台北外匯市場發展基金會委託計畫

虛擬貨幣之探討─以比特幣為例

研究人員：邱唯婷、湯佳勳

日期： 中華民國一零七年七月

摘要

說到區塊鏈(blockchain)，大多數的人會直接連結到區塊鏈技術發展至今首次最成功的應用─比特幣(BitCoin)，不過區塊鏈技術的重要性遠高於利用此技術發展的數位貨幣。區塊鏈可視為一個去中心化、分散式帳簿、公開透明共用的大型網路帳本，被密碼學原理與電腦程式所保護與自動執行。節點上的發生的所有交易數據將壓縮成區塊，和全部的節點複製共用，形成鏈狀(chain)的資料儲存結構；由於所有節點都會複製交易數據，而所有節點可以共同驗證帳本數據的正確性，可追蹤性高。在去中心化的區塊鏈網絡中，交易數據是由所有節點驗證，而非傳統具公信力的第三方仲介機構，完成交易、稽核、監管的成本低，並能節省相當高的作業成本與時間，也能夠大幅提升陌生交易雙方之間的信任度。本文第一部分透過至今發展較成熟的比特幣應用，解釋區塊鏈系統主要特性。

第二部分則為比特幣期貨的介紹。透過集中化交易市場，比特幣期貨之可放空、具財務槓桿效果、增加部位期限結構調整彈性及價格發現等特性，提供投資人對避險、投機、套利等交易目的之工具。芝加哥期權交易所(CBOE)與芝加哥期貨交易所(CME)於 2017 年 12 月陸續發行之比特幣期貨均採現金交割，然而最終結算價格之計算則有較大差異。由於現金交割方式對於現貨持有者的避險效果較不直接，加以不易建立最終結算價格，故市場上期望能推出採行實物交割之比特幣期貨。舊金山 FED 表示比特幣期貨的推出與比特幣價格快速下跌之期間相近，是因為期貨改變了投資人之交易行為，進而使比特幣價格滑落，且認為比特幣的基本價格是難以預測的，但當樂觀和悲觀的投機需求取得平衡後，比特幣價格仍將由市場交易目的需求之供需決定。

目　　錄

圖　目　錄

表　目　錄

壹、區塊鏈

區塊鏈技術的發明，讓使用者得以實施去中心化(decentralize)的交易，不必再依賴無形的信賴基礎或第三方權威機構。而透過分散式記錄的帳簿，使得每台電腦都可保留並共同維護完整交易紀錄的資料庫，在區塊鏈網絡上發生的交易因此無法被竄改或停止，藉此達到公開透明的效果。此外，區塊鏈技術的應用很大部分倚靠密碼學原理，透過密碼學，利用時間戳以明確交易發生的順序、數位簽章進行防偽的身分驗證，雜湊函數來串接資料以形成不可逆的資料鏈（區塊鏈）。最後，透過每台電腦持續耗費電力資源以驗證交易的挖礦機制，使區塊鏈網路得以自動解決交易的衝突。

由上述的說明可得知區塊鏈的特色，在於分散式帳簿(distributed ledger technology, DLT)、共同維護公開帳簿(public ledger)、具備時間戳(timestamps)、防止交易竄改(tamper resistant)、自動解決交易衝突(conflict resolution)等。在目前所有區塊鏈技術的應用中，比特幣是最為人所知的一項應用。電子貨幣可被用來做物品交換，就像美元、歐元、人民幣和其他國家的貨幣。以下利用比特幣的運作方式，說明區塊鏈的各點特色。

一、分散式帳簿(Distributed Ledger Ttechnology, DLT)

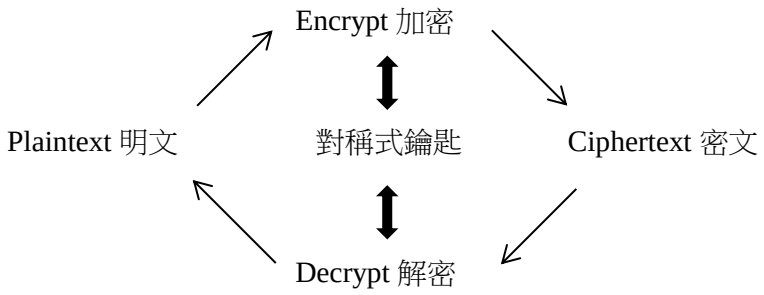
在比特幣網路中的帳簿(ledger)，它是記錄著所有的交易紀錄軌跡的電子檔案。而這帳簿並非存放在一個中央機構，而是將無數份副本散佈存放在區塊鏈網絡上的每一台電腦，也就是節點(node)中。使用分散式帳簿的優點在於每一個節點均保留所有交易紀錄的軌跡，在使用中央機構系統的情況，個人只能得知自身的交易紀錄和帳戶餘額，而在區塊鏈網絡裡，每個節點均儲存所有發生的交易紀錄，惟節點儲存的交易紀錄僅能顯示交易流動的軌跡，對於帳戶的個人隱私資訊則是利用哈希函數(hash function)生成的私鑰（數位簽章）及公鑰（錢包位置）進行機密信息的保護。

二、密碼學應用─公鑰與私鑰

比特幣用戶首先要取得一個或多個電子錢包(wallet)作為交易的工具。電子錢包中包含多個帳戶，每個帳戶可包含多個私鑰。每個錢包被密碼學加密法所保護，必須使用一對獨特且相對的公鑰和私鑰才能解鎖並進行交易，使得虛擬貨幣的交易不同於傳統的方式，有更高的防偽性。

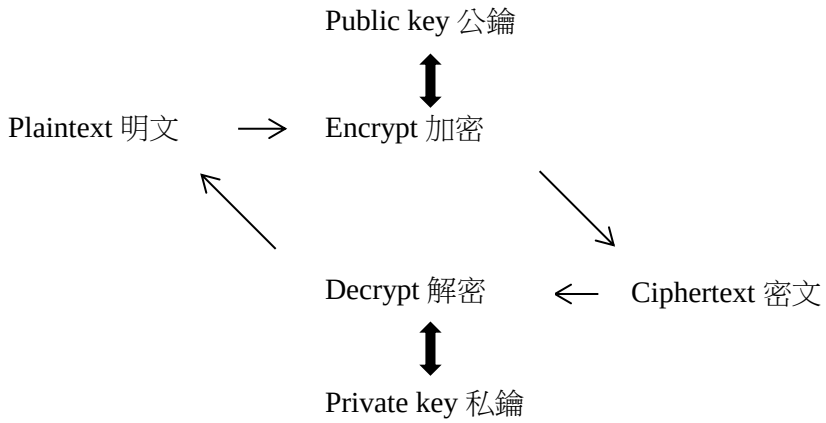
傳統的對稱式的密碼系統，使用相對應的鑰匙(key)進行加密與解密（圖 1），使用此法的情況下不論加密的難度有多高，只要第三方得到相應的解密鑰匙，便可以成功的替資料解密。

圖 1 對稱式密碼系統



而在比特幣的區塊鏈系統中，使用公鑰替內容加密，並使用私鑰替密文解密，此方式可更好的確保加密的內容不會簡單的被破解。比特幣不採用傳統的 RSA 加密演算法(Rivest Shamir Adleman, 1977)，而使用橢圓曲線數位簽章演算法（ECDSA）來製作公鑰與私鑰，使用此演算法的結果使得中由私鑰很容易算出公鑰，但是公鑰不容易逆推算回私鑰（圖 2）。

圖 2　ECDSA 系統之加密與解密過程



比特幣位址由公鑰得出，公鑰常公開發佈，使得比特幣用戶能利用公鑰產生的一組比特幣位址進行轉帳交易；而私鑰則由私人保管。如果一個訊息被公鑰加密，只有配對的私鑰才能解密讀到訊息。使用私鑰加密後，會產生一個電子簽章，藉此確認交易訊息的發送來源和真偽。電子簽章內容是由交易訊息和私鑰所組成的一串文字，所以特定的電子簽章不能用在其他的交易訊息上。如果第三方更改交易訊息中任何一個字元，電子簽章將因為雪崩效應(avalanche effect)[1]造成輸出值大幅度的改變，所以駭客很難更改以加密的交易訊息或是得知交易金額，達到防止交易被竄改的效果(tamper resistant)。

三、公開帳簿(public ledger)

虛擬貨幣去中心化的核心概念，使得每個節點中都保有一份交易軌跡的帳簿，並藉由持續更新自己節點內留存的交易資訊，以共同維護此公開交易紀錄。而在區塊鏈

[1]在密碼學中，雪崩效應(avalanche effect)指加密演算法的一種理想屬性，當輸入發生微小的改變（如二進位位元順序反轉）時，將導致輸出的不可區分性的改變（輸出中每個二進位位元有50%的機率發生反轉）。雪崩效應使得利用輸出數據反推原始輸入數據的難度大增，而比特幣使用的 SHA-1 哈希函數即擁有良好的雪崩效應特性。

系統中，並非透過紀錄每個帳戶目前所擁有的「餘額」，只有紀錄網絡上每筆「交易紀錄」，所以欲得知某帳戶內尚可花用的虛擬貨幣時，必須分析及驗證所有曾經跟特定錢包地址產生交易的紀錄。

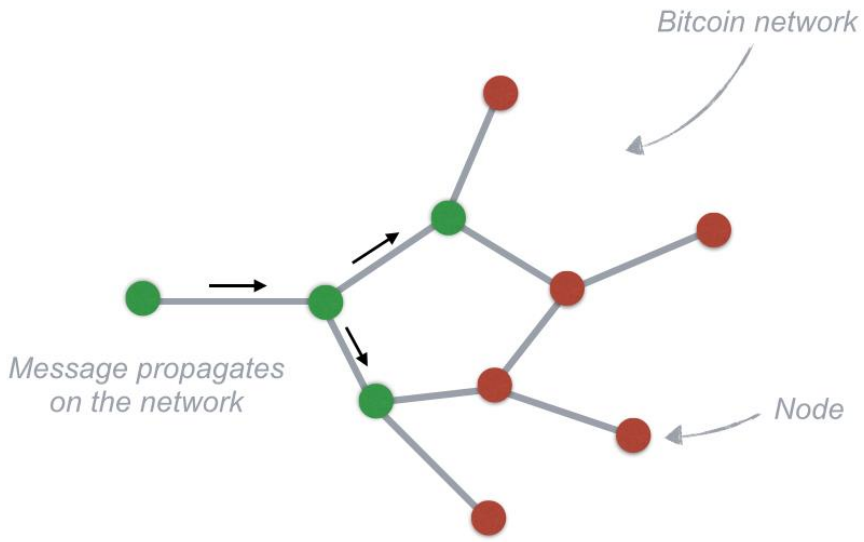
目前的支付系統如銀行、信用卡、證券交易系統或第三方支付系統，核心都是基於帳戶(account based)的設計，由關係資料庫支撐。資料庫系統必須確保兩點，第一是確保遵守業務規則得到遵守，第二是確保資料庫事務性(ACID)。但利用資料庫系統來維護帳簿存在著若干缺點，如雙重支付問題(double spending)的解決方案，將可能使資料庫系統的內容無限膨脹。

雙重支付問題，簡言之就是必須確保證每一筆數字現金都只會被花費一次，避免出現重複支出的情況。而資料庫系統在面臨此問題時，必須在每筆交易後都更新一次全體的餘額表（不論個別帳戶是否進行交易），才能確保款項正確入帳。

四、未被花費的交易支出(UTXO)

針對雙重支付的問題，區塊鏈系統與現行的資料庫帳務系統分別採用「未被花費的交易支出」方式及「餘額」方式留存交易資訊。區塊鏈之點對點系統沒有中心化的總帳簿，與現行的餘額系統相比，其優點在於能節省同時更新所有帳戶紀錄的資訊儲存成本，但缺點為交易需要經過大多數節點確認才能達成共識，如果信息傳遞有時間差，就無法同時確認所有帳戶餘額，以下介紹兩種紀錄方式之差異。

圖 3 區塊鏈交易信息點對點的傳遞方式



資料來源：Michele D'Aliessi(2016)

每筆交易都有若干筆交易輸入（資金來源），與若干筆交易輸出（資金去向）；藉由花費(spend)交易輸入，產生交易輸出，而交易所產生的輸出就是「未被花費的交易輸出」(Unspent Transaction Output, UTXO)。UTXO 亦可稱為一個標示著目前可使用（未被支付）的資金的狀態(state)，比特幣交易的資金流轉，就可想像為 UTXO 不斷更新至最新的可供花費資金的狀態的過程。

舉例而言，假設以下情況：

<交易一> 張三的節點解出哈希函數，成功的將自己的候選區塊放到最長鏈的鏈尾並獲得挖礦獎勵 12.5 枚比特幣（請參考第九節）。

<交易二> 張三將此挖礦獎勵中的 2.5 枚轉帳給李四。

<交易三> 李四與張三各支付 2.5 枚比特幣給王五。

可由下表中帳戶交易狀態欄，比較使用餘額法與未被花費的交易輸出法時的交易紀錄差異。

表 1　餘額方式與 UTXO 方式下的帳戶交易狀態

<table>
<tr><th></th><th>Balance/餘額</th><th>UTXO/未被花費的交易輸出</th></tr>
<tr><td>帳戶
交易
狀態</td><td>
1. 張三挖到 12.5 枚比特幣
<table>
<tr><th>帳戶名</th><th>餘額</th></tr>
<tr><td>張三</td><td>12.5</td></tr>
<tr><td>李四</td><td>0</td></tr>
<tr><td>王五</td><td>0</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
2. 張三把其中 2.5 枚比特幣給李四
<table>
<tr><th>帳戶名</th><th>餘額</th></tr>
<tr><td>張三</td><td>10</td></tr>
<tr><td>李四</td><td>2.5</td></tr>
<tr><td>王五</td><td>0</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
3. 李四和張三各出 2.5 枚比特幣給王五
<table>
<tr><th>帳戶名</th><th>餘額</th></tr>
<tr><td>張三</td><td>7.5</td></tr>
<tr><td>李四</td><td>0</td></tr>
<tr><td>王五</td><td>5</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
</td><td>
1. 張三挖到 12.5 枚比特幣
<table>
<tr><td colspan="4">coinbase 交易　交易號: #1001</td></tr>
<tr><td rowspan="2">交易輸入</td><td colspan="3">交易輸出(UTXO)</td></tr>
<tr><td>第幾項</td><td>數額</td><td>收款人地址</td></tr>
<tr><td>挖礦獎勵</td><td>(1)</td><td>12.5</td><td>張三地址</td></tr>
</table>
2. 張三把其中 2.5 枚比特幣給李四
<table>
<tr><td colspan="4">普通交易　交易號: #2001</td></tr>
<tr><td>交易輸入</td><td colspan="3">交易輸出</td></tr>
<tr><td>資金來源</td><td>第幾項</td><td>數額</td><td>收款人地址</td></tr>
<tr><td rowspan="2">#1001(1)</td><td>(1)</td><td>2.5</td><td>李四地址</td></tr>
<tr><td>(2)</td><td>10.0</td><td>張三地址</td></tr>
</table>
3. 李四和張三各出 2.5 枚比特幣給王五
<table>
<tr><td colspan="4">普通交易　交易號: #3001</td></tr>
<tr><td rowspan="2">交易輸入</td><td colspan="3">交易輸出</td></tr>
<tr><td>第幾項</td><td>數額</td><td>收款人地址</td></tr>
<tr><td>#2001(1)</td><td>(1)</td><td>5.0</td><td>王五地址</td></tr>
<tr><td>#2001(2)</td><td>(2)</td><td>7.5</td><td>張三地址</td></tr>
</table>
</td></tr>
</table>

由表1就可以發現，採用餘額法紀錄時必須同時維護系統內所有帳戶的正確餘額，以確保交易正確的執行，使同一筆金流不重複出現在其他的帳戶中。而每次交易都更新全體餘額表的結果，必然造成資料庫內大量的冗餘信息。相較之下 UTXO 方式的資料庫僅記錄著當前系統裡每一筆的 UTXO，在節點接受交易時，僅需要去 UTXO 資料庫裡查詢交易引用的 UTXO 是否存在（存在，即表示此 UTXO 確實尚未被支付），以及查詢此 UTXO 的擁有者是不是當前新交易的付款者（避免花費他人的交易輸入）。

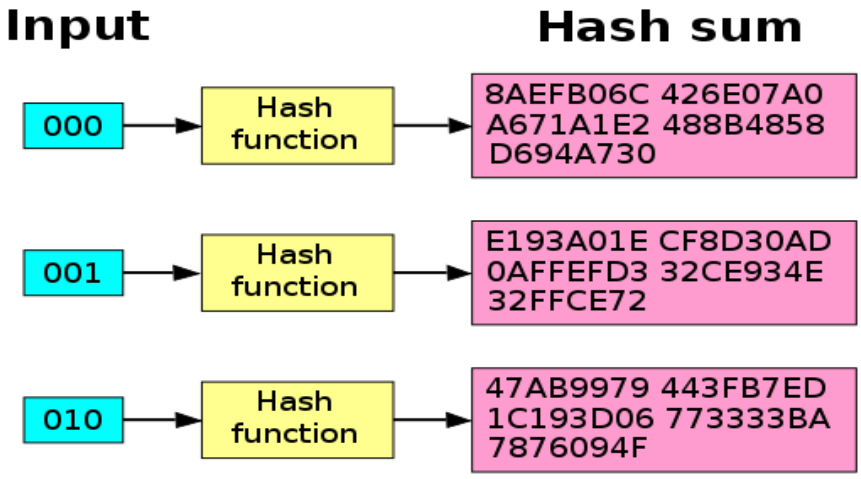
五、區塊(block)

比特幣網絡將多筆交易訊息包成一組資料塊，稱為區塊，每個區塊包含的若干個比特幣交易訊息，和一個連到前個區塊的連結。而比特幣網路同時在每個區塊內加入時間戳記(timestamp)，藉此排出交易發生的先後順序，一個區塊跟著另一個區塊，跟隨著時間軸形成一條資料區塊的長鏈，此就為區塊鏈。

在時間序列上，同個區塊內的交易訊息被認為是同時發生，還未被打包進區塊的交易訊息會被視為未確認狀態。每個節點(full node)都可以自己選擇若干個交易訊息，打包成內容不同的區塊（交易訊息包），發送到網絡上，並建議其他節點自己打包的這個區塊為鏈上的最新候選區塊。因為任何節點都可以打包並發送候選區塊，區塊鏈系統使用加密哈希函數(cryptographic hash function)，運用工作量證明機制(proof of work, POW)來決定鏈上的最新區塊。

哈希函數是一種單向函數(one-way function)，輸入訊息(message)並產出摘要(digest)。哈希函數可將任意長度的二進制字符串轉換為固定長度的二進制字符串，此固定長度的二進制字符串就為其哈希值。

圖 4 哈希函數的雪崩效應



每一個區塊所包含的資訊，包括區塊容量大小(block size)、區塊頭(block header)、該區塊所打包的交易數量(transaction counter)，以及在此區塊中每一筆交易的交易明細(transactions)的哈希值。其中區塊頭包含許多重要資訊，如追蹤區塊鏈協議升級的版本號(version)、前一區塊的區塊頭之哈希值(previous block header hash)、工作量證明相關及彙整交易紀錄的中繼資料。

接著，區塊鏈系統利用工作量證明機制來決定哪個候選區塊能成為鏈上的最新區塊。系統的加密哈希函數設計了一道複雜的數學題，各節點打包的候選區塊只要找到正確答案，就可以成爲鏈上的最新區塊。正確的答案是以一個數字的形式呈現，各節點用試誤法(trial and error)反覆嘗試，找出符合題目要求的正確解答。隨著比特幣網路中加入的節點越多，集體算力的增強將使得找出正確解答的速度越來越快，故系統為了控制區塊產生的速度維持在大約每 10 分鐘一個，將定期調整產生新區塊（哈希函數數學題）的難度。

六、工作量證明機制(Proof of work, POK)

以上試誤的過程，就稱為工作量證明。工作量證明是一種對應服務與資源濫用、或是阻斷服務攻擊的經濟對策。一般是要求使用者（節點）進行一些耗時的複雜運算以得出解答。利用密碼學，此解答之取得雖然需花費很長的時間，但卻可被第三方快速地驗算，以此耗用的時間、裝置與能源做為擔保成本，以確保服務與資源是被真正的需求所使用，即是工作量證明的原理。

而此技術成為了加密貨幣的主流共識機制之一，利用哈希函數的特性，輸入函數 h(　)任意值 n，將對應到一個h(n)結果，此結果 n 也就是函數的解，哈希值。而 n 只要微小的變動，就會引起哈希值的雪崩效應，所以幾乎無法從h(n')反推回 n。因此，藉由指定 h(n)的哈希值符合特定的難度條件，讓使用者進行大量的窮舉運算，就可以

達成工作量證明。此耗費大量時間、裝置或能源，以得到特定獎勵的過程，被中本聰在比特幣的論文中比喻成金礦消耗資源將黃金注入經濟，也就是形象化的「挖礦」(mining)一詞的由來。

七、區塊鏈的鏈狀(chain)結構

完成工作量證明、成功找到哈希函數答案的節點，就可以把自己的候選區塊加到目前最長鏈的尾端，並將此最新區塊以及正確解答發送給全網，廣播給其他節點。比特幣網路中接收到此區塊以及解答的其他節點，將驗證新區塊的正確性及有效性（意即將答案帶入數學題中，視此答案是否合於哈希函數規定的難度要求），若驗證此區塊為正確有效，各節點就將這個新區塊接在自身儲存鏈的最尾端。藉由不斷的廣播、傳送（參考圖 3），各接收節點皆會驗證此區塊的正確性，達到分散式帳簿(DLT)的功能。

之後，各個節點將再度進行下一個區塊的打包與其工作量證明，並在最長鏈上開挖下一個區塊。設想反例的一種情況，若是目前區塊鏈網路中區塊高度(block height)已有節點正確解出哈希函數答案，而有一節點不接受此區塊，並繼續開挖自身備選區塊。接受了最新區塊的其他節點（假設此新區塊的高度為 n），將在驗證後將此高度 n 的區塊納入鏈中，並開始挖掘區塊高度為 n+1 的備選區塊；而不接受最新區塊的節點則持續原先的行為，繼續挖掘高度 n 的備選區塊。由於區塊鏈網路的設計，使得所有節點都必須接受網路中的有效之「最長鏈」，故除非該不接受最新區塊節點的算力能超越其他節點，搶先解出高度 n+2 區塊哈希函數並成為最長鏈，否則較短之鏈將不會被網路中的其他節點接受，亦無法建立共識。

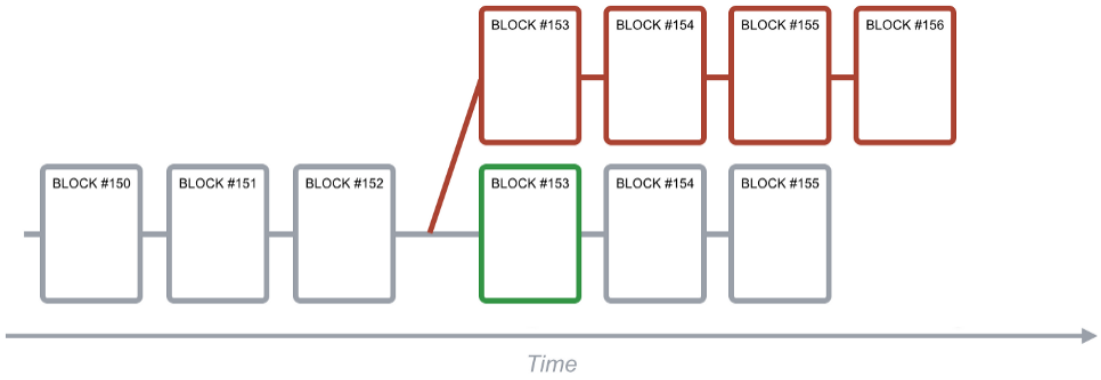
按照最長鏈原則，所有節點都將接受現行網路中最長的鏈，並在繼續開挖新的備選區塊，而形成區塊鏈資料鏈狀結構紀錄的要件，為節點在開挖最新備選區塊石，將前一認證區塊的區塊頭進行哈希函數處理，得到的哈希值會被成為下一個的候選區塊

的一部分，前一區塊的區塊頭之哈希值，是形成區塊鏈鏈狀結構最關鍵的連結，利用在每個區塊中包含上一個區塊的區塊資訊，使每一個區塊與前一個區塊資料產生無形的連結，並能確保區塊時間序列及歷史紀錄的正確性。這麼做可讓這些被驗證完的交易區塊依序串接形成鏈狀結構，一旦節點哈希值不正確，便會立刻被其他節點驗證出來，並拋棄此鏈採納其他的最長鏈。而透過哈希函數將原始資訊轉換固定長度的字符串，每個節點都將線下保有一份經過哈希加密的交易紀錄，此特性亦使區塊鏈具有防輕易竄改(tamper-proof)的特性。

八、自動解決交易衝突(conflict resolution)

區塊鏈網路得實行去中心化的另外一項特徵，就是得自動解決交易衝突的特性，不論其為善意或惡意之交易衝突。區塊鏈網路自動解決交易衝突的具體作法為，在符合密碼學原理的哈希函數規定下，永遠接納最長的區塊鏈條。

圖 5 交易衝突



資料來源：Michele D'Aliessi(2016)

善意的交易衝突，為區塊鏈網路中各節點在實施工作量證明時，在極小的機率下，

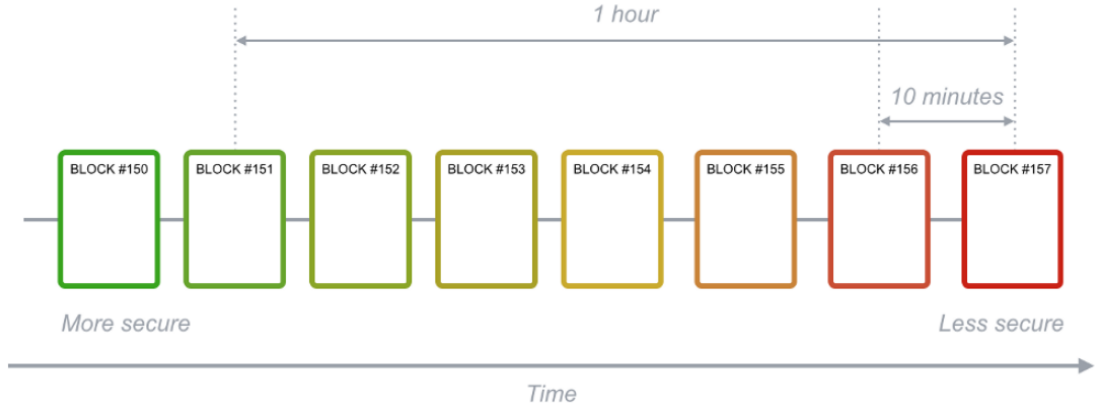
可能發生多個節點同時找到符合哈希函數要求的正確答案的情況。在此情況發生時，由於區塊鏈網路中的資訊將透過節點不斷傳遞流通，節點收到的資料將存在時間差，不同的節點可能接收到不同的最長區塊鏈，在區塊鏈長度都相同的情況下，此兩條（多條）區塊鏈均同時為正確的最長鏈。

於是接收到不同最長鏈的節點又開始進行新一輪的工作量證明，將新的候選區塊加到最長鏈的尾端，因為區塊鏈的鏈狀結構必須將前一個區塊的交易資訊做為參數加入哈希函數中，故根據不同的「前區塊」打包的後續區塊將面臨完全不同的哈希數學題，不同支鏈上的區塊就可視為相異的交易資訊塊。節點將持續進行工作量證明，直到區塊鏈網路中有更長鏈出現，此時節點將捨棄目前自身的候選區塊，經驗證後採納新的最長鏈，再於最長鏈的尾端繼續打包新的區塊，只接納最長鏈的特色使得區塊鏈系統得自動的解決交易衝突。

惡意的交易衝突，則存在於節點嘗試利用鏈尾模糊現象，進行重複支出的操作。惡意節點可以在發出支付訊息並收到貨物後，立即再發出另一個取消交易的訊息，因為比特幣網路的交易規則為止接納最長長度的鏈，故該節點只要能使包含取消交易訊息的鏈成為現行網路中的最長鏈，則可使全部的節點均接受此取消交易的訊息，成功達成重複支出的操作。

比特幣系統防止這類攻擊的方式，則是利用密碼學的哈希函數的工作量證明機制。該惡意節點的解題速度必須高於網絡上所有的節點，才可能把包含取消交易的候選區塊放到鏈的尾端，等同於該惡意用戶必須與整個網絡上節點們競速，因為比特幣網路上有大量的節點，在確切的時間點假造多個區塊來進行攻擊是相當困難的。

圖 6 區塊鏈的交易安全



資料來源：Michele D'Aliessi(2016)

比特幣網路的節點在即時發送交易後，平均需要 10 分鐘才可確認完成並包含在區塊的尾端，確認代表的意涵為網路上有至少一個節點認可交易中未被花費的交易支出(UTXO)的合法性。一旦交易被打包入區塊鏈中，它會被它後面的區塊所掩埋，後接區塊的工作量證明將呈指數增長，加強此共識並降低交易內容更動（如取消交易）的風險。

一般而言，經過 6 個區塊確認後的交易結果已具備可信性並無法被逆轉。惡意節點必須控制強大的算力來追趕前一筆交易的確認速度，當落後 6 個區塊來追趕之前的交易時，將需耗費非常大的計算量。從經濟的角度考慮，擁有如此強大算力的節點並無誘因去追趕經 6 次確認的區塊，因在此過程中浪費的資源用來正經挖礦將可獲得更高的收益。

九、回饋機制(rewards)

在比特幣網路中，為了平衡軟體錯誤或錢包密碼遺失所造成比特幣的通貨緊縮，

並鼓勵各節點進行第五節中提到的工作量證明機制，以確認交易、防止雙重支付問題，系統會獎勵解開數學題的節點一定數量的挖礦獎勵。挖礦獎勵是一種激勵機制，推動使用者建立節點、打包備選區塊、共同驗證並維護整體區塊鏈的資料儲存鏈有效性，順帶貢獻一些計算效能來幫助整個網絡的運算和穩定。

節點按照一定的挑選方式，將接收到的交易資訊打包入備選區塊，每個區塊都會允許發行一定數量的新比特幣，用來激勵成功找到解答、並將區塊新增至最長鏈上的節點。比特幣系統按照預定的貨幣增發節奏決定發行的比特幣數量，藉由控制解出哈希函數的難度值，將區塊產生的速度控制在每 10 分鐘發行一個。最初，比特幣系統設計成功確認區塊的節點可獲得 50 個比特幣的獎勵，但此一獎勵會在每出現 21 萬個區塊後折半[2]，收斂的效果使得比特幣的總數量不會超過 2,100 萬個。

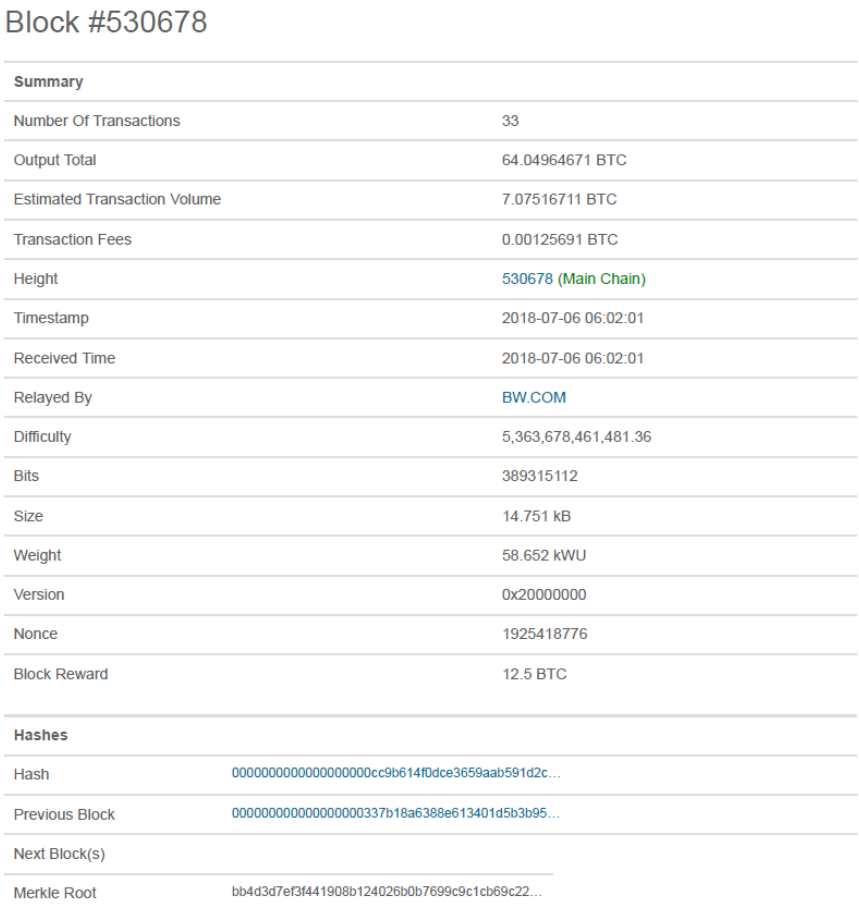
比特幣的挖礦獎勵的減半頻率，約為每 4 年發生一次，故總數為 2,100 萬枚的比特幣預估將在 2140 年全數挖得，而隨著新發行比特幣數量的下降，節點對挖礦的興趣會減少，為了避免節點停止挖礦，系統允許每筆交易訊息可以附帶一點回饋金，性質類似處理交易的手續費用，節點便可以獲得額外的利益，使得手續費獎勵將成為比特幣系統發展後期節點挖礦的主要動機。

與 VISA 每秒可以處理千筆交易的速度相比，比特幣的區塊鏈系統每秒僅得紀錄約 7 筆交易，隨著比特幣交易量的增加，各筆交易驗證的等待時間也增加，使得新發生的交易只能藉由支付更多手續費的方式，來提高被驗證的優先順序。由於節點在不超過區塊容量大小的前提下，可以自行決定將未確認池中任何交易打包至區塊中，因此節點將優先選擇手續費較高的交易來打包入區塊，賺取手續費收入。跟銀行收取的

[2] 第一次減半發生於 2012 年 11 月 28 日 15:24:55UTC，約是首枚比特幣於 2009 年挖出後的四年後，挖礦獎勵由 50 個減半為 25 個比特幣。第二次減半發生於 2016 年 7 月 9 日 16:46:13 UTC，挖礦獎勵由 25 個減半為 12.5 個比特幣。目前每個區塊得新發行的挖礦獎勵為 12.5 個比特幣。

手續費相比，比特幣的交易的手續費回饋較少，且僅與該交易耗用的數據量相關，跟交易的金額無關。

圖 7 比特幣交易回饋金



Block #530678

Summary	
Number Of Transactions	33
Output Total	64.04964671 BTC
Estimated Transaction Volume	7.07516711 BTC
Transaction Fees	0.00125691 BTC
Height	530678 (Main Chain)
Timestamp	2018-07-06 06:02:01
Received Time	2018-07-06 06:02:01
Relayed By	BW.COM
Difficulty	5,363,678,461,481.36
Bits	389315112
Size	14.751 kB
Weight	58.652 kWU
Version	0x20000000
Nonce	1925418776
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000000cc9b614f0dce3659aab591d2c...
Previous Block	0000000000000000000337b18a6388e613401d5b3b95...
Next Block(s)	
Merkle Root	bb4d3d7ef3f441908b124026b0b7699c9c1cb69c22...

資料來源：Bitcoin Block Explorer – Blockchain 網站

圖 7 中的「Transaction Fee」欄位，即為比特幣區塊鏈現行第 530678 塊區塊中所有交易包含的手續費回饋（0.0125691 枚比特幣）。未來節點的挖礦獎勵遞減，在挖礦的電力成本固定的情況下，節點勢必得收取更多的交易手續費來回收成本。包含挖礦獎勵與手續費回饋機制，使整個區塊鏈網路得以維持流動性，流通性對於區塊鏈網路而言事關重大，目的就在於獎勵原本和網路毫無關係的使用者（節點），讓他們願意投入電腦設備、電力、算力，協助整個區塊鏈生態的運行。

貳、比特幣期貨

2017 年 12 月芝加哥期權交易所（Chicago Board Options Exchange, CBOE）與芝加哥期貨交易所（Chicago Mercantile Exchange, CME）推出比特幣期貨商品，提供一項能滿足投資人對比特幣避險、投機、套利等交易目的之工具，另亦有助於提高市場流動性及價格發現等功能。

以下分為五部份來探討比特幣期貨，第一部分，介紹比特幣期貨的功能及交易策略，第二部分，比較 CBOE 和 CME 發行的比特幣期貨合約，第三部份， 分析比特幣期貨交割方式，第四部份，描述投資比特幣期貨的風險，第五部分，探討比特幣期貨對比特幣現貨價格之影響。

一、比特幣期貨的介紹

期貨合約即合約雙方約定於未來特定時間、價格交換特定金額的現貨，交割方式可為實物交割或現金交割，實物交割即提供實體標的物作為交換，現金交割則是以交易所的最終結算價格來計算未平倉部位的盈虧，收付現金以終了期貨合約。

(一)、比特幣期貨的功能

相較於比特幣現貨，比特幣期貨有可放空、具財務槓桿效果、增加部位期限結構調整彈性及價格發現四項功能，分述如下：

1. 可放空：比特幣期貨允許投資者賣空比特幣，因此藉由比特幣期貨可達到對比特幣避險、投機或套利等交易目的，有利於投資者進行風險移轉及提高投資效率。
2. 具財務槓桿效果：僅需繳交合約價值的部分比例作為保證金，即可透過期貨交易看多或看空比特幣價格。
3. 增加部位期限結構調整彈性：由於比特幣期貨具不同到期日的合約，可讓投資者更

靈活地調整比特幣部位的期限結構。

4. 價格發現功能：期貨價格反映出供需雙方對未來的供需關係和價格走勢的預期，加以其槓桿特性可吸引眾多不同交易目的(例如避險、投機等)的參與者進入期貨市場，進而增加市場流動性，因此有助於發揮其價格發現功能。

(二)、比特幣期貨的交易策略

比特幣期貨具有可放空、槓桿及可調整期限結構等特性，因此有避險、投機和套利等交易策略，以下為加密貨幣對沖基金 BlockTower Capital 對比特幣期貨交易策略的介紹：

1. 看多(An Outright Long Position)：讓看好比特幣價格的投資者，在不持有比特幣現貨的情況下看多比特幣價格，使其免於比特幣被偷竊或遺失的風險。
2. 避險(Hedging Long Position)：對於提供商品或服務賺取比特幣或藉由採礦等方式持有比特幣現貨者，可透過放空比特幣期貨，來規避比特幣現貨價格波動的風險。
3. 相關部位的合約交換(Exchange of Contract for Related Position, ECRP)：期貨價格與現貨價格出現不合理的價差時，套利者可以買(賣)比特幣期貨，同時作反向的實體比特幣交易，建立一個近似無風險的交易，透過買低賣高來套利。例如，期貨價格比現貨價格高時，買入現貨並作空等價的期貨，等待交割時賺取價差。
4. 投機(Speculation)：投資者由於特定事件(例如，法規、採礦難度等改變)、動能(momentum)或均值回歸(mean-reversion)等原因推測比特幣價格走勢，進而作多或作空比特幣期貨，以獲取投機利潤。
5. 時間價差交易(Calendar Spread Trades)：買賣不同到期日的比特幣期貨，以獲取時間價值的價差策略，或用以調整比特幣部位的期限結構。例如，投資人目前持有一月到期的期貨合約，而他想將該期貨合約延長至三月份，此時可利用時間價差交易，賣一月份到期的合約同時買入三月份到期的合約。

二、CME 與 CBOE 比特幣期貨合約之比較

表 2 XBT 與 BTC 期貨合約比較

發行交易所	芝加哥期權交易所（CBOE）	芝加哥期貨交易所（CME）
合約名稱/代碼	CBOE Bitcoin Futures/XBT	CME Bitcoin Futures/BTC
發行時間	2017/12/10	2017/12/18
合約規模	1 個比特幣	5 個比特幣[3]
保證金	初始保證金: 44% 維持保證金: 40%	初始保證金: 47% 維持保證金: 43%
最終結算價	最終結算日 16：00（美東時間）Gemini 交易所的集合競價價格	最後一個交易日 CME CF 比特幣參考價格(BRR)
交割方式	現金交割	現金交割
最小變動價位	outright 合約：5 美元 calendar spread 合約：0.01 美元	outright 合約：25 美元 calendar spread 合約：5 美元
價格波動限制	±10%、±20% [4]	±7%、±13%、±20% [5]
交易時間 (根據美國東部時間，Eastern Time zone, ET)	■ 常規交易時段： 週一至週五 9:30 至 16:15 ■ 延長交易時段： 週一：前一日 18:00 至當日 9:30 週二至週五：前一日 16:30 至當日 9:30	週一至週六：前一日 17:00 至當日 16:00
合約期限	可掛牌最近 4 個週、最近 3 個連續月及 3 個季月(3/6/9/12 月）合約；但初期 CBOE 將掛牌最近 3 個連續月合約	最近 2 個連續月（不在季月中）到期的合約及最近 2 個季月（3/6/9/12 月）
最後交易日	■ 週合約：到期週週五前的第二個交易日 ■ 其餘合約：到期月第三個	到期月的最後一個星期五

[3] 假設 CME CF 比特幣參考價格(BRR)為$9,000，則 BTC 價格為$45,000。

[4] 與「前日交易結算價格」比較，價格變動幅度大於±10%時，交易暫停 2 分鐘；價格變動幅度大於±20%時，交易暫停 5 分鐘。

[5] 與「前日交易結算價格」比較，價格變動幅度大於價格波動限制(±7%及±13%)時，先觀察兩分鐘，若價格波動仍達限制，則交易暫停兩分鐘(投資人仍可新增、修改或取消掛單，但交易在這段時間不會進行搓合)，後進入下個價格波動限制(±13%及±20%)，當日價格變動幅度不得大於±20%。

	週五前的第二個交易日 ■ 遇假日則提前一天	
持倉限額	■ 現貨月合約(即最接近到期日者)，在最終結算日前的第 5 個交易日起，限量 1,000 份合約。 ■ 所有不同到期日的合約，共計限量 5,000 份合約。	■ 現貨月合約，限量 1,000 份合約。 ■ 非現貨月合約，限量 5,000 份合約。
大宗交易最低限額	■ 最少 50 份合約(不同到期日的期貨合約分開計算) ■ 大宗交易的最小變動價位是 0.005 美元/合約	■ 最少 5 份合約

資料來源：CBOE、CME

(一)、CME 與 CBOE 比特幣期貨合約相似處

CBOE 的 BXT 期貨合約與 CME 的 BTC 期貨合約有三個相似處，第一，交割方式均採現金交割，第二，由於比特幣價格波動性較高特性，因此相較於其他期貨商品有較高的保證金要求，且有價格波動過大時之暫停交易機制，第三，有持倉量限制，以避免特定投資人壟斷市場。

(二)、CME 與 CBOE 比特幣期貨合約相異處

BXT(CBOE)及 BTC(CME)的合約規模及最終結算價格有較大的不同。在合約規模方面，CBOE 為一個比特幣，相較之下 CME 期貨合約規模較大，為五個比特幣，較適合機構投資者。在最終結算價格方面，CME 採用最後一個交易日的 CME CF 比特幣參考價格(Bitcoin Reference Rate, BRR)，而 CBOE 則採最終結算日 16：00（美東時間）Gemini 交易所的集合競價價格，以下分述兩交易所比特幣期貨採用的最終結算價格及其優缺點。

1. CME BTC 的最終結算價格 - BRR

(1) BRR 係由 CME 和 Crypto Facilities Ltd. 依據四家選定的比特幣交易所在特定時間的成交價量數據，經時間加權計算成之美元計價的比特比參考價格，BRR 於

每日 16:00 至 16:30 間公佈。

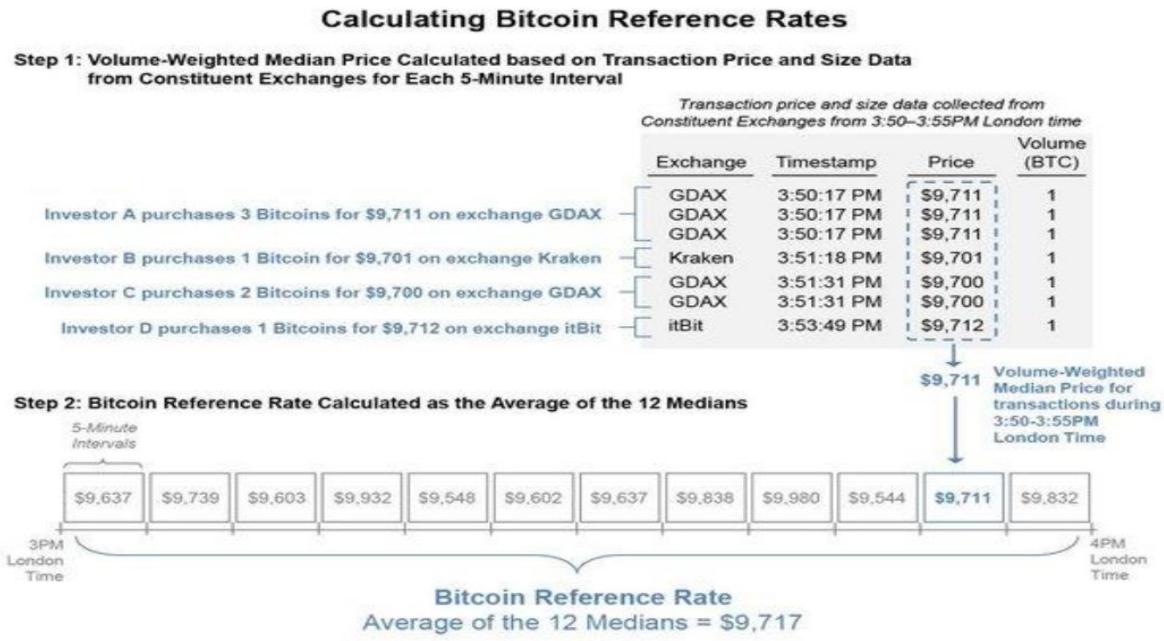
(2) BRR 計算規則及範例如下：

i. 蒐集 Bitstamp, GDAX, itBit 及 Kraken 四家比特幣交易所在倫敦時間 15:00 至 16:00 成交價量的時序資料，並劃分成 12 等分(即每等分 5 分鐘)。

ii. 依據每個時間等分的交易價格和成交量，計算出成交量加權中位數交易價格 (Volume-weighted median trade price)。

iii. 將得到的 12 個中位數作簡單算術平均，即可求出 BRR。

圖 8 BRR 計算範例



資料來源：Nicole Moran, Yesim Richardson and Robert Letson (2017)

(3) 就目前 BTC/USD 現貨交易來看，BRR 選定的 Bitstamp, GDAX, itBit 及 Kraken 四家比特幣交易所 BTC/USD 的日交易總額，市占率約為全球所有交易所的 40.08%[6]。

(4) Ari Paul, Ian D'Souza (2018)介紹比特幣期貨的文章表示，期貨合約需有一致性

[6] 參考 CryptoCompare 網站，2018/5/24 資料。

的參考價格，參考價格可基於多個交易所或是單一交易所的平均價格，然而參考多個交易所得到的平均交易價格，較易受到異常交易或價格操弄的影響，因此該文章較推崇採用單一交易所的平均價格作為期貨的參考價。

(5) BRR 雖然是參考四家交易所價格所得出的參考價，但 BRR 以每時間區間的成交價格中位數作平均，而採用中位數的優點為，較不易受到離群值和價格暫時大幅波動的影響，因此能緩解上述問題。

2. CBOE BXT 的最終結算價格 – Gemini 的集合競價價格

(1) Gemini 交易所於每日紐約時間 8:00 及 22:00 對 BTC/USD 進行集合競價[7]，CBOE 以每日首輪集合競價之結果作為比特幣期貨的最終結算價格。

(2) 首輪集合競價，於紐約時間 8:00 開始接受集合競價訂單，15:50 至 15:59 每分鐘進行一次集合競價模擬，並公告指示性價格，15:59 開始不允許撤銷 AO(Auction-Only)限價訂單[8]，但仍可接受 AO 委託。15:59:15 至 15:59:45 每 15 秒鐘進行一次集合競價模擬，並公告指示性價格，16:00 完成並公佈本輪集合競價結果，該集合競價結果即為 CBOE 比特幣期貨的最終結算價格。

(3) Gemini 以拍賣的方式有助於提高市場流動性及價格發現功能，有助於讓集合競價結果反映出市場行情。此外，Gemini 受紐約金融服務部門(New York State Department of Financial Services, NYSDFS)的監管，須遵循資本準備金要求、市場透明度等相關法規架構，因此有相當的價格可信度。

(4) CBOE 僅採用 Gemini 的集合競價結果作為最後結算價格，然而 Gemini 交易所

[7] 集合競價成交價格，即為能滿足最大成交量之決定價格，須滿足所有高於決定價格之買方數量與低於決定價格之賣方數量。

[8] AO(Auction-Only)限價訂單，即當市價達到或優於特定價格時立即成交，但僅參與集合競價有效，而不參與逐筆交易的委託。

每日 BTC/USD 交易量僅佔全球所有交易所的 5.45%[9]，其價格代表性則可能成為考量。

三、比特幣期貨交割方式之探討

CBOE 的 BXT 與 CME 的 BTC 期貨合約皆採現金交割，即以最終結算價格來計算未平倉部位的盈虧，收付現金以終了期貨合約。現金交割優點如下，首先，交割成本相對實物交割低，且不會有比特幣現貨不足以交割的問題，再者，未持有現貨者，亦可參與期貨交易，看多或看空比特幣價格，有助於投資人減少儲存比特幣現貨的成本或免於比特幣遺失的風險。

然而，現金交割的缺點為，第一，對於現貨持有者的避險效果較不直接，且較不易發揮提高現貨市場流動性的功能，第二，不易建立具備代表性、公信力、不被操縱性及即時揭露等要素的最終結算價格，若最終結算價格難以公正客觀的反應現貨市場價格，則可能降低期貨價格和現貨價格的關聯性，進而影響避險需求。

2018 年 3 月中旬，英國倫敦交易所 Coinfloor 表示即將推出實物交割的比特幣期貨合約[10]，Coinfloor 的共同創辦人 Mark Lamb 表示，比特幣的流動性提供者希望有實物交割的期貨合約，以讓他們對曝險部位避險。

Coinfloor 表示實物交割的比特幣期貨具下列優點，第一，讓持有比特幣現貨者，例如挖礦者或以比特幣進行勞務商品交換者等，達到較直接的避險效果，第二，可選擇用加密貨幣貨或法定貨幣作為保證金，讓融資方式更具彈性。第三，實物交割以比特幣現貨交割來終結合約，提供較高的訂價透明度，可免於現金交割結算指標不公正客觀或被操縱的風險。另，Coinfloor 之比特幣期貨合約初始保證金比率僅 20%，維持

[9] 參考 CryptoCompare 網站，2018/5/24 資料。

[10] 參考 UK cryptocurrency exchange allows investors to unlock Bitcoin financial potential at scale.

保證金比率僅 15%，相較於 CBOE 和 CME 比特幣期貨要求約 40%保證金來得低。

然而，實物交割會增加維持費用及交割成本支出，可能影響進入期貨市場的意願及妨礙到期時期貨價格和現貨價格的收斂性。

四、比特幣期貨的風險

比特幣期貨為發展初期的新興期貨合約，故與成熟的期貨商品相比，其更易因經濟、政治、市場、監管等方面的變化，衍生出不同之風險。CME 列舉許多比特幣期貨的風險因素[11]，本文將之彙整成「金融風險」、「監管與監督風險」、「網路風險」和「公眾對比特幣興趣乏然之風險」四大面向：

表 3 比特幣期貨的風險

比特幣期貨的風險	**金融風險**：槓桿風險/價格波動性/流動性風險
	監督管理風險：一般管理風險/特定國家監管風險
	網路風險
	公眾對比特幣之認同

(一) 金融風險

1. 槓桿風險

比特幣期貨槓桿特性，因此投資人僅需繳交交易合約價值的一部分作為保證金，即可參與比特幣投資，然而當價格大幅下跌時，投資人可能有大幅損失，或是發生超額損失，亦即所存入的保證金尚不足以彌補損失金額。

2. 價格波動性

比特幣期貨價格波動率受比特幣價格大幅波動影響，且比特幣價格具高波動性。Buy Bitcoin Worldwide[12] 表示比較資產價格的波動率，比特幣價格波動性較黃金及主要貨幣等其他資產高，該網站提供之比特幣波動指數約為 4%左右(2018/5/10)，

[11] 參考 CME 比特幣期貨-風險因素

[12] 參考 Buy Bitcion Worldwide 網站

相較之下黃金價格平均波動率僅約 1.2%，而主要貨幣匯率波動率約 0.5%至 1%。

3. 流動性風險

由於比特幣期貨仍在發展階段，在法規監管、市場接納度等方面的不確定性因素，可能影響比特幣市場供需及市場利用該商品進行商業和投機行為之興趣，進而反映在比特幣期貨市場流動性上。

(二) 監督管理風險

1. 一般監管風險

加密貨幣和區塊鏈仍在發展階段，其監管環境亦不斷在演變。首先，政府或監管干預可能隨著加密貨幣協議的技術發展而改變。再者，有關比特幣的發行、最終結算、轉讓或其他處置及比特幣持有人之權利義務等相關法律規範鮮有先例，該等法規之詮釋與應用仍在精進中，因此為比特幣交易的監管帶來不確定性。

另由於比特幣交易具匿名性、僅有限的參與者身分識別和驗證及缺乏中央監督機構等特性，因此在反洗錢暨反資助恐怖主義方面的規範可能受到較多的要求。而未來若頒佈新的比特幣相關法律規範，亦可能會影響到比特幣和比特幣期貨的價格與流動性，甚至是清除其全部價值。

2. 特定國家監管風險

全球對比特幣的監管並不一致，主因比特幣的法律分類因司法管轄區而有所差異，例如將比特幣定位為貨幣、商品、虛擬貨幣、虛擬商品或其他財產等。目前比特幣在部分國家不受監管貨監管寬鬆，但部分國家則有限制或禁止比特幣相關的活動，如獲取、持有、出售或使用比特幣可能為違法行為，這將對比特幣和比特幣期貨價格與流動性造成不利影響。

(三) 網路風險

交易所的網路安全失效與破壞、駭客侵入、濫用資產或敏感資訊、破壞資料或造成

操作擾亂為目的未經授權地存取數位系統等網路攻擊、詐欺或政府監管等原因，可能構成操作和資訊安全風險，進而導致比特幣交易所被關閉，投資人可能因此遭遇部分或全部帳戶的餘額損失，亦可能扭曲比特幣的價格與流動性並衝擊總體比特幣交易所市場的信心，拖慢大眾對比特幣的接納。

(四) 公眾對比特幣的認同

比特幣本身不具使用價值(如不動產)、沒有被動收益(如股票、債券)及尚未獲得所有國家政府公信力給予的價值背書等因素，造成比特幣內在價值受到質疑，比特幣尚未普遍被認可或當作一種價值單位或貨幣，另由於比特幣為新興資產且由於其高度波動性、監管環境尚未發展完善、對比特幣的法律定位等眾多因素產生的風險，公眾對比特幣的認同亦隨特定事件而產生變化，這將影響比特幣和比特幣期貨的價格與流動性。

五、比特幣期貨對比特幣現貨價格之影響

2018 年 5 月舊金山聯邦儲備銀行(FED)提出一份關於「期貨交易如何影響比特幣價格」13之研究報告，文中表示 2017 年 12 月中旬，比特幣價格快速下跌與比特幣期貨的推出可能有關連。

由圖 9 可見 2009 年比特幣發行後至 2017 年 2 月 22 日，比特幣價格維持在$1,150 以下，在接下來的十個月比特幣價格快速上升，直至 2017 年 12 月 17 日達到$19,511 之歷史高位，後比特幣價格開始下跌，惟此期間 S&P500 價格無劇烈變動，顯示比特幣價格非由整體市場波動造成。

舊金山 FED 認為比特幣價格下跌之時點與 CME 發行比特比期貨(2017 年 12 月 18

[13] Galina Hale, Arvind Krishnamurthy, Marianna Kudlyak, and Patrick Shultz (2018), "How Futures Trading Changed Bitcoin Prices"

日)之日期相近，非純屬巧合，而是因為期貨改變了投資人之交易行為，進而使比特幣價格滑落。

圖 9　比特幣價格和 S&P500 股價指數

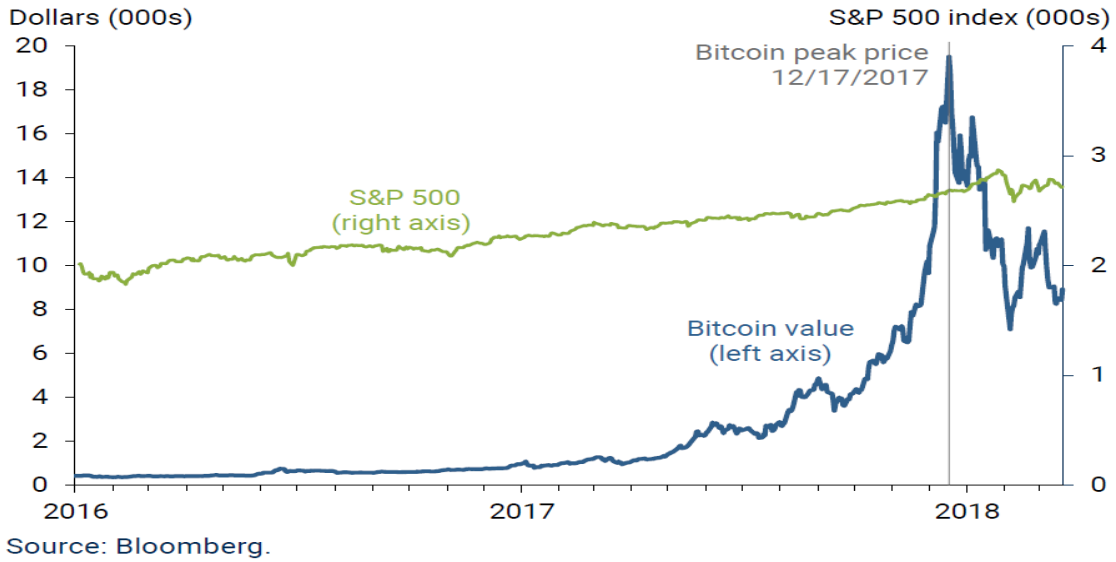
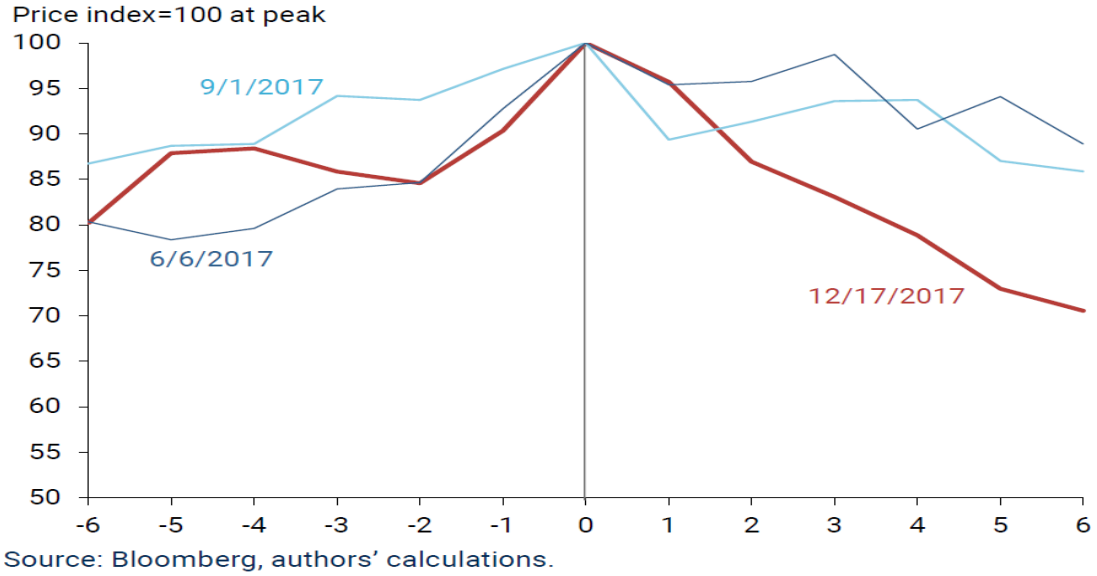


圖 10 為 2017 年比特幣價格三次大幅下跌之比較，橫軸表示價格高點前後的天數，而橫軸為零(價格指數為 100)即價格最高之日期，圖中顯示比特幣價格下跌幅度最大的一次為 2017 年 12 月 17 日達到高位後，亦為 CME 發行比特幣期貨之前一日。

圖 10　2017 年比特幣價格跌幅之比較



比特幣期貨之發行使投機者得以看空比特幣，不像以往只能看多比特幣價格，投資人僅買入有助於推升價格，期貨發行後市場不再僅有看多比特幣價格的樂觀投機者，亦有對比特幣價格悲觀的投機者，投資人交易行為之改變導致比特幣價格下跌。

這現象如同 Fostel 和 John Geanakoplos (2012)對房市的研究中指出，樂觀投機者在允許投機者放空的金融創新商品推出前，推升了資產價格，但可放空商品推出後，悲觀投機者的交易行為造成資產價格下跌，例如房貸證券化及將債券等級分類(tranching)等金融創新，吸引對房市樂觀的投資者進入房市，帶動其成長，然而信用違約交換[14](credit default swaps, CDS)的推出，讓對房市展望悲觀的投資人亦得參與房貸市場，降低資產價格，最終造成房市泡沫。

舊金山 FED 解釋，可將比特幣之需求分為兩種，源自於作為購買商品和服務的支付之交易目的需求，或因預期比特幣價格上升而持有比特幣之投機需求，在比特幣期貨推出前，因交易目的或投機目的持有比特幣者皆看多比特幣價格，然而比特幣期貨之發行，允許投資人看空比特幣價格，終結了單邊投機需求(one-sided speculative demand)，此將對比特幣現貨價格造成向下之壓力，例如，預期比特幣價格下跌的悲觀投機者，可訂定一個未來交割價格低於目前現貨價格的期貨合約，若未來現貨價格真的下跌，則悲觀投機者可從中獲利。但隨著期貨的交割價格下降，亦對現貨價格造成向下的壓力。此外，新的投資機會將造成比特幣現貨市場需求下降，進而拖累比特幣價格。以上兩個原因造成比特幣價格下跌，悲觀投機者因此更進一步的放空，更增加價格向下的壓力。

另外，CBOE 發行比特幣期貨時(2017 年 12 月 10 日)，比特比價格尚未開始下跌，而是在 CME 發行比特幣期貨時(2017 年 12 月 18 日)才開始從高點滑落，舊金山 FED

[14] 信用違約交換(CDS)亦即契約買方支付風險貼水，並將標的資產的信用風險移轉給契約賣方，因此當標的資產之信用品質惡化時，契約賣方就要依照契約提供補償予契約買方。

認為主要是因為在 CME 加入比特幣期貨市場後，比特幣期貨每日交易量才大幅上升之緣故。

舊金山 FED 認為比特幣的基本價格(fundamental price)是難以預測的，但當樂觀和悲觀的投機需求取得平衡後，比特幣價格仍將由市場交易目的需求之供需決定，當交易目的需求成長高於(低於)供給，預期比特幣價格將上揚(下跌)，影響比特幣供需之因素分述如下：

比特幣的供給由市場現有的比特幣和挖礦者新增的比特幣所組成，而挖礦者的供給，取決於其挖礦之成本和收益比較，根據 Hayes(2015)估計比特幣挖礦成本為$250，近似於當時比特幣現貨之價格，因此隨著比特幣價格及挖礦成本上揚，採礦者比特幣供給難以大幅增加。

比特幣之交易目的需求取決於以下三個因素，第一，替代品的多寡，當不同的加密貨幣被廣泛當作交易媒介時，比特幣的需求將因此而下降。第二，若傳統金融機構能接受以比特幣作為擔保品，則比特幣的需求將增加。第三，官方認定及法規能接受比特幣作為支付工具，監管限制或交易費可能下降，進而增加比特幣之需求。

參考文獻

1. Nakamoto Satoshi(2009), “Bitcoin: A Peer-to-Peer Electronic Cash System.”
2. Michele D'Aliessi(2016), “How Does the Blockchain Work?”
3. Jakobsson, Markus; Juels, Ari. Proofs of Work and Bread Pudding Protocols. Communications and Multimedia Security (Kluwer Academic Publishers). 1999: 258–272.
4. Crypto facilities(2017) , “CME CF Bitcoin Reference Rate(BRR) Methodology Guide”
5. Nicole Moran, Yesim Richardson and Robert Letson(2017), “Bitcoin Futures: A Closer Look At CME’s Contract Design”
6. Ari Paul, Ian D’Souza(2018), “An Introduction to Bitcoin and Cboe XBT Bitcoin Futures”
7. Galina Hale, Arvind Krishnamurthy, Marianna Kudlyak, and Patrick Shultz, Federal Reserve Bank of San Francisco (2018), “How Futures Trading Changed Bitcoin Prices”
8. Ana Fostel and John Geanakoplos (2012) , American Economic Journal: Macroeconomics 2012, 4(1): 190–225, “Tranching, CDS, and Asset Prices: How Financial Innovation Can Cause Bubbles and Crashes”
9. CME(2017), “Managing Bitcoin Futures Expiration: Rolling Forward”
10. CBOE(2017), “The Beginner’s Guide to Bitcoin Futures”