共識機制、流動性與貨幣價格：

以工作量證明與權益證明為核心

吳坤融

經濟研究所一年級

2018 七月

前言

自從 2009 比特幣 (Bitcoin) 首次發行以來，基於區塊鏈 (Blockchain) 技術的加密貨幣 (Cryptocurrency) 已證明技術層面可行性。現階段，加密貨幣所採行的共識機制 (Consensus Mechanism) 大部份為基於算力 (Hash rate) 的工作量證明 (Proof-of-Work) 。主要原理是透過計算複雜的雜湊函數 (hash function) 來取得驗證交易的資格。然而，由於工作量證明需要耗費大量的電力資源來運作，而且所新增的額外算力，未能有效提高系統的交易量。因此基於貨幣持有量的權益證明 (Proof-of-Stake) 被視為解決上述缺點的解決方案。

然而，權益證明仍有吾人待思考的問題，首先就系統安全而言，工作量證明以消耗算力作為誠實記帳的誘因，只要算力不大規模集中在少數節點的情況下，能有效減少雙重花費 (Double-spending) 攻擊發生的可能性。運行工作量證明的比特幣證明其有效之運作。權益證明則是以抵押貨幣作取得記帳的機會，以新發行的貨幣作為誠實記帳的獎勵，同時以沒收抵押之貨幣作為不誠實記帳的懲罰，但目前主流加密貨幣仍以 PoW 為主 (見表 1)。採用權益證明是否能有效的防範雙花攻擊仍有待證明。

其次，由於 PoS 是以貨幣本身做為抵押，在一定的期間內不得動用。驗證期間過

後，若驗證成功則以發放新發行的貨幣按比例發放做為區塊獎勵 (Block Reward)。這使得 PoS 貨幣本質較接近具有固定收益的資產。就經濟學的理性預期下，人們傾向持有 PoS 貨幣以賺取未來的收益，而非作為交易媒介。Wei (2018) 分析 456 種加密貨幣的市場流動性與收益率的關係，實證出流動性在報酬預測性扮演十分重要的角色。以模型解釋價格與流動性以及作為交易媒介的接受程度是有其必要。

本文想討論上述兩點懸而未決的面向，進而回答以下三個議題：

(1) 以貨幣搜尋模型來探討不同共識機制下，對貨幣經濟數據本身的影

(2) 內生化兩種機制下貨幣的市場接受比例。

(3) 以機制設計的角度制定合理的區塊獎勵與懲罰。

排名	加密貨幣	共識機制	市值(US$ Billion)	占比
1	Bitcoin	PoW	$109.37	43%
2	Ethereum	PoW	$45.82	18%
3	XRP	皆非	$18.07	7%
4	Bitcoin Cash	PoW	$12.69	5%
5	EOS	PoS	$7.21	3%
6	Litecoin	PoW	$4.60	2%
7	Stellar	皆非	$3.68	1%
8	Cardano	PoS	$3.56	1%
9	IOTA	PoW	$2.90	1%
10	Tether	PoW	$2.71	1%
		前十大合計	$210.62	82%
		加密貨幣總市值	$257.02	100%
		PoW合計	$178.09	69%
		PoS合計	$10.77	4%

表 1：前十大加密貨幣之市值

文獻回顧

以下兩篇為文中提及加密貨幣的貨幣搜尋模型的文章。

Fernandez-Villaverde (2017) 討論私人能自行發行貨幣時，各種貨幣的競爭關係。他指出在極大化發行者利潤的設定下，純粹的私人貨幣經濟體不能有效率的分配。即便在價格穩定的狀況下亦如此。另外，在沒有政府介入的情況下，若能引入生產性資本，

私人也能制定出可以達到效率分配的政策。

Chiu and Koeppl (2017) 指出比特幣系統會產生 1.4%消費的福利損失，而這個損失能透過減少挖擴及多依賴貨幣增長作為區塊獎勵來大幅減輕，如改用其他像 PoS 的共識機制則效率能進一步提昇。加密貨幣在做為小額交易時能達到最佳效果。

模型

本文以 Lagos and Wright (2005) 作為基本模型，引入 PoS 與 PoW 兩種貨幣。並以 Lester et al (2009) 中對多資產的設定描繪不同貨幣的接受程度。

模型中所有人皆活無窮期，分布在 [0,1] 之間的 continuum，兩群同為 1/2 測度的人分別稱為買家與賣家。各期之間的跨期折現因子為 $\beta \in (0, 1)$。每一期又分為 Decentralized Market 與 Centralized Market 兩個子期。

在 DM 中，買賣家須一對一隨機配對進行特殊財的交易。買家消費 q 單位的特殊財可得到 u(q) 單位的效用，且滿足 $u'(q) > 0, u''(q) \leq 0, u(0) = 0, u'(0) = \infty, u'(\infty) = 0$，而賣家生產 q 單位的商品須付出 c(q)，且滿足 $c'(q) > 0, c''(q) \geq 0, c(0) = 0$。在 DM 交易可使用 PoS 與 PoW 貨幣進行，外生給定 σ, 1-σ 為兩個貨幣在所有交易中會被接受的機率，以此設定捕捉不同貨幣的接受程度。

到了 CM，每個人都可生產與消費。消費 X 單位的一般財後, 皆會獲得 U (X) 的效用， U (X) 的性質為 $U'(X) > 0, U''(X) < 0, U'(0) = \infty, U'(\infty) = 0$。而提供 H 單位的勞動力，會產生 −H 的負效用, 同時每單位的勞動力賺取 1 單位的薪資。

以 PoW 為共識機制的貨幣總量為 K，k 則為個人所持有的量。在 PoW 機制下，買賣家必須在進入 DM 之前決定是否付出 -d 單位的負效用，以利在 DM 市場能使用 PoW 貨幣來進行交易。同樣地，以 PoS 為共識機制的貨幣總量為 S，s 則為個人所持有的量。在 PoS 的機制下，買賣家必須在進入 DM 之前決定是否抵押 a 比例的 PoS 幣，若抵押則可在 DM 用剩下的 (1 – a)s 單位 PoS 進行交易，而抵押的 as 的 PoS 在離開 DM 後可自由使用。

為衡量貨幣的價值，以 φ 為 PoS 貨幣的價格，ψ 為 PoW 貨幣的價格。在持有 PoS 進入 CM 後的則發放 rk 做為區塊獎勵，其中 $r \geq 0$，而持有 PoW 貨幣的人則可以在 CM 得到新發行的貨幣 $T > 0$ 做為區塊獎勵。以下是貨幣供給的限制式。

$$(K - K_{-1}) = T$$

$$(1+r)\, S_{-1} = S$$

均衡

我們從 CM 的 quasilinear 的效用函數知道，人們帶入下一期 k 和 s 與當期內財富的轉移無關，且考慮 stationary equilibrium 的條件下，可求出下列的 CM 中的 value function.

$$W(k,s) = max\ \{U(X) - H + \beta V(k,s)\}$$

$$s.t.\ X = H + \varphi((1+r)s - s_{+1}) + \psi(k - k_{+1}) + \psi T$$

以及帶入下一期 DM 的 value function，由於在進入 DM 之前，決策者可以選擇是否投入成本來使用 PoS 或 PoW 來作為交易媒介，Vb(k,s)為買家的 value function 分為以下四種情形分析。下標 s,w 為事前已投入成本，0 則為沒有任何投入，而賣家生產量為 q，支付量為 d。

$$Vb_s(k,s) = \sigma\,[u(q) + W(k,s-d)] \ + \ (1-\sigma)[\,W(k,s)]$$

$$Vb_w(k,s) = \sigma\,[W(k,s)] \ + \ (1-\sigma)[u(q) + W(k-d,s) - d]$$

$$Vb_{sw}(k,s) = \sigma\,[u(q) + W(k,s-d)] \ + \ (1-\sigma)[u(q) + W(k-d,s) - d]$$

$$Vb_0(k,s) = W(k,s)$$

同理，賣家的 value function 也可以寫成下列四種。且由於加密貨幣只有發送者需要付出手續費，所以這邊沒有 –d 項。

$$Vs_s(k,s) = \sigma\,[-c(q) + W(k,s+d)] \ + \ (1-\sigma)[\,W(k,s)]$$

$$Vs_w(k,s) = \sigma\,[W(k,s)] \ + \ (1-\sigma)[-c(q) + W(k+d,s)]$$

$$Vs_{sw}(k,s) = \sigma\,[-c(q) + W(k,s+d)] \ + \ (1-\sigma)[-c(q) + W(k-d,s)]$$

$$V_{s0}(k,s) = W(k,s)$$

以上，我們已經完成基本模型的設定，總結目前為止，模型是外生給定兩種貨幣的接受程度 σ，而買家賣可以在進入 DM 之前決定是否投入成本使用其中一種或兩種貨幣作為交易媒介。

以下猜測均衡情況，直覺上作為區塊獎勵的 r, T 會提昇的接受度，相反的 d 與 a 則分別降低接受度。然而如果 r, T 差距太大的話，可能會造成一種貨幣完全不被拿來交易的均衡。而 r, T 的絕對數值也是會影響流動性的因為。可能存在一個區間 r*, T*，如果超過的話則因為報酬太高則不被用來交易，太低的話則因為獎勵過小，交易好處太小而不被使用。同樣的推論也適用於 d 與 a，應該會有一個區間是被交易使用的。由於 T 會影響到 PoW 貨幣的供給量，T 越大則 ψ 越小，而 r 與 φ 亦然。

內生化接受程度之構想

上述模型最大的問題在於，將貨幣的接受程度與買賣家個人對投入成本以作為交易媒介的決策分離。也就是說，買賣家投入成本的多寡竟然對貨幣整體的流通程度不影響。較為直覺的想法為，必然有一個 Microfoundation 的因素影響人們選擇該貨幣作為交易貨幣的。以 Lester et al.(2011)的想法，是以取得每一種資產辨識技術成本的不同來形塑不同的接受程度。然而這顯然不適用於加密貨幣的情況，因為不論 PoS 或 PoW 的加密貨幣，基於公開帳本的不可竄改性，人們都能以幾乎相同且近乎零成本的取得加密貨幣的辨識技術。

比較好的方向是探討不同共識機制下對雙重花費出現機率的大小，在雙重花費出現時，賣方以為收到作為對價的加密貨幣而交出貨品，事後買家以竄改帳本使得賣方不能使用收到的貨幣，本質上就是收到偽幣。只是在共識機制設計時，都試圖提高雙花攻擊的成本，形同提高製作偽幣的成本。

進一步分析 PoS 與 PoW 兩種機制提高雙花攻擊成本方式，會發現兩者是相當不同的機制設計。如果引入機制設計的概念則可以將模型中原本外生的 a, d, T, r，透過

Incentive Compatible Constrain 簡化為兩個參數。另外我猜測，因為求解機制設計的過程需要用到貨幣的價格，或許進一步內生化其中一個參數。

參考資料

[1] Ricardo Lagos and Randall Wright. A unified framework for monetary theory and policy analysis. Journal of Political Economy, 113:463– 484, 2005.

[2] Benjamin Lester, Andrew Postlewaite and Randall Wright. Information, Liquidity, Asset Prices, and Monetary Policy. Review of Economic Studies, 2012.

[3] Jesus Fernandez-Villaverde and Daniel Sanches, Can Currency Competition Work? NBER Working Paper No. 22157, 2016.

[4] Jonathan Chiu and Thorsten Koeppl, The Economics of Cryptocurrencies Bitcoin and Beyond, SSRN, 2017.

[5] Wang Chun Wei, Liquidity and market efficiency in cryptocurrencies, Economics Letters, 2018.