作的技術細節，而是著重於比特幣的貨幣屬性。

## 比特幣作為數位現金

要理解數位現金技術的重要性，最好先觀察一下這個世界在比特幣發明之前，所使用兩種不同的「非重疊」支付類別：

1. 現金支付：由雙方親自進行。這類付款具有即時和完成的便利性，且不需要交易任一方以外的信任。執行付款沒有延遲，任何第三方都無法有效干預以停止這類付款。主要的缺點在於雙方必須實際存在同一時間地點，而隨著電信業的蓬勃發展，這種缺點也越來越明顯，因為大家希望彼此不必在附近就能交易。
2. 中介支付：需要有受信任的第三方才能進行。這類付款包括支票、信用卡、記帳卡、銀行轉帳，匯款服務以及較新的發明例如 PayPal 等。根據定義，中介支付便是需要有幫交易雙方處理匯款的「第三方」。其主要優點是允許付款雙方不必存在於同一時間地點，付款人付款時身上也不一定要有錢，而主要缺點是執行交易時所需的信任，也就是第三方必須妥協於可能發生的風險，以及付款完成到收款人可以花這筆錢之間，所需花費的成本和時間。

這兩種形式的支付都有其優點和缺點，大多數人在一般經濟交易裡，也會求助於兩種支付的結合。在比特幣發明之前，中介支付包括（但不限於）所有形式的數位支付。自電腦誕生以來，數位內容的本質便是它們並不稀有，可以無限制的複製，因此不可能用它們作為貨幣，因為傳送它們就是在進行複製。任何形式的電子支付都必須透過中間人才能進行，原因是擔心「重複付款」的危險：也就是當我們無法保證付款人對他的資金誠實，確保不會多次使用同一筆錢，所以必須有一個受信任的第三方監督著帳戶，來驗證執行付款的完整性。亦即「現金交易」僅限於直接聯繫的物理範圍，而所有「數位支付」，都必須經由第三方監督。

在經過許多程式人員多年的創新試驗和錯誤，並且依靠大量的技術，讓比特幣成為了第一個不必依賴可靠第三方監督，便能進行數位支付的技術解決方案。作為第一個可驗證的稀缺數位物件，比特幣可說是「數位現金」的第一個實例。

透過可信賴第三方進行交易有幾項缺點，因而使數位現金成為許多人追求的更佳主張。「第三方」本質上就是一個外加的安全弱點<sup>註1</sup>——在交易中牽涉到額外的一方，本來就會增加風險，因為它幫「偷竊或技術故障」開啟了新的可能性。此外，透過中間人支付，會使在野政黨容易受到執政當局的監視與限制。換句話說，訴諸任何形式的數位支付時，沒有其他選擇只能信任第三方，而政治當局卻可對該第三方進行管理，並依政治當局的說法，在安全、恐怖主義或洗錢藉口下，遇上停止支付的風險。更糟糕的是，中介支付還經常涉及到詐欺的風險，也會增加交易成本，並延長最後的結算與付款時間。

換句話說，中介支付奪走了擁有者將貨幣作為交易媒介的大部分控制能力，包括高流通性與可隨時出售的特性。而貨幣在歷史上延續最久的重要特徵便是「可交換性」（任何單位的貨幣可以兌換成其他單位）與「流通性」（貨幣所有者用市價快速賣出的能力）。人們選擇可交換和流通的貨幣，因為他們想要控制自己錢的主權，錢的主權便包括花這筆錢需要的所有許可；而其他人也想持有它的願望，也強化了這筆錢的控制能力。

雖然中介支付損害了貨幣的某些理想特性，不過實體現金交易並沒有這些缺點。但由於現代電信的進步，遠距進行的貿易與就業情況也越來越多，實體現金交易變得不切實際。數位支付的風潮正在減少人們對自己現

---

註1 見 Nick Szabo，2001 年，「信任第三方便是安全漏洞所在（*Trusted Third Parties Are Security Holes*）」，你可在 [nakamotoinstitute.org](http://nakamotoinstitute.org) 上取得。

金所擁有的主權，讓他們轉向各處興起的第三方支付，而且人們也只能信任，別無選擇。此外，本來沒人可以自己生產黃金的時代，也變成由中央銀行控制的法幣匯率，當然也會削弱人們對自己財富的控制權。當央行擴大貨幣供應量為政府運作提供資金時，便會讓人民在貨幣價值緩慢下降時求助無門。若沒有對政府發行貨幣進行管制，累積資本和儲蓄財富就會變得越來越不切實際。

中本聰（Satoshi Nakamoto）創造比特幣的動機便是想要有一種「純粹的點對點電子現金形式」，且不需信任的第三方對交易進行認證，其供應也不會被任何其他方所改變。換句話說，比特幣將實體現金（不需中介、具有交易終結性）的理想特徵，帶到了數位領域，並將它們與貨幣政策鐵律相結合，也就是這種貨幣「不能被操縱」，或以意料之外的「通貨膨脹」方式，並使持有人以外的外部人士受益。中本聰透過利用一些重要但尚未被廣泛理解的技術，成功實現了這個目標：分散式點對點網路，無單點故障、使用散列、套用數位簽名與工作量證明<sup>註2</sup>。

中本聰在非常周全嚴格證明與驗證的基礎上，建立了比特幣，消除了對第三方信任的需求。我們可以持平的說，比特幣的核心運作特徵便是「驗證」，只有這樣比特幣才能完全消除對信任的需求<sup>註3</sup>。每個交易都必須由網路上的每個成員記錄下來，以便他們共享一個相同的餘額和交易分類帳。每當網路成員將一筆金額轉移給另一個成員時，所有網路成員都可以驗證發件人是否有足夠的餘額，且節點會相互競爭，成為第一個每隔十分鐘使用新的交易區塊更新分類帳的人。節點要將一塊交易提交給分類

---

註2 本章附錄中提供了前三種技術的簡要說明，而本章和第10章也會詳細討論工作量證明。

註3 Konrad Graf，「關於比特幣的起源：貨幣演化的階段（On the Origins of Bitcoin: Stages of Monetary Evolution）」，2013年，參閱 [www.konradsgraf.com](http://www.konradsgraf.com)。

帳，必須擴張其處理能力來解決高難度的複雜數學問題，但得到的正確解決方案卻很容易驗證。

這就是工作量證明（PoW，proof-of-work）系統，只有正確的解決方案，才能讓該區塊被所有網路成員認同與驗證。雖然這些數學問題與比特幣交易無關，但它們對於系統的操作是不可或缺的，因為它們會強迫驗證節點而消耗大量處理能力，如果包含了假交易就會浪費掉處理能力。一旦節點正確地解出了工作量證明並宣布交易，網路上的其他節點便會投票支持其有效性，一旦多數人投票批准該區塊，節點就會將交易加到新區塊，修改前一區塊，並解決此新工作量證明。最重要的是，這些向網路提交有效交易區塊的節點，還會收到**區塊獎勵**，包括添加到供應中的全新比特幣，以及所有交易人員支付的交易費用。

這個過程被稱為「挖礦」，類似於貴金屬的開採，也是解決工作量證明的節點被稱為「礦工」的原因。區塊獎勵可以彌補礦工為工作量證明所投入的資源。在現代的中央銀行中，創造出來的新貨幣通常會用在融資貸款和政府支出，而在比特幣中，新貨幣只用於那些花費資源努力更新分類帳的人。中本聰設定比特幣大約每十分鐘產生一個新區塊，在比特幣操作的前四年裡，每個區塊包含 50 個比特幣的獎勵，之後減半為 25 個，並且每四年進一步減半。

比特幣的建立數量是預先設計好的，無論花多少努力和精神在工作量證明上，都無法改變增加的速度。這是透過一種稱為「難度調整」的過程來實現，它可能是比特幣設計裡最巧妙的部分。隨著越來越多的人選擇持有比特幣，提升了比特幣的市場價值，使得開採新比特幣更有利可圖，也就會讓更多礦工花更多資源來解決工作量證明問題。更多的礦工也就意味著更多的處理能力，因此也可更快產生工作量證明的解決方案，而提高新比特幣的發行量。但隨著處理能力的提高，比特幣也會跟著將解開挖礦獎勵數學問題的難度提高，以確保區塊繼續以大約十分鐘左右產生。

「難度調整」是獲得健全貨幣最可靠的技術，也可限制庫存流量比率的上升，如此才能讓比特幣與其他貨幣有根本上的不同。因為任何貨幣價值上升之後，便會導致更多的資源專門用於該貨幣的生產，增加該貨幣的供應量。而隨著比特幣的價值上升，用更多資源來努力生產比特幣，並不會立即產生更多的比特幣。相反的，它只會增加向比特幣網路提交有效交易所需的處理能力，這點反而會使網路更安全，更難被危害。所以比特幣是有史以來發明過最「硬」的錢（最健全的貨幣）：價值的成長不會增加其供應量；反而只會讓交易網路更安全，不受攻擊。

就其他的貨幣而言，隨著價值上升，有能力生產該貨幣的人，便會開始進行大量生產。無論是雅浦島石幣、貝殼、白銀、黃金、銅或政府法幣等，每個人都有想要生產更多貨幣的動機。為了貨幣價格上漲而想產生新貨幣的難度越高，該貨幣就越可能被廣泛接受和使用，社會也會越繁榮，因為這意味著個人在創造財富方面的努力，將轉向服務彼此而非賺錢。這是一項對社會「沒有」價值附加的活動，因為不論有多少貨幣供應量，都已足夠經營任何經濟體。黃金成為每個文明社會的主要資金，正是因為它是最難生產的，但比特幣的難度調整使其更難生產。黃金價格的大幅上漲從長遠看，依舊會導致產量增加，但無論比特幣的價格上漲多少，其供應量都維持不變，而且還會增加交易網路的安全性。

比特幣的安全性，在於解決將交易提交到分類帳所需的工作量證明的成本，與驗證其有效性所需成本，兩者之間的「不對稱性」。它需要不斷增加的電力與處理能力來記錄交易，但驗證交易有效性的成本接近於零，而且無論比特幣成長多少都將維持這種關聯性。若有人試圖向比特幣分類帳提交欺詐交易，只會造成解決工作量證明上的資源浪費，觀察節點幾乎不耗費成本便退回解決方案，並扣留該提交礦工的區塊獎勵。



隨時間推移，變更記錄越來越困難，因為所需的能量大於已經消耗的能量，而能量的耗費也只會隨著時間成長。這種高度複雜的演變過程，已經發展到需要大量的處理能力與電力，但卻能夠協助產生無可爭議的所有權和交易分類帳，不必依賴任何單一第三方的可信度，因此比特幣可說是建立在 100% 驗證和 0% 信任的基礎上<sup>註 4</sup>。

比特幣的共享分類帳可以比作第 2 章討論到雅浦島的 Rai 石，因為這筆錢並不會用於實體交易。在雅浦島民會面時，宣布將石頭的所有權從一個人轉移到另一個人，整個城鎮也都會知道誰擁有哪塊石頭。比特幣網路中的成員會向所有網路成員廣播這筆交易，並且會驗證傳送者是否具有交易所需的額度，然後將收取方記錄下來。在數位貨幣存在的範圍內，它們只是分類帳上的條目，並且以驗證過的交易，把分類帳上的貨幣所有權，從發送者改到接收者上。貨幣的所有權透過公開位址而非持有者名稱來分配，然後透過取得所有權的私鑰，來保護該址所擁有的貨幣，私鑰則是類似於密碼的字串<sup>註 5</sup>。

雖然 Rai 石頭的物理重量使得它們不太具有可分割性，但比特幣並沒有這樣的問題。比特幣的供應量最多為 21,000,000 個比特幣，每個比特幣可分割為 100,000,000 個「聰 (satoshis)」，使其在各種規模上都具有高度的可銷售性。雖然雅浦島石幣只有在人口較少且彼此認識的小島上，

---

註 4 我不打算把這本書和讀者拖到形而上學的問題裡，但對我來說，比特幣的交易總帳，可能只是世界上唯一的客觀事實。你可以爭辯（正如許多哲學家所做的那樣），每一個事實都是主觀的，它的真實性是基於陳述或聽到它的人，但是比特幣的交易總帳是透過將電力和處理能力轉化為真理，而不必依存於任何人的言語。

註 5 擁有比特幣的唯一方法是控制私鑰。如果有人設法取得你的私鑰，他們就會擁有你的比特幣。竊取私鑰就像盜竊實體美元或黃金一樣；它是最終端且不可逆轉的，也沒有管理當局可以讓你打電話來撤銷盜竊行為。這是比特幣作為貨幣不可避免的一部分，也是想投資比特幣的人，在將任何一筆錢投入比特幣之前，必須充分理解的重點。保護私鑰不是一項簡單的任務，而無法保護私鑰則非常危險。

進行一些島上的交易才比較適用，但比特幣在跨越空間的特性上，具有更優越的可銷售性，因為全球任何人都可以透過網際網路，連上這些數位化的分類帳。

維持比特幣個別節點誠實的原因，是因為如果他們不誠實，會立刻被發現，讓不誠實的效果就像沒做事一樣，卻還花費了更高的成本。整體而言，能夠讓大家誠實的原因，在於如果他們成功破壞交易分類帳的完整性，比特幣的整體價值主張便會被破壞，比特幣的貨幣價值也將崩潰為零。因此共謀串通不光是成本很高，破壞本身還會導致戰利品變得毫無價值。換句話說，比特幣依賴於經濟上的激勵，使得詐欺耗費的成本遠高於獎勵。

沒有任何單一實體可以依賴於維護分類帳而存在，而未經多數網路成員同意的話，任何個人也都不能改變其中的記錄。決定交易有效性的不是單一權威者所說的話，而是在網路上各節點所運行軟體的共同決定。

比特幣用在記錄交易的 Merkle 樹狀數據架構的發明者 Ralph Merkle，有一套描述比特幣的獨特說法：

比特幣是新生活形式的第一個範例，它在網際網路上生活和呼吸。它的存在是因為它付錢讓人們幫他維生，它的存在是因為它執行一項很有用的服務，讓人們願意付出代價來執行。它的存在是因為任何地方的任何人，都可以執行其程式碼的拷貝版本，它的存在是因為所有正在運行的比特幣軟體，都不斷的相互交談。它的存在是因為如果任何一個拷貝版本被破壞，便會被迅速丟棄而不必大驚小怪，它的存在是因為它完全透明：任何人都可以看到它的程式碼並確切地看到它的作用。

它無法改變、無法與之爭論，不能被篡改、也不會被破壞，它無法停止、甚至不能被打斷。

如果核戰摧毀了一半的地球，它也會繼續生存下來，不會被破壞。它會繼續提供服務，它會繼續付錢給人們幫它保持活力。

關閉它的唯一方法是關閉託管它所在的每個伺服器。

這點很難，因為許多伺服器託管在不同的國家或地區，而且很多人隨時都需要使用這些伺服器。

實際上真正能殺死它的唯一方法，便是讓它提供的服務變得無用與過時，讓大家都不想使用它。如果過時，就沒人願意為它付出代價。沒有人想擁有它，它便無法支付任何人，然後就會被餓死。

但只要有人想要使用，它就很難被殺死、腐化、停止或中斷。<sup>註6</sup>

比特幣是一種技術，其存在的原因跟輪子、刀械、手機或任何技術的存在完全相同：因為它替用戶提供了使用上的好處。用戶、礦工和節點營運者，都在經濟上從跟比特幣的互動中得到回報，這就是它得以繼續發展的原因。值得補充的是，所有使比特幣工作的各方，都可單獨進行操作，沒有那一方對比特幣來說特別重要。如果有任何人想改變比特幣，比特幣也完全有能力繼續運作，因為沒有任何人可直接輸入任何東西。這點也有助於我們理解第 10 章所將提到的比特幣「不可變」特性，以及為何嘗試對比特幣代碼進行嚴格修改，將會創造出比特幣的仿冒版。而這種仿冒版，決不可能重現維持比特幣運作與不可變的「經濟平衡」動機。

---

註 6 Ralph Merkle, 「資料存取物件，民主與管理 (DAOs, Democracy and Governance)」, *Cryonics* 雜誌, 第 37 卷, 第 4 期 (2016 年 7 月至 8 月): 第 28-40 頁; Alcor 出版, [www.alcor.org](http://www.alcor.org)。

比特幣也可以被理解為一個自發、新興的獨立公司，它提供了一種新的貨幣形式和一種新的支付網路。該公司沒有管理或企業結構，因為所有決策都是自動化和預先編寫好的。一般開源項目中的志願程式師，可對代碼進行更新和改進，但是用戶可以選擇是否要採用。該公司的價值主張是他們的貨幣供應，在面對需求和價格上漲時，其貨幣完全不具任何彈性；相反的，由於採礦難度調整，需求增加只會變相形成更安全的網路。礦工會在採礦基礎設施中，投入電力和處理能力來保護網路，因為他們可以從中獲得獎勵。

比特幣用戶支付交易費，並從礦工處購買比特幣，因為他們希望使用數位貨幣，並希望從長期的升值中獲利，因此也會在購買過程中，為礦工投資的礦池網路提供資金。礦工對 PoW 採礦硬體的投資，因為會使網路更加安全，所以可以當成公司的資本。而對比特幣網路的需求越大，礦工的獎勵和交易費用就越有價值，也就需要更多的處理能力來產生新的比特幣。亦即增加公司的資金，讓網路更安全，又會讓比特幣更難生產。這變成一種經濟安排，對所有參與者來說都是有效且有利可圖，因此能讓比特幣網路繼續以驚人的速度成長。

透過這種技術設計，中本聰便能發明出數位化的「稀缺性」。比特幣是數位商品的第一個實例，稀有且不能無限複製。雖然在數位網路裡，將數位物件從一地傳送到另一地的做法微不足道，就像傳送電子郵件、文字訊息或檔案下載一樣，但更準確描述這種過程的說法，應該說是複製而非傳送，因為數位物件仍舊留在傳送者身邊，可以被無限複製。然而比特幣卻是數位商品裡的第一個例外，也就是它的傳送過程並非複製，而是讓該數位物件不再為傳送者所擁有。

除了數位化的「稀缺性」之外，比特幣也是「絕對稀有」的第一個範例，它是唯一具有「固定數量」的動態（在數位或物理上）商品，而且絕對不能想像它能增加數量。在比特幣發明前，商品的「稀缺性」始終是相對的，但不是絕對的。常見的「誤解」便是認為任何物質商品，都是數量有限或絕對稀有的。因為我們所能生產任何商品的最高數量，絕不是因為它在地球上的普遍存量，而是受限於繼續製造它所需要的時間與努力。比特幣憑藉其絕對的稀有性，可以跨越時間而持續暢銷，這也是它的一個關鍵重點，我們將會在第 9 章裡，進一步解釋比特幣作為價值儲存的作用。

## 供應、價值和交易

從「理論」上講，的確可能生產出具有可預測的「穩定或低供應成長率」資產，並使它作為貨幣角色，但事實證明，這件事比理論上更為棘手。政府絕不允許私人團體發行自己的私人貨幣，違背政府資助自己成長的主要方式。因此政府總希望能夠壟斷貨幣生產，而且還要時時面對過度增加貨幣供應量的「誘惑」。但隨著比特幣的發明，這個世界終於找到了一種「綜合形式」的貨幣，這種貨幣有最堅強的保證，也就是可以維持低供應成長率。比特幣完全趕走了貨幣政策中的宏觀經濟學家、政客、總統、革命領導人、軍事獨裁者與電視名嘴等。它的貨幣供應量成長，取決於比特幣網路上所有成員採用的程式化功能。這種貨幣在剛開始時，膨脹的計劃看起來像是可以改變，不過那段期間已經過去了。就所有實際意圖和目的而言，比特幣的通貨膨脹計劃就像它的交易記錄一樣，是完全不可變動的<sup>註 7</sup>。雖然比特幣出現的最初幾年，供應量的成長非常高，其供應量計劃

---

註 7 有關比特幣的不變性和抗變化討論，請參考第 10 章。

「不變性」的保證，看起來似乎也並不可信，但隨著時間經過，供應量的成長率逐漸下降，維持供應量計劃方面的可信度也持續上升，而且每天看起來都未對比特幣網路造成重大改變。

比特幣區塊大約每十分鐘被添加到共享分類帳。在比特幣網路誕生時，區塊獎勵被設定為每區塊 50 比特幣。大約每隔四年，或在發出 210,000 個區塊之後，區塊獎勵便會減少一半。第一次減半發生在 2012 年 11 月 28 日，之後新比特幣的發行量降至每區塊 25 個。2016 年 7 月 9 日，它再次減半至每區塊 12.5 個比特幣，並將在 2020 年降至 6.25 個。根據這個時間表，供應量將繼續以遞減的速度成長，在 2140 年左右的某個時間點接近 2100 萬個，此時便不再發行比特幣（見圖 14）。

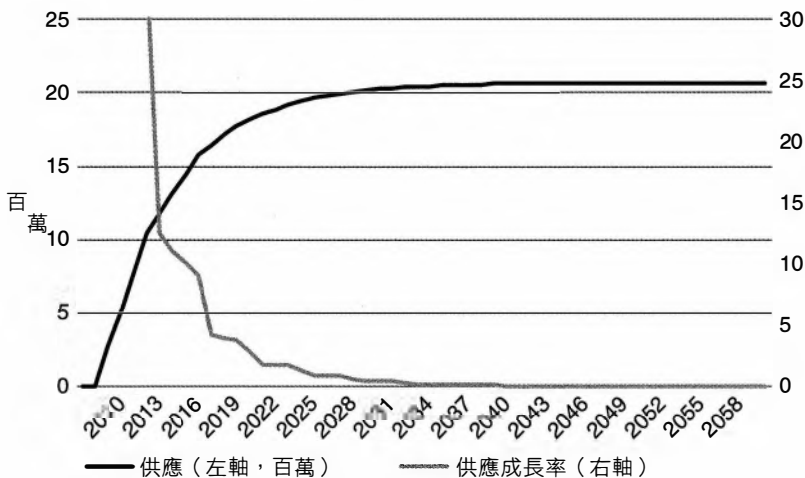


圖 14 比特幣供應與供應成長率比較（假設剛好每十分鐘產生一個區塊）

因為新幣只是在發行新區塊的情況下生產，每個新區塊都需解決工作量證明的問題，因此產生新比特幣需要花費實際的成本。隨著市場上比特幣的價格上漲，更多節點加入競爭 PoW 的解決方案，以獲得區塊獎勵。PoW 問題的難度也隨之增加，使獲得獎勵的成本變得更高。因此，生產比特幣的成本，通常會隨著市場價格而上漲。

設定這個供應量成長計劃之後，中本聰將每個比特幣分成 100,000,000 個單位，並在稍後以他的假名，稱此細分單位為 satoshis（聰）。讓每個比特幣可以再細分成 8 位數的小單位，代表供應將繼續以遞減的速度成長，直到 2140 年左右，數字全部填滿，並達到 21,000,000 個比特幣為止。然而，成長率下降意味著到 2025 年時，大約會開採出前 2000 萬枚比特幣，剩下的 100 萬枚則在接下來的一個多世紀內開採完畢。

新出現的比特幣數量並沒有跟演算法預測的數量完全相同，因為新區塊並非精確的每十分鐘開採一次，而難度調整也非精確的過程，而是一個每兩週調整一次的校準動作，可能超過或低於其目標，這點要依有多少新礦工加入採礦行列而定。在 2009 年時，很少人使用比特幣，因此發行量遠低於供應計劃時間表，而在 2010 年則超過了供應預測的理論值。雖然確實的數字會有所不同，但這種與理論成長的差異程度，會隨著供應量的成長而逐漸降低。其中不變的是比特幣數量的上限，以及供應成長率將會繼續下降。因為逐漸變少的比特幣數量，加入了不斷增加的庫存量之中。

到 2017 年底，已經開採了 1677.5 萬枚，佔所有比特幣的 79.9%。2017 年的年供應成長率為 4.35%，低於 2016 年的 6.8%。表 6 顯示了 BTC（比特幣）的實際供應成長及其成長率<sup>註 8</sup>。

---

註 8 資料來源：blockchain.info。

表 6 比特幣供應和成長率

年	2009	2010	2011	2012	2013	2014	2015	2016	2017
總 BTC 供應 (百萬)	1.623	5.018	8.000	10.613	12.199	13.671	15.029	16.075	16.775
全年發展率 (%)		209.13	59.42	32.66	14.94	12.06	9.93	6.80	4.35

仔細研究未來幾年比特幣供應計劃，可以讓我們對供應和成長率進行預估。實際數字肯定會有些不同，但差距不會太大（見表 7<sup>註 9</sup>）。

表 7 比特幣供應和成長率（預計）

年	2018	2019	2020	2021	2022	2023	2024	2025	2026
總 BTC 供應 (百萬)	17.415	18.055	18.527	18.855	19.184	19.512	19.758	19.923	20.087
全年發展率 (%)	3.82	3.68	2.61	1.77	1.74	1.71	1.26	0.83	0.82

圖 15 是依據過去 25 年來，全球主要儲備貨幣的廣義貨幣供應量和黃金的成長率，來推斷未來 25 年與比特幣供應率的比較。透過這些計算，可以看到比特幣供應量將在未來 25 年增加 27%，而黃金供應量將增加 52%，日元增加 64%，瑞士法郎增加 169%，美元增加 272%，歐元增加 286%，英鎊增加 429%。

註 9 資料來源：作者計算。



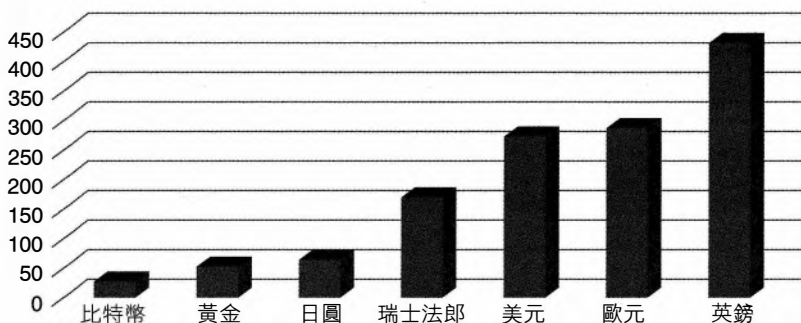


圖 15 預計未來 25 年，比特幣與主要國家貨幣供應量成長率的比較 (%)

這個表格可以幫助我們理解比特幣的可銷售性，以及它如何實現作為貨幣的功能。由於供應成長率在 2025 年之前降至黃金以下，因此比特幣的「供應限制」，可能讓它受到大量的需求，以便做為價值儲存之用；換句話說，它可以「跨越時間」而具有可銷售性。而它的數位特性則可方便安全的在世界各地傳送，用其他金錢形式從未見過的方式「跨越空間」暢銷，最後，它可細分為 100,000,000 聰的單位，也讓它可以「跨越規模」來銷售。此外，比特幣也消除了任何試圖貶低或沒收它的權力機構控制，讓比特幣可以完全避開政府法幣的主要缺陷。數位時代的來臨，為生活各個層面帶來改進和效率，比特幣便在「間接交易」的貨幣解決方案中，呈現出巨大的技術躍進，可能跟從牛和鹽進步到黃金和白銀一樣的重要。

傳統貨幣的供應量持續增加且購買力下降，但比特幣迄今為止儘管進展溫和，其實際購買力仍然大幅增加；儘管供應量有所增加，但供應成長率反而下降。由於驗證交易的礦工會得到比特幣作為獎勵，因此這些礦工在維護網路完整性方面具有強烈動機，反過來又可以讓貨幣價值上升。

比特幣網路於 2009 年 1 月開始營運，剛開始是少數人才有的密碼學郵件列表上，一個不太明顯的項目。也許比特幣生命中必須達成的最重要里程碑，就是網路數位貨幣從經濟上毫無價值到擁有市場價值的那一天，

也就是代表比特幣通過市場的測試：網路已成功運作，足以讓人願意以實質的金錢，交換擁有比特幣。在現實世界裡，這個日子發生於 2009 年 10 月，當時名為 New Liberty Standard 的線上交易所，以 0.000994 美元的價格出售了比特幣。而在 2010 年 5 月，比特幣進行了現實世界裡的第一次購買行為，因為有人付了 10,000 比特幣，購買價值 25 美元的兩個披薩，亦即一個比特幣的價格為 0.0025 美元。一直到後來，越來越多的人聽說了比特幣，開始感興趣而購買，因此比特幣價格持續上漲<sup>註 10</sup>。

市場對比特幣的需求來自以下事實：它要運行第一個（迄今為止，可以說是唯一的）具有功能性與可靠性的數位現金系統<sup>註 11</sup>。這個網路在早期成功運作的事實，得以在密碼學家和自由主義者的小社群裡，擁有數位貨幣的「收藏價值」。這些人會想要用自己的電腦進行採礦，最後甚至開始彼此購買比特幣<sup>註 12</sup>。比特幣的限制嚴格、無法複製的特性，也有助於創造這種最初的收藏狀態。在被人購買並在比特幣網路上使用後，開始獲得經濟價值，也因更多人想將它作為價值儲存，比特幣開始了貨幣化的過程。這一系列活動符合 Ludwig von Mises 關於貨幣起源的「回歸理論（Theory of Regression）」，也就是貨幣商品開始變成市場商品後，就會被作為交換媒介。比特幣在小社群中的這種收藏狀態，跟貝殼、石幣與貴金屬的觀賞價值沒什麼不同，不過它是一種可以獲得明顯價值提升的貨幣。

---

註 10 這兩筆交易的細節可以在 Nathaniel Popper 的「數位黃金（*Digital Gold*）」中找到。

註 11 有關為何比特幣的仿冒品不能被描述為數位現金的詳細討論，請參考第 10 章。

註 12 關於這一點有個不錯的討論，請參考 Kyle Torpey，「這就是 Goldbugs 所錯過的比特幣『內在價值』（Here's What Goldbugs Miss About Bitcoin's "Intrinsic Value"）」，富比士數位現金。請參閱 <https://www.forbes.com/sites/ktorpey/2017/10/27/heres-what-gold-bugs-miss-about-bitcoins-intrinsic-value/2/#11b6a3b97ce0>。

由於是新出現且剛開始散佈，因此比特幣的價格會隨需求程度出現波動，不過由於任何當局權威都無法因應比特幣價格上漲，任意強加其貨幣供應量，因此可以用來解釋比特幣購買力迅速上升的事實。亦即當比特幣的需求激增時，比特幣礦工無法像過去的銅礦工那樣超時加班以增加產量，也沒有中央銀行可以介入增加比特幣的數量，並造成市場貨幣氾濫（就像葛林斯潘建議央行對黃金所做的對應一樣）。市場面對需求不斷成長的唯一解決方式便是價格上漲，漲到足以激勵持有者將一些比特幣出售給新加入的人。如此便可解釋為何在比特幣問世 8 年間，價格從 2009 年 10 月 5 日的第一筆記錄交易中的 0.000994 美元上升到 2017 年 10 月 5 日的 4,200 美元，八年內增加了 422,520,000%，複合年成長率為 573%（見圖 16<sup>註 13</sup>）。

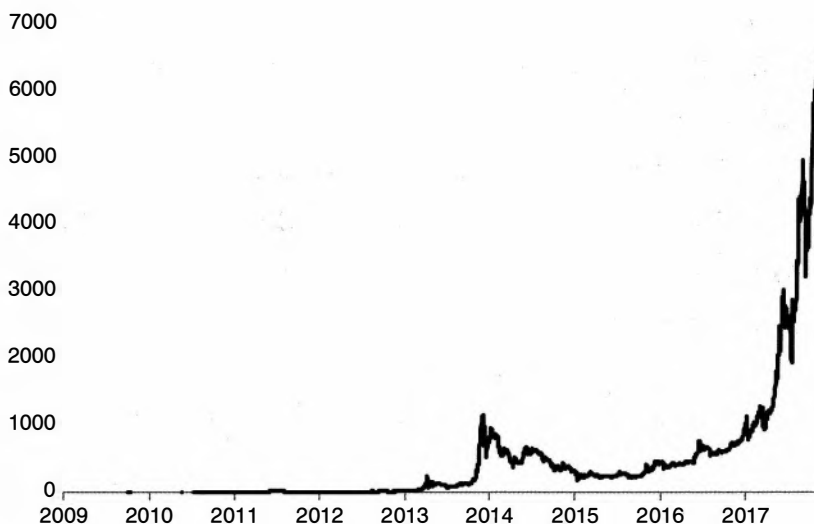


圖 16 比特幣的價格（以美元計算）

註 13 資料來源：Coindesk 比特幣價格指數。請參閱 [www.coindesk.com/price](http://www.coindesk.com/price)。

因為比特幣價格上漲，人們便可以把它當作價值來儲蓄，而不僅是把它花掉。如果沒有一些人願意在很長一段時間內持有該貨幣，那麼繼續拋售該貨幣將使其價格維持下降，讓它無法升值。到 2017 年 11 月時，流通中的所有比特幣總市值約在 1100 億美元，使其價值大於多數國家的廣義國家貨幣供應量總值。如果比特幣是一個國家貨幣，其貨幣價值將是全球第 56 大國家貨幣，大約在科威特或孟加拉國的貨幣供應量範圍內，比摩洛哥和秘魯都來得大，但小於哥倫比亞和巴基斯坦。如果與狹義貨幣供應量進行比較，比特幣的供應價值更在世界排名第 33 位，其價值與巴西、土耳其和南非的狹義貨幣供應接近<sup>註 14</sup>。比特幣可能是網際網路最顯著的成就之一，在一個由匿名程式員設計的網路範圍裡，自覺與自願完成的線上經濟，然後在九年內逐漸成長，並比大多數民族和國家的貨幣供應，具有更高的價值<sup>註 15</sup>。

這種保守的貨幣政策以及市場價值的相對升值，對比特幣的成功運作來說相當重要，當然這也是礦工願意消耗電力和處理能力，並誠實驗證交易的原因。如果比特幣是透過寬鬆貨幣政策所建立，例如凱因斯主義者或貨幣主義經濟學家所推薦的那種形式，它的貨幣供應量便會隨著用戶數量或交易量的成長而升高，但在這種情況下，它就只會是一群密碼學愛好者在線上的邊緣實驗罷了。既不會有大量的處理能力用來挖掘它，也沒有必要大量投資來驗證交易和解決工作量證明，因為你就只能獲得由於更多人使用而貶值的比特幣了。現代法幣與經濟學家主張的擴張性貨幣政策，從未通過自由市場的考驗，而是像之前提過的一樣，都是透過政府法律來強制實施。比特幣作為一個並不強迫他人使用的自願系統而言，如果無法

---

註 14 CIA 世界概況。請參閱 <https://www.cia.gov/library/publications/the-world-factbook/>。

註 15 應該用一粒鹽來比較，因為它們實在無法完全準確的類比。政府的貨幣供應不僅由中央銀行創造出來，也由銀行本身製造，但比特幣不存在這樣的過程。貨幣供應量的衡量標準也會因國家而異，它們會把金融資產當成貨幣供應的一部分。

吸引大量需求，其成功作為數位現金的地位，也將無法得到保證。雖然比特幣交易可以在不需第三方信任下執行，但其交易網路仍很容易受到利用大量處理能力、惡意行為者的攻擊。換句話說，如果沒有保守的貨幣政策和難度調整，比特幣便只能在「理論上」成功的作為數位現金，在廣泛執行時依舊會很不安全。在這種情況下，第一個惡意競爭者會碰到比特幣的「健全貨幣難以大量生產」政策，使分類帳的更新和新比特幣的產生，逐漸變得更加昂貴。因為更新分類帳的高成本，會使礦工必須更誠實的更新分類帳，反而讓比特幣網路比起其他不健全貨幣競爭者更為安全。

比特幣的價格成長，反映出該網路對用戶所提供的使用量與實用性，也不斷的持續成長。交易網路上的交易數量迅速成長：2009 年有 32,687 筆交易（每日交易量為 90 筆交易），2017 年交易量則增加到超過 1.03 億筆交易（平均每日交易量為 284,797 筆交易）。2018 年 1 月時，累計交易數量接近 3 億筆。表 8<sup>註 16</sup> 和圖 17<sup>註 17</sup> 顯示了年度的交易成長。

雖然交易成長令人印象深刻，但它與比特幣「貨幣總存量」的成長並不相符，事實證明這樣的交易數量，遠小於跟比特幣價值相近的貨幣經濟體交易數量；因為每日 300,000 交易量，大約只是小城鎮裡進行的交易數量，而非中等規模經濟體（約等同比特幣供應價值）的交易數量。此外，由於比特幣區塊的當前大小被限制為「1 百萬位元（megabyte）」，只要一天有 500,000 個交易量，便會接近比特幣網路的執行以及所有節點記錄的「上限」。即使達到此一限制，比特幣也廣為人知，但其貨幣價值的成長和日常交易的價值也沒有減少。這表示比特幣的擁有者，大多會將其視為價值儲存而非交換媒介，這點我們將在第 9 章詳加討論。

---

註 16 資料來源：blockchain.info。

註 17 資料來源：blockchain.info。

表 8 年度交易量和平均每日交易量

年度	交易量	平均每日交易量
2009	32,687	90
2010	185,212	507
2011	1,900,652	5,207
2012	8,447,785	23,081
2013	19,638,728	53,805
2014	25,257,833	69,200
2015	45,661,404	125,100
2016	82,740,437	226,067
2017	103,950,926	284,797

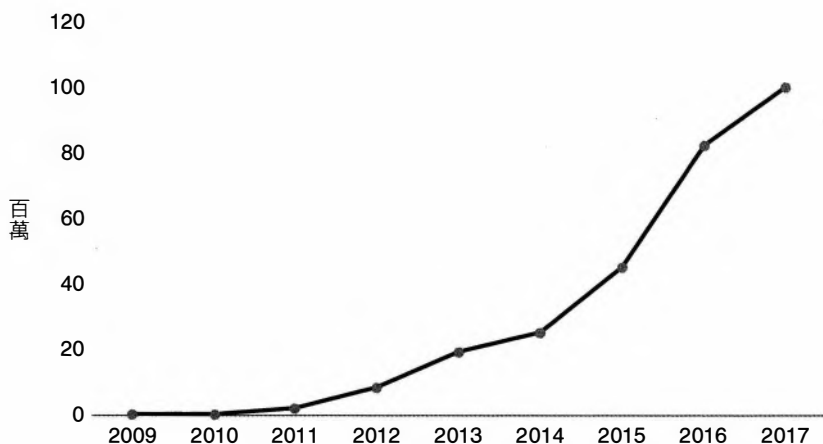


圖 17 比特幣網路的年度交易量

交易的市場價值，會隨著交易網路的生存週期而增加。但由於比特幣交易的特殊性質，讓它很難準確估計以比特幣或美元交易的確實價值。如果從「下限」來預估，可以看到 2017 年的每日平均交易量約為 260,000 比特幣，而且在比特幣的生命週期裡，其貨幣成長率高度波動。雖然交易裡的比特幣價值，隨著時間經過並未明顯增加，但將這些交易的市值以美元計算，到了比特幣九歲生日的 2017 年，交易總額為 3756 億美元。在交易時以美元計價的話，目前比特幣等於已經處理了價值 0.5 兆美元的交易（見表 9<sup>註 18</sup>）。

表 9 比特幣網路交易年度總值（美元）

年度	交易總美元價值
2009	0
2010	985,887
2011	417,634,730
2012	607,221,228
2013	14,767,371,941
2014	23,159,832,297
2015	26,669,252,582
2016	58,188,957,445
2017	375,590,943,877
總計	499,402,199,987

註 18 資料來源：blockchain.info。

比特幣網路成長的另一個衡量標準，便是處理交易所需交易費用的價值。雖然比特幣交易在理論上是免費處理，不過因為處理它們的責任交給了礦工，而且費用越高，他們就越可能更快獲得價值。早期交易量很少時，礦工可能會處理不包含費用的交易，因為新比特幣的區塊補貼本身，就已值得礦工付出的努力。隨著對比特幣交易的需求成長，礦工可以選擇優先考慮費用更高的交易。截至 2015 年底，每筆交易的費用低於 0.1 美元，在 2016 年初左右，開始上漲到每筆交易費用超過 1 美元。隨著 2017 年比特幣價格的快速上漲，截至 11 月底，平均每筆交易費用已經漲到 7 美元（見圖 18<sup>註 19</sup>）。

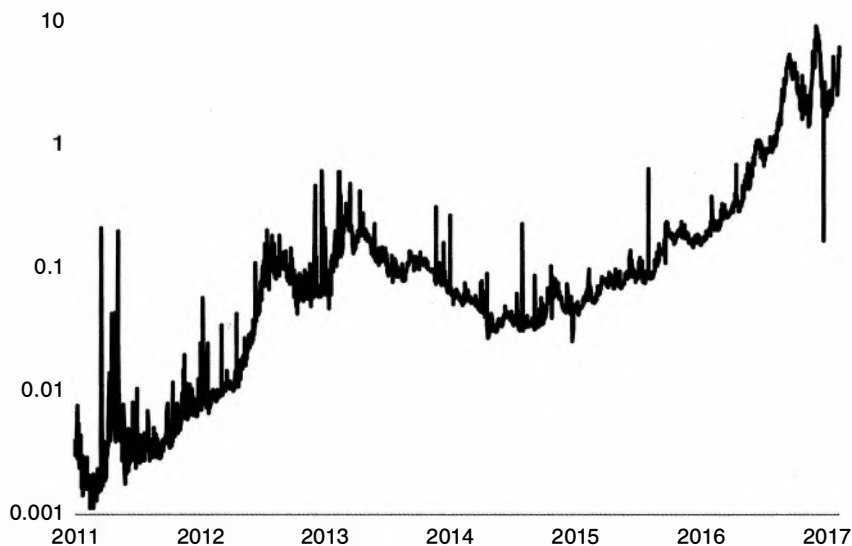


圖 18 比特幣網路交易費用平均美元價值，對數尺標。

註 19 資料來源：blockchain.info。



雖然比特幣的價格隨著時間經過而普遍上漲，但這種上漲的波動很大。圖 19 顯示了過去五年比特幣交易的 30 天「日收益標準差」<sup>註 20</sup>。雖然波動率似乎正在下降，但跟國家貨幣與黃金相比仍然非常高，而且這種趨勢仍不明顯，無法確定是否會繼續下降。圖 19 是包含的美元指數的 30 天波動率，可供觀察。

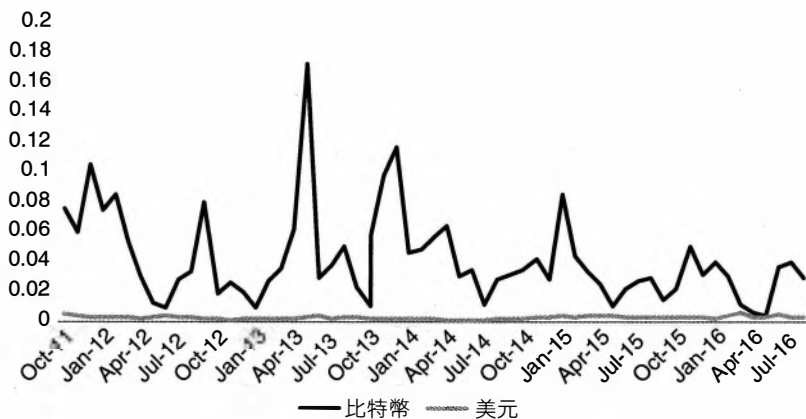


圖 19 比特幣和美元指數的 30 日波動率

檢查黃金和主要國家與加密貨幣的價格數據，顯示這些貨幣的市場價格波動性存在了顯著差異。針對黃金、主要法定貨幣與比特幣，收集過去五年的每日回報，便可發現主要國家貨幣的標準差，均比比特幣大了 7 倍以上（見表 10<sup>註 21</sup>）。

註 20 資料來源：作者基於「聖路易斯聯邦儲備局經濟數據」裡的美元數據，以及來自 coindesk.com 的比特幣數據，所計算的結果。

註 21 所有貨幣的價格均以美元計算，美元則以美元指數計算。「聖路易斯聯邦儲備局經濟數據」的國家貨幣數據、「世界黃金協會」的黃金數據，比特幣則來自 coindesk.com 的數據。

**表 10** 2011 年 9 月 1 日至 2016 年 9 月 1 日期間，每美元貨幣市場價格的平均每日百分比變化和標準差

	平均每日百分比變化	標準差
人民幣	0.00002	0.00136
美元	0.00015	0.00305
英鎊	0.00005	0.00559
印度盧比	0.00019	0.00560
歐元	-0.00013	0.00579
日圓	0.00020	0.00610
瑞士法郎	0.00003	0.00699
黃金	-0.00018	0.01099
比特幣	0.00370	0.05072

比特幣的波動性來自它的供應量不靈活，而且無法針對需求變化做出反應，因為它的程式被設計為以「預定」速率成長。對於任何一般商品而言，需求的變化會影響該商品生產者的生產決策：需求增加會讓他們決定增加產量，除了緩和價格上漲也可提高獲利能力；需求減少則會導致商品生產者減少產量，讓他們得以減少損失。國家貨幣也存在類似情況，中央銀行會預先透過設定貨幣政策參數，來抵消市場的波動，以維持貨幣購買力的相對穩定。由於比特幣的供應時程完全無法滿足需求，也沒有中央銀行來管理供應的問題，因此波動是非常可能的，尤其在每天需求變化非常不穩定的早期階段，金融市場與比特幣之間的交易就像是嬰兒般的摸索。

但隨著市場規模擴大，金融機構處理比特幣的日漸複雜與深化後，這種波動性便可能下降。而隨著市場規模與流通性越來越大，對比特幣需求的日常變化可能會相對變小，因而使市場參與者能從價格變化中獲利，讓價格波動平緩下來。要實現這個目標，只有在擁有比特幣的大量市場參與者，願意長期持有這些比特幣的情況。如此便可提高比特幣供應的市場價值，而且只用一小部分的供應量，就能維持市場交易的大量流動性。

如果比特幣網路在任何時刻都能達到穩定規模，流入和流出資金流量也相對平等，比特幣的價格便可以穩定下來。在這種情況下，比特幣將獲得更多穩定性，也會有足夠的流通性，不會隨著日常市場交易而顯著波動。而且只要使用比特幣的行為繼續成長，其升值便能吸引更多使用者，造成更進一步的升值，使波動率繼續下降。而只要比特幣維持成長，其幣值就會像新創公司的股票價格一樣快速成長。如果比特幣的成長停止並穩定下來，便會停止吸引高風險的投資潮流，而成為一種正常的貨幣資產，預估每年應該都會略微升值。

## 第八章附錄

以下是三種比特幣所使用技術的簡要說明：

**散列：**一種函數計算轉換的過程，可以將任何數據作為輸入，使用不可逆的數學公式，轉換為「固定大小」的數據（稱為 hash）。換句話說，使用這個函數為任何數據生成一個大小一致的 hash 是很方便的，但幾乎不可能倒過來從 hash 中確定原始數據字串。它對於比特幣的操作非常重要，

因為 hash 會用於數字簽名、工作量證明、Merkle 樹根節點、交易記錄索引、比特幣支出與接收地址以及其他各種應用程序。Hash 本質上可以公開一段數據作為識別，但卻不會洩露關於該數據的任何資訊，因此可以用於安全且無信任的檢查，看各方是否具有相同的數據。

**公鑰加密：**依賴一組數學相關數字的身分驗證方法，包括私鑰、公鑰與一個或多個簽名。必須保密的私鑰可以生成能自由散佈的公鑰，因為無法倒過來以公鑰來確定私鑰。此方法用於身分驗證，例如某人公開他的公鑰後，他可以 hash 一些數據，然後使用他的私鑰對該 hash 進行簽名，以創建其數位簽名。任何具有相同數據的人，都可以創建相同的 hash，並用來創建簽名；然後便能將此簽名與之前收到的公鑰進行比對，並看到它們在數學上是相關的，證明以該私鑰簽署 hash 所涵蓋的數據。比特幣便利用公鑰加密技術，允許在開放的不安全網路上進行安全的價值交換。比特幣持有人只有在附有私鑰的情況下才能使用他的比特幣，而與該幣相關的公共地址可以廣泛散佈。所有比特幣網路的成員，均可透過確認傳送來自正確的私鑰擁有者，驗證交易的有效性。在比特幣中，證明擁有貨幣所有權的唯一方式便是私鑰的所有權。

**點對點網路：**一種網路結構，當中的所有成員彼此均具有相同的權利與義務。沒有中央協調者可改變網路規則。不同意網路功能的節點經營者，並不能將他們的意見強加給該網路上的其他成員，或是覆蓋別人的權限。最著名的點對點網路範例便是 BitTorrent，這是一種在網路上共享文件的協議。一般在集中式網路中，成員是從託管檔案的中央伺服器裡下載文件，但在 BitTorrent 網路中，用戶可以直接相互下載分成小塊的文件。一旦某用戶下載了一段文件，該用戶即可成為此文件的種子，允許別人從自己電腦裡下載。透過這種設計，大型文件可以相對快速地傳播，無需大型

伺服器 and 廣泛的基礎設施來散佈檔案，同時還可以防止單點故障而損害流程。網路上共享的每個文件都受 hash 加密保護，很容易進行驗證，以確保共享該文件的任何節點均未損壞文件。在執法部門打擊了 Napster 這類集中化的文件共享網站後，BitTorrent 的去中心化特性代表執法部門永遠無法關掉它。隨著全球用戶網路的不斷成長，BitTorrent 在某種程度上，大約佔了全球所有網際網路流量的三分之一。比特幣使用了類似於 BitTorrent 的網路，BitTorrent 網路成員共享的內容為電影、歌曲或書籍等的數位資料，而比特幣網路成員共享的則是所有比特幣交易的分類帳。

## 9

# 比特幣有什麼用途？

---

## 儲存價值

---

認為「資源是稀少且有限」的觀念，是對「稀缺」特性的誤解，這也是經濟學背後的關鍵概念之一。地球上存在的每種原始材料的「絕對數量」，對我們來說是天文數字，人類甚至無法衡量或全面理解，因此也絕對不會構成人類生產它們的真正限制。例如我們幾乎只對地表搔了點癢，尋找人類需求的礦物，而搜索的越多、挖掘的越深，找到的資源也就越豐富。如果說有什麼原因，真的構成任何資源在目前數量與實際數量有所限制，那就是人類所能生產該資源的「時間」數量，因為這是唯一真正稀有的資源（直到比特幣的創建）。已故經濟學家 Julian Simon 在其出色作品《終極資源》（*The Ultimate Resource*）一書中，解釋了唯一有限的資源，實際上也是「資源有限」真正適用的唯一事物，便是人類的「時間」。每個人在地球上的時間有限，這是我們作為個體

所面對的唯一「稀缺性」問題。在一個社會裡，我們唯一缺少的是社會成員可以用來生產不同商品和服務的「總時間」。只要人類的時間繼續下去，總能產生更多的任何商品。商品的真實成本，來自不再需要生產該商品的「機會成本」。

在人類歷史上，我們從未耗盡任何單一的原料或資源，而且幾乎目前所有資源的價格，都低於該資源在歷史上的任何時刻，因為技術的進步，讓我們能夠以更低的成本，在這個時代裡生產它們。人類不僅沒有耗盡原料，在消費需求增加的情況下，每種資源的已知蘊藏量，也會隨著時間推移而增加。如果要以「資源有限」進行理解的話，那麼隨著我們消耗掉更多的資源，該資源的現有庫存量將隨著時間下降。但即使我們消費得更多、價格下降得更快，尋找和挖掘資源技術的改進，也都能讓我們發現越來越多的資源。石油是現代經濟的重要命脈，也有相當可靠的統計數據，因此也是最好的例子。各位請看圖 20 所示，即使消費與產量每年都持續增加，探勘石油的已知蘊藏儲量也以更快的速度成長<sup>註 1</sup>。根據英國石油公司的數據統計，2015 年石油年產量比 1980 年高出 46%，而消費量則高出 55%。另一方面，石油儲量增加了 148%，大約是生產和消費成長的三倍。

在地殼中不同分佈程度的資源，也都有類似的統計數據。資源的稀有性，決定了從地殼中提取資源的相對成本。較普遍的金屬如鐵和銅發掘容易，因此相對便宜，較貴的金屬如銀和金則相對較貴。然而，這些金屬生產量的限制，仍然在於它們相對於彼此生產的「機會成本」，而不是它們的「絕對數量」。例如黃金是地殼中的稀有金屬，已經被開採了數千年，隨著技術的進步與時間經過，開採的產量也越來越多（如第 3 章所示），便是最好的證明。如果地殼中最稀有金屬的年產量每年都在增加，那麼談論任

---

註 1 資料來源：BP 統計評論。

何自然元素在實質上的數量限制，都是沒有意義的。「稀缺性」只與物質資源相關，提取成本的差異性是該物質稀有程度的決定性因素。正如 Julian Simon 所說，唯一的「稀缺性」就是人類必須生產這些金屬的「時間」，這就是為何全球工資持續上升，使得產品和材料比起人工來說，持續顯得更為便宜。

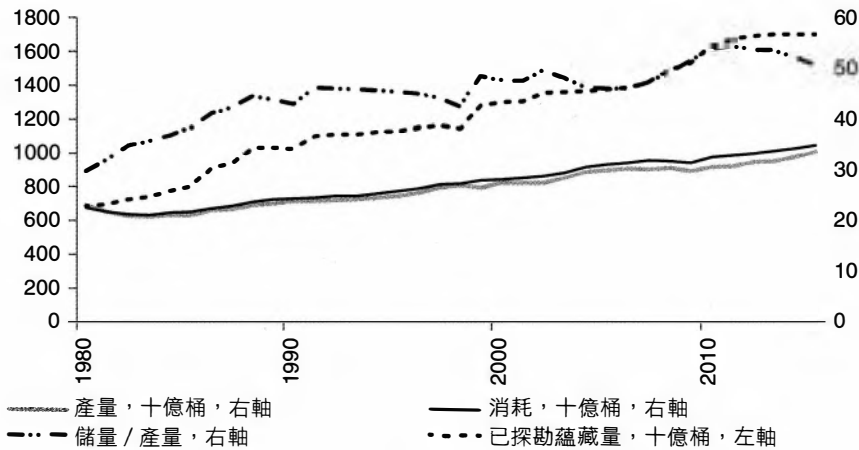


圖 20 1980 ~ 2015 年全球石油消費量、產量、已探勘蘊藏量與儲藏量佔年產量相比

這是人們最難理解的經濟概念之一，也助長了「環保運動」無窮無盡的歇斯底里，並在數十年來透過「世界末日」來恐嚇我們。Julian Simon 以著名的「10 年賭局」，挑戰這種二十世紀最重要的歇斯底里，竭盡全力打擊這種現象。而 Paul Ehrlich 曾寫過幾本這類歇斯底里的書，認為因為重要資源耗盡，所以地球處於災難的邊緣，他也對這些資源耗盡的日期，進行預測。於是 1980 年時，Simon 向 Ehrlich 挑戰任選原物料以及任何一段超過一年的時間，向他打賭 10,000 美元，賭的就是這些金屬的價格（根據通貨膨脹調整後），在賭局結束後的價格，將低於賭局開始時的價格。Ehrlich 選擇了銅、鎳、鎢、錫和鎢，這些都是他預測地球將會耗盡的材料。然而，在



1990 年，這些金屬的價格均已下降，年產量水平也有所提高。而且在這段期間，世界人口增加了 8 億人，是十年前後的增幅最大的一段期間。

事實上人類越多，這些原物料的生產就會越多。更重要的是，正如經濟學家 Michael Kremer<sup>註 2</sup> 所說，或許人類進步的根本動力不是原物料，而是遇到問題時的解決技術。「技術」在本質上既是一種「非排他性」商品（意即一旦有人發明了某種東西，其他所有人都可以複製，並從中獲益），也是一種「非競爭性」商品（意即從該發明獲益的人，並不會降低其他人使用它的獲益）。以輪子為例，一旦有人發明了輪子，其他人都可以複製並製造自己的輪子，而他們自己使用輪子，也不會降低其他人從輪子獲得方便的能力。地球上巧妙的想法很少見，只有少數人能自己想出來，因此人口數較多會比較少的社會，產生更多的技術和思想。而由於每個人都能獲益，所以我們最好生活在人口較多的世界裡。地球上存在的人越多，就會想到越多的技術和富有成效的想法，人類也就越能彼此複製這些想法，從中受益。因而在相同人類時間裡提高產能，並藉此改進生活水準。

Kremer 以「隨著地球人口增加，人口成長率增加而非減少」來說明這點，如果人類是資源消耗的主要負擔，那麼人口越多，每個人可獲得的資源數量越少，經濟成長率和人口成長率應該也會越低，如同 Malthusian 模型所預測。但由於人類本身就是資源，而富有成效的思想是經濟生產的驅動力，更多的人類會產生更有成效的思想與技術、以及更多的人均產量和維持更多人口的能力。此外，Kremer 也說明了人口較多的獨立大陸，便可見證比人口稀少的地區，擁有更快速的經濟成長和進步。

---

註 2 Michael Kremer，「人口成長和技術變革：西元前 100 萬年到 1990 年（Population Growth and Technological Change: One Million B.C. to 1990）」，經濟學雜誌季刊，第 108 卷，第 3 期（1993 年）：第 681-716 頁。

把原物料稱為「資源」是一種謬誤，因為人類並非這些「來自天堂的甘露」的被動消費者。原物料始終是人類勞動和創造力的產物，因此人類才是最終的「資源」，因為人類的時間、精力和聰明才智，一定可以用來生產更多東西。

人類面對時間的永恆困境，關連到在他們從目前一直到未來的時間裡，如何儲存自己生產出來的價值。雖然人類的時間是有限的，但其他一切東西實際上都是無限的，只要投入更多的人類時間，便可生產出更多的東西。而無論人類選擇什麼物品作為價值來儲存，它的價值都會上升，也因為更多東西可以永遠生產出來，所以可能會有其他人生產更多該物品，獲取儲存在其中的價值。例如雅浦島民遇上奧基夫帶著炸藥和更先進的船隻，製造了更多 Rai 石，並獲得儲存在現有石頭中的價值；非洲人則面臨歐洲人帶著裝滿琉璃珠的船隻，獲得了儲存在珠子中的價值。除了黃金之外，任何當作貨幣媒介的金屬，都會面臨過度生產而導致價格崩潰。如同第 4 章所討論的，現代經濟體遇上凱因斯主義的中央銀行，永遠假裝在對抗通貨膨脹，事實上卻逐漸或快速的侵蝕貨幣價值。就像美國人最近開始用房子作為儲蓄的媒介，房屋供應量增加許多，導致了房市狂跌。隨著貨幣持續通貨膨脹，這種大量泡沫化的情況，可被理解為「尋找有用的價值儲存」所做的「投機性」賭注。只有黃金最接近這種問題的解決方案，因為它的化學特性使任何人都無法快速膨脹供應量，也因此形成了人類歷史上最輝煌的時代之一。但政府控制黃金的舉動，很快就限制了它的貨幣角色，然後還以政府發行的貨幣加以取代，記錄也非常糟糕。

這些例子都為比特幣驚人的技術成就，提供了啟示。這是人類史上首次訴求一種供應量受到「嚴格限制」的流通商品。無論有多少人使用比特幣網路，也不管它的價值上升多少或挖礦設備如何先進，實際上就只能存在 2100 萬比特幣，而且無法在技術上增加供應量，來滿足日漸增加的需求。如果有更多人想要擁有比特幣，滿足需求的唯一方法便是讓現有供應

量升值。由於每個比特幣可以分成 1 億個 satoshis（聰），所以便可透過使用更小的單位來成長，讓比特幣升值，因此也創造了一種新型的資產，非常適合用來儲存價值。

在比特幣發明前，各種形式的貨幣數量可說都是無限的，因此它們在時間經歷下，儲存價值的能力並不完善。然而比特幣不變的貨幣供應量，使它成為在人類有限時間裡，儲存自己生產價值的最佳媒介，也因此讓它成為人類有史以來發明過的最佳價值儲存媒介。換句話說，比特幣是「購買未來」最便宜的方式，因為無論價值上漲多少，比特幣是唯一保證不會貶值的媒介（見圖 21<sup>註 3</sup>）。

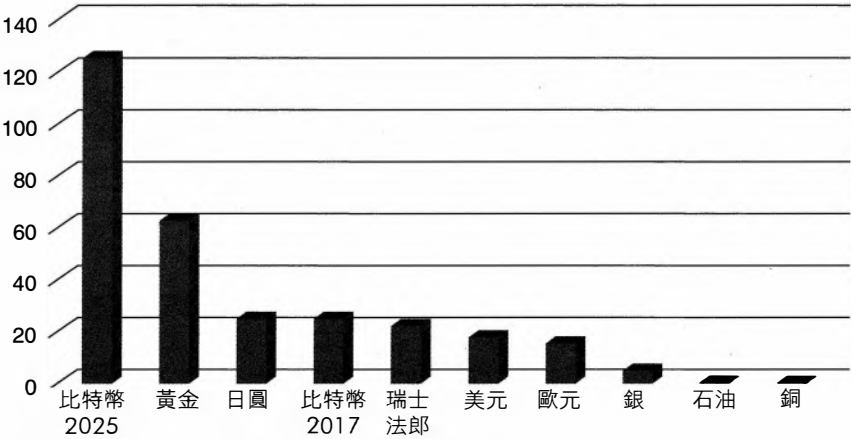


圖 21 全球可用庫存總量除以年產量

註 3 資料來源：美國黃金地質調查數據、白銀研究所白銀數據、Blockchain.info 和作者對比特幣的計算、BP 世界能源石油統計評論、美聯儲經濟數據的國家貨幣數據，請參閱 <https://fred.stlouisfed.org>。作者對銅的估計。

在 2018 年時，只有 9 年歷史的比特幣，已被全球數百萬人採用<sup>註 4</sup>，目前的供應成長率堪比全球性的儲備貨幣。就第 1 章討論的庫存流量比而言，2017 年比特幣的現有庫存，比 2017 年生產的新幣數量約多了 25 倍。這仍不到黃金庫存流量比的一半，但是在 2022 年左右，比特幣的庫存流量比將超越黃金，而到 2025 年，將會是黃金的兩倍左右，並繼續快速成長下去。考慮到第 3 章所討論的金礦開採，黃金應該也大致維持相同的情形。直到 2140 年左右，不再有新的比特幣供應，庫存流量比變成了「無限」，這將會是首次有貨幣或商品達成此一目標。

比特幣供應量減少以及供應成長率不斷下降的重要意義，即在相較於新供應量而言，現有比特幣的供應量要大得多。從這個意義上看，比特幣採礦類似於開採金礦，因而可以確保比特幣作為貨幣媒介時，比起那些供應量可以輕易增加的貨幣來說，可用相對較少的時間與精力來獲得新供應的比特幣；而這些多出來的時間和精力，便可致力於有用的經濟生產，然後又可以用來兌換比特幣。隨著區塊補貼減少，用在比特幣挖礦的資源，其獎勵會主要來自處理交易本身，因此可以繼續保護交易網路，而不是用來創建新的比特幣。

在人類歷史的大部分時間裡，某些實體物品會被用來當成價值儲存。但價值儲存的功能並不需要一定是實體形式，而是要找到價值儲存的供應量難以增加的媒介。比特幣沒有任何實體存在，純粹是能夠實現嚴格「稀缺性」的數位產物，過去從未出現任何實體物質可以像這樣的分割與傳輸。比特幣允許人類以數位方式傳輸價值，而不依賴於實體形式，這樣便可在幾分鐘內完成跨越全世界的大筆資金轉移。比特幣的「嚴格」數位稀

---

註 4 並沒有簡單的方法可以估計比特幣用戶的數量，因為每個用戶本身可以擁有任意數量的錢包地址。2017 年估計此一數字的各種嘗試，預估了用戶數約在 1000 萬到 1 億之間，這可能是我們所能得到最接近的準確估計。

有性，結合了實體貨幣媒介的最佳元素，而且沒有任何移動與運輸上的物理缺陷，因此比特幣可以稱為有史以來發明過的最佳技術之一。

## 個人主權

作為第一種數位現金形式，比特幣第一個也最重要的價值主張，便是讓世界上任何人都可獲得「擁有主權基礎」的貨幣。任何擁有比特幣的人，皆可獲得一定程度的經濟自由，這點在比特幣問世之前並不可能實現。比特幣持有者可以在全球範圍內傳送大量價值，無需徵求任何人許可。比特幣的價值不依賴於世界任何地方的任何物理元素，因此永遠不會被政治或犯罪世界的實體力量，加以阻止、摧毀或沒收。

本發明對二十一世紀政治現實的重要意義，在於從現代國家出現以來，個人首次能夠擁有明確的技術解決方案，以逃避他們所處政府的財政影響力。值得注意的是，對這種技術重要性的最佳描述，可以在 1997 年寫的一本書裡找到，這本書在比特幣創建之前 12 年出版，並預見了一種與比特幣非常相似的數位貨幣，以及它將改變人類社會的影響。

在《君主個體》（*The Sovereign Individual*）中，James Davidson 與 William Rees-Mogg 認為現代民族國家，在強制性法律、高稅收和極權主義衝動等方面，已經發展到對公民自由的沉重壓制，幾乎與歐洲中世紀的教會時期相當，還像是成熟後破繭而出一樣。而由於沉重的稅收、對個人控制以及儀式負擔等，種種支持教會的成本讓歐洲人無法忍受，因而出現了更新更有效的政治和經濟組織形式，取代教會並讓它變得無足輕重。機械、印刷機、資本主義與現代民族國家的興起，也催生了工業社會時代以及現代公民意識。

五百年後，工業社會和現代民族國家變得有點壓迫、僵化與惱人。新技術的出現，消耗了國家的力量與存在的理由。該書的挑釁主旨便是「微處理器將推翻並摧毀民族國家」。新的組織形式將會來自資訊科技，可以破壞國家的賦稅權力，讓公民不會被迫為政府的服務支付超出預期的稅費。數位革命也將摧毀現代國家對其公民的權力，降低民族國家作為組織單位的重要性，並賦予個人前所未有的權力和對自己生活的完整主權。

感謝電信界的革命性成就，讓我們可以看到此一過程正在進行。雖然「印刷術」讓世界上的窮人，可以獲得被教會壟斷且禁止的知識，但印刷仍然存在著「實體」書籍的限制，因為這些書總可能被沒收、禁止或銷毀。而網路世界並沒有這種威脅，幾乎所有人類知識都存在於其中，個人可以隨時造訪，無需受到政府的控制或審查。

同樣地，資訊也可用來進行貿易與就業，顛覆了政府的限制和規定，最好的例子便是 Uber 和 Airbnb 等公司，這些公司在沒有政府管理下便能成功引進產品，徹底推翻了傳統形式的監管。現代人只要在同意和相互尊重的基礎上，建立出身分和保護系統，就能在線上跟其他陌生人進行交易，無需求助於強制性的政府法規。

廉價的電信上網形式出現，也顛覆了地理位置對工作的重要性。許多商品的生產者，現在可以選擇定居在任何喜歡的地方，而他們的工作內容，也越來越具有資訊性和非物質性，可以立即傳送到全球各地。政府法規和稅收變得越來越弱，因為個人可以在適合他們的地方生活或工作，並透過網際網路傳送工作成果。

越多經濟生產價值採取「非物質產品」的形式，土地和物質資產的相對價值便會下降，過去那種大量佔有某物質資產所得到的回報，也會隨之降低。因為每個人的生產力與本身意願息息相關，生產資本也更加體現

在個人本身，讓侵擾它的「暴力威脅」越來越空洞。過去當農民的生產與生存繫於不屬於自己的土地時，暴力威脅可以有效的使他們更勤奮而讓地主獲益。同樣的，工業社會對物質生產的資本及實體產出的嚴重依賴，也讓國家的暴斂橫征相對簡單，正如二十世紀血淋淋的證明一樣。但隨著個人的心智能力成為社會的主要生產力後，暴力威脅的效果大打折扣。人類可以輕鬆地搬遷到不受威脅的司法管轄區，或者可以純粹在電腦上工作產出，政府甚至無法知道這些人在生產什麼。

數位化過程裡還缺最後一塊拼圖，也就是貨幣與價值的「轉移」。即使資訊科技可以突破地理限制和政府控制，但「支付」的部分，仍會受到政府和國家壟斷的銀行，所進行的嚴格控制。如同所有政府強制執行的壟斷一樣，銀行業多年來一直抵制創新和變革，因為這些創新和變革多半會使消費者受益，限制了銀行賺取手續費用或租金的能力。各國經濟擴展並變得更加全球化後，這種壟斷變得越來越嚴重。Davidson 和 Rees-Mogg 以非凡的先見之明，預測新的「數位貨幣逃生口」將會採取的形式：加密安全的貨幣形式，獨立於政府當局之外，也沒有會被阻止或沒收之類的實體貨幣限制。雖然在這本書撰寫的年代裡，一切似乎像是一種相當古怪的預測，但它現在已經成為全世界數百萬人使用的活生生現實事件，當然它的重要性可能還需要被廣泛理解才行。

比特幣和一般的密碼技術是「防禦性」的技術，可讓保護財產和資訊的成本，遠低於攻擊的成本。它使竊盜的行為變得極其昂貴和不確定，因而有利於任何想要和平生活，不想侵略別人的人。比特幣花了很長的一段時間，用來糾正上個世紀出現的權力失衡，因為當時政府將資金投入中央銀行，並讓個人完全依賴銀行來維持生存和福利。歷史上的健全貨幣版本，並不具備數位貨幣的這些優勢。黃金的物理性質使其容易受到政府控制，大量黃金也無法輕易移動，因此用它進行支付的話，必須集中在一般銀行與中央銀行，這便讓政府「沒收」黃金的動作變得很容易。

從另一方面看，使用比特幣來驗證交易非常輕鬆，幾乎不必花費成本，因為任何人都可以從連接網際網路的各種設備，免費造訪交易分類帳<sup>註5</sup>。雖然比特幣的推廣可能需要第三方中介的推行，但它跟黃金結算有幾個重要的不同之處。首先，第三方交易最後會在公開取得的分類帳上進行結算，從而提高帳目的透明度和審計的可能性。其次，比特幣也能為現代個人提供「退出」極權主義、管理主義、凱因斯主義和社會主義國家的選擇機會。對於這些「剝削」居住在他們土地上的生產者而存活的政府，比特幣便是對這種「現代瘟疫」的最簡單「技術解決」方案。如果比特幣繼續成長而占全球財富的更大份額時，可能就會迫使政府變得越來越像一種「自願型」的組織形式，只能透過提供人民願意支付的主題服務，讓他們「自願」繳稅。

關於比特幣的政治願景，我們可以透過研究比特幣源頭的「密碼運動」思想，加以理解。用 Timothy May 的話來說就是：

強大、牢不可破的公鑰密碼學，結合網路空間中的虛擬網路社群，將在經濟和社會系統的本質上，產生有趣、深刻的變化。「加密無政府狀態」是在網路空間上實現的無政府資本主義，超越國界，讓個人自由做出希望達成的經濟安排……加密無政府狀態正在從他們的實體鄰居（法幣）及政府手上，解放個人自由。這些鄰居根本沒辦法知道他們到底是網路上的什麼人。對自由主義者來說，強大的加密技術提供了避開政府的方法<sup>註6</sup>。

---

註5 具有網際網路功能的設備以及網際網路連接線都很便宜，而且變得越來越便宜。

註6 Timothy C. May,「加密無政府狀態和虛擬社區（*Crypto Anarchy and Virtual Communities*）」，1994年，可參閱 [nakamotoinstitute.org](http://nakamotoinstitute.org)。



May 所描述的「無政府資本主義」願景，便是奧地利學派的美國經濟學家 Murray Rothbard 所提出的政治哲學。在《自由的倫理》（*The Ethics of Liberty*）中，Rothbard 將自由主義者的無政府資本主義，解釋為自由意志和自我所有權理念上，唯一的「邏輯連貫」含義：

另一方面，考慮自由倫理的普遍狀態，以及在這種倫理下所獲得的人身和財產的自然權利時，每個人在任何時間或地點，都可被以下這些基本規則所涵蓋：一個人擁有「自己」的所有權、擁有已佔用和轉變過的「過去未用資源」所有權；以及源自該基本所有權而得來的「所有頭銜」的所有權，不論「頭銜」是透過自願交換或自願給予的禮物均可。這些規則——我們稱之為「自然所有權規則」——均可明確應用。無論時間或地點如何，也不管社會的經濟成就如何，這種倫理下的「所有權」都會得到保護。任何其他社會制度都不可能成為普遍的自然法則；因為若某個人或某團體對另一個人（或霸權規則的參與者）有任何強制規則，就不可能對所有人套用相同規則。因此只有在一個沒有統治者、純粹自由主義的世界，才能滿足自然權利和自然法則的資格，或者更重要的是，可以滿足全人類「普遍道德」的條件<sup>註7</sup>。

不侵略原則是 Rothbard 無政府資本主義的基礎。在此基礎上，無論來自政府或個人的任何侵略，都不具有道德的正當性。而比特幣完全是自願的、認真的和平，為我們提供了完全基於「自願合作」的世界貨幣基礎設施。跟一般描繪無政府主義者的「帽 T 式流氓裝扮」的刻板印象有所不同，比特幣的無政府主義招牌完全是和平的，為個人提供了免於政府控制和通貨膨脹所必需的工具。它試圖將自己交給任何可能的人，如果它成長

---

註7 Murray Rothbard，「自由的倫理（*The Ethics of Liberty*）」，紐約，NY：紐約大學出版，1998 年，第 43 頁。

並且取得成功，那麼它的功勞便是讓自己作為一種「和平的」中立技術，以便獲得金錢和解決方案，絕非「強加給」別人的技術。

在可預見的未來，由於比特幣仍然處於非常低的「普遍接受」水平，因此可以為那些需要「繞過」政府在銀行業限制的人，提供一個具有成本效益的選擇，也可不受政府通貨膨脹的影響，並以「動態價值」的方式儲存財富。如果它被廣泛採用的話，那麼比特幣鏈上交易成本可能會大幅上升，正如之前關於「擴展規模」所討論的那樣，對個人來說較難繞過政府規則與限制，去執行不被察覺的線上交易。然而在此情況下，比特幣的廣泛採用，也會降低政府透過通貨膨脹提供資金的能力，而對個人自由產生更大的正面影響。二十世紀的政府貨幣允許了「重度干涉管理型國家」出現，因此帶有極權主義和專制主義的色彩。而在使用健全貨幣的社會裡，政府因為無法強制干涉經濟生產，因此不太可能長期生存下去，因為沒有東西能資助它們繼續運作。

## 國際化與線上結算

過去黃金是全球支付結算和儲存價值的媒介，任何組織都無法大量增加其供應量。它的價值來自自由市場，並非任何人必須擔負的責任。當十九世紀的通信和旅行的範圍逐漸擴大，需要距離更長的金融交易時，黃金便從人們手中釋出到一般銀行金庫，最後則進入中央銀行。然後在黃金標準下，人們會持有紙張收據形式的黃金或寫下支票來代替，不需要搬移實體黃金，因此可以大幅改進全球貿易的速度與效率。

由於政府沒收黃金並發行自己的貨幣，個人和銀行之間的全球結算工作，不再以黃金來完成，而是變成以國家貨幣浮動價值進行結算，因而如

第 6 章所說，為國際貿易帶來重大的問題。比特幣的發明從根本上，為國際結算創造了一種新的獨立替代機制，它不需依賴任何中介，便可完全獨立於現有金融基礎設施之外運作。

任何使用比特幣節點的人，都能在未經許可的情況下發送自己的貨幣，而且不會暴露身分的這種能力，便是黃金和比特幣之間的重要差異。比特幣並不一定要儲存在電腦上；你的比特幣存款私鑰，是一串可以記下來的字元或單字。移動比特幣私鑰當然會比搬動金庫更輕鬆，也更容易傳送到世界各地，不必冒被偷竊或沒收的風險。政府收回人民的黃金儲蓄，強迫他們使用據說是由黃金儲備支持的貨幣進行交易。但你可以將大量比特幣儲蓄存放在政府碰不到的地方，並且可以用很少的數量，透過中間人進行交易。跟其他貨幣形式比起來，比特幣技術的本質會使政府處於嚴重劣勢，使得沒收更加困難。

此外，擁有比特幣的人，可追蹤區塊鏈上所有比特幣資產的這種能力，會使權力機構覺得把處理比特幣的銀行，當成「最後貸款人」會很不切實際。即使在貨幣可以兌換成黃金的國際黃金標準鼎盛時期，中央銀行也很少會有足夠的黃金來支付全部的貨幣供應，因此很可能會增加紙幣供應量來支援貨幣兌換。這點對比特幣來說要困難得多，因為比特幣會給會計部門帶來加密數字的確定問題，如此也有助於揭露出只有局部儲備的銀行之不足。

未來使用比特幣進行小額支付，可能不會透過散佈式分類帳進行，如同第 10 章將討論到關於「規模大小」所解釋的那樣，可能會透過「第二層」架構來進行。比特幣可被視為線上交易的新興儲備貨幣，類似線上銀行的組織將向用戶發行以比特幣作為儲備支持的代幣，並將比特幣保存在「冷儲存 (cold storage)」中，每個人都能夠即時審查中介機構持有的數量，也可以透過線上驗證和徵信系統來驗證是否發生通貨膨脹。這將允許線上執行無限數量的交易，而無需為區塊鏈上的交易支付高額交易費用。

隨著比特幣繼續朝著具有更高市場價值和更高交易費用的方向發展，它開始變得越來越像一種儲備貨幣，而非日常貿易用或交易時的貨幣。即使在本文撰寫時，比特幣仍處於相對較低的大眾接受程度。多數比特幣交易都沒被記錄在區塊鏈上，而是發生在交易所與使用比特幣的各類型線上平台，例如賭博和賭場網站等。這些企業透過自己的「內部記錄」向客戶貸出或借入比特幣，然後在客戶確實存入或取出資金時，才在比特幣網路上進行交易。

雖然有著「數位現金」的優點，但比特幣在比較上的優勢，可能不是在於「取代」現金支付，而是在於允許「遠距離」現金支付。過去一般個人小額付款，可以透過多種選擇進行：例如實體現金、以貨易貨、優惠、信用卡、銀行支票等。而現在支付結算領域的先進技術，讓我們有了更多的支付選擇，並且是以極低的成本解決了小額支付的問題。因此比特幣的優勢可能不在於跟這些少量、短距離的支付競爭；比特幣的競爭優勢，在於將現金結算的最終結果帶入數位世界，亦即它創造出了最終結算的最快速方法，可以超長距離和跨越國家邊境的進行大額支付。跟那些小額近距離支付相比，比特幣有了明顯的優勢。只有少數貨幣可以全球性的接受支付，例如美元、歐元、黃金和國際貨幣基金組織的「特別提款權（Special Drawing Rights）」。絕大多數國際支付都是以其中之一來計價，其他幾種主要貨幣只佔了很小的支付比例。要在國際上以這些貨幣發送幾千美元的價值時，成本通常需要數十美元，並花上幾天時間，還必須接受金融機構「法醫式侵入」檢查。這些交易的高成本主要在於交易貨幣的波動，以及不同國家、機構之間的結算問題，因為需要用到多層中介的協助。

在不到十年的時間裡，比特幣已經實現了相當程度的全球流通性，用在國際支付的代價也遠低於現有的國際轉帳。這並不是說比特幣將取代國際匯款市場，而是純粹說明它在國際流通的潛力。目前這些國際流通的數量，遠遠大於比特幣的區塊鏈可以處理的數量，如果更多這類大額支付轉移到比特

幣時，交易費用便會上升以限制其需求。事實上這點對比特幣也不會有任何影響，因為發送這些個人付款，並不會超過比特幣的負擔能力。

比特幣是沒有「對手風險（counterparty risk 指對方不履行合約）」的貨幣，其網路可以在幾分鐘內提供大額支付的最終結算。因此，我們最好將比特幣理解為跟中央銀行與大型金融機構之間「競爭」結算付款，而且由於它可以驗證的記錄、加密安全性以及對第三方安全漏洞的隱蔽性，讓比特幣在相較之下更為有利。使用主要國家貨幣（美元、歐元）結算時，本身便有貨幣匯率波動的風險，也會涉及現有各層交易中介的信任度。中央銀行和大型金融機構之間的結算需要幾天時間，有時甚至要數週才能算清楚。因此在結算期間，各方均需面對重大外匯交易和對手風險。黃金是唯一無責任的傳統貨幣媒介，因此沒有交易對手的風險，但搬移大量黃金是一項極其昂貴的操作任務，且過程充滿了風險。

比特幣既沒有交易對手風險，也不必依賴任何第三方驗證，特別適合扮演黃金在「黃金標準」中擔任的角色。就國際金融體系的角度而言，比特幣不會給任何國家提供「過高的特權」來發行全球儲備貨幣，也不必依靠自己的經濟表現，所以屬於一種中性貨幣。由於比特幣獨立於任何特定國家的經濟之外，因此它的價值不會受到貿易結算量的影響，可以避免困擾二十世紀的所有匯率問題。此外，比特幣的最終結算並不依賴於任何交易方，而且不需任何單一銀行做為實際仲裁者，因此它可以成為全球「對等網路」的理想選擇，而非依賴全球霸權的集中指示。比特幣網路基於一種貨幣形式，其供應量無法被任何單一成員銀行所膨脹，使它成為比國家貨幣更具吸引力的儲存價值提議。因為一般國家貨幣的創建用意，便是增加供應來為政府提供資金。

即使每天都結算帳戶，比特幣的交易能力，仍遠遠超過目前中央銀行所需的數量。比特幣目前每天約 350,000 筆的交易量，可以讓每個 850

家銀行的全球網路，每天與網路上的其他銀行進行一次交易（網路中特定連結的數量等於  $n(n-1)/2$ ，其中  $n$  是節點數）。

850 個中央銀行的全球網路，可以透過比特幣網路來相互進行每日的最終結算。如果每個中央銀行為大約 1000 萬客戶提供服務，那就可以涵蓋到整個世界的人口。這是先假設比特幣的容量不會以任何方式增加，也就是在最糟糕的情況下。如同我們將在下一章中所討論的觀點，即使不以「反向不兼容（不管舊記錄）」的方式來改變比特幣的架構，也還有幾種方式可以增加分類帳的記載容量，以允許數千家銀行之間的日常結算。

在一個沒有政府可以創造更多比特幣的世界裡，這些比特幣中央銀行將會相互自由競爭，努力提供實體和數位方式的「比特幣支持」貨幣工具，以及「比特幣支持」的支付解決方案。如果沒有最後的貸款人，局部準備金銀行的各項業務，將成為非常危險的安排。因此我希望從長遠看，唯一能夠生存的銀行形式，將會是 100% 由比特幣支持的金融工具。然而，這是經濟學家爭論的焦點，只有時間能夠證明情況是否會如此。這些銀行將在比特幣區塊鏈之外的客戶間結算付款，然後透過區塊鏈在銀行彼此之間，進行最後的每日結算。

雖然這種比特幣的觀點，聽起來可能像是背叛了比特幣最初的「完全點對點」現金的願景，但這並不是一個新的願景。來自中本聰的第一個比特幣交易接收者 Hal Finney，在 2010 年的比特幣論壇上寫道：

事實上，「比特幣支持」的銀行有非常好的存在理由，也就是發行自己的數位現金貨幣，用來兌換比特幣。比特幣本身並無法擴展到世界上每一筆金融交易，然後向所有人發佈交易並將記錄包含在區塊鏈中。因此比特幣需要有一個更靈活也更有效率的二級支付系統。同樣地，比特幣完成最終交易所需時間，對中等到大量價值的購買，也顯得不切實際。

但比特幣支持的銀行將會解決這些問題，也可以像在貨幣國有化之前的銀行那樣工作。而且不同的銀行可以有不同的政策，有些比較積極、有些比較保守、有些是局部儲備、有些則可能是100%比特幣支持。利率也可能會有所不同，某些銀行的現金可能會以低於其他銀行的優惠價格進行交易。

George Selgin 仔細研究了「競爭性自由銀行」理論，他認為這種系統將會穩定、抗通貨膨脹且能自我調節。

我相信這將成為比特幣的最終命運，也就是變成「高能貨幣」，作為發行「數位現金」銀行的儲備貨幣。大部分比特幣交易將會發生在銀行之間，用來結算淨轉帳。私人交易比特幣將較為罕見…… 好吧，就像現在以比特幣為基準的購買行為一樣<sup>註8</sup>。

比特幣經濟體的交易數量仍可以像現在一樣多，但這些交易的結算，不會發生在比特幣的分類帳上，因為分類帳資料的恆久不變與信任度，沒必要浪費在一般個人消費支付。無論當前支付解決方案的侷限性如何，都將因為把「自由市場競爭」帶進銀行和支付領域（也就是帶入現代世界經濟中最僵化的產業之一）而大量獲益。因為自由市場可以解決僵化，讓政府所控制的銀行和支付，不再用來創造政府運作的資金。

如果比特幣價值繼續成長，並且可以被更多的金融機構使用，它就會成為「新形態中央銀行」的儲備貨幣，這些中央銀行可以存在於數位世界或實體世界。但如果國家中央銀行想用比特幣來補充儲備的話，可能就要深入思考。因為在目前全球貨幣體系中，國家中央銀行主要以美元、歐元、英鎊、IMF 標準提款權與黃金作為儲備。這些儲備貨幣除了用來結算

---

註8 比特幣對話論壇，2010年12月30日。你可在<https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211> 觀看。

中央銀行之間的帳戶，還擔負著捍衛各國貨幣市場價值的責任。如果比特幣以過去幾年所經歷的方式繼續升值，它很可能會吸引中央銀行「放眼未來」的注意力。

若比特幣持續升值，便可為中央銀行的貨幣政策與國際帳戶結算，提供更多靈活性。但也許目前中央銀行想持有比特幣的真實情況，是為了對後續發展情況的保險措施。由於比特幣的供應受到嚴格限制，中央銀行如果花點錢來獲得一小部分比特幣，可能會是個明智之舉，因為可以用來「預防」比特幣價格持續飛漲的情況。若比特幣繼續升值而中央銀行完全未持有任何比特幣，那麼他們自己的儲備貨幣和黃金的市場價值，將會因比特幣的升值而下降，也使得中央銀行若在以後決定收購儲備時，處於劣勢。

比特幣目前可能仍被許多人視為一個奇怪的網際網路實驗，但隨著時間經過，它也繼續的生存和升值，並且開始吸引追求高淨值的個人、機構投資者，然後可能是中央銀行的真正關注。中央銀行開始使用比特幣的時機，便是全部銀行都會參與的比特幣反擠兌運作。因為第一個購買比特幣的中央銀行，等於在提醒其他央行注意這種可能性，並使許多銀行急於採取行動。第一家購買的中央銀行，應該會讓比特幣的價值大幅上漲，從而使後來的銀行購買成本越來越高。在這種情況下，最明智的做法是讓中央銀行先購買一小部分比特幣。如果中央銀行有制度上的能力，可以購買貨幣而不必宣布出來，會是更加明智的行動方案，可以讓中央銀行以低價累積比特幣。

比特幣也可以在面臨國際銀行業務限制，或對以美元為中心的全球貨幣體系不滿意時，用來作為中央銀行有用的儲備資產。採用比特幣儲備的可能性本身，便在它可以作為中央銀行與美國貨幣當局之間，討價還價的「籌碼」，當局應該不願意看到任何中央銀行背叛，把比特幣當成結算方法之一，因為這會吸引其他人一起參與。



雖然中央銀行大多忽視比特幣的重要性，但這可能是他們必須長期承受的昂貴代價。儘管要中央銀行家認定這個事實可能比較困難，但比特幣確實是其業務上的直接競爭對手，而且該業務已經被市場競爭封鎖了一整個世紀。比特幣讓支付和最後結算的全球匯款處理上，可以用較低的成本執行，還能以優越、可預測的演算法，取代人為導向的貨幣政策。因此現代中央銀行的商業模式正在被打亂，中央銀行現在無法像過去一樣，透過法律來阻止競爭，他們現在面對的是數位競爭對手，可能無法用現實世界的法律來加以約束。如果國家中央銀行不使用比特幣的即時清算以及穩健的貨幣政策，便是在為數位新興企業打開大門，讓他們從這個市場獲取更多價值儲存與結算成果。

假設現在是古羅馬時期，正在遭受貨幣崩潰的經濟後果，接著把美元比做 aureus，中本聰就像是我們這個時代的君士坦丁，比特幣就是他的 solidus，而網際網路就是君士坦丁堡。比特幣對於那些被迫在政府不斷貶值的貨幣媒介裡進行交易和儲蓄的人來說，就像是一艘貨幣的「救生艇」。根據前面的分析，比特幣的真正優勢在於它是一種可靠長期的儲存價值，是一種允許個人進行「無授權交易」的主權貨幣形式。在可預見的未來，比特幣的主要用途將來自這些競爭優勢，而不是提供無所不在或低廉交易費用的能力。

## 全球計價單位

比特幣的最終應用並非很快就能具體實現，但鑑於比特幣的獨特性，仍會激起人們的好奇心。自黃金標準時代結束以來，全球貿易受到不同國家貨幣價值差異的阻礙，破壞了人們使用單一交換媒介進行間接交換的能力，反而建立了一個奇怪的模仿「以物易物」的世界，因為在跨境購買東

西之前，還必須先購買生產者的當地貨幣。因而嚴重阻礙了人們跨境經濟計算的能力，並導致大規模外匯產業的成長。而且這個行業產生的價值很小，實際上只是在改善貨幣民族主義的可怕後果。

黃金標準為這種外匯問題提供了解決方案，用單一形式的貨幣，獨立於任何一個政府或機構的控制之外，以作為全世界的貨幣標準。各種貨幣價格可以根據黃金進行校準，並以黃金單位來表示，以方便跨境計算。然而，黃金的實體重量讓它必須被集中管理，並在中央銀行之間進行結算。而一旦黃金集中起來，其誘惑性就讓政府無法抗拒，隨後政府控制黃金，然後以他們更能控制供給量的法定貨幣加以取代，結果就讓健全貨幣變得不再健全。

比特幣是否有可能作為全球貿易和經濟活動的計價單位，目前還是個爭議性的問題。為實現這種可能性，比特幣必須被世界上的大多數人使用，最可能的情況就是將它作為儲備貨幣的「間接」使用。然後觀察比特幣供應的穩定性，是否也會使它的價值一起穩定下來，因為與持有的數量相比，比特幣的日常交易量將顯得微不足道。目前由於比特幣佔全球貨幣供應量的比例不到 1%，因此對比特幣的大量個人交易，便可對價格產生極大影響；需求上的微小變化，亦可能導致價格的大幅波動。然而這只是目前情況的特性，因為現在比特幣作為全球結算網路和貨幣的角色時，仍然只占全球結算付款和貨幣供應的一小部分。今天購買比特幣的情況，可被視為對「網路快速成長」與「貨幣作為價值儲存」上的投資，因為它占額仍然很小，並且可以讓規模與價值都快速的翻倍成長。如果比特幣在全球貨幣供應和國際結算交易中的份額，變成全球市場的主要份額時，那麼對它的需求水平就更能預測和穩定下來，從而導向貨幣價值的穩定。假設比特幣成為世界上唯一使用的貨幣，那麼它將不再具有較大的增值空間。到了那個時候，對它的需求將變成只是持有流動資金的需求，目前所看到的「投機性」投資需求也將消失。在此情況下，比特幣的價值會隨著整個

世界人口的「時間偏好」而變化，當比特幣作為價值儲存的需求增加時，將導致其價值微幅升值。

若從長遠來看，不受任何威權控制供應量的比特幣，創造出來的價格波動可能會逐漸減少。因為比特幣可預測的供應量與用戶數量的成長相互結合，可以降低比特幣需求在日常波動下所左右價格的程度，造市商（market maker）也可以利用對沖的方式來平緩供需波動，創造更穩定的價格。

這種情況類似於黃金標準下的黃金（詳見第 6 章所提到 Jastram 的研究）。幾世紀以來，當黃金作為貨幣標準時，在供應的穩定和逐步增加下，它的價格並不會明顯增加或減少，因此黃金得以成為跨越時、空交易的理想貨幣單位。

但是這種情況忽略了黃金和比特幣之間的根本區別，也就是黃金在工業和裝飾應用中，具有大量且高度彈性的需求。黃金獨特的化學性質，確保無論其貨幣角色如何，始終都能處於高需求狀態。即使黃金作為貨幣的需求發生變化，例如貨幣需求減少而導致金價下跌，但在工業上仍已準備好無限量的使用黃金。黃金的特性也讓它成為多種產品用途上的最佳選擇，這些產品可能因為黃金價格昂貴，才會選擇較劣質的替代品。即使全球中央銀行都處理掉所有的黃金儲備，在珠寶業和工業上的黃金需求，仍可能會吸收所有多出來的供應量，因而金價只會暫時降低。地殼裡蘊藏量的稀有性，可以確保黃金相對於其他材料和金屬而言，仍然是昂貴的。這種特性有助於黃金崛起作為貨幣的角色，而不必擔心國家是否使用黃金標準，或黃金作為貨幣需求的全球性變化如何，因為該特性可以確保黃金隨著時間經過，仍然具有相對穩定的價值。這種相對穩定性反過來鞏固了黃金作為貨幣資產的吸引力，並確保了大家對黃金的需求，當然也可以理解

為中央銀行在停止貨幣兌現黃金後幾十年內，不肯出售黃金儲備的真正原因。如果中央銀行出售其黃金儲備，其淨效應將是未來幾年在工業應用上，使用更多的黃金，對黃金價格的實際影響非常有限。在這樣的交易中，中央銀行只會獲得本來就可以自己印製的法定貨幣，然而卻會失去比法定貨幣更有價值的資產。

對於比特幣的等值「非貨幣」需求，可以理解為持有人並非想要作為價值儲存，而是作為使用這個網路的先決條件。但這點跟工業對黃金的需求完全不同，他們的黃金需求完全獨立於貨幣需求之外，因此對比特幣營運網路的需求，跟對作為價值儲存的需求密不可分。我們不能期望比特幣一邊加重自己的貨幣角色，一邊又能改善市場價值的波動性。

從這個方面看，比特幣嚴格的稀有性，使它成為一個非常具有吸引力的價值儲存選項，而且如果它持續看漲，應該會有越來越多的持有者願意長期忍受波動，就像目前的情況。從另一方面看，比特幣價值持續波動，將妨礙它作為計價單位的作用，而且前提是至少要等到比特幣成長為當前的數倍價值，然後也有一樣多的全球人口百分比接受它，才有機會。

然而考慮到目前的世界人口，只曾生活在波動不停的法定貨幣相互轉移世界裡，因此比起穩定黃金標準下孕育的幾代人來說，比特幣的持有者應該更能容忍波動性。只有最好的法定貨幣可以在短期內保持穩定，但法定貨幣在長期下的貶值是顯而易見的。而黃金一直保持了長期的穩定，但短期內也有機會變得相對不穩定。因此比特幣缺乏穩定性這點，似乎不會成為阻止成長和使用的致命缺陷，因為所有貨幣的替代品也都相對不穩定。

目前這些問題並無法得到明確答案，只有現實世界才能說明這些動態將會如何開展。貨幣價值起伏狀態是人類行為的自發性產物，而不是人類

設計出來的理性產物<sup>註9</sup>。個人的行為出於自身利益、技術可能性和供應與需求的經濟現實，決定了他們行為的結果，讓他們想要堅持、調適、改變或創新。

這些複雜的相互作用，產生了一種自發性的貨幣秩序；這是一種並非透過學術辯論、理性規劃或政府授權所產生的秩序。在理論上看似更好的貨幣技術，在實踐中不一定能取得成功。比特幣的波動性可能會使貨幣理論家將它視為又一種貨幣媒介而忽略，但貨幣理論並無法超越人類行為所導致市場上出現的自發秩序。比特幣作為一種價值儲存時，可能會繼續吸引更多的儲蓄需求，導致它與所有其他形式的貨幣相比，繼續大幅增值，直到最後變成任何尋求獲利人士的首選。

如果比特幣能達成某種價值上的穩定，它將優於使用本國貨幣進行全球支付結算，就像今天的情況一樣。因為國家貨幣的價值波動是依據每個國家和政府的設定條件，而當它們被廣泛採用為全球儲備貨幣時，對發行國家來說，也造成了「過高的特權」。正常的國際結算貨幣，應該要能對不同國家的貨幣政策保持中立，這也就是為何黃金在國際黃金標準期間，能夠發揮卓越作用的原因。比特幣在扮演這個角色方面，會比黃金更有優勢，因為它的結算可以在幾分鐘內完成，而且交易的真實性可以透過任何有網際網路連線的人快速驗證，幾乎不需任何費用。另一方面，黃金需要更多的運送時間，其清算也仰賴負責結算和轉移黃金的這些具有「不同信任程度」的中介機構。因此黃金可以維持在面對面現金交易中的貨幣角色，而把比特幣用在專注於國際結算。

---

註9 有關此一重要差異的更多資訊，請參閱 Adam Ferguson，「一篇關於公民社會歷史的論文（*An Essay on the History of Civil Society*）」，倫敦：T·Cadell，1782年。另見 Vernon Smith，「經濟學中的理性（*Rationality in Economics*）」，紐約：劍橋大學出版社，2008年。

# 10

## 比特幣的疑問

---

**根** 據第 8 章解釋比特幣運作的經濟基礎，以及第 9 章討論到比特幣的主要潛在使用案例，本章將討論圍繞比特幣運作的一些最明顯的問題。

### 比特幣採礦是一種資源浪費嗎？

---

加入比特幣網路的任何人都會生成一組公共地址和一個私鑰。其作用類似於電子郵件地址及密碼：當你使用私鑰從帳戶發送比特幣時，人們可以將比特幣發送到你的公共地址。這些地址也可以用 QR code 條碼格式呈現。

進行交易時，發送者將其廣播給所有其他網路成員（節點），大家可以驗證發送者是否擁有足夠的比特幣來實現交易，並驗證他並未將這

些比特幣也花在其他交易上。一旦交易被比特幣網路上的多數節點驗證，就會被記錄在所有網路成員共享的公共分類帳上，讓所有成員都更新這兩個交易成員的餘額。雖然任何網路成員都可輕易驗證交易的有效性，但這種給每個成員都有一票的投票系統，也可能被駭客以創建大量節點投票，驗證自己的假交易。因此只有透過成員所花費的「處理週期」來建立認證的準確性，換句話說，就是採用「工作量證明」系統，比特幣才能解決「雙重支付」的假交易問題，無需信任第三方的驗證。

從本質上看，工作量證明涉及網路成員彼此之間，競相解決難解但易於驗證的數學問題。在十分鐘間隔內驗證的所有比特幣交易，都被轉錄並組合成一個區塊。節點會相互競爭以解決某個交易區塊的 PoW 數學問題，第一個產生正確解決方案的節點，將答案廣播給網路上的成員，網路成員可以非常快速地驗證其正確性。一旦大多數網路節點驗證了交易和 PoW 的有效性，就會發出一定數量的比特幣以獎勵正確解決 PoW 的節點。獎勵所獲得的比特幣稱為「區塊補貼」，而產生新比特幣的過程便被稱為「採礦」，因為它是增加比特幣供應的唯一方式，就像採礦是增加黃金的唯一方法一樣。在區塊補貼以外，正確解決 PoW 問題的節點，也會獲得發幣者給予的交易費用，交易費用和區塊補貼的總和便是區塊獎勵。

儘管乍看之下，解決這些問題似乎是對計算能力與電力的浪費，但工作量證明對於比特幣的運作非常重要<sup>註1</sup>。藉由電力和處理能力的支付來產生新比特幣的做法，讓 PoW 成為目前為止，發現到的唯一一種可靠與昂貴

---

註1 比特幣是否浪費電力的問題核心，在於對「價值」基本主觀性質上的誤解。全世界產生了大量電力以滿足消費者需求，而電力是否被浪費的唯一判斷標準，應該在於支付費用的消費者。願意支付比特幣網路營運成本的人，因為處理交易所獲得的獎勵，有效的為消耗的電力提供了資金，也就是說電力的生產是為了滿足消費者的需求，而且沒有被浪費掉。從功能上來說，PoW 是人類為創造數位硬幣而發明的唯一方法。如果人們發現值得付出代價，這些電力就不算浪費。

的數位商品生產方法，也使比特幣得以成為一種健全貨幣。找到數學問題的解決方案，必須消耗掉大量處理能力和電力，讓花費時間與處理能力的節點，有非常強烈的動機，不會想在區塊中包含任何無效交易，以便可以接收區塊獎勵。因為驗證交易與 PoW 解決方案的效率，比起 PoW 的解決過程要便宜得多，所以想將無效交易輸入區塊的節點，幾乎注定會失敗，因為它們花掉的處理能力，並不會得到回報。

PoW 使得寫入區塊的成本變得非常高，而驗證其有效性的成本卻非常低，因此幾乎可以消除任何嘗試創建無效交易的動機。如果有人真的嘗試了，就變成浪費電力和處理能力又得不到區塊獎勵。因此比特幣可以理解為透過付出處理能力，將電能轉換為真實記錄的一種技術。那些花費電力的人會得到比特幣的獎勵，因此有強烈的動機來保持比特幣紀錄的完整性。由於這種技術為誠實交易提供了強有力的經濟動機，因此比特幣的分類帳到目前為止，在營運期間幾乎是無法破壞的，完全沒有任何「雙重支付」攻擊被確認成功交易的案例。這種交易比特幣分類帳的完整性，不必依賴任何一方誠實的情況下即可實現。只依靠驗證，比特幣就能使詐騙交易失敗，且無需信任任何人便能完成交易。

如果攻擊者試圖將詐騙交易插入比特幣分類帳，就必須讓網路上的大部分處理能力，接受他的詐欺行為。而網路中的誠實節點，並不會有這樣做的動機，因為這麼做會破壞比特幣的完整性，讓他們自己獲得的回報貶值，浪費已經花費的電力和資源。因此，攻擊者唯一的希望就是動員一定數量的處理能力，也就是達到比特幣網路構成的 50% 以上，來驗證他的欺詐行為，並將其構建為好像是有效的交易。在比特幣早期，網路背後的總處理能力規模還小時，這種舉動本來是有可能的。但由於當時比特幣網路中的經濟價值，幾乎不存在或者微不足道，因此並沒有人想實現這種攻擊。而隨著網路的不斷發展和更多成員所帶來的處理能力，攻擊比特幣網路的成本也不斷上升。



對驗證交易節點的獎勵，便可證明是處理能力的有效利用。2017 年 1 月，比特幣網路背後的處理能力，已經相當於 2 兆台消費型筆電。比起世界上最大的超級電腦處理能力還大 200 萬倍以上，比起世界前 500 強超級電腦的處理能力總和，也要大上 20 萬倍。透過直接產生貨幣的處理能力，讓比特幣成為世界上最大的單一用途電腦網路。

處理能力成長的另一個影響因素，便是交易驗證和 PoW 問題的解決節點，已經從個人電腦進步到專門設計的專用處理器，以便能在運行比特幣軟體時，達到最佳效率。這些應用集成電路（ASIC）於 2012 年首次推出，它們的出現使比特幣網路的處理能力更加有效，因為任何「非比特幣專用處理元件」的其他無關計算過程，都不會跳出來浪費電力。獨立專門礦工的全球分散式網路，已經可以保護比特幣分類帳的完整性。因為這些礦工都沒有別的目的，只會專心驗證比特幣交易和解決工作量證明。如果比特幣因為任何原因而失敗，這些 ASIC 礦機會變得完全無用武之地，其擁有者的投資將完全白費，因此他們有強烈的動機來維護比特幣網路的誠信。

想要改變網路記錄的人，必須投入數億美元（或數十億美元），建造新的 ASIC 處理器來改變現狀。就算攻擊者成功的改變了記錄，可能也無法從中獲得任何經濟利益，因為破壞比特幣網路之後，會讓比特幣的價值崩跌而趨近於零。換句話說要破壞比特幣，攻擊者不僅要花很多錢，而且根本沒有回報。事實上，即使這樣的嘗試成功，網路上的誠實節點，也可有效地返回攻擊之前的交易記錄並恢復操作。然後攻擊者必須繼續負擔大量的運行成本，以繼續攻擊這些誠實節點所產生的共識。

在早期的時候，比特幣用戶運行節點，並用它們來執行自己的交易，然後驗證彼此的交易，因此每個節點同時都是錢包、驗證者與礦工。但隨時間演進，這些功能已經被大幅分開。ASIC 處理器現在專門用於驗證交易，以接收區塊獎勵（也就是他們通常被稱為礦工的原因），節點營運商可

以產生無限的錢包，讓企業為用戶提供方便的錢包，以方便發送和接收比特幣，而不必自行操作節點或在驗證交易上花費處理能力。這點讓比特幣可以脫離各相同節點之間的純粹對等網路，但是主要的去中心化功能重點以及比特幣網路的分散式性質，依舊完好無缺，因為大量節點仍然存在，不會倚重任何一方來運作網路。此外，專門的採礦方式，也讓支持網路的處理能力，已經成長到它所能達成的驚人規模。

早期價值很低或幾乎沒有價值的時候，比特幣網路本來有可能被攻擊者劫持與摧毀，但由於這個網路的經濟價值不大，似乎還沒驚動任何人。隨著網路上的經濟價值增加，攻擊網路的動機也可能會增加，但這樣做的成本上升得更多，因此並沒有被攻擊的情況發生。但也許比特幣網路在任何時間點下的真正保護，來自比特幣的價值完全取決於網路的「完整性」。任何成功改變區塊鏈、竊幣或重複支付的攻擊，對攻擊者來說都沒什麼價值，因為對所有比特幣網路成員來說，都可能破壞網路，嚴重降低使用網路與持有比特幣的需求，因而造成價格崩跌。換句話說，比特幣網路的防禦不只在於攻擊的代價昂貴，即使攻擊成功，攻擊者的戰利品也會變得毫無價值。作為一個完全自願的系統，比特幣只有在誠實的情況下才能運作，否則用戶很容易就會離開。

比特幣處理能力的分散，以及改變代碼會遇上的強大阻力，加上毫不妥協的貨幣政策，都使比特幣能夠生存下來，並在價值上增長到如今的程度。新手很難理解比特幣在這些年來，必須承受多少邏輯與安全性的挑戰，才能達到目前的規模。請牢記網際網路為駭客創造了多少機會，讓他們攻擊各種網路和網站來獲得樂趣和利潤，因此比特幣的成就也變得越來越令人吃驚。全世界的電腦網路和電子郵件伺服器，每天都有越來越多的安全漏洞，這些系統為攻擊者提供的多半是獲取數據或機會的政治目的。從另一方面看，雖然比特幣價值數十億美元，卻仍能繼續安全可靠的運作，這是

因為它從建立的第一天開始，便在高度敵對的環境中運行，經常要面對無情的攻擊。因為全世界的惡意程式人員和駭客，都試圖使用各種技術加以破壞，不過它仍舊能夠按照精確的本質規範繼續運作。

## 失控：為何沒有人可以改變比特幣

「比特幣的本質是一旦 0.1 版本發佈後，其核心設計便會在剩下的生命週期中，持續保持穩定。」

—*Satoshi Nakamoto*（中本聰），2010 年 6 月 17 日

比特幣的彈性特質到目前為止，並不侷限於成功擊退攻擊而已；它還可以抵制任何變更或修改特性的企圖。大部分懷疑比特幣的人，都未能充分認識這種說法的真實深度與含義。如果把比特幣與中央銀行進行比較，它將會是世界上最「獨立」的中央銀行。如果把比特幣與民族國家進行比較，它也會成為世界上主權最獨立的民族國家。比特幣的主權源於這樣的事實：大家都知道，比特幣共識規則的運作方式，會讓大家非常抵制對它的變動。因此可以毫不誇張地說，沒有人可以控制比特幣，人們唯一選擇的是使用它或不使用它。

這種「不變性」並非比特幣軟體才有的特點，對任何具有編碼技術的人而言，改變比特幣的程式代碼並非難事。但比特幣是以貨幣和網路經濟為基礎，其難度在於讓每個成員都接受對軟體進行相同的更改。允許個人連接到比特幣網路節點的軟體，是以「開源軟體（open source software）」的方式執行，最初是由中本聰與已故的 Hal Finney 和其他一些程式人員合作提供。從那時候開始，任何人都可以隨意下載和使用該軟體，並對其進

行更改。這在比特幣實作過程裡，創造了一個自由競爭的市場，任何人都可以自由對軟體進行更動或改進，並將其呈現給其他用戶使用。

隨著時間演進，來自世界各地的數百名電腦程式人員，自願花時間改進節點軟體，並在此過程裡提高了各個節點的功能。這些程式人員形成了幾種不同的實作建置，其中最大和最受歡迎的實作被稱為「比特幣核心（Bitcoin Core）」<sup>2</sup>。其他幾種實作也同樣並存著，用戶可以隨時改變其來源代碼。而節點要成為網路一部分的唯一要求，便是它必須遵循其他節點形成的共識規則。改變鏈的結構、交易的有效性、區塊獎勵或系統其他參數，因而破壞共識規則的節點，其交易便會被其他節點拒絕。

定義比特幣參數的過程，正如同蘇格蘭哲學家 Adam Ferguson 所說，是「人類行為的產物，而非人類設計的產物<sup>註2</sup>」的一個範例。儘管中本聰和 Hal Finney 等人，在 2009 年 1 月的軟體已經製作了一個工作模型。比特幣的程式代碼從當時開始，又透過數千名運行節點的用戶所選擇的數百名開發人員的貢獻，得到顯著的發展。但並沒有中央權威機構決定比特幣軟體的發展，也沒有一個程式設計師能夠決定任何結果。得到採用而運行的實作關鍵，在於被大家證明遵守了原始設計的參數。這些對軟體所進行的變動，最好理解為對單個節點與網路交流方式的改進，而非對比特幣網路或共識規則的更改。雖然討論這些參數不屬於本書的範圍，但它們只要遵守以下標準的即可：採用的節點與其他節點離開共識規則時，所有其他節點必須更新，以便讓此節點的變動保留在網路上。如果許多節點都採用了新的共識規則，那麼出現的就是硬分叉（hard fork。變動後新舊版本不相容，會產生新幣）。

---

註 2 Adam Ferguson，「一篇關於公民社會歷史的論文（*An Essay on the History of Civil Society*）」，倫敦：T. Cadell，1782 年。

因此，比特幣的編碼程式人員無論如何都無法控制比特幣，只有當他們在某種程度上，提供了節點營運商想要採用的軟體才可以。但程式人員不是唯一無法控制比特幣的人，具有大量散列處理能力的礦工們，也無法控制比特幣。無論他們有多少散列功率可以用來處理無效區塊，大多數的比特幣節點也都不會對它們進行驗證。因此，如果礦工試圖改變網路規則，他們生成的區塊將被操作節點的網路成員們輕易忽略掉，他們解決工作量證明問題所花費的大量資源，也不會得到任何獎勵。因為礦工只是比特幣礦工，他們根據現行共識規則生產有效交易的區塊。

這裡可以談一下「節點營運商能控制比特幣」的說法，這在「抽象群體」的方式下是正確的，更實際一點的說，節點營運商只能控制自己的節點，並自行決定加入哪些網路規則，以及他們認為哪些交易有效或無效。節點在選擇共識規則時受到嚴格限制，如果它們強制執行與網路共識不一致的規則，其交易將被拒絕。每個節點都有強烈的動機來維護網路共識規則，並與這些共識規則上的節點保持相容。每個單獨節點的能力不足以強迫其他節點更改代碼，因為強烈的集體意見會保持住當前的共識規則。

總之，比特幣程式人員若想要別人採用他們的程式代碼，就必須面臨遵守共識規則的強烈動機。礦工也必須遵守網路共識規則，以獲得他們在工作量證明上所花費的資金。網路成員面臨著堅持共識規則的強烈動機，以確保他們能夠搞清楚網路上的所有交易。任何單獨的程式人員、礦工或節點營運商對網路都是可有可無的。如果他們偏離共識規則，最可能的結果便是自己浪費了資源。只要網路為參與者提供積極的獎勵，接續替代的參與者就可能會出現。因此，比特幣的共識參數可以理解為主權，在比特幣存在的情況下，它將根據這些參數和規格而存在。比特幣營運中這種非常強烈的共識意見，讓它在貨幣供應計劃或重要經濟參數上的改變極為困難。也因為這種穩定的均衡，比特幣才能被視為健全貨幣。如果比特幣偏離這些共識規則，它的價值主張就會被嚴重損害。

據作者所知，目前並沒有重大的協調在嘗試改變比特幣的貨幣政策<sup>註3</sup>。到現在為止，較簡單的嘗試改變某些代碼的技術規範都失敗了。由於比特幣網路的「分散式」性質，讓看似無害的改變協議都很難實現，而且還必須讓許多不同派系與敵對陣營，願意在大家還不知道影響如何的情況下同意改變。同時安全性嘗試與測試對現狀的熟悉程度，看起來仍然完全熟悉而且可靠。因此比特幣的現狀，可以理解為一個穩定的「謝林點（Schelling point）」<sup>註4</sup>，它為所有參與者提供有用的激勵措施，遠離可能會帶來很大損失的風險。

如果比特幣網路的某些成員，決定引入與其他網路成員不兼容的新版軟體，來更改比特幣代碼中的參數，那麼結果就會是一個分叉（fork），它會有效地創建出兩個獨立的貨幣和網路。只要任何成員留在舊網路上，他們就會受益於網路的基礎設施、採礦設備、網路效應和名稱識別。為了使新的分叉成功，必須讓大多數用戶、挖礦能力以及所有相關的基礎架構，同時遷移到新鏈上。若未獲得絕大多數節點支持，最可能的結果便是兩種比特幣同時在交易所上架。如果分叉後面的人希望自己所在的分叉能成功，便需在舊分叉上出售他們的舊幣，然後希望其他人也這樣做，讓舊幣的價格崩潰，新分叉的價格會上漲，從而帶動所有的採礦電力和經濟網路遷移到新的網路上。但由於比特幣運作的任何參數變化，代價都是犧牲一部分成員，只對另一部分成員有利，因此不太可能形成轉向新幣的共識。更廣泛地說，大多數比特幣持有者只是「持有」比特幣，而且很可能是因為被比特幣規則的自動化性質及無第三方限制所吸引而購買。這些人不太

註3 在2012年首次將區塊獎勵減半之後，一些礦工試圖以50枚比特幣的獎勵繼續開採區塊，但由於節點拒絕了這些礦工開採的區塊，迫使他們切換回原來的通貨膨脹計劃。

註4 謝林點（Schelling point）是指個人在沒有與他人交流的情況下所使用的策略。因為這點看起來很自然，大家會希望其他人也選擇這種策略。由於沒有正式的方法來評估到底有多少比特幣節點，因此每個節點成員的「謝林點」，都會希望堅持現有的共識規則，並避免投奔到新的網路。

可能冒險將變更網路的根本處理權，交給提出不兼容代碼庫的新群組。到底是否會存在這樣的多數，並不是這場討論的重點，比較重要的是要有夠多的節點數，確保繼續使用目前的系統參數（除非操作上真的遇到某種原因而被破壞）。

除非目前設計裡真的出現了災難性的失敗，否則大多數的節點，可能都會選擇繼續使用舊鏈的實作，因為這樣當然比選擇進入分支的人來說更為安全。決定進入分叉的最大問題，在於幫助分叉成功的唯一方法，便是在舊鏈上出售舊幣。但應該沒人想出售舊幣以便搬到新網路上，因為這樣只會發現並非所有人都願意移動，而且新網路上的新幣價值也會隨之崩潰。總而言之，除非絕大多數人願意一起轉移，否則不太可能採用也具有共識規則的新實作。而任何沒有多數轉移的變動，幾乎肯定會對所有相關人員造成經濟災難。因為任何這類轉移到新實作的舉動，可能都會讓提議變更的一方，具有對比特幣未來發展方向的重大控制能力。但這些原來持有比特幣的人，也就是成功轉變所需要的這群人，很可能會在意識形態上，反對擁有控制比特幣權力的任何團體，因此不太可能支持這樣的舉動。所以這個群體的存在，會讓「支持分叉」對每個人來說都是高風險的舉動。目前為止，比特幣已經抵抗了所有改變企圖。在具有利益衝突的各方之間，想協調組織一場「同時轉移」，就要面對其中許多人本身就帶有強烈的「不可變」概念，也就是除非出現任何迫切的理由，才能讓他們想要擺脫目前的實作。

舉例來說，增加貨幣發行率以提高獎勵礦工幣量的修改，可能會吸引到礦工，但它並不會吸引目前的比特幣持有人，因此不太可能採用這種提議。同樣地，增加比特幣網路區塊大小的編輯，可能會使礦工受益於允許他們在每個區塊內運行更多交易，收取更多交易費用，擴大他們在採礦設備上的投資回報。不過這樣可能就不會吸引比特幣的長期持有者，因為他們擔心更大的區塊會導致區塊鏈變大，使運行整個節點變得更加昂貴，因而減少了網路

中的節點數量，讓網路變得更加集中，也更容易受到攻擊。開發用於運行比特幣節點軟體的程式人員，也無法對任何節點施加改變；他們所能做的只是提出代碼，而用戶可以自由下載他們喜歡的任何代碼和版本。只要是與現有實作相容的代碼，都會比任何不相容的代碼更容易被下載，因為後者只能在網路上的絕大多數節點都願意運行它時，才可能成功。

因此，比特幣表現出極強的「現狀」傾向。目前為止，只對代碼進行了微小而無爭議的改變，而且每一次改變網路的嘗試，都以喧囂的失敗告終，讓長期堅信比特幣的人們，更加喜歡他們的貨幣，而不是為了比特幣的不變性和抵抗力而喜歡。這些嘗試中最引人注目的是增加個別區塊的大小，用途是增加交易記載量。有幾個計畫收集了一些非常著名的和過時的比特幣名人的名字，並花很多錢試圖取得公眾注意力。Gavin Andresen 是比特幣相關人士中，最常公開的人之一，他非常積極地推動多項嘗試，想將比特幣分叉以便可以擁有更大的區塊，其中也有許多利益相關者，包括一些技術嫻熟的開發商和資金雄厚的企業家等。

最初 Andresen 和開發人員 Mike Hearn，在 2015 年 6 月提出比特幣 XT，目的在將區塊的大小從 1MB 增加到 8MB。但大多數節點拒絕更新為他們的軟體，並且希望維持在 1MB 的區塊上。Hearn 隨後被一家「財金機構的區塊鏈財團」聘用，將區塊鏈技術引入金融市場，並發表了一篇部落格文章，以配合宣傳他在「紐約時報」上的熱情形象，說他在比特幣即將失敗時，拼命的想要拯救比特幣。Hearn 宣布「比特幣實驗的解答」，理由是交易能力的成長不足，已經成為比特幣成功的致命障礙，並宣布他已售出所有比特幣，當天的比特幣價格約為 350 美元。在接下來的兩年裡，比特幣價格增加了四十多倍，而他所加入的「區塊鏈財團」則尚未生產出任何實際商品。



Gavin Andresen 絲毫不受影響，立即提出一項新嘗試，以「比特幣經典 (Bitcoin Classic)」的名義對比特幣進行分叉，可以把區塊大小提升到 8MB。然而這種嘗試並沒有更好，到了 2016 年 3 月，支持它的節點數開始失敗。接著增加區塊大小的支持者，在 2017 年重組為「比特幣無限 (Bitcoin Unlimited)」，一個更廣大的聯盟，包括最大的比特幣採礦處理器製造商，以及控制比特幣網域名 bitcoin.com 的有錢人，並花費大量資源以推廣更大的區塊。然後出現了很多媒體炒作，讓許多在主流媒體和社交媒體上關注比特幣新聞的人，都能感受到危機；然而事實上仍然沒有出現分叉，因為大多數節點繼續在 1MB 上運行相容的實作。

最後在 2017 年 8 月，一群程式人員提出名為「比特幣現金 (Bitcoin Cash)」的比特幣新分叉，其中包括許多之前提出增加區塊尺寸的人。比特幣現金的命運，活生生說明了比特幣分叉沒有得到普遍共識支持的問題。因為大多數人選擇留在原來的鏈上，支持比特幣的交易所或企業的經濟基礎設施，仍然主要集中在原來的比特幣上，這使得比特幣硬幣的價值遠高於比特幣現金的價值，比特幣現金價格持續下滑，直到 2017 年 11 月下跌到只剩 5% 比特幣價值的低點。分叉不僅無法獲得經濟價值，而且還存在嚴重的技術問題，讓分叉幾乎無法使用。由於新鏈具有與比特幣相同的散列算法，礦工可以將處理能力用在兩條鏈上，獲得兩邊的獎勵。但由於比特幣比起比特幣現金更有價值，而且比特幣背後的處理能力仍遠大於比特幣現金，因此比特幣礦工可以在比特幣現金有高回報的時候，再轉移過去。這就讓比特幣現金陷入一個不幸的兩難困境：如果採礦難度過高，生產區塊和處理交易便會有很長的延遲；但如果難度設定得太低，硬幣開採速度非常快，供應量也會迅速增加。這種增加速度會超過比特幣鏈，快速增加了比特幣現金幣的供應，並將導致比特幣現金的獎勵很快耗盡，因而減少未來礦工想要為它採礦的動力。最可能的情況便是再產生一個硬分叉，調整供應成長量，才能繼續為礦工提供獎勵。這個問題只發生在從比特幣分叉出去的區塊鏈上，但對比

特幣本身來說卻不會如此。比特幣採礦必須一直使用最大的處理能力，隨著礦工有越多的採礦能力，處理能力會一直遞增。但當其他幣從比特幣中分離時，其幣值越低，難度越低，便可能經常受到影響，因為幣值較高的龐大採礦能力，會越界進行「快速採礦」。

在這個分叉未能挑戰比特幣的主要地位之後，另一項將比特幣區塊翻倍的企圖，也由於在比特幣經濟中活躍的這些初創公司，其推動者們意識到行動很難達成共識，而且最後可能只會得到另一種幣和另一個網路而已，所以挑戰已經在 11 月中取消了。比特幣忠貞人士已學會嘲笑這些嘗試，也意識到無論產生多少炒作宣傳，任何改變比特幣共識規則的嘗試，都將產生另一種「山寨比特幣」，就像複製比特幣內容的這些替代幣一樣，無法具備比特幣的唯一重要特點：不變性。從上面的討論中，我們可以清楚的看出比特幣的優勢不在它的速度、便利性或友善的用戶體驗等。比特幣的價值來自於具有不可改變的貨幣政策，所以沒有人能輕易改變它。任何以「改變比特幣規格」為起點的群體，無疑都少了這個讓比特幣變得有價值的唯一特點。

雖然比特幣用起來很簡便，但卻難以改變。比特幣是自願參與的，所以沒有人一定必須使用它，但那些想要使用它的人別無選擇，只能按照規則行事。以任何想法來改變比特幣都是不可行的，如果嘗試的話，就會變成另一場毫無意義的淘汰賽，只會加入已經存在的數千個失敗行列中。比特幣必須按照原來的方式使用，也就是接受它的條款並使用它所提供的內容。對於所有實際的意圖和目的而言，比特幣都是具有主權的：它按照自己的規則運行，沒有外人可以改變這些規則。將比特幣的參數看作類似於地球、太陽、月亮或星星的自轉公轉，可能會較有幫助。這是依我們所能控制以外的力量而生存，無法加以改變。

## 反脆弱

比特幣是 Nassim Taleb「反脆弱」概念的體現，他將其定義為從逆境和混亂中獲益。比特幣不僅強壯的足以抵抗攻擊，而且可以說在技術和經濟層面能夠反脆弱。雖然殺死比特幣的嘗試迄今為止都失敗了，但這些攻擊已經讓程式人員發現弱點並加以修補，反而使比特幣能變得更強大。此外，對網路的每一次攻擊失敗，都是一個印記，可以用來對參與者和外人證明與宣傳比特幣網路的安全。

由志願軟體開發人員、審查人員和駭客組成的全球團隊，將專業、財務和知識方面的興趣，用在改進或加強比特幣代碼與網路。在代碼規範中發現的任何漏洞或弱點，將吸引某些程式人員提供解決方案、進行辯論與測試，然後將它們提交給網路成員以供採用。迄今為止發生過唯一的變化是操作上的改變，這種改變可以讓網路更有效的運作，而非改變比特幣操作的本質。同時這些程式人員可以擁有比特幣，因此也能有經濟上的激勵來確保比特幣的成長和成功。反過來看，比特幣的持續成功在經濟上獎勵了這些程式人員，從而使他們能夠投入更多的時間和精力維護比特幣。一些致力於維護比特幣的著名開發人員，已經藉由投資比特幣而變得富有，他們可以將這個任務當作主業，而不必從其他地方獲得報酬。

在媒體報導方面，比特幣似乎是「所有宣傳都是好宣傳」格言的完美體現。作為一項不易被理解的新技術，就跟許多其他技術一樣，比特幣總是會受到不正確和完全敵對的媒體報導。99bitcoins.com 網站收集了多年來，200 多篇關於「比特幣將亡」的知名報導案例。其中一些作家認為比特幣違反了他們的世界觀——這些通常與國家貨幣理論，或是凱因斯主義者對彈性貨幣供應的重要信念有關——並拒絕考慮他們自己出錯的可能性。相反的，他們得出結論認為比特幣的存在是錯誤的，因此他們預測比特幣很

快就會死亡。其他的人則堅信比特幣必須改變以維持成功，因此當比特幣未能按照他們所想要的方式改變時，就認為它必定會滅亡。這些人對比特幣的攻擊促使他們寫作，引起越來越多人注意。比特幣的這類訃文越多，它的處理能力、交易次數和市場價值就越高。包括作者在內的許多比特幣人士，會藉由注意到它被「賜死」了多少次，以及它如何繼續成功運作，來體會比特幣的重要性。比特幣的訃文並無法阻止它的運作，但似乎已經幫助它得到更多的宣傳，並喚醒公眾的好奇心，儘管面對有敵意與惡劣的新聞，但比特幣仍持續運作。

關於比特幣「抗脆弱」的一個很好的例子，出現在 2013 年秋天，當時聯邦調查局逮捕了聲稱是 Silk Road 網站的負責人。這個網站是一個真正的免費線上交易市場，允許用戶線上買賣他們想要的任何東西，包括非法毒品等。由於當時一般大眾心目中的比特幣，與毒品和犯罪相互關聯，因此多數分析師預測，關閉網站將破壞比特幣的運作。所以當天比特幣的價格從 120 美元左右跌至 100 美元區間，但接下來則迅速反彈並開始快速上漲，在幾個月內便達到每比特幣 1,200 美元。撰寫本文時，比特幣從未再跌到 Silk Road 網站關站前的價格。經歷 Silk Road 網站關閉事件而毫髮無傷，證明它的表現當然不只是一種犯罪貨幣，而且在整個事件中，它還獲得了關於 Silk Road 的媒體報導免費宣傳。

比特幣反脆弱的另一個例子出現在 2017 年 9 月，中國政府宣布關閉境內所有比特幣交易所。最初的反應是因恐慌情緒導致價格下跌約 40%，結果只經過幾個小時價格便開始復甦，而且在幾個月內，價格便上漲超過政府禁令前一倍多的價格。雖然禁止交易的比特幣，可能因流通性減少而被視為使用上的障礙，但其結果似乎只加強了比特幣的價值主張。更多境外交易開始在中國發生，其中像 localbitcoins.com 這類網站上的交易量激增。很可能是因為中國的停止交易所造成的反效果，因為它促使中國人長期持有比特幣，而非短期交易。

## 比特幣可以「擴容」嗎？

撰寫本文之際，圍繞在比特幣上最引人注目的爭論之一，涉及到擴大容量或增加交易能力的問題。比特幣的 1MB 區塊代表交易容量每天大約不到 500,000 筆，目前比特幣的交易量已接近這個數字，因此過去幾個月的交易費用大幅增加。一項名為 Segwit 的技術解決方案，可能會讓交易容量擴成目前的四倍，但由於比特幣的去中心化與分散式特性，因此比特幣區塊鏈可以處理多少交易，會很明顯的受到嚴格限制。每個比特幣交易都記錄在所有網路節點中，而每個網路節點都需保留一份所有交易的完整分類帳。這項必要性代表記錄交易的成本，將遠高於任何只需一個記錄和幾個備份的「集中式解決方案」。把最有效的支付處理系統集中在一起的理由，是因為保留多個分散式記錄會比只保留中央記錄來得昂貴，而且還要擔心它們的同步更新問題，所以目前只能透過比特幣工作量證明來實現。

集中支付解決方案（如 Visa 或 MasterCard）使用一個集中式分類帳（所有交易都將提交到該分類帳），以及完全獨立的備份系統。Visa 每秒可處理約 3,200 筆交易，即每年 1008 億筆交易<sup>註 5</sup>；比特幣目前的 1MB 區塊每秒最多可處理 4 筆交易，每天處理 350,000 筆交易，或每年處理約 1.2 億筆交易。若用比特幣來處理 Visa 的 1000 億筆交易，每個區塊需要大約 800MB，亦即每隔十分鐘，每個比特幣節點就要增加 800MB 的數據。在一年內，每個比特幣節點將為自己的區塊鏈增加大約 42TB 的數據，即 42,000GB。這樣的數字完全超出目前或未來商用電腦的處理能力範圍。一般消費級電腦或外接硬碟的容量平均約 1TB，亦即大約 Visa 一週

註 5 Visa, Inc. 初探，參閱 <https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf>。

的交易量。所以從某些角度看，值得來研究一下 Visa 處理這些交易所使用的電腦設備。

2013 年的一份報告顯示，Visa 擁有一個被形容成是「數位諾克斯堡」的數據中心，使用 376 台伺服器、277 台交換機、85 台路由器和 42 台防火牆<sup>註 6</sup>。當然，Visa 的集中式系統是「單點故障（single point of failure，縮寫為 SPOF）」的類型，因此必須採用大量的備援設備和備用容量來防止意外。在比特幣下，多節點同時存在可讓每個節點均非重要關鍵，因此安全性和容量的需求較小。儘管如此，每年要增加 42TB 數據的節點，需要用到非常昂貴的電腦，而每天處理所有事務所需的網路頻寬，也將會是巨額的費用，對於分散式網路來說，顯然會因複雜昂貴而行不通。

這類中心在全球屈指可數：只有 Visa、MasterCard 和其他一些支付處理中心。如果比特幣試圖處理這樣的容量，就不能以同樣規模的數千個分散式中心來跟集中式解決方案競爭；而必須集中化並僅使用少數的數據中心來完成。為了使比特幣保持分散式，網路上的每個節點必須花費一些合理的費用，才能在可商用的個人電腦上運行，而節點之間的數據傳輸，必須是一般消費者使用頻寬所能支援。

很難想像比特幣可以在區塊鏈上執行跟集中系統相同規模的交易，這解釋了為何交易成本會上升，而且如果網路繼續成長，交易費用也可能會繼續上升。比特幣交易擴大交易數量規模的可能性應該來自鏈外交易，有很多更簡單的技術可用於小額和普通支付。亦可確保比特幣合理使用大量處理能力，而且不會對最重要的兩項特性，亦即「數位健全貨幣」與「數位現金」

---

註 6 Tony Kontzer，「進入 Visa 的數據中心（Inside Visa's Data Center）」，*Network Computing*。參閱 <http://www.networkcomputing.com/networking/inside-visas-data-center/1599285558> 觀看。

有所妥協。雖然目前並沒有這兩種功能的替代技術，但有許多技術可以用較低的成本提供小額支付和消費支出。而且在目前銀行技術上，便可簡單可靠的實現這些選擇性的技術。同時，比特幣亦不應使用在大量的商店付款，因為要收到第一次確認就需 1 到 12 分鐘。商家和客戶不可能等待時間如此久的付款，即使「雙重支付」攻擊的風險，對於一次小額付款來說並不算什麼，但對於接受大量交易的商家來說就相當重要。就像對「Bitcoin Dice」的攻擊一樣，稍後我們會在有關比特幣攻擊的章節裡討論。

對於想要將比特幣當作數位化長期價值儲存的人，或希望在不受政府管制情況下進行重要交易的人來說，高額的交易費用是值得付出的代價。而以比特幣的特性來保存價值的人，並不需要進行多次交易，因此高額的交易費也很值得。而對無法透過一般銀行系統進行的交易，例如人們試圖把自己的錢從遭受通貨膨脹和資本控制的國家移出時，比特幣的高交易費更是值得付出的代價。即使在比特幣目前使用率較低的情況下，對數位現金和數位健全貨幣的需求，都已把交易費用拉高到無法與 PayPal 等集中解決方案或小額支付信用卡競爭。然而，這並不能阻礙比特幣的成長，一切都在證明比特幣的市場需求是作為數位現金和數位儲存價值，而非由小額支付所推動。

如果比特幣的受歡迎程度繼續成長，那麼還有一些潛在的擴容解決方案，可以不必改變比特幣的結構，例如改為利用交易結構來增加支付數量即可。讓每次比特幣交易可以包含多個輸入和輸出，並使用稱為 CoinJoin（合幣）的技術，將多個支付組合在一起成為一個交易，這種允許幾個輸入和輸出組合的方式，只會用到原本所需空間的一小部分。如此就有機會讓比特幣的交易量每天增加到數百萬次。隨著交易成本不斷上升，這種方法很有可能成為受歡迎的解決方案。

比特幣擴容的另一種可能性便是數位移動 USB 錢包，以實體方式防止篡改，並可隨時檢查結餘。這些 USB 隨身碟可裝載特定數量的比特幣私鑰，允許持有者以隨身碟提取。就像實體現金一樣的使用方式，每個持有者也都可以驗證這些隨身碟裡的價值。隨著交易費用的不斷上漲，對比特幣需求的成長並未減緩，從價格漲勢就證明了這點。這表示用戶對交易的重視程度，遠高於必須支付的交易成本。所以並非交易費用拖慢了比特幣的普及，事實上應該是把重要交易留在鏈內，不重要的交易則移至鏈外。比特幣最重要的用途，在於作為價值儲存和不被察覺的支付，因此它的交易費用非常值得。當人們購買比特幣來長期持有時，會產生一次性的小額交易費用，跟一般佣金和賣家溢價比起來根本微不足道。對於那些希望逃避資本管制，或者向面臨經濟困難的國家匯款的人來說，這樣的交易費用非常值得考慮，因為比特幣可能是唯一的選擇。隨著比特幣的採用普及，交易費用可能會高到足以影響支付比特幣的人，對他們形成經濟壓力，迫使產生更多的擴容解決方案，這些解決方案可以增加交易容量，而非做出影響網路規則的變更或強行分叉。

除了這些可能性之外，目前多數比特幣的交易都是在鏈外進行，但只能在鏈上結算。基於比特幣的商業行為，例如賭場或遊戲網站等，只使用比特幣的區塊鏈進行客戶存款和提款，但在其平台上，所有的交易都會記錄在本地資料庫中，並以比特幣計價。由於業務量相當大，也缺乏關於其專有平台交易的公開數據，加上比特幣經濟的快速動態變化，因此無法準確估計這些交易的數量，但保守估計它們大約為比特幣區塊鏈交易數量的 10 倍以上。事實上比特幣幾乎已經被當成在比特幣經濟裡，大部分交易的「儲備資產」。如果比特幣繼續成長下去，我們很快就會看到鏈外交易數量的成長速度，高於鏈上的交易。



這種分析可能跟隨著比特幣崛起的論點相互矛盾，原先是要促使比特幣終結中央銀行和銀行業務。然而要數百萬甚至數十億人，直接使用比特幣網路來執行每筆交易的想法，也會因為每個網路成員都必須記錄其他成員的每個交易，而顯得不切實際。隨著交易數量成長，這些記錄變得更龐大，將會造成計算上的重大負擔。另一方面，比特幣作為價值儲存的獨特屬性，也可能會隨著需求不斷增加，讓它難以作為純粹的點對點網路而生存。比特幣若要繼續成長，就必須有區塊鏈外處理支付的解決方案，而這些解決方案正在競爭市場中擺脫困境。

銀行這種機構不會消失的另一個重要原因，在於監管的便利性。雖然許多比特幣純粹主義者，相當重視能持有自己的錢，不被金融機構監管便能取用而帶來的可貴自由，但絕大多數人卻不想要這種自由，因為害怕自己的錢被盜或被綁架，不想要這種「自行保管」的錢。在當今普遍流行的「反銀行」言論中，尤其是在比特幣圈子裡，很容易讓人忘記銀行「存款業務」是全球數百年來要求的「合法業務」。人們很樂意付錢讓他們的錢得以安全存放，隨身只需要攜帶少量的錢，以面臨較低的損失風險。反過來看，金融卡的廣泛使用取代了現金，讓人們可以隨身攜帶小額資金，也可能造成現代社會比以前的情況更為安全，因為大多數潛在的攻擊者意識到他們不太可能遇到攜帶大量現金的受害者，而且在受害人取消被搶的金融卡之前，能夠盜取大量金額的可能性也很低。

即使比特幣的網路有辦法每天支持數十億筆交易，也不需要進行其他第二層支付協議，但有許多（即使不算大多數）擁有大量比特幣的持有者，終究會求助於目前越來越多的比特幣保管服務，幫助他們安全儲存比特幣。這是一個全新的行業，也很可能會迅速發展，以便為不同安全性和流通性的比特幣儲存，提供技術上的解決方案。無論這個行業採取什麼樣的形式，它所能提供的服務及發展方向，都將塑造出未來基於比特幣所建立的「銀行系統」輪廓。我不想預測這些服務將採取什麼形式，以及

將來可能具有哪些技術能力，只能說它應該會在建立市場聲譽之上，使用加密驗證機制來運作。實現此目標的一種可能技術被稱為「閃電網路（Lightning Network）」，這是一項正在開發的技術，透過允許節點運行「鏈外支付」管道，來承諾明顯增加交易容量，亦即只使用比特幣分類帳來驗證有效餘額，而非轉移比特幣。

2016 年和 2017 年，隨著比特幣達到最大日常交易次數，網路也繼續成長，第 8 章的數據也清楚證明了這點。比特幣擴容是為了鏈上交易價值的成長，而非交易數量的增加。越來越多交易在鏈外進行，並在處理比特幣的交易所或網站上進行結算，因而將比特幣變成了較像結算網路而非直接支付網路。一般普遍認為，這並不代表比特幣擺脫了作為現金的功能。雖然「現金（cash）」的用法目前多半表示用於小額消費者交易的資金，但該術語的原始含義是指一種「不記名」的貨幣工具，其價值可以直接轉移而無需由第三方結算或承擔責任。在十九世紀時，「現金」一詞還指的是中央銀行的黃金儲備，「現金結算」則是指銀行間直接轉移實體黃金。如果這種分析正確，比特幣的價值和鏈外交易也繼續成長，而鏈上交易的成長較少時，比特幣便能更方便的理解為「現金」一詞的舊含義，亦即類似於黃金的現金儲備，而非作為小額交易的紙鈔現金。

總之，在不必改變比特幣體系結構的情況下，增加比特幣交易數量的可能性還有很多，而且不必讓目前所有節點營運商同步升級。擴容解決方案將來自節點營運商，用來改良將比特幣交易數據發送給其他網路成員的方法，這點可能要透過上述的合併交易、鏈外交易和支付管道來實現。隨著時間演進，鏈上擴容的解決方案，似乎無法滿足比特幣日益成長的需求，因此第二層支付解決方案的重要性，可能會繼續成長而導致出現類似目前銀行的新型金融機構，使用加密技術並且主要是在線上營運。

## 比特幣是犯罪分子專屬嗎？

比特幣從一開始就存在的常見誤解之一，就是它會成為犯罪分子和恐怖分子的絕佳貨幣。從一長串已發佈的新聞內容來看，並沒有事實能證明恐怖分子或犯罪集團，專門使用比特幣來進行活動。其中的許多文章已經被收回<sup>註7</sup>，不過他們將這個想法深印在許多人腦海中，當然也包括那些被誤導的罪犯。

實際情況是全球各地均可造訪比特幣分類帳，且無法改變。只要比特幣仍然運作，便會完整保留每筆交易紀錄。所以比特幣是「絕對匿名」的說法並不正確，應該說絕對可以匿名使用。雖可能但無法保證可以在現實身分和比特幣地址之間找到連結，並在連結建立後，透過地址來追蹤所有交易。談到匿名時，我們可以將比特幣視為與網際網路上的匿名一樣：它取決於你隱藏的程度以及別人看到的樣子。然而比特幣的區塊鏈，會讓在網路上隱藏足跡的動作更加困難。處理掉設備、電子郵件地址或 IP 位址很容易，只要不再使用它們即可，但很難把資金的足跡完全刪除到只剩一個比特幣地址。因此就本質而言，比特幣的區塊鏈結構並不適合隱私。

這些都在說明任何在實際上有受害者的犯罪，其犯罪分子若使用比特幣是非常不明智的。「匿名」特性便意味著這些地址可以關聯到現實世界的某些身分，而且即使在犯罪發生多年以後也還可以追溯。警察、受害者或僱用的任何調查人員，即使多年後仍可能找到與犯罪者身分的相關連結。

---

註7 Stein, Mara Lemos, 「晨間風險報告：用比特幣資助恐怖主義的說法可能被誇大了（The Morning Risk Report: Terrorism Financing Via Bitcoin May Be Exaggerated）」。  
華爾街日報，2017 年。

比特幣的支付足跡本身，就是許多線上毒販被認定和抓到的原因，他們多半誤信了比特幣的相關炒作，以為真的可以完全匿名。

比特幣是一種金錢的技術，金錢則是犯罪分子隨時使用的東西。任何形式的金錢都可能被犯罪分子利用或助長犯罪，但比特幣的永久分類帳特性，讓它特別不適合「可能會被調查、有受害者形式」的犯罪。不過，比特幣確實可能會助長「無受害者」形式的犯罪，因為沒有受害者，就代表沒有人會試圖建立「罪犯」的身分。事實上，一旦你相信二十世紀的國家官僚式宣傳後，便會出現這種「無受害者」的罪行。雖然自重的選民或官僚，都會認為他們具有為道德立法的特權，但只要一項行動「沒有」受害者，確實很難定罪。對於這些非法但並無道德爭議的行為，比特幣可能會有用，因為沒有受害者試圖追捕肇事者。而這類無害活動在區塊鏈中顯示的是個別交易，其內容有各種可能性。因此可以預期這些沒有消費者的犯罪，例如線上賭博或規避資本管制等，可能就會使用比特幣，但謀殺和恐怖主義則不太可能使用。藥物交易似乎也會發生在比特幣區塊鏈上，但這可能比較取決於毒癮者的渴望而非他們的正確判斷，因為執法部門會鎖定使用比特幣的大量藥物購買者。雖然很難找到這項問題的相關統計數據，但用比特幣購買藥物會比用實體金錢買藥來得更危險的事實，並不會令人感到驚訝。

換句話說，比特幣雖然會增加個人的自由，但不一定會讓他們更容易犯罪。它不是我們應該擔心的工具，而應該將它視為跟和平與繁榮未來，緊密連結的工具。

利用比特幣犯罪的事件裡，比較引起注意的類型應該就是勒索軟體：這是一種未經授權侵入電腦，然後將受害者文件加密，受害者必須以比特幣向勒索者付款，才有辦法解密文件。雖然這種形式的犯罪在比特幣之前便已出現，但自從比特幣發明以後，這種犯罪變得更加方便。毫無疑問的，這是使

用比特幣增加了犯罪行為的最明顯案例。然而，大家應該可以理解這些勒索軟體的犯罪，是利用了電腦安全性的鬆散而建立。若有某家公司可以讓整個電腦系統被要求等值幾千美元比特幣的匿名駭客鎖住，該公司本身的問題，顯然要比這些駭客大得多。對駭客的激勵可能是數千美元而已，但對公司的競爭對手、客戶和供應商來說，獲取這些數據的動機可能要高得多。事實上，比特幣勒索軟體可以讓公司檢測並找出電腦的安全漏洞，這種過程也正在引導企業採取更好的安全預防措施，並使電腦資安成為一個茁壯的行業。換句話說，比特幣可以讓電腦安全市場「貨幣化」，雖然駭客最初可以從中獲益，但長遠來看，生產性企業將會得到最佳的安全資源。

## 如何殺死比特幣：初學者指南

許多比特幣人已經有了「比特幣無論如何都能生存下來」的準宗教信仰。其背後的處理能力和遍布全球的大量節點驗證交易，意味著它對變化具有高度抵抗力並且可以維持不變。大多數不熟悉比特幣的人，經常認為它注定會失敗，因為它難以避免駭客的攻擊，就像任何數位的東西一樣。而一旦理解了比特幣的操作，就會清楚知道「駭」它可不是件簡單的任務。不過，比特幣還可能面臨幾種其他威脅，因為「電腦安全」是一個難以處理的根本問題，涉及到不可預測的攻擊者所發現的新攻擊角度。解釋所有對比特幣的潛在威脅並加以評估，可能超出了本書所能處理的範圍<sup>註8</sup>。因此本節僅檢視一些較為明顯的威脅，以及跟本書主題「比特幣作為健全貨幣」相關的威脅。

---

註8 J. W. Weatherman 已經啟動了一個開源項目，用來評估對比特幣網路的威脅，你可在 [BTCthreats.com](http://BTCthreats.com) 上看到。

## 駭客

比特幣對攻擊的抵抗力源於三種屬性：它的「純粹簡單」、除了確保這種簡單設計的安全性以外什麼都不做的「巨大處理能力」、任何變化必須達成分散式節點的「共識」才能生效。請想像一下這樣的數位規模，相當於把整個美國軍隊的士兵和裝備，放在學校操場周圍以防止他人侵入，這樣各位應該就能大致了解比特幣是如何被過度強化。

比特幣本質上是虛擬硬幣所有權的分類帳，硬幣只有 2100 萬個，加上擁有者的幾百萬個地址，以及每天不超過 500,000 個交易在移動這些硬幣。操作這種系統所需的計算能力是微不足道的，100 美元的筆電就可以一邊上網，一邊使用比特幣交易。但比特幣網路之所以不是只在一台筆電上運行的原因，便是因為這種安排需要信任筆電的擁有者，也就變成一個相對簡單的駭客目標。

所有電腦網路都把它們的安全性，依賴在某些對攻擊者來說難以穿透的電腦上，並把這些電腦拿來作為最可靠的記錄之用。另一方面，比特幣對電腦安全採取了完全不同的作法：它不需要單獨保護任何一部電腦，並且在假設所有電腦節點都是「敵對攻擊者」的前提下運行。比特幣並非在任何網路成員之上建立信任，而是會驗證他們所做的一切。透過工作量證明進行驗證的過程，消耗掉大量的處理能力，事實證明這種做法非常有效，因為它會使比特幣的安全性依附於強大的處理能力，從而對存取或憑證的攻擊問題免疫。如果每個人都被認為是不誠實的，那麼每個人都必須支付大筆費用才能將交易登記到共同記錄中，一旦檢測到欺詐的行為，每個人都將失去這些費用。經濟激勵措施使得不誠實行為的代價極為昂貴，不太可能取得成功。

若用是「破壞交易分類帳」的方法來破解比特幣，詐騙式的將比特幣轉移到特定帳戶，或讓該幣無法使用，就會變成要求節點向區塊鏈發佈無效區塊，讓網路採用此新區塊並讓大家繼續接著建立區塊。由於節點檢測欺詐行為的成本非常低，而添加一個區塊交易的成本很高，並且還在不斷攀升中，網路裡的多數節點也都比較希望比特幣繼續存活下去，因此詐騙式攻擊者不太可能贏得這場戰鬥。隨著添加區塊的成本升高，這種攻擊也會變得更加困難。

比特幣的設計核心，對「提交新交易區塊」的成本與「驗證交易有效」的成本之間，存在著差異懸殊的不對稱性。雖然在技術上可以偽造記錄，但經濟激勵措施卻會堅決反對偽造，因此交易分類帳構成了目前為止，無庸置疑的最有效交易記錄。

## 51%的攻擊

51%的攻擊是一種使用大量哈希值來生成詐欺交易的方法，藉由把相同的硬幣花兩次，然後取消其中一個交易並欺騙接收者。事實上，如果控制大量哈希值的強力礦工，設法快速解決掉工作量證明問題，便有機會可以在接收確認的公共鏈上先傳送比特幣給某人，同時以另一個交易挖掘區塊鏈的另一個分叉，然後再用同一個比特幣傳送到另一個屬於攻擊者的地址。第一個鏈上的接收者收到確認時，攻擊者努力用他的處理能力來使第二個鏈更長。如果他能成功地使第二個鏈條長於公共鏈，則攻擊成功，第一個交易的接收者就會發現收到的比特幣消失。

攻擊者能夠控制的哈希值越多，就越有可能使欺詐鏈比公共鏈更長，然後反轉交易和利潤。雖然原則上聽起來很簡單，但在實踐中卻要困難得多。接收者等待確認的時間越長，攻擊者成功的可能性就越小。如果接收者願意等待六次確認，則攻擊成功的可能性會降至無限低。

從理論上講，51%的攻擊在技術上是非常可行的。但在實際運作時，經濟激勵措施會完全與之對抗。成功執行51%攻擊的礦工，將嚴重破壞使用比特幣的經濟動機以及對比特幣的需求。隨著比特幣採礦業發展成資本密集型產業，大量投資以努力生產比特幣，礦工們已逐漸對比特幣網路的完整性，產生穩定且長期的興趣，因為他們的回報取決於這個網路。目前並沒有任何比特幣交易，在確認後仍完成的「雙重支付」攻擊。

比特幣界目睹過的最接近成功的「雙重支付」攻擊是在2013年，當時比特幣投注網站 Bitcoin Dice，被人利用大量採礦資源進行「雙重支付」攻擊，贏走約1000個比特幣（當時價格約值10萬美元，方法大致上是贏錢就確認交易，輸錢就雙重支付）。不過這次攻擊成功的原因是因為 Bitcoin Dice 正在接受「零確認」交易，使得攻擊成本相對較低。如果他們透過至少「一次確認」來接受交易，攻擊就很難成功。這也是比特幣區塊鏈不適合大量消費支付的另一個原因：因為要花1到12分鐘生成一個新區塊來產生交易確認。如果有大型支付處理商，願意承擔以「零確認」來批准支付的風險，就有可能被利用大量採礦資源所協調的「雙重支付」攻擊，當成利潤豐厚的待宰肥羊。

總之，如果支付的接收者，不肯等待幾個區塊來確認交易的有效性，理論上是有可能受到51%的攻擊。然而在實際行動中，經濟激勵應該會讓這些哈希能力者，強烈反對把自己的投資浪費在這種用途上，因此，對於等待至少一次確認的節點成員，並沒有真正成功的51%攻擊。

如果純粹出於利潤動機，51%的攻擊可能不會成功，但這種攻擊也可能在「無利潤動機」的情況下進行，其用意是想摧毀比特幣網路。政府或私人企業都有能力決定取得龐大的比特幣的採礦能力，徵用大量的比特幣網路礦機，然後使用巨大的哈希值發起持續性雙重支付攻擊，詐騙許多用戶並破壞對比特幣網路安全的信心。然而，採礦的「經濟特性」會嚴重抗



拒這種情況。處理能力在全球市場競爭激烈，比特幣採礦是世界上最大、最賺錢、成長最快的處理能力。攻擊者可能會考慮花費佔「目前」散列能力 51% 的成本，然後將這筆錢用來購買必要設備。但是動員如此大量資源來購買比特幣採礦設備時，直接會導致礦機價格大幅上漲，讓現有礦商礦工有利可圖，於是他們便會投入更多資金來購買更多採礦設備。這也將導致礦機生產商對採礦能力的生產，進行更大規模的資本投資，於是又會大幅降低採礦能力的成本，並使比特幣的哈希值更快速的成長。作為一個剛加入市場的局外人來說，攻擊者明顯處在不利的地位，因為他購買的大量採礦設備，導致採礦處理能力的成長更快，超出他原先預估的 51% 散列能力。反過來看，建立處理能力來攻擊比特幣的資源越多，比特幣處理能力的成長也會越快，變得更難攻擊。因此，同樣的情況，雖然 51% 攻擊在技術上可行，但由於比特幣網路的經濟特性，讓這種攻擊很難成功。

如果是一個「國家」規模的攻擊者，可以控制其國內現有的採礦基礎設施，並在無利可圖的情況下想破壞比特幣網路的安全時，比特幣礦區在地理上分佈廣泛的事實，會讓這項挑戰需要全球各國政府通力合作才能辦到。不過實現這種攻擊的更好方法，可能不是透過實體接管採礦設備，而是透過「硬體後門」來加以實現。

## 硬體後門

瓦解或破壞比特幣網路的另一種可能方式，便是破壞運行比特幣軟體的「硬體」，讓它可以被外部侵入。例如在執行挖礦的節點電腦上植入無法偵測到的惡意軟體，允許外部人員侵入硬體，然後可以在啟動 51% 攻擊時，停用該設備或遠端遙控該設備。

另一個例子則是透過安裝在用戶電腦上的間諜軟體，透過他們的私鑰來動用比特幣。這類攻擊的規模如果夠大，可能就會嚴重破壞將比特幣作為資產和需求的信心。

兩種類型的攻擊在技術上都是可行的，但跟之前的另外兩種攻擊有所不同，因為它們不必完全成功，只要製造足夠的混亂來損害比特幣的聲譽和需求即可。由於生產採礦設備的製造商較少，因此攻擊採礦設備較可能成功，這點也成為比特幣失敗的關鍵重點。然而隨著比特幣採礦的成長，也開始吸引更多的硬體製造商加入製造採礦設備，如此便可以減少某家製造商遭受攻擊時，對整體比特幣網路造成的災難性影響。

而就運行節點的單獨個人電腦來看，這種利用硬體對比特幣網路所造成的風險，並不太可能被系統化執行，因為全世界有無數的電腦製造商，生產可以使用比特幣網路的電腦設備。若有任何一家電腦生產商遭到損害，消費者便可轉向其他生產商購買。此外，用戶也可以在離線電腦為其地址產生私鑰，這些私鑰永遠不必連接到網際網路。如果你是偏執狂的話，甚至可以在離線電腦上生成地址和私鑰，另存後立即銷毀原始私鑰。因為儲存在這些離線虛擬私鑰上的比特幣，可以躲過網路上任何類型的攻擊。

對抗這類攻擊最重要的防禦，便是比特幣的「無政府主義者」和「密碼狂」傾向，讓他們更加相信驗證而非信任。比特幣人通常在技術上比普通人的能力更強，他們對自己使用的硬體和軟體檢查得非常仔細。而開源軟體界的「同行評審（peer review）」文化，也可作為這類攻擊的重要防禦。由於比特幣網路的分散式特性，此類攻擊較可能造成個人的重大花費和損失，甚至導致網路的系統性中斷，但很難造成整體比特幣網路陷入停滯，或甚至摧毀對比特幣的需求。現實情況是比特幣的「經濟激勵」會讓它變得有價值，而非任何硬體形成它的價值。任何單一硬體設備對比特幣

的操作都是非必要的，完全可以用其他設備代替。但儘管如此，如果比特幣的相關硬體廠商，可以在設計時讓硬體設備具備多樣性，降低系統性攻擊的機會，比特幣網路的生存和穩健性就更能得到提升。

## 網際網路和基礎設施的攻擊

關於比特幣最常見的另一個誤解，就是可以用關閉基礎通訊設施或是關閉網際網路的方式，來關閉比特幣網路。這種問題的出現在於大家誤解了比特幣，以為它是傳統意義上專用硬體和基礎設施裡的「網路」，具有可能遭受攻擊和危害的關鍵弱點。事實上，比特幣是一種軟體協議；一種內部的流程，可以在全球分佈的數十億台電腦中的任何一台執行。比特幣沒有任何「單點故障」，它並不依賴世界上某個地方有個不可或缺的硬體架構。任何執行比特幣軟體的電腦，都可以連接到比特幣網路進行操作。從某種意義上說，它類似於網際網路，因為它是一種允許電腦連接在一起的協議；並不是指連接它們的基礎電腦設備。比特幣相關資訊所需傳輸的數據量並不大，只佔網際網路總流量的一小部分。比特幣並不需要像網際網路上其他用途所需的大流量基礎設施，因為它的區塊鏈實際上每 10 分鐘只傳輸 1MB 的數據。全世界有無數的有線和無線技術用於傳輸數據，任何特定用戶只需要其中一種連線技術，就可以連接到比特幣網路。為了創造一個比特幣用戶無法相互連結的世界，而去損害整個世界的資訊、數據和基礎設施，絕對會造成毀滅性的災難。因為現代社會的生活大量倚仗相互的連結，許多重要的服務和重大的生死問題，都依賴於這些基礎通信設施來維持連結。嘗試同時關閉所有網際網路基礎設施，可能會對嘗試攻擊的任何社會造成重大損害，卻還無法阻止比特幣的流通，因為那些被分散的機器，還可使用協議和加密通信相互連結。世界各地有太多的電腦和連結設備由更多的人使用中，因此任何力量都無法讓它們「同時」停止運轉。唯

一發生這種情況的場景，可能就是某種「世界末日」的場景了，不過那時應該也不會有人想知道比特幣到底還能不能運作。在比特幣經常被談到的所有威脅中，我認為這是最不可信或最沒意義的一種。

## 節點成本上升和節點數下降

我們不必想像未來的科幻場景裡，有人想要破壞人類的電信基礎設施，並且努力的嘗試刪除軟體程式。比特幣在設計的基礎上，存在著更為現實的威脅。比特幣作為健全貨幣的特性，代表其供應量無法迅速增加，而且作為不受檢查的數位現金，也不會有第三方干預的可能性，這些完全取決於網路「共識規則」的特性難以改變，貨幣供應量當然也無法改變。如前所述，破壞這種穩定現狀的前提，在於「擺脫」目前的共識規則，這是風險非常高且負面的舉動，尤其是在網路上的其他成員，並沒有跟著一起採用「新共識規則」的情況下更是危險。但是，這個舉動的風險實在太高且不太可能發生，因為執行該軟體的節點數量夠多，在它們之間進行串通可能不切實際。但萬一運行比特幣節點的成本明顯增加，便可能會讓很多用戶難以運行節點，因而減少網路上的節點數量。如果是只剩幾十個節點的網路，便不再是有效的去中心網路，因為操作它的少數節點很可能串通，改變網路共識規則，以得到他們自己的利益，甚至破壞網路。

我認為這點仍然是比特幣在中期和長期發展裡，最嚴重的技術威脅。就目前而言，個人執行節點的主要限制因素是網際網路頻寬。只要區塊保持在1MB以下，應該是可以管理的。增加區塊大小的硬分叉，會導致節點運行成本上升，造成操作節點數量減少。但是就像前面提過的威脅一樣，雖然在技術上一定可行，但仍然不可能實現，因為系統的經濟激勵措施會阻礙這種威脅，正如目前為止普遍「拒絕」增加區塊大小的嘗試所證明的一樣。

## SHA-256 哈希算法的突破

SHA-256 散列函數是比特幣系統運行不可或缺的一部分。簡而言之，散列是一個過程，可以將任何數據流作為輸入，並使用不可逆的數學公式，轉換成固定大小的數據集（稱為散列）。換句話說，使用這個函數為任何數據生成一個哈希值是微不足道的，但我們無法從哈希值回溯原始數據串。而隨著處理能力的提升，電腦在將來有可能會逆運算出這些散列函數，如此將會使所有比特幣地址變得容易盜取。

我們很難判斷這種情況是否會發生以及何時可能發生，果真如此，便會對比特幣構成非常嚴重的技術威脅。解決這個問題的技術方法是切換到更強大的加密形式，但棘手的部分是必須協調一個硬分叉，讓網路的大多數節點都放棄舊的共識規則，搬到新散列函數加密的新共識規則鏈上。先前提到在協調分叉難度所討論過的問題都會碰到，但因為這次是面對算法被突破的真實威脅，任何選擇留在舊鏈上的比特幣持有者，都很容易受到駭客攻擊，因此造成絕大多數用戶節點，很可能都會參加這個新的硬分叉。剩下唯一有趣的問題，就是這個硬分叉是否能讓所有用戶遷移到同一個鏈，或者是否會讓比特幣舊鏈因不同加密法而散成好幾個分叉？雖然 SHA-256 加密肯定有機會被破解，但網路用戶的經濟激勵應該是切換到更強的算法，而且是「一起」切換到同一個新算法上。

## 回歸健全貨幣

雖然大部分關於比特幣如何失敗或被摧毀的討論，都集中在技術攻擊上，但攻擊比特幣更有希望的方法，便是破壞它在使用上的經濟激勵。如果想用前面提到的任何方式來攻擊或摧毀比特幣，似乎都不太可能成功，因為這些攻擊在根本上與推動使用比特幣的經濟激勵相互衝突，就像政府以法律禁止使用方向盤或刀具一樣不可行，因為只要該項技術對人類有

利，便難以禁止使用，人們會繼續尋找各種合法或不合法的方式來使用。禁止某項技術的唯一方法並非禁用，而是發明更好的替代品或減少使用它的需求。例如打字機雖然永遠不會被禁止或立法停用，但個人電腦的崛起，確實很有效的扼殺了打字機的生存空間。

比特幣的需求，源起於世界各地都有人想繞過政治的控制來進行交易，並想擁有能夠抵抗通貨膨脹的價值儲存。只要政治當局對個人轉移資金的需求，繼續施加約束和限制；只要政府資金仍是寬鬆貨幣，貨幣供應量仍可依照政治家的決定輕易擴大，那麼對比特幣的需求便會繼續存在，而且它無法擴大的供應成長量，更可讓它的價值隨著時間經歷而推升，於是吸引更多人將比特幣作為價值儲存。

所以我們可以假設一下：如果整個世界的銀行和貨幣體系，被十九世紀後期的黃金標準取代的情況。當時的個人自由和健全貨幣是最重要的，因此對比特幣的需求可能就會顯著下降。這種做法會導致比特幣的需求大幅減少，讓它的價格跟著大幅下跌，於是讓比特幣持有者蒙受損失，增加了比特幣的波動性，於是它會退回多年前的價格水準。而隨著比特幣價格波動增加，以及相對可靠且相對穩定的國際黃金標準儲備貨幣的可用性提高，使用比特幣的激勵也會明顯下降。在一個政府有所規範且通貨膨脹受到黃金標準約束的世界裡，黃金的先發優勢和相對穩定的購買力，將成為比特幣難以逾越的障礙，也會降低比特幣用戶的快速成長，因而阻止它達到夠大的規模或穩定的價格。

然而，在現實的情況裡，全球恢復使用健全貨幣或政府允許自由轉移資金的可能性很小，因為這種概念跟世界各地多數政治家和選民的觀念截然不同，這幾代人一直被灌輸「政府」應該對金錢和道德加以控制，因此認為這些限制對任何社會的運作都是必要的。此外，即使有機會進行這種政治和貨幣轉型，比特幣供應成長率的下降，也可能繼續讓它成為對許多

人具有吸引力的「投機」賭注，因而讓比特幣進一步成長並有機會扮演更大的貨幣角色。在我的評估中，「全球貨幣回歸黃金標準」可能是對比特幣的最大威脅，但它不僅不太有機會發生，也不太可能徹底摧毀比特幣。

另一種打擊比特幣的可能性，便是發明一種優於比特幣的新形式健全貨幣。許多人似乎認為「模仿」比特幣的其他加密貨幣可以達成這個目標，但我堅信複製比特幣設計的其他數位硬幣，都無法與比特幣競爭健全貨幣的地位，原因我將在本章下一節詳細討論，其內容在講比特幣是唯一真正去中心化的數位貨幣，它自發地成長為礦工、程式人員和用戶之間的「精密平衡」，沒有人可以控制它。只有如此才有可能開發出這種設計的貨幣，一旦此貨幣明顯可行，任何「複製」的嘗試，都將是一個由上而下、集中控制的網路，永遠不會逃脫其創作者的控制。

因此，當我們談到比特幣的結構和技術時，任何複製它的數位硬幣都不可能取代比特幣。實作數位現金和健全貨幣的新設計與技術時，很可能會產生這種「複製」型的競爭對手。當然在一種創新技術被發明之前，實在無法預測未來將會出現這種技術，而且經歷多年來對數位現金問題的熟悉，讓我們都很清楚比特幣並非「容易設計」的全新發明。

## 替代幣

雖然比特幣是點對點電子現金的首例，但肯定不會是最後一個。一旦中本聰把比特幣公開後，比特幣也成功獲得了價值和採用者，因此許多人便複製生產出類似的貨幣。Namecoin 是第一個使用比特幣代碼並於 2011 年 4 月開始營運的貨幣。根據 [coinmarketcap.com](http://coinmarketcap.com) 網站的數據，截至 2017 年 2 月為止，世界上至少出現了 732 種數位貨幣。

雖然一般認為這些數位貨幣與比特幣之間存在競爭關係，其中可能會有在未來能夠超越比特幣的機會，但事實上它們並沒有辦法與比特幣競爭，因為它們永遠不會有跟比特幣一樣作為數位現金和健全貨幣的特性。為了使某種數位系統可以作為數位現金，它必須能夠不受任何第三方的控制；其運作也必須根據協議並符合用戶的意願，而且任何第三方都無法阻止這些支付行為。經過多年觀察「替代幣（altcoin，又稱山寨幣）」的創建，似乎不可能有任何替代幣，有機會重新建立比特幣這種在利益相關者之間，相互存在的對抗地位，可以用來阻止任何一方控制其中的支付行為。

比特幣是由一位匿名程式師設計的，他的真實身分仍然未知。他將這個設計發佈在一個給愛好密碼學的程式人員所使用的冷僻郵件列表中，並在幾個月後收到回饋，接著他與已故的程式設計師 Hal Finney（2014 年 8 月去世）啟動了比特幣網路。與 Finney 進行了幾天交易，並測試軟體的使用後，更多成員開始加入網路進行交易和挖礦。中本聰在 2010 年中期消失，只留下「轉往其他項目」，然後就沒人聽過他的消息<sup>註 9</sup>。很可能有大約 100 萬比特幣存放在中本聰的帳戶中，但是這些錢沒被動過。中本聰真的非常謹慎，確保自己不會被肉搜出來，直到今天，沒有任何確實的證據，可以確定 Satoshi Nakamoto（中本聰）的真正身分是誰。如果他想被認出來，應該早就挺身而出了。如果他留下任何可以追蹤到身分的證據，那麼很可能已經找到他了。他的所有著作和通訊內容，都被調查人員和記者瘋狂追尋而徒勞無功。現在該是參與比特幣的每個人，停止詢問

---

註 9 此後，Nakamoto 可能還出現過兩次，一次是否認他的真實身分是名為 Dorian Prentice Satoshi Nakamoto 的日裔美國工程師，這是被「新聞週刊」雜誌認為真正的 Nakamoto 的人，不過證據很薄弱，只有他的名字和電腦能力上的巧合。另一次則是對比特幣擴容的辯論提出意見。不過目前尚不清楚這些電子郵件是否真的是由 Nakamoto 本人所發，或者是否有人洩露了他的電子郵件帳戶，因為我們知道他曾經用過的電子郵件帳戶，已經被洩露出來了。



Nakamoto 身分問題的時候了，因為這跟接受技術與運作無關，就像輪子的發明者到底是誰，一樣的不再重要。

由於 Nakamoto 和 Finney 已不在我們身邊，所以比特幣並沒有任何中央權威人物或領導者能在發展過程中，決定比特幣的方向或行使影響力。即使是與中本聰密切接觸的 Gavin Andresen（也是比特幣界最常見的面孔之一），都無法對比特幣發展方向產生影響。媒體經常引用據說是中本聰發送的最後一封電子郵件，裡面提到：「轉往其他項目，Gavin 和大家都做得很好」<sup>註 10</sup>。Gavin Andresen 多次嘗試增加比特幣區塊的容量，但他提出的所有建議都未能獲得節點營運商關注。

比特幣在第 8 章提過的所有指標裡，繼續成長和發展，任何個人或團體對它的權威性，都已經減弱到無足輕重。比特幣可以當作一個自有主權的代碼，因為沒有任何外部權威可以控制它的行為。只有比特幣的規則可以控制比特幣，任何實質改變規則的可能性，都顯得不切實際，而且因為成員們對「維持現狀」的偏好，會持續形成每位參與成員的激勵。

比特幣代碼的主權是以工作量證明作為後盾，讓它成為雙重支付問題與成功數位現金的真正有效解決方案。正是這種無需信任第三方的特性，讓其他數位貨幣無法複製。任何在比特幣之後才建立的數位貨幣，都將面對嚴重的存在危機：因為比特幣已經存在，擁有更多的安全性、處理能力和穩定的用戶群，任何想要使用數位現金的人，自然不會喜歡規模較小且感覺不太安全的替代品。由於複製代碼產生新硬幣這件事幾乎是零成本，因此模仿的硬幣大量出現，除非有個團隊致力於培育、成長、編碼與保

---

註 10 作者無法確定這封電子郵件的真實性，但該電子郵件已被廣泛引用，以致於麻省理工學院技術評論（MIT Technology Review）上，發表了一篇關於 Andresen 的長文，題目為「真正建立比特幣的人（The Man Who Really Built Bitcoin）」，宣稱就比特幣的發展而言，Andresen 甚至比 Nakamoto 更為重要。

護，否則任何單一數位貨幣都不可能發展出明顯的成長動力。比特幣作為第一個發明的數位貨幣，所展示出的數位現金和健全貨幣價值，便足以確保需求會不斷的成長，也只有當它背後的建立者，是個完全沒花錢幫它推銷的「匿名」程式設計師時，它才會真正的成功。由於所有替代幣都非常容易重新建立，因此並沒有像奢侈品一樣的真实世界需求性，必須有人積極的建立和增加這種需求性。

這就是為何目前幾乎所有的替代幣都有一個團隊在負責；他們開始為這個替代幣項目、推銷、設計行銷材料，並把自己當成新聞一樣，發新聞稿給媒體，而且會在大家都還沒聽到消息之前，先挖走大量硬幣。這些團隊是眾所周知的名人，無論他們如何努力嘗試，都無法證明他們不會主動控制貨幣的走向，破壞數位貨幣不該由任何第三方編輯或控制的特性。換句話說，在比特幣精靈走出神燈之後，任何試圖建立替代比特幣的人，都只能透過大量投資來維持該替代幣，以便有效的進行控制。只要有某一方對數位貨幣擁有主權，那麼這種貨幣就不能作為一種數位現金形式，而應該說成是一種中介支付形式——而且效率會非常低。

如此便給替代幣的設計者帶來兩難：如果沒有開發商和行銷團隊的積極管理，任何數位貨幣都不可能在超過 1000 多種的數位貨幣之海裡，吸引到任何關注或資本。一旦團隊積極管理、開發和行銷，便無法可靠證明貨幣不會被這些人控制。由於一組開發者們控制著大部分硬幣、處理能力和程式編碼上的專業知識，因此這種貨幣實際上便是一種集中控制的貨幣，並由團隊利益決定它的發展道路。集中式的數位貨幣並沒有錯，在沒有政府限制的情況下，最好能在自由市場上擁有這些競爭對手。但是集中式貨幣存在著一些深刻、根本的錯誤，採用了高度繁瑣且效率不足的設計，使它的優點只剩下消除了單點故障。

對於以 ICO（Initial Coin Offering、數位貨幣首次公開募資）起始的數位貨幣，這種問題會更加明顯，因為這會讓一群高曝光率的開發人員與投資者公開交流，使整個項目有效變成一個集中項目。以太坊（Ethereum、比特幣之外市值最高的數位貨幣）的嘗試與磨難，活生生說明了這一點。

去中心化自治組織（DAO）是以太坊網路上首次實施的智慧合約，攻擊者為這份智慧合約投入超過 1.5 億美元後，便能執行代碼，將 DAO 所有資產的三分之一，都轉移到自己的帳戶。這樣的攻擊並不能算是竊盜，因為所有存款人本來就已接受這些錢只能由程式代碼控制，攻擊者除了執行由儲存者自己接受的代碼之外，什麼也沒做。在 DAO 被駭之後，以太坊開發人員竟然創建了一個新版本的以太坊，也就是刪除這種令人為難的錯誤，然後沒收攻擊者的資金，分發給受害者。這種重新加入「主觀」人性化管理，跟「客觀」的將程式碼納入法規內完全不同，也等於質疑了智慧合約的整個基本原理。

如果處理能力第二大的網路，可以在交易不符合開發團隊利益的情況下，改變區塊鏈記錄，那麼替代幣真的用「處理能力」來調節貨幣成長量的概念，將會無法成立。持有貨幣、處理能力和編寫程式的技能，都集中在一群像企業夥伴一樣的人手裡，當然會破壞採用區塊鏈結構的整個目的。

此外，實在很難預見這些私人發行的貨幣，在背後有一個明顯可見的團隊時，還能夠有機會提升到「全球貨幣」的地位。如果貨幣顯著升值，這一小撮建立者將變得極為富有，彷彿具有過去徵收「鑄幣稅」的那種權力，這通常是現代世界裡的民族國家才能扮演的角色。因此中央銀行和國家政府，並不太可能會給這種破壞它們權威的人好臉色看。中央銀行可以很容易的讓這些貨幣背後的團隊被摧毀，或直接改變他們的操作方式，以避免這些貨幣與國家法幣競爭。所以並沒有任何單一的替代幣，能

夠展現跟比特幣一樣具有令人印象深刻的變革彈性，因為這是取決於真正的去中心化性質，以及每個人遵守目前共識規則的強烈動機。我們之所以可以這麼說，是因為它在網際網路的曠野成長九年之後，依舊沒有任何權力可以控制它，而且還可以很有技巧的排除掉那些想要改變它的「高度協調或資金充足」的活動。相較之下，替代幣是具有「友好人士」的明顯友好文化，可以讓大家在團隊項目裡共同努力。雖然這點對一個新創企業來說很好，但對於希望展現數位貨幣在固定貨幣政策的「信用承諾」來說，簡直就是一種詛咒。任何特定替代幣背後的團隊，若決定改變貨幣政策，應該很容易就能達成。例如，以太坊尚未對未來的貨幣政策有任何明確的願景，也想把這件事情留給社群討論。雖然以太坊的社群精神可能產生奇蹟，但這樣並無法建立一個全球性的健全貨幣，不過持平的說，以太坊並沒有宣稱自己要做全球性的健全貨幣。無論是因為有意識的，或為了避免被政治當局請去問話，或者說是營銷噱頭也好，大多數替代幣都不會把自己推銷為比特幣的競爭對手，而會說成是執行「與比特幣不同」的任務。

沒有任何案例證明替代幣宣稱「自己也能做到」比特幣原始設計的某個用途時，會為它帶來什麼好處。而且除了比特幣之外，也沒有其他替代幣發明了比特幣不具備的差異功能或特徵。然而這些替代幣卻都擁有「自由交易的貨幣」，因為這點對執行線上應用的複雜系統來說不可或缺。

這種新網路應用程式需要「自己的」去中心化貨幣，其想法上像是絕望的傻子在盼求，雖然自己無法解決「用戶需求」的問題，但希望能在經濟上有利可圖。然而現實世界的企業不發行自己的貨幣是有原因的，因為沒人想擁有只能在一個企業裡消費的貨幣。持有資金的關鍵是希望讓持有的流動資金，越容易花越好。若是持有只能在特定供應商使用的貨幣，其提供的流通性就會很少，而且很難達成任何目的。人們會自然的傾向持有流動性較強的支付手段，任何事業若堅持以自己的自由交易貨幣支付，只會為潛在客戶帶來極高的成本和風險。

即使真的需要某種形式的「代幣」運行的企業，例如遊樂園或賭場等，他們的代幣跟流通貨幣比較起來，在價值上是固定的，因此客戶很清楚知道他們得到了什麼，可以進行準確的經濟計算。如果有人說這些所謂革命性的去中心化貨幣，真的提供了任何現實世界裡具有價值的應用，而且也用了自己的自由交易貨幣來支付，實在是令人難以置信。

事實上，在審視這塊領域多年後，我還沒有找到一種能提供任何市場需求的產品或服務的數位貨幣。而高度吹噓的「未來」去中心化應用，似乎從未到來，但一般認為對替代幣營運至關重要的硬幣，每月仍持續增加數百個。讓人不禁懷疑，這些革命性貨幣的唯一用途，是否就在讓建立者賺大錢。

除了比特幣之外，沒有其他貨幣可以真的聲稱不受任何人控制，因此，想利用「支撐比特幣的複雜結構」的整個觀點做宣傳，並沒有任何實際意義。複製比特幣的設計，然後製作一個稍微不同的模仿品，這點並沒有任何原創性或難度。目前為止，也已經有數千種這樣的模仿品。經過一段時間以後，應該會看到更多這類數位硬幣進入市場，稀釋其他替代幣的品牌。非比特幣的數位貨幣，總結起來是輕鬆賺錢的，沒有任何替代幣會被認為有自己的特殊優點，因為它們在表現上並沒有任何不同，都跟比特幣所表現的一樣，但與比特幣的區別在於它們的供應和設計，非常容易被改變，然而比特幣貨幣政策裡的所有意圖和目的則是堅定不移的。

在這些貨幣當中，是否有人能提供除了比特幣市場需求以外的成功服務？這是個懸而未決的問題，但顯而易見的是，它們無法與比特幣競爭成為「無信任」的數位現金。因為雖然它們都選擇遵行比特幣的儀式，但若只是假裝正在解決額外的事情，並不會激發人們對它們的信心，只會讓人覺得一切是為了讓它們的創建者變得更富有罷了。模仿中本聰設計的成千上萬仿製品，也許是最真誠的「致敬」形式，但他們一直未能提出超越中

本聰所提供的更多東西，也就證明了他的成就真的非常獨特。比特幣設計唯一有價值的補充，便是由能力極強的志願程式設計師們所無私完成的，他們花了很長的時間來優化比特幣程式代碼。而現在許多不那麼稱職的程式員，以市場行銷和毫無意義的流行語，重新打包中本聰的設計，想要獲得大量資金，但完全沒有添加具有任何現實世界實際需求的功能。這些替代幣的成長，無法脫離政府資金尋求輕鬆投資的背景想法，因此很容易在大規模投資中，形成巨大泡沫。

## 區塊鏈技術<sup>註 11</sup>

由於比特幣價值的驚人上升，加上操作程序和技術細節的難度，因此存在了大量的混淆誤解。也許最持續也最高調的混淆是以下這種觀念：比特幣操作的機制——將交易放入鏈接在一起形成分類帳的區塊——也可以用來解決或改善經濟、社會問題，甚至進行「革命性的創新」，就像現在發明的每個新奇玩具一樣。「比特幣並不重要，但潛在的區塊鏈技術是有希望的…」，這是從 2014 年至 2017 年期間，由某些銀行業執行長、記者和政客共同反覆考量的口頭禪。不過他們擁有一個共同點：不了解比特幣到底如何運作（圖 22）。

---

註 11 本節重點大量討論我的論文：「區塊鏈技術：有什麼用途？（Blockchain Technology: What Is It Good For?）」，發表在《銀行與金融法評論》，第 1 期，第 33.3 卷，2018 年。

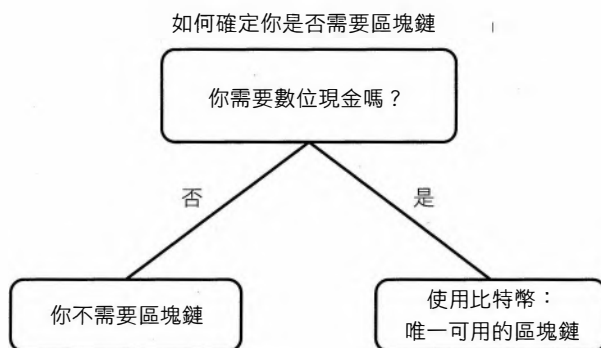


圖 22 區塊鏈決策圖

區塊鏈技術的僵化思考是「草包族科學 (cargo cult science)」的絕佳範例，這是物理學家費曼 (Richard Feynman) 所帶起的一個想法。根據報導，美國軍方在第二次世界大戰期間，為協助南太平洋島嶼的軍事行動而蓋了許多飛機跑道。飛機飛來的時候，通常會順便帶禮物給島上的居民，因此過去島民常常享用到這些禮物。而戰爭結束後，飛機不再飛回這些跑道，當地人想盡辦法要讓飛機和貨物可以飛回來，因此在絕望中，他們試著模仿長期以來的軍用機場地面管制員的行為，認為如果他們把一個人放在一個帶天線的小屋裡，並且點燃火把，就像過去軍事地面管制員所做的那樣，那麼飛機就會飛回來帶給他們禮物。這樣的策略明顯行不通，因為地面管制員的程序並非憑空創造飛機；它們只是一項精心製作的技術過程裡的一個組成片段，從飛機的製造開始到離開基地之間，都是南太平洋島民所無法理解的內容。

就像這些島民一樣，認為可以將區塊鏈技術作為產生經濟效益一環的人，並不了解它只是一個更大的技術過程裡的一部份。比特幣建立分類帳的真實和有效性的機制，非常錯綜複雜，但它有一個明確目的：在不需要信任第三方的情況下，在網路上發行貨幣與移動價值。「區塊鏈技術」在某種程度上存在，但並非一種有效廉價或快速的線上交易方式。與集中式的

解決方案相比時，「區塊鏈」的實際效率低且速度慢，唯一提供的優勢是不需要第三方中介信任。因此這種技術唯一可能的用途，只在「無信任」對用戶有相當重要的價值時，但也會因此讓成本增加並損失效率。而它可以成功消除第三方中介的唯一過程，便是移動網路原生硬幣的過程，因為這些區塊鏈的代碼對鏈外的任何事物來說，並無集中控制的能力。

我們可以透過比較來了解比特幣運行交易的方法「效率極低」，如果移開「去中心化、工作量證明的驗證、挖礦與無需第三方信任」的絆腳石，直接運行比特幣的集中版，它就變成生成硬幣的演算法，以及用來處理大約每天 300,000 筆交易的硬幣所有權「資料庫」。這些任務相當簡單，任何現代個人電腦都能可靠執行。事實上，一台普通、現成的消費型筆電，每秒可以處理大約 14,000 筆交易，或者換算成當前比特幣每日交易量，可以在 20 秒內完成<sup>註 12</sup>。而如果用這台陽春的筆記型電腦，處理比特幣的全年交易量，幾乎不必花超過兩小時。

然而，在筆電上運行這種貨幣的問題，在於它需要信任筆電所有者以及筆電本身的安全和保障。為了讓如此簡單的軟體系統運行且不需任何一方信任，也讓欺騙交易記錄或改變貨幣發行速度的企圖無法得逞，目前就只發現唯一一種可行設計，也就是比特幣的去中心化點對點網路「工作量證明」。這不是一個簡單的軟體問題，這是電腦程式員花幾十年時間嘗試不同設計，才發現有辦法證明這一點。今天一台好的消費級筆電的哈希值，大約為每秒 10MHash，而比特幣網路每秒大約集中處理 20EHash，相當於 2 兆台筆記型電腦。換句話說，為了消除對信任的需求，運行簡單貨幣和資料庫軟體的處理能力，需要增加大約 2 兆倍。當然在貨幣及交易上並

---

註 12 詳見 Peter Geoghegan 的部落格文章，解釋他是如何在個人電腦上實現此一目標。參閱 <http://pgeoghegan.blogspot.com/2012/06/towards-14000-write-transactions-onmy.html>。



不需要如此多的處理能力，讓整個系統「無信任」才需要。這種對於使用區塊鏈技術運行的任何計算過程，必須滿足兩個標準：

首先，去中心化所帶來的收益，必須足以證明額外成本的合理性。對於任何「仍需某種形式信任」而讓第三方實施一小部分信任的過程而言，花在去中心化的額外成本是非常不合理的。為了處理法律管轄範圍內真實企業的合約，仍會造成這些合約在實施上的相關法律監督，這些監督便能超越網路共識，使得去中心化所花費的額外成本毫無意義。這點同樣適用於金融機構資料庫的去中心化，這些資料庫也還需作為彼此或客戶，在自己營運上的可信任第三方。

其次，初始過程本身必須夠簡單，以確保能夠在許多節點上運行分佈式分類帳，而且要讓區塊鏈不會變得太笨重而無法發佈。但隨著整個過程不斷重複，區塊鏈的大小將會增加，並讓分散節點難以紀錄區塊鏈的完整副本，因而確保只有少數大型電腦可以操作區塊鏈並使其分散化。請注意這裡帶有分類帳的節點，與解決工作量證明的專用礦工之間的區別，第 8 章討論過：礦工需要花費巨大的處理能力將交易提交給聯合分類帳，而節點只需要很少的電力與處理能力，便能保留分類帳副本，以驗證礦工交易的準確性。這就是為何節點可以在一台個人電腦上運行，而礦工會具有成千上萬台個人電腦的處理能力。如果分類帳本身的操作變得過於複雜，節點就需要用到大型伺服器而非個人電腦了，這便會破壞節點分散的可能性。

比特幣區塊鏈對每個區塊的大小設置了 1MB 的限制，因而限制了區塊鏈的成長速度。這項限制可以讓簡單的電腦也能夠維護和運行節點。如果每個區塊的大小增加，或者區塊鏈被用於更複雜的過程（例如區塊鏈狂熱者所吹捧的那些用途），那麼整個系統就會變得太大而無法在個人電腦上運行。若將網路的運行集中在大型機構所擁有與營運的幾個大型節點上，便會打破整個去中心化的特點。

目前為止，「無信任」的數位現金是區塊鏈技術唯一成功實施的原因，在於它是一個乾淨簡單的技術流程，讓它的分類帳成長可以相對緩慢。這代表比特幣網路的成員，可以在世界各地使用家裡的電腦進行連接，可以預測通貨膨脹有所限制，也只需要很少的處理能力即可。但這樣形成的去中心化與無信任，可以為終端用戶提供巨大的價值，如第 8 章所述。目前所有其他貨幣媒介，都是由能夠使供應膨脹的一方所控制，以便可以從需求增加中獲利。對於法定貨幣、非貴重金屬以及黃金來說都是如此。黃金由中央銀行大量持有，可以出售到市場上，防止它過快升值而取代法定貨幣。但自從取消黃金標準以來，比特幣是第一個成為世界上任何人都可以輕鬆持有的健全貨幣。這種不太可能發生的「輕量級計算與重要經濟意義」的組合，便是為何比特幣網路的處理能力，會增加到史上最大網路的意義所在。事實證明在經過八年多的時間裡，並未找到另一個有足夠重量級價值的用途，可以合理的分佈在數千個節點成員身上，同時又能足夠輕量化的允許分散開來。

這種分析的第一個含義，就是任何在比特幣協議裡改變區塊大小的議題，都不太可能通過的原因。不僅因為前面提到的「不變性」原因，還因為它可能會妨礙大部份節點營運者管理自己的節點。但他們可以自行決定要運行哪個軟體，我們也可以安全的假設大量固執的節點營運者，將會繼續使用目前的軟體，繼續持有他們手上的比特幣。任何嘗試升級比特幣軟體的舉動，只會變成另一個毫無價值的替代幣，就像目前已存在的數百種替代幣一樣。

這種分析的第二個含義是「區塊鏈技術」的應用。這些經常被吹捧為銀行或資料庫界的革命性技術，也將注定完全失敗。除了花俏的演示外，它們通常沒有別的用途，也永遠不可能轉移到現實世界來，因為無信任第三方對於想操作它們來拓展業務而言，永遠是一種「低效率」的方式。這種專門設計來消除第三方中介的技術，最終可能會被用在本來打算取代的中介機構上，其別有企圖的目的，將超出可能的用途範圍。

雖然有許多更方便、更簡單的方法可以記錄交易，但區塊鏈是消除對信任第三方需求的唯一方法。交易被提交到區塊鏈，驗證者為了獲利競相驗證交易，在交易中沒有一個人可以依賴或必須被信任。相反的，詐欺交易會被其他網路成員立即檢測和退回，因此他們有強烈的動機來確保網路的完整性。換句話說，比特幣是一個完全基於「繁瑣且昂貴」的驗證系統，因此它可以消除各方之間的任何信任或責任的需求：也就是 100% 的驗證和 0% 的信任。

而跟圍繞著比特幣的大量炒作訊息不同的是，這種消除對第三方信任的需求，對商業和生活上的所有用途來說，並非絕對是件好事。一旦理解了比特幣的運作機制，就可以明顯的知道轉移到不依賴信任第三方的系統時，需要付出的代價。好處在於個人主權可以凌駕於協議、抗審查、限制貨幣供應成長與技術參數的不變性，缺點則在於需要強大的處理能力來執行相同的工作量。除了天真的未來主義式炒作之外，沒有任何理由讓人相信這是值得花這麼多錢的魔鬼交易。唯一可能值得這種如此權衡交換的場合，應該是用來管理「全球同質性跨國健全貨幣」的情況，其中包含兩個重要的因素：首先，運行這種系統的超高成本，可以藉由取得局部的全球貨幣市場來慢慢彌補，因為其市場價值約有 80 兆美元。其次，如同前面說過的，健全貨幣的特性在於沒有人能夠控制它，因此可預測的「不可變」演算法，相當適合這類任務。這個問題我思考多年，因為在任何其他事業用途裡，都找不到相等重要性的類似用途，可以值得去掉中介所帶來的高額成本，加上透明簡單到取消所有人的自由裁量權等，也都是很值得的優點。

拿汽車來類比應該會很有啟發性。1885 年，Karl Benz 將一台內燃機加到馬車上，用它誕生了第一輛自動交通工具時，這個動作的明確目的是將馬從馬車上移走，讓人們不必經常處理馬糞。Karl Benz 並沒有試圖讓馬可以跑得更快。如果把重金屬引擎裝在馬背上，並不會使它跑得更快；只會減慢馬的速度，馬糞也依舊存在。同樣地，如第 8 章所解釋，讓比特幣

網路運行所需的巨大處理能力，消除了藉由信任第三方來處理支付或確定貨幣供應的需求限制。如果第三方依舊存在，所有處理能力都將是毫無意義的浪費電力。

只有時間才能證明比特幣的模式是否繼續受到歡迎和採用，它有可能成長而取代許多金融中介機構，也可能停滯甚至失敗且消失，唯一不可能發生的，就是比特幣的區塊鏈設計變成對中介有利，而非消除掉信任第三方的用途。

對於任何進行支付、交易或記錄保管的信任第三方而言，區塊鏈是一種昂貴且效率低的技術。非比特幣的區塊鏈會結合兩個世界裡最糟的部份：區塊鏈的複雜結構加上信任第三方的成本與安全風險。難怪發明了八年後，區塊鏈技術除了在專門設計給商業應用的比特幣之外，還沒有在任何一個成功的、準備上市的商業應用裡，有所突破。

但情況反過來講，媒體、政府、學術界、工業界和世界經濟論壇，都已就區塊鏈技術的潛力進行大量的宣傳、會議和高調的討論。政府和機構已經在風險資本、研究和市場行銷方面投入數百萬美元，這些都是被炒作所誘惑，但並未得到任何實際結果。

儘管那些「區塊鏈顧問」已經建立了股票交易、資產登記、投票和支付清算的原型。但正如佛蒙特州政府最近得到的結論顯示：這些區塊鏈技術都沒有進行商業應用，因為它們比依賴資料庫和軟體套件的簡單方法更為昂貴<sup>註 13</sup>。

---

註 13 Stan Higgins，「佛蒙特州稱區塊鏈記錄系統太昂貴」，Coinbase.com，2016 年 1 月 20 日。

而在銀行界，確實沒有率先採用比自己目前所用更先進技術的良好紀錄。雖然摩根大通首席執行長 Jamie Dimon 於 2016 年 1 月，在瑞士達沃斯宣傳區塊鏈技術，但他們自己銀行的開放式金融交易介面——一種從 1997 年開始為聚合商提供客戶資訊的中央資料庫——居然已經停用了兩個月。

相較之下，比特幣網路誕生於中本聰推出該技術兩個月後的區塊鏈設計裡。直到今天，它仍然不間斷地運行並且成長到價值超過 1500 億美元的比特幣。區塊鏈是解決電子現金問題的方法。因為它有效，所以它迅速成長，而中本聰匿名工作，並且只透過電子郵件簡單地溝通了大約兩年，完全不需要任何投資、風險投資、會議或廣告等。

從這裡的討論可以明顯看出，「區塊鏈技術」的存在，而且真的可以用來解決任何具體問題的概念，實在非常可疑。把區塊鏈結構理解成是在比特幣還有模仿者操作及測試網路的一部分，可能會更精確。然而，「區塊鏈技術」這個術語經常被拿來簡化說明。本章下個部分探討區塊鏈技術最常被吹捧的應用範例，而後面的部分則會確定這些問題的主要障礙。

## 區塊鏈技術的潛在應用

與區塊鏈技術相關的新創公司 and 研究項目，大致得出了結論，認為區塊鏈的潛在應用可分為三個主要領域：

### 數位支付

目前支付清算的商業機制依賴集中分類帳，用來記錄所有交易並維持帳戶餘額。在實際操作時，交易會從交易方傳輸到中介，檢查有效性後，兩個相關帳戶都會被調整。而在區塊鏈中，交易會被傳輸給所有網路節點，也就涉及到更多傳輸與更多處理能力和時間。同時交易也成為區塊鏈

的一部分，複製到每個成員的電腦上。這比集中清算更慢也更昂貴，也有助於解釋為何 Visa 和 MasterCard 每秒可以清算 2,000 筆交易，而比特幣最多可以清算 4 筆。比特幣的區塊鏈並非用來進行更快、更便宜的交易，而是用在不需信任第三方中介的交易：交易被清算是因為節點競相驗證它們，但沒有節點必須被信任。要讓目前的第三方中介機構，想像它們可以透過使用一種技術改進其表現能力，但會大量犧牲效率與速度，而且目的只是為了「移除自己」，這點當然行不通。對於由中央方控制的任何貨幣而言，集中記錄的交易會更為有效。我們可以清楚地看到區塊鏈的支付應用，必須使用區塊鏈自己的去中心化貨幣，而非採用集中控制的貨幣。

## 合約

目前的合約是由律師起草、法院判決，執行則交由警方。而以太坊類的智慧合約（smart contract）密碼系統，將合約編碼為區塊鏈，使其自動執行，不可能上訴或撤銷，也超出法院和警察的管轄範圍。「程式碼就是法律」是智慧合約程式設計師們的座右銘。這個概念的問題在於律師用來起草合約的語言，較容易被更多人理解，而智慧合約起草人使用的代碼語言，較少人能理解。全世界可能只有幾百人擁有技術專長，能夠充分了解智慧合約的含義，但他們也還可能漏掉一些明顯的軟體錯誤。即使越來越多人熟練建立這些合約所必需的程式語言，但最熟悉它的這些少數人，仍持續比其他人更有優勢。在程式碼的競爭裡，最熟練的人總是比起其他人更有戰略上的優勢。

一切情況都在以太坊網路的去中心化自治組織（DAO）首次實施智慧合約時，變得更為明顯。攻擊者為這份智慧合約投入超過 1.5 億美元後，執行程式碼將 DAO 所有資產的三分之一轉移到自己的帳戶。如同之前所說，將這次攻擊描述為竊盜可能不太準確，因為所有存款人都已把他們的錢交給程式碼控制。攻擊者除了執行存款人接受的程式碼之外，什麼也沒

做。而在 DAO 遭駭後，以太坊開發人員竟然創建了一個新版本的以太坊，讓這場令人感到難堪的錯誤從未發生。這種重新加入「主觀」的人性化管理，跟「客觀」的將程式碼納入規則內完全不同，也質疑了智慧合約的整個基本原理。

從處理能力來看，以太坊的以太幣是比特幣以外的第二大區塊鏈。比特幣區塊鏈無法有效的回復，但以太坊竟然可以回復損失，這就代表比比特幣更小的所有區塊鏈，都會變成該幣營運商有效控制下的集中資料庫。事實證明，程式碼並不是真正的法律，因為這些合約的營運商可以更更改合約執行的內容。智慧合約並沒有用程式碼來取代法院，但是它們已經用軟體開發人員取代了法院，這些人在仲裁方面缺乏經驗、知識或責任。法院和律師是否不會受到影響仍有待觀察，因為這種分叉的後果，目前還在繼續探索中。

DAO 是第一個智慧合約，也是目前唯一在區塊鏈上的複雜應用。根據經驗，從它如果真的發生到將來更廣泛的實施之間，還有一段很長的路要走。目前所有其他應用都只存在於原型中，也許在假設的未來裡，程式撰寫的知識更為普遍後，程式碼更具可預測性也更可靠，這樣的契約就可能會變得更加普遍。但是，如果運行這類合約只增加了處理能力的需求，仍然需要由區塊鏈工程師主觀進行編輯、分叉和推翻時，那麼整場練習便沒有任何目的，只會產生流行語和宣傳而已。智慧合約的未來形式，比較可能是存在於信任第三方所營運的安全集中式電腦上，而且要有可以撤銷合約的能力。如此便是把區塊鏈智慧合約的現實形式化為可編輯的，而且可以降低處理能力需求，並減少可能危害的攻擊能力。

對於實際營運的區塊鏈來說，只有簡單的合約才能找到需求，這些合約的代碼必須很容易得到驗證與理解。在區塊鏈上而不在集中式電腦上使用此類合約的唯一理由，便是合約以某種形式用到了該區塊鏈裡的貨幣。

而其他沒有使用區塊鏈分散式系統這種額外負擔的合約，通常可以擁有更好的執行與監督能力。目前唯一有意義的區塊鏈合約應用，就是簡單的時間編程支付和多重簽名錢包等，都是用區塊鏈本身的貨幣執行，而且主要都是在比特幣網路上。

## 資料庫與記錄管理

區塊鏈是可靠且防止篡改的資料庫與資產註冊器，但條件應該是僅限於有用到原生貨幣的區塊鏈，而且只有在貨幣有足夠價值，使網路得以具有足夠強大的處理能力參與抵禦攻擊時才會可靠。對於任何其他實體或數位資產來說，區塊鏈只能負責建立資產與區塊鏈中的資產聯繫。在這裡使用的區塊鏈，並不會有效率較高或資料透明上的好處，因為區塊鏈只授予寫入權限的一方為可靠，將區塊鏈引入該方的記錄保存，會使動作變慢，而且不會增加任何安全性或不變性，因為缺少了工作量證明。因此當運行資料庫所需的處理能力和時間增加時，便需保留對第三方中介的信任。使用數位貨幣保護的區塊鏈，可以用在公證服務上，其中合約或文件被散列到一個交易區塊上，允許任何一方訪問合約，並且確保顯示的版本正是當時被散列的版本，這樣的服務才能為稀有的區塊空間提供交易市場，但對於沒有原生貨幣的任何區塊鏈都是行不通的。

## 區塊鏈技術的經濟缺點

研究了技術上的前三項潛在應用，接著要談廣泛採用區塊鏈會遇上的五個主要障礙。

### 1. 冗餘（Redundancy）

區塊鏈網路上的每個成員都必須記錄每項交易，這是非常昂貴的冗餘動作，因為這個設計的唯一目的是要去除中介。而對於任何中介來說，無



論是在財務或法律方面，在保留中介的同時添加冗餘是非常沒有意義的。因為銀行並不需要與其他銀行分享所有交易的記錄，也沒有理由讓銀行想要在電力和處理能力上花費大量資源，來彼此記錄其他金融機構的交易。這種冗餘增加了成本，卻沒有可以理解的好處。

## 2. 擴容（Scaling）

在所有節點都記錄所有交易的分散式網路上，會讓公共交易分類帳的大小呈指數成長，其速度會比網路成員的成長數量還來得快。分散式網路成員的儲存和計算負擔，將遠大於相同規模的集中式網路。區塊鏈便會經常面臨有效擴容的障礙，這就解釋了為何比特幣開發商尋求擴容解決方案。他們正在從純中心化的區塊鏈模型，轉向在第二層（如閃電網路）清算付款或靠中間商的鏈外交易，亦即在擴容與去中心化之間做出妥協。如果建構區塊鏈以容納更大量的交易，區塊便要做得大一點，但這樣會提高加入網路的成本，導致加入的節點變少。因此，整個區塊鏈網路將傾向於集中化。擁有大量交易最具成本效益的方法，便是在一個節點上集中紀錄。

## 3. 法規遵從（Regulatory Compliance）

區塊鏈擁有自己的貨幣（如比特幣），其存在無關法律；政府當局幾乎沒有辦法影響或改變其運作。聯邦儲備委員會主席甚至說過：他們根本無權管理比特幣<sup>註14</sup>。比特幣網路大約每十分鐘發布一個新的區塊，其中包含的是在這十分鐘內完成的所有有效交易，沒有別的內容。如果區塊有效，交易便清算，如果無效則不會清算，而監管機構並無法推翻這種網路處理能力下的共識。將區塊鏈技術應用於法律或金融等受到嚴格監管的行

---

註 14 S. Russolillo,「葉倫談比特幣：聯邦無權進行監管（Yellen on Bitcoin: Fed Doesn't Have Authority to Regulate It in AnyWay）」，華爾街日報，2014 年 2 月 27 日。

業時，若使用比特幣以外的貨幣，便會有監管和法律上的問題。法規的設計基礎與區塊鏈的基礎大不相同，其規則也無法輕鬆調整來適用於區塊鏈操作，而且所有記錄還必須大方開放給所有網路成員。此外，區塊鏈的線上營運方式的不同監管規則，也超越了司法管轄範圍。

#### 4. 不可逆轉（Irreversibility）

由中間人操作的付款、合約或資料庫，遇到發生人為或軟體錯誤時，可向中間人提出申訴來輕鬆撤銷。但在區塊鏈中，事情會變得無比複雜。一旦確認了一個區塊並且附加了新區塊之後，就只能透過 51% 哈希值的網路處理能力來反轉任何交易，以回滾（roll back）網路。除了這些節點必須同意同時移動到修改後的區塊鏈，也要希望其他 49% 的人不想創建自己的網路，並且加入新網路。因為網路越大，就越難以挽回任何錯誤的交易。畢竟區塊鏈技術的主旨是在線上重現金融交易，因此也包括現金交易的不可逆轉性。交易的補救和修訂，對監管的中介方並無任何好處。一般銀行業務裡經常會出現人為和軟體錯誤，但採用區塊鏈結構，只會導致這些錯誤的修復成本變得更高。DAO 事件便揭示了區塊鏈上的逆轉會有多麼昂貴和延宕，需要數週的編碼和公關活動才能讓網路成員同意採用新版軟體。即使如此，舊鏈仍然存在，舊網路的大量價值和散列能力也被帶走。這種損失造成了前面存在兩個交易記錄的狀況，一個是 DAO 攻擊成功，另一個是沒有成功。

如果處理能力第二大的網路，都可以在交易不符合開發團隊利益的情況下改變其區塊鏈記錄，那麼任何其他區塊鏈真正受處理能力監管的概念，就都不可行了。而事實上，這便是由私人企業裡的一群同事，在手中握有「集中的」貨幣價值、處理能力和編寫程式技能，讓這種精緻結構的原始目的無法實現。

由於第 9 章所討論的原因，讓這種逆轉在比特幣中非常不切實際，也不太可能發生。主要是因為比特幣網路中的每一方，都只能透過同意現有的共識規則加入網路。在整個比特幣生態系統中，不同成員之間的「利益對抗」，代表這個網路始終只能透過吸引願意接受共識規則的人，以及他們的自願貢獻而成長。在比特幣中，共識規則是不變的，用戶可以選擇留下或離開。而那些模仿比特幣設計建立的其他區塊鏈項目，總會有一個小組負責設置系統規則，因此有能力加以改變。比特幣的成長是透過人類活動所建立的共識規則，但其他替代幣項目都是透過積極的人性化設計和管理而發展。經過多年抵制改變後，比特幣贏得了「不可變」的聲譽，但沒有其他區塊鏈項目敢說出這句話。

而「可變的」區塊鏈，等於是工程謬論裡的「無意義」功能運動：因為用了複雜而昂貴的清算法來移除信任中介並奠立不變性，卻又授予中介可推翻這種不變性的能力。目前在這些領域的最佳實踐，包括具有可逆性與監督能力的法律和監管機構，但他們採取的是更便宜、更快速也更有效的方法。

## 5. 安全

區塊鏈資料庫的安全性，完全依賴對交易驗證和工作量證明所付出的處理能力。我們可以把區塊鏈技術理解為：將電力轉換成可驗證且無爭議的所有權和交易記錄。為了系統安全，花費處理能力的驗證者，必須獲得支付系統本身的貨幣來進行補償，才能讓激勵的動機與網路的健康壽命保持一致。如果以任何其他貨幣來資助處理能力，區塊鏈就會變成由資助處理能力的人，維護下的私人記錄。於是系統的安全性，便取決於集中式系統方資助礦工資金的安全性，但這種情況變成是在共享分類帳上的一種權衡交易，所以很可能會產生安全漏洞。建立在經由處理能力驗證基礎上的開放式中心化，其系統越安全就會越開放，網路成員的數量也會越多，驗

證處理能力更會增強。而在大量網路成員都能寫入區塊鏈的情況下，每個新加入的網路成員都會是潛在的安全威脅，因此依賴「單點故障」的集中式系統安全性便會降低。

## 區塊鏈技術作為數位貨幣生產機制

目前為止，區塊鏈技術唯一成功的商業應用便是數位貨幣（電子現金），尤其是比特幣的成就。區塊鏈技術最常見潛在應用——支付、合約和資產註冊方面，只有在使用區塊鏈的去中心化貨幣的範圍內運行，才有可行的機會。本身沒有貨幣的區塊鏈，都不曾從原型階段轉移到商業實施階段，因為它們無法與市場目前的最佳實踐相互競爭。比特幣的設計已在網際網路上免費提供了九年，開發人員可以複製和改進以引入新的商業產品，但實際上並沒有出現過這樣的產品。

市場測試表明，交易記錄和工作量證明的冗餘，只能用來生成數位貨幣與沒有第三方中介的支付網路。數位貨幣的所有權和交易，可以只用非常少量的數據傳達。其他需要更多數據要求的經濟案例，例如大規模支付與合約等，在區塊鏈模型下會變得難以執行。對於涉及中介的任何應用，區塊鏈提供的解決方案並沒有現實上的競爭力。而在依賴中介機構信任的行業中，無法廣泛採用區塊鏈技術，因為在只需中介商即可的情況下，會使運行區塊鏈的所有成本變得多餘。區塊鏈技術的任何商業應用，只有在其營運是依賴於數位貨幣的使用時，才會具有商業意義，並且還要在數位貨幣的去中介化所提供的經濟利益，大於使用常規貨幣和支付管道時，才有機會。

良好的工程技術通常源起於一個明確的問題，並且試圖找到它的最佳解決方案。理想的解決方案不僅可以解決問題，還會根據其定義，排除任何無關或多餘的問題。比特幣創造者的動機是想創造一種「點對點電子現

金」，並為此目標建立其設計。除了那些對比特幣機制的無知的人之外，我們實在沒有理由期望區塊鏈可以適用在其他用途上。歷經九年和數百萬用戶的試煉，我們可以很肯定的說，他的設計已經成功地產生了數位貨幣，而且毫不意外的，除了數位貨幣之外沒有別的應用。這種電子化的現金可在商業上與數位上應用，但若將區塊鏈技術作為一種獨立的技術創新，並可在各種領域應用而進行的討論，實在毫無意義。因此區塊鏈最好被理解為在創建對通貨膨脹有所限制的「點對點電子現金」機器裡，所不可或缺的齒輪。



## 致謝

---

本書在比特幣開發人員 David Harding 的幫助、指導和技術專長中獲益匪淺，他有令人欽佩的天份，平易的傳達了這些複雜的技術主題。我也很感謝 Nassim Taleb 同意為本書撰寫前言，並幫我找到出版商。而在約翰威立出版社（John Wiley & Sons, Inc.）裡，也非常幸運地能與一位信任這本書的編輯合作，並鼓勵我努力不懈地改進，為此，非常感謝 Bill Falloon 以及整個 Wiley 團隊的專業和效率，還有感謝 Rachael Churchill 給本書徹底且迅捷的校對。

許多朋友都讀過這本書的早期草稿，也都給我很好的回饋來改進本書，非常感謝。特別感謝 Ahmad Ammous、Stefano Bertolo、Afshin Bigdeli、Andrea Bortolameazzi、Michael Byrne、Napoleon Cole、Adolfo Contreras、Rani Geha、Benjamin Geva、Michael Hartl、Alan Krassowski、Russell Lamberti、Parker Lewis、Alex Millar、Joshua Matettore、Daniel Oliver、Thomas Schellen、Valentin Schmit、Omar Shams、Jimmy Song、Luis Torras 與 Hachem Yassine。

這本書是多年學習過程的結果，在此期間，很幸運地能向一些非常聰明的人求教。我特別感謝 Tuur Demeester、Ryan Dickherber、Pete Dushenski、Michel Fahed、Akin Fernandez、Viktor Geller、Michael Goldstein、Konrad Graf、Pontus Lindblom、Mircea Popescu、Pierre Rochard、Nick Szabo、Kyle Torpey 和 Curtis Yarvin 的著作和討論，協助我發展對比特幣的理解。

本書的研究和編輯得益於我非常有天份的研究助理們 Rebecca Daher、Ghida Hajj Diab、Maghy Farah、Sadim Sbeity 和 Racha Khayat 的努力工作，非常感謝他們。George Hall 教授慷慨地從他的研究論文中提供數據，也讓我感激不盡。

最後，如果沒有志願開發者把珍貴的時間，奉獻在努力不懈的開發和維護協議上，那麼這本書和比特幣都不可能實現。因此，我非常感謝他們對這個項目的無私和奉獻精神。

# B

## 參考書目

---

- Ammous, Saifedean. 「Blockchain Technology: What Is It Good For?」  
*Banking & Finance Law Review* 33, no. 3 (Issue 1, 2018).
- Bank of International Settlements. *Triennial Central Bank Survey. Foreign Exchange Turnover in April 2016*, 2016.
- Barzun, Jacques. *From Dawn to Decadence: 1500 to the Present—500 Years of Western Cultural Life*. New York: HarperCollins, 2000.
- Bernanke, Ben S. 「Deflation: Making Sure 'It' Doesn't Happen Here.」  
*In Remarks by Governor Ben S. Bernanke Before the National Economists Club*, Washington, D.C., November 21, 2002.
- Bly, Nellie. *Around the World in Seventy-Two Days*. New York: Pictorial Weeklies, 1890.
- Böhm-Bawerk, Eugen. *Capital and Interest: A Critical History of Economical Theory*. Vol. 1. Macmillan, 1890.



- Brown, Malcolm, and Shirley Seaton. *Christmas Truce: The Western Front December 1914*. Macmillan, 2014.
- Buchanan, James M., and Gordon Tullock. *The Calculus of Consent: Logical Foundations of Constitutional Democracy*. Liberty Fund Indianapolis, 1962.
- Bunch, Bryan, and Alexander Hellemans. *The History of Science and Technology: A Browser's Guide to the Great Discoveries, Inventions, and the People Who Made Them from the Dawn of Time to Today*. Houghton Mifflin Harcourt, 2014.
- Coase, Ronald. 「The Nature of the Firm.」 *Economica* 4, no. 16 (1937): 386–405.
- Courtois, Stephane, Nicolas Werth, Karel Bartosek, Andrzej Paczkowski, Jean-Louis Panné, and Jean-Louis Margolin. *The Black Book of Communism: Crimes, Terror, Repression*. Harvard University Press, 1997.
- Davidson, James, and William Rees-Mogg. *The Sovereign Individual: The Coming Economic Revolution*. McMillan, 1997.
- De Soto, Jesús Huerta. *Money, Bank Credit, and Economic Cycles*. Auburn, AL: Ludwig von Mises Institute, 2009.
- Diamond, Douglas W., and Philip H. Dybvig. 「Bank Runs, Deposit Insurance, and Liquidity.」 *Journal of Political Economy* 91, no. 3 (1983): 401–419.
- Fekete, Antal. 「Whither Gold?」 *International Currency Prize 1996* (1996). [www.professorfekete.com/articles/AEFWhitherGold.pdf](http://www.professorfekete.com/articles/AEFWhitherGold.pdf).
- Felix, David. *Keynes: A Critical Life*. ABC-CLIO, 1999.
- Ferguson, Adam. *An Essay on the History of Civil Society*. London: T. Cadell, 1782.
- Friedman, Milton, and Anna Schwartz. *A Monetary History of the United States, 1867–1960*. Princeton University Press, 2008.

- Gilder, George. *The Scandal of Money: Why Wall Street Recovers but the Economy Never Does*. Regnery Publishing, 2016.
- Glubb, John. *The Fate of Empires and Search for Survival*. Blackwood, 1978.
- Graf, Konrad. *On the Origins of Bitcoin: Stages of Monetary Evolution* (2013). [www.konradsgraf.com](http://www.konradsgraf.com)
- Grant, James. *The Forgotten Depression: 1921: The Crash That Cured Itself*. Simon & Schuster, 2014.
- Greaves, Bettina Bien. *Ludwig von Mises on Money and Inflation: A Synthesis of Several Lectures*. Ludwig von Mises Institute, 2010.
- Greenberg, Andy. *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*. Penguin, 2013.
- Halévy, Élie, and May Wallas. 「The Age of Tyrannies.」 *Economica* 8, New Series, no. 29 (1941): 77–93.
- Hall, George. 「Exchange Rates and Casualties During the First World War.」 *Journal of Monetary Economics* 51, no. 8 (2004): 1711–1742.
- Hanke, Steve H. and Charles Bushnell. 「Venezuela Enters the Record Book: The 57th Entry in the Hanke-Krus World Hyper Inflation Table.」 *The Johns Hopkins Institute for Applied Economics, Global Health, and the Study of Business Enterprise, Studies in Applied Economics*, no. 69 (December 2016).
- Haslam, Philip and Russell Lamberti. *When Money Destroys Nations*. Penguin UK, 2014.
- Hayek, Friedrich. *Monetary Theory and the Trade Cycle*. Jonathan Cape, London, 1933.
- \_\_\_\_\_. *Monetary Nationalism and International Stability*. Fairfield, NJ: Augustus Kelley, 1989 (1937).

- \_\_\_\_\_. 「The Use of Knowledge in Society.」 *American Economic Review* 35, no. 4 (1945): 519–530.
- \_\_\_\_\_. 「The Intellectuals and Socialism.」 *The University of Chicago Law Review* 16, no. 3 (1949): 417–433.
- \_\_\_\_\_. *A Tiger by the Tail*. Vol. 4. Laissez-Faire Books, 1983.
- \_\_\_\_\_. *Denationalization of Money*. Institute of Economic Affairs, 1976.  
Hazlitt, Henry. *The Failure of the New Economics*. NJ: D. Van Nostrand Company, Inc, 1959.
- Higgs, Robert. 「WorldWar II and the Triumph of Keynesianism.」 *Independent Institute* (2001). <http://www.independent.org/publications/article.asp?id=317>
- Holroyd, Michael. *Lytton Strachey: The New Biography*. Norton & Co., 2005.
- Hoppe, Hans-Hermann. 「How Is Fiat Money Possible? Or, The Devolution of Money and Credit.」 *The Review of Austrian Economics* 7, no. 2 (1994).
- Hoppe, Hans-Hermann. *Democracy: The God That Failed*. New Brunswick: Transaction Publishers, 2001.
- Huebner, Jonathan. 「A Possible Declining Trend for Worldwide Innovation.」 *Technological Forecasting and Social Change* 72, no. 8 (2005): 980–986.
- Ibn Khaldun, Abd Alrahman. *Al-Muqaddima*. 1377.
- Jastram, Roy W. *The Golden Constant: The English and American Experience 1560–2007*. Edward Elgar, 2009.
- Kent, Roland G. 「The Edict of Diocletian Fixing Maximum Prices.」 *University of Pennsylvania Law Review* 69 (1920): 35.
- Keynes, John Maynard. *A Tract on Monetary Reform*. Macmillan, 1923.

- \_\_\_\_\_. *The General Theory of Employment, Money, and Interest*. Palgrave Macmillan, 1936.
- \_\_\_\_\_. *Essays in Persuasion*. W. W. Norton, 1963.
- Komlos, John, Patricia Smith, and Barry Bogin. 「Obesity and the Rate of Time Preference: Is There a Connection?」 *Journal of Biosocial Science* 36, no. 2 (2004): 209–219.
- Kremer, Michael. 「Population Growth and Technological Change: One Million B.C. to 1990.」 *Quarterly Journal of Economics* 108, no. 3 (1993): 681–716.
- Levy, David, and Sandra Peart. 「Soviet Growth and American Textbooks: An Endogenous Past.」 *Journal of Economic Behavior & Organization* 78, no. 1–2 (2011): 110–125.
- Liaquat Ahamed. *Lords of Finance: The Bankers Who Broke the World*. Penguin, 2009.
- Lips, Ferdinand. *Gold Wars: The Battle Against Sound Money as Seen from a Swiss Perspective*. New York: Foundation for the Advancement of Monetary Education, 2001.
- Mallery, Otto Tod. *Economic Union and Durable Peace*. New York: Harper, 1943.
- May, T. C. *Crypto Anarchy and Virtual Communities*. 1994. Available on [nakamotoinstitute.org](http://nakamotoinstitute.org)
- McConnell, Campbell, Stanley Brue, and Sean Flynn. *Economics*. New York: McGraw-Hill, 2009.
- Mencken, H. L., and Malcolm Moos (eds.), *A Carnival of Buncombe*. Baltimore: Johns Hopkins Press, 1956.
- Menger, Carl. 「On the Origins of Money.」 *The Economic Journal* 2, no. 6 (1892): 239–255.

- Merkle, R. 「DAOs, Democracy and Governance.」 *Cryonics* 37, no. 4 (July/August 2016): 28–40; Alcor, [www.alcor.org](http://www.alcor.org)
- Mischel, Walter, Ebbe B. Ebbesen, and Antonette Raskoff Zeiss. 「Cognitive and Attentional Mechanisms in Delay of Gratification.」 *Journal of Personality and Social Psychology* 21, no. 2 (1972): 204–218.
- Mises, Ludwig von. *Human Action. The Scholar's Edition*. Auburn, AL: Ludwig von Mises Institute, 1998.
- \_\_\_\_\_. *Profit and Loss*. Ludwig von Mises Institute, 2008.
- \_\_\_\_\_. *Socialism: An Economic and Sociological Analysis*. Ludwig von Mises Institute, Auburn, AL. 2008 (1922).
- \_\_\_\_\_. *The Theory of Money and Credit*, 2nd ed. Irvington-on-Hudson, New York: Foundation for Economic Education, 1971.
- Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* (n.p., 2008).
- Narayanan, Arvind et al. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.
- Paar, Christof, Bart Preneel and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2009.
- Philippon, Thomas, and Ariell Reshef. 「An International Look at the Growth of Modern Finance.」 *Journal of Economic Perspectives* 27, no. 2 (2013): 73–96.
- Popper, Nathaniel. *Digital Gold*. Harper, 2015.
- Raicho, Ralph. *The Costs of War: America's Pyrrhic Victories*. NJ: Transaction Publishers, 1999.
- Rothbard, Murray. *America's Great Depression*, 5th ed. Auburn, AL: Ludwig von Mises Institute, 2000.

- \_\_\_\_\_. 「The Austrian Theory of Money.」 *The Foundations of Modern Austrian Economics* (1976): 160–184.
- \_\_\_\_\_. 「A Conversation with Murray Rothbard.」 *Austrian Economics Newsletter* 11, no. 2 (Summer 1990): 1–5.
- \_\_\_\_\_. *Economic Depressions: Their Cause and Cure*. Auburn, AL: Ludwig von Mises Institute, 2009.
- \_\_\_\_\_. 「The End of Socialism and the Calculation Debate Revisited.」 *The Review of Austrian Economics* 5, no. 2 (1991): 51–76.
- \_\_\_\_\_. *The Ethics of Liberty*. New York, NY: New York University Press, 1998.
- \_\_\_\_\_. *Man, Economy, and State*. Ludwig von Mises Institute, 2009.
- Salerno, Joseph. *Money: Sound and Unsound*. Ludwig von Mises Institute, 2010.
- Samuelson, Paul Anthony. *Full Employment after the War*. New York: McGraw-Hill, 1943.
- Saunders, Frances Stonor. *The Cultural Cold War: The CIA and the World of Arts and Letters*. The New Press, 2000. ISBN 1-56584-596-X.
- Schuettinger, Robert L., and Eamonn F. Butler. *Forty Centuries of Wage and Price Controls: How Not to Fight Inflation*. Ludwig von Mises Institute, 1979.
- Schumpeter, Joseph A. *Capitalism, Socialism and Democracy*. Routledge, 2013.
- Simon, Julian. *The Ultimate Resource*. Princeton University Press, 1981.
- Singh, Simon. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor, 2000.
- Skousen, Mark. 「The Perseverance of Paul Samuelson's Economics.」 *Journal of Economic Perspectives* 11, no. 2 (1997): 137–152.

- Smith, Vernon. *Rationality in Economics*. New York: Cambridge University Press, 2008.
- Steil, Benn. *The Battle of Bretton Woods: John Maynard Keynes, Harry Dexter White and the Making of a New World Order*. Princeton University Press, 2013.
- Stein, Mara Lemos. 「The Morning Risk Report: Terrorism Financing Via Bitcoin May Be Exaggerated.」 *Wall Street Journal*, 2017.
- Sutton, Antony. *Wall Street and the Bolshevik Revolution*, Crown Publishing Group, 1974.
- Szabo, Nick. 2001. *Trusted Third Parties Are Security Holes*. Available on NakamotoInstitute.org
- Szabo, Nick. *Shelling Out: The Origins of Money*. (2002). Available on NakamotoInstitute.org
- Taleb, Nassim Nicholas. *Antifragile: How to Live in a World We Don't Understand*. London: Allen Lane, 2012.
- \_\_\_\_\_. *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*. Random House, 2005.
- \_\_\_\_\_. *The Black Swan: The Impact of the Highly Improbable*. Random House, 2007.
- Thiel, Peter. *From Zero to One: Notes on Start-ups, or How to Build the Future*. Crown Business, 2014.
- Zweig, Stefan. *The World of Yesterday: Memoirs of a European*. Pushkin Press, 2009.

## 網路資源

---

- [bitcoin.org](http://bitcoin.org)：中本聰用來宣布比特幣、分享白皮書、分發代碼所使用的原始網域名稱。它也由幾位貢獻者繼續營運，作為一個良好的訊息來源。
- [en.bitcoin.it/wiki/](http://en.bitcoin.it/wiki/)：關於比特幣訊息的開放型百科全書，包含許多有用且通常是最新的比特幣相關訊息。
- [nakamotoinstitute.org](http://nakamotoinstitute.org)：Satoshi Nakamoto Institute（中本聰學會）保存了密碼學社的主要來源文獻，並將重點關注於比特幣的歷史和經濟學。這裡還保存了所有 Nakamoto 著名作品的檔案，包括比特幣白皮書、他發送的電子郵件和他在論壇發表過的內容等。
- <http://lopp.net/bitcoin.html>：由 Jameson Lopp 所維護的一個優秀、全面且定期更新的比特幣資源網頁。





# 比特幣標準 | 中央銀行的去中心化替代方案

作者：Saifedean Ammous

譯者：吳國慶

企劃編輯：莊吳行世

文字編輯：詹祐甯

設計裝幀：張寶莉

發行人：廖文良

發行所：基峰資訊股份有限公司

地址：台北市南港區三重路 66 號 7 樓之 6

電話：(02)2788-2408

傳真：(02)8192-4433

網站：www.gotop.com.tw

書號：ACD018100

版次：2019 年 03 月初版

建議售價：NT\$480

商標聲明：本書所引用之國內外公司各商標、商品名稱、網站畫面，其權利分屬合法註冊公司所有，絕無侵權之意，特此聲明。

版權聲明：本著作物內容僅授權合法持有本書之讀者學習所用，非經本書作者或基峰資訊股份有限公司正式授權，不得以任何形式複製、抄襲、轉載或透過網路散佈其內容。

版權所有 • 翻印必究

國家圖書館出版品預行編目資料

比特幣標準：中央銀行的去中心化替代方案 / Saifedean Ammous

原著；吳國慶譯。-- 初版。-- 臺北市：基峰資訊，2019.03

面；公分

譯自：The Bitcoin Standard

ISBN 978-986-502-050-7(平裝)

1.電子貨幣 2.電子商務

563.146

108001573

## 讀者服務

- 感謝您購買基峰圖書，如果您對本書的內容或表達上有不清楚的地方或其他建議，請至基峰網站：「聯絡我們」\「圖書問題」留下您所購買之書籍及問題。(請註明購買書籍之書號及書名，以及問題頁數，以便能儘快為您處理)

<http://www.gotop.com.tw>

- 售後服務僅限書籍本身內容，若是軟、硬體問題，請您直接與軟體廠商聯絡。
- 若於購買書籍後發現有破損、缺頁、裝訂錯誤之問題，請直接將書寄回更換，並註明您的姓名、連絡電話及地址，將有專人與您連絡補寄商品。