穩定幣的運作方式及其對傳統金融產業的影響

知識力科技執行長 曲建仲

近期世界各國積極通過穩定幣草案，金管會也在2025年6月將《虛擬資產服務法》納入穩定幣規範，初步共識是金融機構優先發行穩定幣，但是沒有限制金融機構，意思是未來可能開放私人企業發行穩定幣。

事實上發行穩定幣的重點不是「由誰發行」而是「如何交易」，也就是用哪一個區塊鏈帳本記帳？那麼穩定幣到底如何運作？本文以圖例與您一起解讀。

跨國「秒級匯兌」免手續費與穩定幣或區塊鏈無關

我們以區塊鏈跨境「秒級匯兌」免手續費的例子來說明：假設台灣的小王匯款30萬新台幣給美國的小美，向發行單位買入1萬枚OO幣，假設一枚OO幣新台幣30元，接著小王用手機應用程式（APP）匯款給美國的小美，這個過程就像從台灣傳簡訊到美國一瞬間就完成，小美拿到1萬枚OO幣就向發行單位換回1萬美元，假設台幣兌換美元為30：1，事實上不必神奇的穩定幣或區塊鏈技術，只要一台伺服器就能做到，如圖1所示。

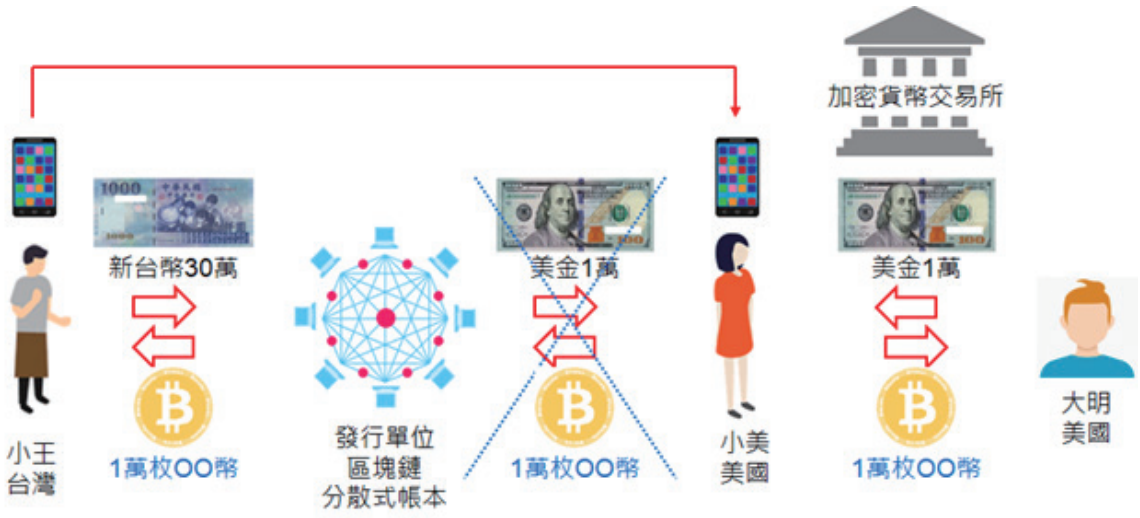

圖1、OO幣跨境匯兌示意圖

問題是發行單位左手收新台幣右手給美元，卻要承擔匯兌風險賺什麼？因此發行單位要做的是到處宣講OO幣未來將會打敗全球銀行金融電信協會（SWIFT）所以未來會漲要趕快投資，結果交易人大明拿出1萬美元，經由加密貨幣交易所買走小美手上的1萬枚OO幣。

結局是台灣的小王免手續費三秒鐘成功匯出1萬美元給美國的小美，交易人大明開心的持有他認為未來會漲的1萬枚OO幣，大家猜猜圖中最開心的是誰？發行單位成功的把OO幣倒出去換成現金，可真是皆大歡喜呀！

前面介紹幣值會漲會跌的OO幣，如果換成幣值不漲不跌錨定法定貨幣的就稱為「穩定幣」，問題是穩定幣不漲不跌，交易人大明為什麼要開心的持有呢？因為當大明做為一個上線，用高價把比特幣倒給下線接盤後，大賺一票就可以換成穩定幣獲利了結與避險，因此他也很開心。

區塊鏈只是一種儲存資料的資料結構

區塊就是「存摺」，區塊鏈就是「存摺鏈」，也就是很多本存摺，所以區塊鏈只是儲存資料的「資料結構」或「資料格式」而已，如果我們把區塊鏈這個資料結構儲存在「幾台電腦」裡稱為「私有鏈」；如果我們把區塊鏈這個資料結構複製幾百份分散儲存在幾百台「聯盟成員」的電腦裡稱為「聯盟鏈」；如果我們把區塊鏈這個資料結構複製幾萬份分散儲存在幾萬台「互不認識」的礦工電腦裡稱為「公有鏈」。

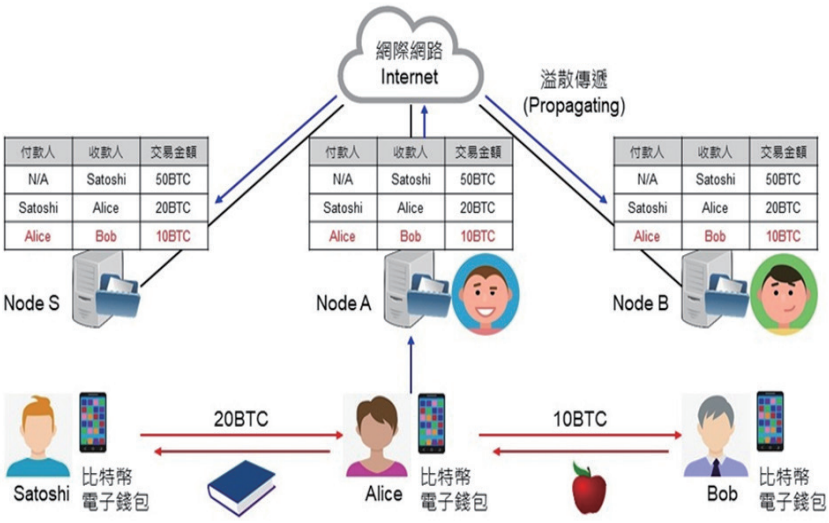

圖2、比特幣的運作方式

比特幣的運作方式如圖2所示，由發明人Satoshi做為第一個礦工，同時號召網路上彼此不認識的A和B做為「礦工」，各自購買電腦安裝「採礦程式」與「比特幣帳本（區塊鏈）」，這台電腦稱為「礦機」，使用者只需要使用手機應用程式（APP）稱為「比特幣電子錢包」就可以匯款，完全不必管比特幣帳本（區塊鏈）如何運作。

例如：Alice把10枚比特幣匯給Bob，這筆交易就傳送給礦工A，寫進自己的比特幣帳本（區塊鏈）裡，付款人是Alice，收款人是Bob，交易金額是10枚比特幣，再由礦工A通知世界各

地的其他礦工，最後每個礦工都把這筆交易寫進自己的比特幣帳本（區塊鏈），最後全世界所有礦工電腦裡的比特幣帳（區塊鏈）理論上應該完全一樣。

什麼是乙太坊智能合約？

區塊就是「存摺」，區塊鏈就是「存摺鏈」，也就是很多本存摺，所以區塊鏈只是儲存資料的「資料結構」或「資料格式」而已，既然是儲存資料，為什麼只能儲存「交易記錄」？為什麼不能儲存「任何資料」呢？因此只要支付手續費就可以請乙太坊礦工記錄任何資料，一段文字、一張圖片、一個合約、一段程式都可以，我們稱為「智能合約」。

舉例來說，曲博想要發行一種穩定幣稱為「知識幣（NTDA）」，但是目前知識幣大家沒聽過不值錢，因此曲博號召不了「知識幣礦工」替他記帳，那該怎麼辦呢？沒關係，只要支付手續費就可以請「乙太坊礦工」替他記帳，但是必須支付乙太幣做為礦工手續費，因此曲博必須花錢去買乙太幣當手續費，如此一來就可以增加乙太幣的流通，讓乙太幣成為大家共同流通使用的加密貨幣。

如果Alice想買100枚知識幣（NTDA）就把100元現金給曲博，而曲博把知識幣匯給Alice，這筆交易就傳送給乙太坊的礦工寫進乙太坊區塊鏈帳本裡，付款人是曲博，收款人是Alice，交易金額是100枚知識幣；接下來如果Alice想把10枚知識幣匯給Bob，這筆交易就傳送給乙太坊的礦工寫進乙太坊區塊鏈帳本裡，付款人是Alice，收款人是Bob，交易金額是10枚知識幣，依此類推。

公有鏈交易的穩定幣如何運作？

目前全世界第一大的穩定幣是「泰達（Tether）」發行的USDT幣，發行量為1,800多億美元，佔有大約60%的市場；第二大的穩定幣是「Circle」發行的USDC幣，發行量為700多億美元，佔有大約24%的市場，其它發行單位佔有大約16%的市場，如圖3所示。

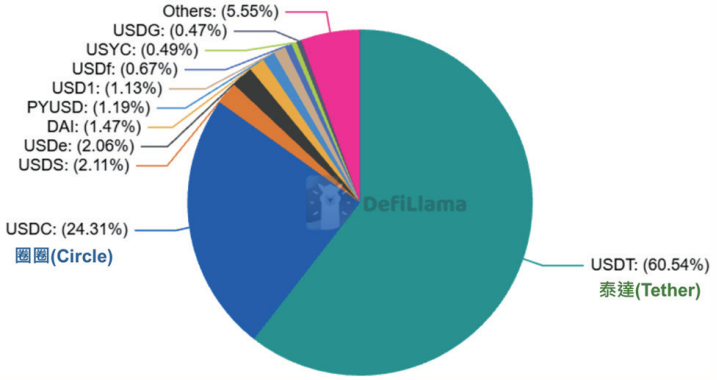

圖3、全球穩定幣發行量分布圖
資料來源：https://defillama.com/stablecoins。

如果Alice想買100枚USDT幣就把100美元現金給泰達，而泰達把100枚USDT幣匯給Alice，這筆交易就傳送給乙太坊的礦工寫進乙太坊區塊鏈帳本裡，付款人是泰達，收款人是Alice，交易金額是100枚USDT幣；接下來如果Alice想把10枚USDT幣匯給Bob，這筆交易就傳送給乙太坊的礦工寫進乙太坊區塊鏈帳本裡，付款人是Alice，收款人是Bob，交易金額是10枚USDT幣，依此類推，這就是利用「公有鏈」交易的穩定幣。

因為公有鏈裡的付款人和收款人只記錄使用者的公開金鑰，由於公開金鑰沒有驗證身分，所以大家不知道是Alice匯給Bob，只知道「某某某」匯多少穩定幣給「某某某」，但是不知道「某某某」是誰，因此公有鏈交易的穩定幣可以用來洗錢。

目前「泰達（Tether）」發行的USDT幣，其中大約46%是利用乙太坊區塊鏈帳本記帳，大約43%是利用波場區塊鏈帳本記帳，如圖4所示；「Circle」發行的USDC幣，其中大約66%是利用乙太坊區塊鏈帳本記帳，大約10%是利用索拉納區塊鏈帳本記帳，如圖5所示。

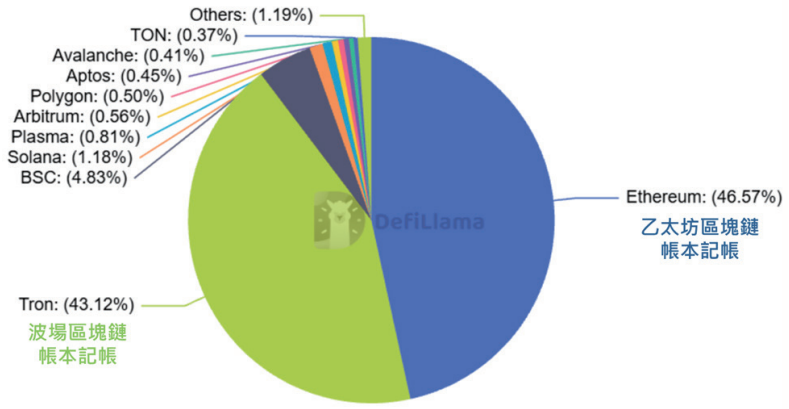

圖4、泰達（Tether）發行的USDT記帳分布圖。
資料來源：https://defillama.com/stablecoin/tether。

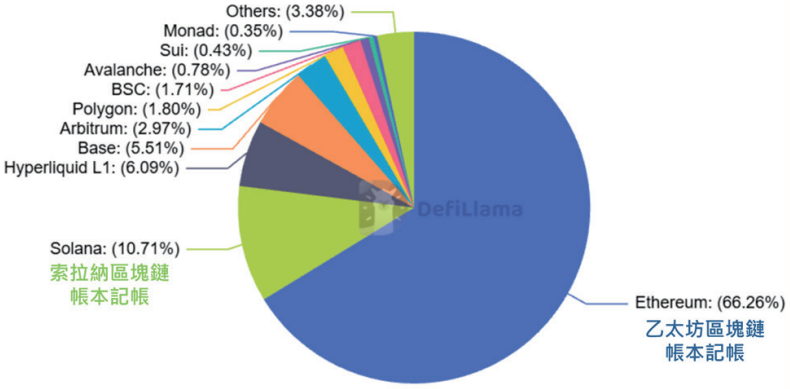

圖5、Circle發行的USDC記帳分布圖。
資料來源：https://defillama.com/stablecoin/usd-coin。

為什麼區塊鏈的交易速度變慢而不是變快？

公有鏈是任何人都可以參與的區塊鏈，任何人都可以讀取、發送、確認交易資料，參與共識過程，通常被認為是「去中心化」的區塊鏈，例如：比特幣使用「工作量證明（PoW）」可以做到「真去中心化」，這麼做要採礦、速度慢、浪費電，使得比特幣的區塊鏈全世界每秒鐘只能寫入6.82筆交易，耗電量卻是傳統金融的一萬倍，但是安全性高。

為了解決「真去中心化」的區塊鏈採礦浪費電的問題，於是他們又發明了「持有量證明（PoS）」，不採礦、速度快、節省電，但是安全性低，因此它是犧牲安全性換來交易速度的。例如：乙太幣原本使用要採礦、速度慢、浪費電、安全性高的「工作量證明（PoW）」，後來改成不採礦、速度快、節省電、安全性低的「持有量證明（PoS）」。

而且持有量證明（PoS）這種演算法會讓礦工持有的加密貨幣愈來愈集中，根本沒有去中心化，因此是屬於「假去中心化」的公有鏈。即使乙太坊區塊鏈使用了的「假去中心化」的持有量證明（PoS），全世界每秒鐘也只能寫入15~30筆交易稱為「第一層網路（Layer 1）」，為了再加快速度，於是又有聰明人發明了所謂「第二層網路（Layer 2）」。

我們前面介紹過區塊鏈只是儲存資料的資料結構，既然「第一層網路（L1）」我把它稱為「外帳」的區塊鏈記帳速度太慢，那就創造「第二層網路（L2）」我把它稱為「內帳」，也就是另外一個區塊鏈來記帳，使用速度更快安全性較低的演算法把交易記錄在「內帳」，等「需要的時候」再寫入速度更慢安全性較高的「外帳」，這樣乙太坊區塊鏈全世界每秒鐘就可以寫入2000~4000筆交易，果然是個好方法吧！

這麼簡單的方法大家都想的到，所以目前乙太坊的第二層網路包括：Mantle（MNT幣）、Arbitrum（ARB幣）、Optimism（OP幣）、Polygon（POL幣）、Movement（MOVE幣）等，總共超過150種，而且各自都發行自己的加密貨幣，大家現在領教到「去中心化」人人都能印鈔票的威力了吧！

為什麼講來講去區塊鏈全世界每秒鐘就只能寫幾千筆交易而已？原因很簡單，因為他們想要用很多台電腦記帳保有「去中心化」卻又想要「快速交易」才會魚與熊掌不可兼得。解決的方法很簡單，只要用「私有鏈」或「假聯盟鏈」來做「第二層網路（L2）」，其實就是用一台或幾台電腦來記帳，這樣全世界每秒鐘要交易幾萬筆都可以，聽起來是不是愈來愈像「儲值卡」了呢？

穩定幣的交易速度這麼慢為什麼過去夠用未來就不夠用？

大家可能覺得好奇，泰達（Tether）發行的USDT幣大約46%和Circle發行的USDC幣大約66%都是利用乙太坊區塊鏈帳本記帳，雖然全世界每秒鐘只能寫入15~30筆交易，在過去為什麼夠用？既然過去夠用為什麼未來就不夠用呢？

全球穩定幣市場總市值在2025年已經突破3,000億美元，每日鏈上真實支付高達300億美元，就是因為過去USDT幣和USDC幣大部分是用來吸金和洗錢，或是加密貨幣的上線割韭菜獲利了結與避險，這種交易金額很大但是交易數量不多，所以這麼慢的交易速度才夠用，未來如果

每個企業都發行穩定幣經由乙太坊區塊鏈這個「去中心化的金融基礎設施」記帳，大量交易可以直接用穩定幣支付，這麼慢的交易速度怎麼夠？

講到這裡大家猜猜看，未來如果USDC幣真的成功取代現金需要大量交易流通該怎麼辦呢？因此曲博在這裡大膽預言，Circle未來很可能建立自己的「圈圈鏈」，其實就是用一台或幾台電腦來記帳的「私有鏈」，這樣全世界每秒鐘要交易幾萬筆都可以，聽起來是不是愈來愈像「儲值卡」了呢？因為Circle已經建立品牌形象，管它什麼鏈便宜能用就好，因此很可能會成功唷！

到時候Circle將成全世界最大的跨國「悠遊卡公司」，台灣的小王可以把現金換成圈圈幣滙給美國的小美，小美拿到圈圈幣再向發行單位換回現金，如圖1所示，使用「圈圈鏈」立刻可以達到「秒級匯兌」，所以這個和儲值卡有什麼不同？

加密貨幣「由誰發行」和「如何交易」為什麼重要？

比特幣或乙太幣都是經由「公有鏈發行」：比特幣是礦工進行採礦運算的「工作量證明（PoW）」來取得礦工獎勵金，大家只能增加運算力來提高中獎機率；乙太幣是礦工進行質押演算的「持有量證明（PoS）」來取得礦工獎勵金，大家只能增加持有量來提高中獎機率，沒有任何單一組織或機構可以決定要給誰多少比特幣或乙太幣，所以這些都是「去中心化發行」。

穩定幣發行是經由「單一組織或機構」寫個程式發行幾千億枚穩定幣倒出去換成幾千億現金，所以都是「中心化發行」，而穩定幣可以經由公有鏈、聯盟鏈、私有鏈來交易，當你想要購買穩定幣，必須告訴發行商「你想要用哪一個區塊鏈帳本記帳」？如果使用公有鏈例如「乙太坊區塊鏈」來記帳，那就是「去中心化交易」，如果使用私有鏈例如「圈圈鏈」來記帳，那就是「中心化交易」。

監管機關不能只管「由誰發行」更要注意「如何交易」？

金管會在2025年6月將《虛擬資產服務法》草案納入穩定幣規範，初步共識是金融機構優先發行穩定幣，顯然認為金融機構被監管，可以確保合法合規，問題是金融機構發行穩定幣之後，經由什麼區塊鏈「交易流通」才是重點。

假設台灣銀行發行「新台幣穩定幣（NTDC）」經由「公有鏈」交易，如果Alice想買100萬枚NTDC幣就把100萬元現金給台灣銀行，而台灣銀行把100萬枚NTDC幣匯給Alice，這筆交易就傳送給乙太坊的礦工寫進乙太坊區塊鏈帳本裡，付款人是台灣銀行，收款人是Alice，交易金額是100萬枚NTDC幣，別忘了，乙太坊區塊鏈是匿名的。

這筆錢一但進入乙太坊區塊鏈，Alice就可以自由匯給全世界任何人不必和中央銀行申報，中央銀行也管不到乙太坊區塊鏈，中央銀行最多只能要求Alice和台灣銀行買NTDC幣的時候必須實名登記，只知道是Alice買走了100萬枚NTDC幣，但是Alice接下來將這筆錢匯給誰就管不到了！這也就是為什麼中國大陸堅決叫停穩定幣，因為洗錢是他們最在意的事情，所以我們的中央銀行同意金融機構發行這種可以洗錢的穩定幣嗎？

可能的解決方法是由中央銀行號召台灣所有銀行合作成立「聯盟鏈」，每家銀行負責管理一台伺服器做礦工，直接使用「實用拜占庭容錯演算法（PBFT）」每秒鐘可以交易幾千筆，甚至由中央銀行指派台灣銀行用一台伺服器建立「私有鏈」，只要增加伺服器的數量和頻寬每秒鐘可以交易幾萬筆，完全可以取代現金流通，甚至可以要求聯盟鏈或私有鏈的礦工實名制記錄每一筆交易人是誰，這樣就不能洗錢了！問題是這樣的穩定幣不就是「儲值卡」了嗎？這樣的穩定幣不就是「數位新台幣」而已嗎？

依照目前公有鏈的交易速度，確實公有鏈交易的美元穩定幣最主要的功能就是跨境匯兌和洗錢，再加上自從Circle被美國政府監管之後大開後門，利用USDC幣結算的交易量暴增，Visa、Mastercard、貝萊德等金融巨頭紛紛選為跨境結算媒介，交易金額快速增加，因為他們發現原來可以跳過SWIFT快速匯兌，又可以節省手續費擺脫銀行的控制何樂不為？至於公有鏈交易的穩定幣可以洗錢顯然不是現在的美國監管機關在意的事情。

美國領導全球金融發展，在川普總統的帶領下將是加密產業發展的大好時機，傳統金融必須嚴陣以待沒有放鬆的本錢，美國貨幣監理署(OCC)才剛核准了五張牌照，讓加密企業轉型銀行化，看到這裡如果你還在傳統金融業工作，是不是該開始好好學習區塊鏈原理了呢？面對穩定幣這樣的金融趨勢，台灣的金融業者與監管機關準備好了嗎？ CNFA

曲建仲

臺灣大學電機工程學系博士，曾任美商德州儀器（TI）資深應用工程師；政治大學、輔仁大學、東吳大學科技管理相關研究所兼任助理教授。

創辦「知識力科技股份有限公司」（Ansforce），致力於建立專家知識分享平台，並經營 YouTube 頻道「曲博科技教室」，將艱深困難的科技知識簡化成一般商務人士能夠理解的內容，在未來科技領導產業創新的時代是所有商務人士的必修課程。