I656496

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I656496 B**

(45)公告日： 中華民國 108 (2019) 年 04 月 11 日

(21)申請案號：107128610 (22)申請日： 中華民國 107 (2018) 年 08 月 16 日

(51)Int. Cl.： *G06Q40/04 (2012.01)* *G06Q20/38 (2012.01)*
G06Q20/40 (2012.01) *G06F17/30 (2006.01)*

(71)申請人：楊少銘 (中華民國) YANG, SHAO MING (TW)
臺北市中正區南海路 1 號 13 樓

(72)發明人：楊少銘 YANG, SHAO-MING (TW)

(56)參考文獻：

US 2011/0153484A1
US 2016/0321751A1
US 2017/0091863A1
US 2017/0366357A1
WO 2017/131929A1

審查人員：黃炳燻

申請專利範圍項數：15 項 圖式數：1 共 29 頁

(54)名稱

弱中心化基金交易系統及其方法

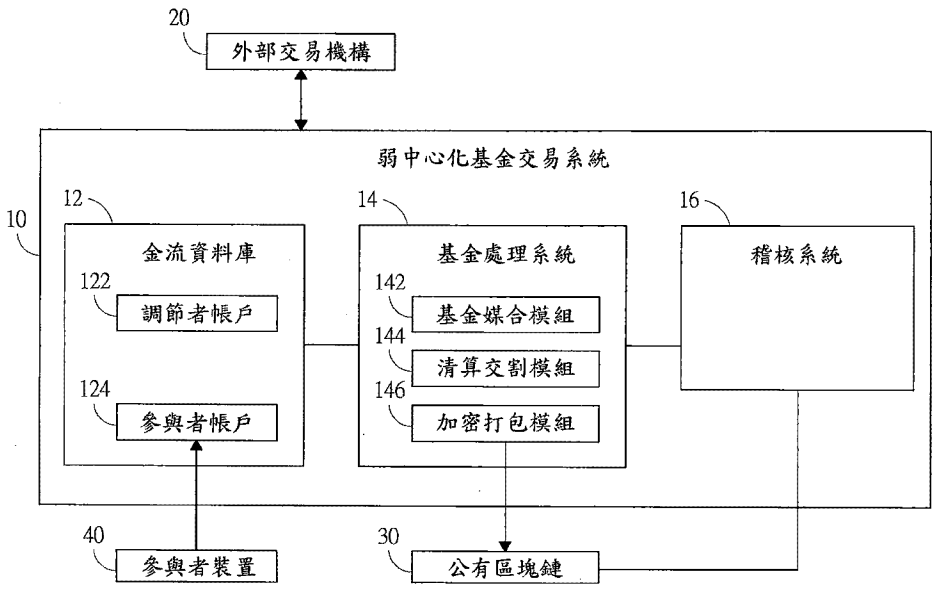
LEAST DECENTRALIZED FUND TRADING SYSTEM AND METHOD THEREOF

(57)摘要

一種弱中心化基金交易系統，包括金流資料庫及基金處理系統。基金處理系統包括基金媒合模組、清算交割模組及加密打包模組。基金媒合模組媒合配對金流資料庫中各參與者帳戶之交易條件指令成買賣搓合資訊。清算交割模組對買賣搓合資訊進行清算程序與交割程序，以產生交易紀錄。加密打包模組將交易紀錄對應之交易收據或結算餘額紀錄到帳本資訊，並對帳本資訊進行加密程序以取得總專屬加密值。總專屬加密值將被紀錄至公有區塊鏈中第 j 個區塊之數位標籤值，且數位標籤值等於總專屬加密值。此外，一種弱中心化基金交易方法亦被提出。

A least decentralized fund trading system is provided. The least decentralized fund trading system includes a money pool database and a fund transaction processing system. The fund transaction processing system includes a fund matching module, a clearing and settlement module and an encrypted packaging module. A plurality of trading condition instruction of counterparty in the money pool database is matched into the trading information by the fund matching module. The trading information is performed a clearing process and a settlement process by the both modules and is generated a plurality of transaction record information. The encrypted packaging module records a receipt transaction and a receipt balance according to the transaction record information into ledger information, and the ledger information is encrypted to obtain a total exclusive encryption value. The total exclusive encryption value is recorded into digit tag value of the j-th block in the public blockchain, and the digit tag value is equal to total exclusive encryption value. In addition, a least decentralized fund trading method is provided.

指定代表圖：



【圖 1】

符號簡單說明：

10・・・弱中心化基金交易系統

12・・・金流資料庫

122・・・調節者帳戶

124・・・參與者帳戶

14・・・基金處理系統

142・・・基金媒合模組

144・・・清算交割模組

146・・・加密打包模組

16・・・稽核系統

20・・・外部交易機構

30・・・公有區塊鏈

40・・・參與者裝置

108年1月18日 修正本

【發明說明書】

【中文發明名稱】弱中心化基金交易系統及其方法

【英文發明名稱】LEAST DECENTRALIZED FUND TRADING SYSTEM AND METHOD THEREOF

【技術領域】

【0001】 本發明是有關於一種弱中心化基金交易系統及其方法。

【先前技術】

【0002】 金融市場的資金供需在自由經濟的發展中扮演著極為重要的角色，而金融市場中具有相當多種之金融商品(financial instrument)，如基金、債券、股市、期貨、選擇權商品等等，可供參與者利用自身資金選擇並進行相關交易行為。

【0003】 共同基金(以下簡稱：基金，Mutual Fund)，是由專業的證券投資信託公司(以下簡稱：基金公司)以發行受益憑證的方式，募集投資人的資金，並將募集而來的資金交由保管機構保管，再委託專業基金經理人進行投資管理運用。當投資有損益時，投資人將依照其投資比例分享其利益。投資基金與一般直接投資，如：外匯、股票等商品，最大不一樣之處，在於它非由投資人直接將資金投入特定金融商品(如：公司股票、債券)，而是藉由買、賣基金公司所發行的受益憑證，也就是說，投資人透過受益憑證，間接投資市場，按該基金所委託的專業經理人，主動式管理運用，換算基金淨值形成每日損益，並由基金公司每日對外公布基金淨值。共同基金的成立，主要是有鑒於投資大眾的小額投資金額並無法形成有效分散風險的投資組合，故將小錢聚集為一筆大錢，來協助投資大眾分散風險，是一種共聚資金、共擔風險、共享投資利潤的投資方式，最大的特色是投資組合的風險分散。

【0004】 基金交易是由單一機構(如銀行、清算所)去執行並持有帳目系

統，本質上為一封閉系統且為中心化架構，然而基於此中心化架構的基金交易存在至少以下問題：一、單一機構(如銀行、清算所)被入侵時，將導致整個交易平台隨之癱瘓，甚至交易記錄可能被惡意篡改，參與者無法確保其交易紀錄是否為公正公開；二、由於各家機構個別執行自訂的交易過程的交易邏輯的執行過程不一致，資料格式不一致，客戶要再次確認交易的執行明細進行資料對帳流程較長，因要每筆交易與全部資料重新核對，依資料量恐需數天時間，使得交易稽核效率低；三、基金贖回時，因其作業冗長，想就該款項再其他申購，需待5-7工作天方能進行；四、基金申購時，基金公司或各基金銷售通路等中介者對於每筆交易均收取手續費，其費用有達3%，且該單位數入帳亦有需3個工作日之久；五、因基金買賣機制與效率的關係，對於申購、贖回都被限制得符合最低額度以上才可進行，投資人想買不足一個基金單位或僅要贖回不足一個基金單位(或例如只想賣出等值新台幣1元的基金單位)，現行機制窒礙難行。

【0005】　綜上所述，可知現有技術基於此中心化架構所進行之基金交易存在至少上述問題，因此實有必要提出改進的技術手段，故如何改良並能提供一種『弱中心化基金交易系統及其方法』來避免上述所遭遇到的問題，係業界所亟待解決之課題。

【發明內容】

【0006】　本發明提供一種弱中心化基金交易系統及其方法，在不改變外部傳統基金交易體系的運作下，透過本發明之弱中心化基金交易系統及其方法，創建內部區塊鏈基金交易生態系，進行新型態的基金交易的模式。稱弱中心化，是相對傳統基金交易採100%中心化機制而言。蓋中心化體制，在交易確認、隱私保護、金融監理等方面較佳；去中心化機制，在公眾信任、陌生交易、降低錯誤、資料透明等面向優勢，兩者各有優劣。然而，金融監理及法令規範有其特殊性，現實中，「完全」去中心化確實有無法滿足社會需要之處，如：某甲

受強制執行，需強制扣其資產，在「去中心化」世界中，甲若不同意簽章，任何人均無法強行之。這時唯有「中心化」機制能解決，以符法治及監理之需。再則，交易過程，並非所有事情皆需所有人共識，也不是任何東西都記上區塊鏈才是最好的。綜上原因，本發明採兩者之長，互補其短的混合(Hybrid)模式，整體設計以「中心化」運作居輔，多以「去中心化」機制為主。

【0007】 本發明的一實施例提出一種弱中心化基金交易系統，包括一金流資料庫以及一基金處理系統。金流資料庫包括一調節者帳戶以及複數個參與者帳戶，其中各參與者帳戶係能提出一交易條件指令，各交易條件指令包含一申購需求或一賣出需求，申購需求及賣出需求分別包含至少一基金種類與相對應之交易單位數量。基金處理系統連接於金流資料庫，基金處理系統包括一基金媒合模組、一清算交割模組以及一加密打包模組。基金媒合模組媒合配對各交易條件指令，於第N個時間單位內產生至少一買賣搓合資訊，其中該基金媒合模組將能相互沖抵的申購需求與賣出需求中配對成買賣搓合資訊，所述能相互沖抵係指申購需求與賣出需求分別為同一基金種類且對應基金種類之相同交易單位數量。而該基金媒合模組對無法相互沖抵的申購需求與賣出需求之一差額，由調節者帳戶對該些差額反向沖抵補足作業成買賣搓合資訊，其中，該些差額係指不同之基金種類或同一基金種類但該同一基金種類之交易單位數量不同而買賣相互沖抵後有餘額，其中N大於或等於1。清算交割模組接收至少一買賣搓合資訊，清算交割模組用以對各買賣搓合資訊，依據各交易條件指令與各參與者帳戶進行一清算程序與一交割程序，此二程序合稱結算。結算完成後，將產生至少一買賣搓合資訊之一交易紀錄，其中各交易紀錄包含一交易收據與一結算餘額。加密打包模組用以接收各交易紀錄對應之交易收據或結算餘額，依據各交易紀錄之時序，分別將各交易紀錄對應之交易收據或結算餘額紀錄到至少一帳本資訊，加密打包模組對複數個帳本資訊進行一加密程序以取得一總專屬

加密值。基金處理系統連接公有區塊鏈，公有區塊鏈係以一區塊鏈技術使複數個區塊鏈接，且公有區塊鏈接收加密打包模組傳輸之總專屬加密值，總專屬加密值將被紀錄至公有區塊鏈中第j個區塊之一數位標籤值，其中j大於1，且數位標籤值等於總專屬加密值。

【0008】 在一實施例中，上述調節者帳戶係與一外部交易機構進行交易以取得對應該些差額之基金種類及對應基金種類之交易單位數量，以施行對該些差額之反向沖抵補足作業。

【0009】 在一實施例中，上述清算程序係為清算交割模組清算各買賣搓合資訊之對應基金種類與交易單位數量及對應之金額；交割程序係為各參與者帳戶交割各買賣搓合資訊之基金種類與對應基金種類之交易單位數量與對應之金額，其中清算交割模組依據各買賣搓合資訊，使各交易條件指令之參與者帳戶之間移轉至少一基金種類與對應基金種類之交易單位數量以取得交易收據，並傳輸各交易收據至對應交易條件指令之參與者帳戶，且依據各交易收據中至少一基金種類之金額與對應基金種類之交易單位數量取得對應之結算餘額。

【0010】 在一實施例中，上述加密程序係為依據至少一帳本資訊之數目，加密打包模組分別對各帳本資訊加密成一專屬加密值，專屬加密值僅對應帳本資訊內之各交易紀錄對應之交易收據或結算餘額，加密打包模組將繼續對至少二個以上之各專屬加密值再次加密，依此循環加密直到專屬加密值的數目等於1，取得總專屬加密值。

【0011】 在一實施例中，上述弱中心化基金交易系統更包括一稽核系統，稽核系統連接基金處理系統以及公有區塊鏈，稽核系統係對基金處理系統之至少一帳本資訊中之交易收據或結算餘額進行驗證稽查。

【0012】 在一實施例中，上述稽核系統係依據公有區塊鏈中數位標籤值，以對總專屬加密值進行驗證。

【0013】 在一實施例中，上述稽核系統係供各參與者帳戶相對應之專屬加密值與其循環加密過程中關聯之專屬加密值，進行驗證稽查。

【0014】 本發明的一實施例提出一種弱中心化基金交易方法，包括以下步驟：複數個參與者帳戶分別提出一交易條件指令，各交易條件指令包含一申購需求或一賣出需求，申購需求及賣出需求分別包含至少一基金種類與相對應之交易單位數量；藉由一基金媒合模組媒合配對各交易條件指令，於第N個時間單位內產生至少一買賣搓合資訊，其中N大於或等於1；藉由一清算交割模組用以對各買賣搓合資訊，依據各交易條件指令與各參與者帳戶進行一清算程序與一交割程序，此二程序合稱結算。結算完成後，將產生相對至少一買賣搓合資訊之一交易紀錄，其中各交易紀錄包含一交易收據與一結算餘額；依據各交易紀錄之時序，藉由一加密打包模組分別將各交易紀錄對應之交易收據或結算餘額紀錄到至少一帳本資訊；藉由加密打包模組對複數個帳本資訊進行一加密程序以取得一總專屬加密值；以及公有區塊鏈接收加密打包模組傳輸之總專屬加密值，總專屬加密值將被紀錄至公有區塊鏈中第j個區塊之一數位標籤值，其中j大於1，且數位標籤值等於總專屬加密值。

【0015】 在一實施例中，上述媒合配對各交易條件指令的步驟中，包括以下步驟：基金媒合模組將能相互沖抵的申購需求與賣出需求配對成買賣搓合資訊，所述能相互沖抵係指申購需求與賣出需求分別為同一基金種類且對應基金種類之相同交易單位數量；基金媒合模組對無法相互沖抵的申購需求與賣出需求之一差額，由調節者帳戶對該些差額反向沖抵補足作業成買賣搓合資訊，該些差額係指不同之基金種類或同一之基金種類但該同一基金種類之交易單位數量不同而買賣相互沖抵後有餘額。

【0016】 在一實施例中，上述反向沖抵補足作業的步驟中，包括以下步驟：調節者帳戶係與一外部交易機構進行交易以取得對應該些差額之基金種類

及對應基金種類之交易單位數量，以施行對該些差額之反向沖抵補足作業。

【0017】 在一實施例中，上述產生相對至少一買賣搓合資訊之該交易紀錄的步驟中，包括以下步驟：清算交割模組依據各買賣搓合資訊，使各交易條件指令之參與者帳戶之間移轉至少一基金種類與對應基金種類之交易單位數量以取得交易收據；清算交割模組傳輸各交易收據至對應交易條件指令之參與者帳戶；以及清算交割模組依據各交易收據中至少一基金種類之金額與對應基金種類之交易單位數量取得對應之結算餘額。

【0018】 在一實施例中，上述進行清算程序與交割程序的步驟中，包括以下步驟：清算程序係為清算交割模組清算各買賣搓合資訊之對應基金種類與該交易單位數量及對應之金額；以及交割程序係為各參與者帳戶交割各買賣搓合資訊之基金種類與對應基金種類之交易單位數量與對應之金額。

【0019】 在一實施例中，上述藉由加密打包模組對複數個帳本資訊進行加密程序以取得總專屬加密值的步驟中，包括以下步驟：依據至少一帳本資訊之數目，加密打包模組分別對各帳本資訊加密成一專屬加密值，其中專屬加密值僅對應帳本資訊內之各交易紀錄對應之交易收據或結算餘額；以及加密打包模組將繼續對至少二個以上之專屬加密值再次加密，依此循環加密直到專屬加密值的數目等於1，取得總專屬加密值。

【0020】 在一實施例中，上述弱中心化基金交易方法，更包括以下步驟：藉由一稽核系統對至少一帳本資訊中之交易收據或結算餘額進行驗證稽查；以及稽核系統係供各參與者帳戶相對應之專屬加密值與其循環加密過程中關聯之專屬加密值，進行驗證稽查。

【0021】 在一實施例中，上述藉由加密打包模組對複數個帳本資訊進行加密程序以取得總專屬加密值的步驟中，包括以下步驟：稽核系統係依據公有區塊鏈中數位標籤值，以對總專屬加密值進行驗證。

【0022】 基於上述，本發明提供一種弱中心化基金交易系統及其方法，提供一門檻低的環境，不需合格中介者介入，進而省去中介者對於每筆交易所收取手續費或管理費之費用，參與者帳戶能在本發明之弱中心化基金交易系統上進行基金交易以物易物交換，任何交易過程透過本發明之分帳管理、紀錄與加密過程使得帳本資訊具有完整性(Integrity)、加密性(Encrypted)、不可篡改性(Incorruptible)、不可否認性(Non-repudiation)與可追溯性(Traceability)，做到公信驗證及交易資料的持續正確性，進一步可透過公有區塊鏈進行分散式儲存，達到對本發明弱中心化基金交易系統及其方法之公眾監督與參與者監督，進而提升參與者對本發明之弱中心化基金交易系統及其方法建立起交易的安全性、公正且易於證明真實性。

【0023】 為讓本發明能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明如下。

【圖式簡單說明】

【0024】

圖1為本發明之弱中心化基金交易系統一實施例的示意圖

【實施方式】

【0025】 以下結合附圖和實施例，對本發明的具體實施方式作進一步描述。以下實施例僅用於更加清楚地說明本發明的技術方案，而不能以此限制本發明的保護範圍。

【0026】 本發明之弱中心化基金交易系統及其方法應用在執行符合雙邊預設條件可自動執行之電腦代碼協定的網路中，例如本發明之清算交割模組以及加密打包模組所執行的程序形成的一傳輸協定(Protocol)，以及該程序與公有區塊鏈雙向通訊，用以實現簿記帳務由傳輸協定(Protocol)轉移到公有區塊鏈，或由公有區塊鏈回查傳輸協定(Protocol)間的橋接流通，達到數據雙向流通及把

關的作用。符合雙邊預設條件可自動執行之電腦代碼協定係一種以訊息化方式傳播、驗證或執行合同的計算機協議，且依據既定的條件及傳輸的資訊來驅動執行指令的電腦程式，在一實施例中，符合雙邊預設條件可自動執行之電腦代碼協定包括但不限於係透過程式語言(例如：Solidity、Serpent、LLL、EtherScript、Sidechain)等等來撰寫，其可包含各種不同的事件(Event)、函數(Function)或參數狀態等等，因此，該協定允許在沒有第三方的情況下進行可信交易，除了對接收到的訊息進行回應，並可以接收與儲存訊息，也可以向外發送訊息，換言之，符合雙邊預設條件可自動執行之電腦代碼協定係一種運行在可複製、共享帳本上的電腦程式，可以接收、處理、儲存及發送訊息。

【0027】 再者，區塊鏈技術是一個去中心化交易系統的概念性驗證，屬於一種加密電子記錄方法，本發明之弱中心化基金交易系統及其方法應用在執行符合雙邊預設條件可自動執行之電腦代碼協定的網路，使得以物易物交換的過程可直接由一方發起，並自動觸發(Trigger)給另一方執行交易。在前述過程中，不需要再通過任何中介機構或第三方機構。區塊鏈技術包括採用如Hashcash演算法來進行算法演算，讓區塊鏈中的各節點有機會參與驗證，達到公正性。因此，區塊鏈技術具有以下之技術特色：P2P(Peer to Peer)網路架構與非對稱性加密技術。P2P(Peer to Peer)網路架構是區塊鏈技術連接各節點的方式，其與傳統的中心化網路架構並不相同。在P2P網路架構中，每個節點的地位相同，也都具有相同的網路計算權力，各節點之間透過協定共享計算資源、軟體或訊息；非對稱性加密技術，係利用公鑰及私鑰對傳輸的訊息進行加密與解密，其中公鑰可以公開發行，用於發送方傳輸加密訊息之用；私鑰用於接收方解密接收到的加密訊息，區塊鏈技術利用此非對稱性加密技術維持個節點間的信任關係。

【0028】 圖1為本發明之弱中心化基金交易系統一實施例的示意圖。請參閱圖1。本發明之弱中心化基金交易系統10得以使用電腦網頁(Web)或利用

APP(Application；以下簡稱APP)應用程式來呈現於各類型之作業系統(包括但不限於Windows、Android或IOS等)之計算機設備，計算機設備可為伺服器、電腦主機、筆記型電腦、平板電腦、智慧型手機或具同等無限傳輸介面等等，本發明不對上述計算機設備加以限制。

【0029】 在本實施例中，弱中心化基金交易系統10係可透過網路耦接至外部交易機構20以及每一個參與者裝置40(圖1僅例示一個參與者裝置40)。本實施例之弱中心化基金交易系統10包括一金流資料庫12、一基金處理系統14以及一稽核系統16。金流資料庫12係可透過硬體(例如積體電路)、軟體(例如處理器執行之程式指令)或其組合來實現通訊連線與邏輯判斷之功能，金流資料庫12包括一調節者帳戶122以及複數個參與者帳戶124。

【0030】 在本實施例中，調節者帳戶122係可為該弱中心化基金交易系統10本身之帳戶，或由自然人或法人機構擔任公正第三者。本實施例能藉由調節者帳戶122與外部交易機構20進行至少一基金下單交易，取得登記之基金受益憑證。所述基金包含基金種類與對應基金種類之交易單位數量。外部交易機構20係包括但不限為一金融機構，其例如包含一保管銀行、一託管銀行(Custodian bank)、一基金公司(Fund House)、一集中保管結算所(Depository & Clearing Corporation)及前述組合等。需說明的是，本實施例之弱中心化基金交易系統10的調節者帳戶122與前述外部交易機構20(例如：保管銀行、託管銀行、基金公司與集中保管結算所)對外所執行之交易指令、開戶、交割、對帳、結算等作業流程是習知的投資交易流程，且其並非本發明之重點，因此不多做贅述。

【0031】 在本實施例中，參與者可透過網站(Web)或利用APP(Application；以下簡稱APP)應用程式作為參與者裝置40，參與者例如為自然人或法人機構。每一個利用參與者裝置40的參與者需先向本實施例之弱中心化基金交易系統10線上開戶，完成開戶手續，成為參與者帳戶124後，方可入金

下單。參與者帳戶124能在本實施例之弱中心化基金交易系統10上提出一交易條件指令，各交易條件指令包含一申購需求或一賣出需求，即投資者透過參與者帳戶124能自行提出基金申購或賣出於本實施例之弱中心化基金交易系統10，等待第N個時間單位，連同該第N個時間單位所有的參與者帳戶124提出之交易條件指令進行基金交易，其中N大於或等於1，時間單位例如為一天，在其他實施例中，時間單位例如為12小時，其端視實際需求而可調整時間單位。需說明的是，在此所述基金交易，係所有參與者帳戶124會將其持有基金之權利移轉至弱中心化基金交易系統10，由弱中心化基金交易系統10去進行一個區塊鏈技術的交換或權利移轉之記帳，或登記在一個保管銀行，保管銀行授權給弱中心化基金交易系統10，換言之，參與者帳戶124係由持有基金種類與其交易單位數量的參與者轉換成弱中心化基金交易系統10內之數位記錄持有者，其中該數位記錄對應參與者帳戶124應有的實質持有的基金種類與其交易單位數量，而本發明之弱中心化基金交易系統10有基金權利名義上之所有權或以任何形式被授予代理執行基金權利，以下作進一步說明。

【0032】 在本實施例中，基金處理系統14連接於金流資料庫12，基金處理系統14係可透過硬體(例如積體電路)、軟體(例如處理器執行之程式指令)或其組合來實現通訊連線與邏輯判斷之功能。基金處理系統14包括一基金媒合模組142、一清算交割模組144以及一加密打包模組146。基金媒合模組142媒合配對各交易條件指令，於第N個時間單位內產生至少一買賣搓合資訊，其中N大於或等於1，時間單位例如為一天，在其他實施例中，時間單位例如為12小時，其端視實際需求而可調整時間單位。基金媒合模組142將能相互沖抵的申購需求與賣出需求配對成買賣搓合資訊，所述能相互沖抵係指申購需求與賣出需求分別為同一基金種類且對應基金種類之相同交易單位數量。另外，基金媒合模組142對無法相互沖抵的申購需求與賣出需求之一差額，由調節者帳戶122對該些差額反

向沖抵補足作業成買賣搓合資訊，該些差額係指不同之基金種類或同一之基金種類但該同一基金種類之交易單位數量不同而買賣相互沖抵後有餘額，其中調節者帳戶122係與外部交易機構20進行交易以取得對應該些差額之基金種類及對應基金種類之交易單位數量，以施行對該些差額之反向沖抵補足作業。

【0033】 舉例而言，某一參與者帳戶124提出申購需求之交易條件指令，基金媒合模組142依據交易條件指令，搜尋其他參與者帳戶124是否有提出賣出需求之交易條件指令。若該申購需求之交易條件指令的基金種類與賣出需求之交易條件指令的基金種類相同，且對應基金種類之交易單位數量也相同，基金媒合模組142將上述能相互沖抵的申購需求與賣出需求配對成一買賣搓合資訊；若該申購需求之交易條件指令的基金種類與賣出需求之交易條件指令的基金種類並不相同，基金媒合模組142將前述申購需求中無法完成配對的基金種類，由調節者帳戶122與外部交易機構20進行下單交易相對應基金種類之基金及對應基金種類之交易單位數量，取得登記之基金受益憑證後，調節者帳戶122不直接交易名義實質登記之基金受益憑證，而係利用該基金受益憑證衍生的實質受益權，對基金種類及對應基金種類之交易單位數量反向沖抵補足作業成買賣搓合資訊；又例如，若該申購需求之交易條件指令的基金種類與賣出需求之交易條件指令的基金種類相同，但對應基金種類之交易單位數量並不相同，基金媒合模組142將前述申購需求中無法完成配對的對應基金種類之交易單位數量，由調節者帳戶122與外部交易機構20進行下單交易相對應基金種類之交易單位數量，取得登記之基金受益憑證後，調節者帳戶122不直接交易名義實質登記之基金受益憑證，而係利用該基金受益憑證衍生的實質受益權，將對應基金種類之交易單位數量反向沖抵補足作業成買賣搓合資訊。需說明的是，上述係以參與者帳戶124提出申購需求之交易條件指令為例，而參與者帳戶124提出賣出需求之交易條件指令亦類同，在此不重複贅述。

【0034】 在本實施例中，清算交割模組144接收至少一買賣搓合資訊，清算交割模組144用以對各買賣搓合資訊，依據各交易條件指令與各參與者帳戶124進行一清算程序與一交割程序，此清算程序與交割程序合稱結算。結算完成後將產生相對至少一買賣搓合資訊之一交易紀錄，其中各交易紀錄包含一交易收據與一結算餘額。詳細而言，清算程序係為清算交割模組124清算各買賣搓合資訊之對應基金種類與交易單位數量及對應之金額。交割程序係為各參與者帳戶124交割各買賣搓合資訊之基金種類與對應基金種類之交易單位數量與對應之金額。清算交割模組144依據各買賣搓合資訊，使各交易條件指令之參與者帳戶124之間移轉至少一基金種類與對應基金種類之交易單位數量以取得交易收據，並傳輸各交易收據至對應交易條件指令之參與者帳戶124，且依據各交易收據中至少一基金種類之金額與對應基金種類之交易單位數量取得對應之結算餘額。

【0035】 舉例而言，某一個參與者帳戶124提出之申購需求之交易條件指令為購買100個交易單位數量的黃金基金，於前述基金媒合模組142搜尋能相互沖抵該申購需求的賣出需求之另一個參與者帳戶124，並配對成一買賣搓合資訊，清算交割模組144依據該買賣搓合資訊，在另一參與者帳戶124扣除100個交易單位數量的黃金基金，並增加其等值對應之金額，並顯示另一個參與者帳戶124之黃金基金之剩餘的交易單位數量，以取得對應另一參與者帳戶124之交易收據或結算餘額。而某一個參與者帳戶124扣除100個交易單位數量的黃金基金之等值對應之金額，並增加並顯示某一參與者帳戶124之黃金基金之交易單位數量，以取得對應某一個參與者帳戶124之交易收據或結算餘額。

【0036】 需說明的是，在本實施例中，清算交割模組144接收至少一買賣搓合資訊的過程中，得加密亦得不對買賣搓合資訊進行加密。在本實施例中，清算交割模組144進行清算程序與交割程序，不分別對清算程序與交割程序的交

易紀錄中交易收據或結算餘額進行加密。在其他實施例中，亦可分別於清算程序與交割程序的交易紀錄中交易收據或結算餘額進行加密。前述加密方式包括但不限於非對稱加密，採取的演算法包括但不限於不可逆的加密演算法。

【0037】 在本實施例中，前述於第N個時間單位內產生至少一買賣搓合資訊，並經由清算交割模組144產生特定數量的交易紀錄，加密打包模組146用以接收各交易紀錄對應之交易收據或結算餘額，依據各交易紀錄之時序，分別將各交易紀錄對應之交易收據或結算餘額紀錄到至少一帳本資訊，為每一受託參與者帳戶124數位記錄其應有持有基金種類與對應基金種類的交易數量單位於至少一帳本資訊。接著，加密打包模組146對複數個帳本資訊進行一加密程序以取得一總專屬加密值。詳細而言，加密程序包括以下步驟。加密打包模組146依據至少一帳本資訊之數目，加密打包模組146分別對各帳本資訊加密成一專屬加密值，專屬加密值僅對應帳本資訊內之各交易紀錄對應之交易收據或結算餘額，換言之，每個帳本資訊有對應之專屬加密值，若有參與者帳戶124或其他帳戶篡改某一帳本資訊內之任一交易紀錄或其對應之交易收據或結算餘額，則專屬加密值會無法對應篡改後某一帳本資訊內之交易紀錄。接著，加密打包模組146將各專屬加密值視為一莫克樹(Merkle Tree)的葉節點(Leaf Node)，加密打包模組146將繼續對至少二個以上之各專屬加密值再次加密，依此循環加密直到專屬加密值的數目等於1，取得總專屬加密值，換言之，加密打包模組146使用一演算法從葉節點依序進行每個階層葉節點之演算加密，直到剩下最後一個，得到根節點的總專屬加密值，前述加密方式包括但不限於非對稱加密，採取的演算法包括但不限於不可逆的加密演算法。若有參與者帳戶124或其他帳戶篡改某一帳本資訊內之任一交易紀錄或對應之交易收據或結算餘額，則專屬加密值會跟隨變動，進而此變動總專屬加密值，使得總專屬加密值無法對應到原本之總專屬加密值，此舉透過本發明之分帳管理、紀錄與加密過程使得帳本資訊具有

完整性(Integrity)、加密性(Encrypted)、不可篡改性(Incorruptible)、不可否認性(Non-repudiation)與可追溯性(Traceability)，做到公信驗證及交易資料的持續正確性。

【0038】 在一實施例中，加密打包模組146會持續接收上述各交易紀錄對應之交易收據，並將每筆交易紀錄對應之交易收據透過上述莫克樹(Merkle Tree)儲存起來產生一交易收據樹(Receipt Transaction Tree)，並將總專屬加密值傳輸至前述符合雙邊預設條件可自動執行之電腦代碼協定的網路，以利後續參與者帳戶124進行驗證稽查。同理，加密打包模組146會持續接收上述各交易紀錄對應之結算餘額，透過上述莫克樹(Merkle Tree)儲存起來產生一結算餘額樹(Receipt Balance Tree)，當收到每筆交易紀錄對應之交易收據的同時，依據每筆交易收據動態更新結算餘額樹，並將總專屬加密值傳輸制前述符合雙邊預設條件可自動執行之電腦代碼協定的網路，以利後續參與者帳戶124進行驗證稽查。

【0039】 在本實施例中，稽核系統16連接基金處理系統14以及公有區塊鏈30，稽核系統16係對基金處理系統14之至少一帳本資訊中之交易收據或結算餘額進行驗證稽查，做到公信驗證及交易資料的持續正確性，降低徇私或錯帳而導致參與者之損失。此外，各參與者帳戶124提出交易條件指令被接收與完成後，會取得交易收據，其對於自己的交易條件指令對應之交易紀錄、交易收據均有自行稽核權限，並且，參與者帳戶124在調閱與自己帳務相關之專屬加密值時，也要同步調閱其他參與者帳戶124的相關加密資料，故該位參與者帳戶124作驗證稽核，等同幫其他參與者帳戶124也進行了稽核。一旦任何葉節點資料有被篡改，推導出的總專屬加密值就會不一致，換言之，除稽核系統16係供各參與者帳戶124相對應之專屬加密值與其循環加密過程中關聯之專屬加密值，進行驗證稽查，透過不可逆且高度困難被篡改的總專屬加密值驗算結果一致，代表驗證結果之莫克樹(Merkle Tree)的資料正確無誤外，本發明開放參與者帳戶124

自行發動稽核，一參與者帳戶124發動稽核，亦等同幫其他參與者帳戶124稽核。此透過專屬加密值的稽核，如同以科學方法辨識個人身分一般，不必辨識其長相、聲音或驗DNA，僅比對其指紋即可確認是何人是同一邏輯。本發明將此概念運用在稽核系統16上，除強化資料驗證的公示性與正確性，並巧妙地保護每一參與者帳戶124的個人資料資與隱私權。

【0040】 在本實施例中，基金處理系統14連接公有區塊鏈30，公有區塊鏈30係以一區塊鏈技術使複數個區塊（Block）鏈接。公有區塊鏈30每個區塊中，包括但不限於區塊頭（Block Header）、前一區塊的加密雜湊(Hash)值等資訊。區塊頭會包含從前一個區塊中的區塊頭所計算出來前一個數位標籤值與該區塊的數位標籤值以及一隨機值(Nonce)，每個區塊經演算加密後被加上一個時間戳(Timestamp)並發布出去，這麼做可讓每一個區塊與前一個區塊資料產生連結，並能確保區塊序列及歷史紀錄的正確性，這是形成區塊「鏈」最關鍵連結。公有區塊鏈30接收加密打包模組146傳輸之總專屬加密值，總專屬加密值將被紀錄至公有區塊鏈30中第j個區塊之一數位標籤值，其中j大於1，且數位標籤值依區塊鏈特性公開且高度困難被篡改，並恆久等於該總專屬加密值。在本實施例中，稽核系統16係依據公有區塊鏈30中數位標籤值，以對總專屬加密值進行驗證，但前述加密打包模組146僅接收加密打包模組146傳輸之總專屬加密值，而所有具體的交易紀錄均在本發明之弱中心化基金交易系統10中，因此，任何人無法藉由僅有公有區塊鏈30被記錄之總專屬加密值去窺得投資交易雙方與其具體交易內容，而若任何人在前述傳輸協定(Protocol)中進行資料篡改，則得到的總專屬加密值則無法與公有區塊鏈30之數位標籤值一致，故本發明可透過公有區塊鏈進行分散式儲存，在可公示稽核的特色下，達到對本發明之弱中心化基金交易系統10之公眾監督與參與者監督之效，不但保護參與者個人資料與交易隱私，又提升參與者對本發明之弱中心化基金交易系統10建立起交易的安全性、

公正且易於證明真實性。

【0041】 在本實施例中，弱中心化基金交易方法係可基於圖1之弱中心化基金交易系統10執行以下步驟。首先，參與者利用參與者裝置40需先向本實施例之弱中心化基金交易系統10線上開戶，完成開戶手續，成為參與者帳戶124後，方可入金下單。接著，每個參與者帳戶124在本實施例之弱中心化基金交易系統10上分別提出一交易條件指令，各交易條件指令包含一申購需求或一賣出需求，即參與者透過參與者帳戶124能自行提出基金申購或賣出於本實施例之弱中心化基金交易系統10。接著，藉由基金媒合模組142媒合配對各交易條件指令，於第N個時間單位內產生至少一買賣搓合資訊，其中N大於或等於1，時間單位例如為一天，在其他實施例中，時間單位例如為12小時，其端視實際需求而可調整時間單位。細部而言，基金媒合模組142將能相互沖抵的申購需求與賣出需求配對成買賣搓合資訊，其中所述能相互沖抵係指申購需求與賣出需求分別為同一基金種類且對應基金種類之相同交易單位數量。另一方面，基金媒合模組142對無法相互沖抵的申購需求與賣出需求之一差額，由調節者帳戶122對該些差額反向沖抵補足作業成買賣搓合資訊，該些差額係指不同之基金種類或同一之基金種類但該同一基金種類之交易單位數量不同而買賣相互沖抵後有餘額，其中調節者帳戶122係與外部交易機構20進行交易以取得對應該些差額之基金種類及對應基金種類之交易單位數量，以施行對該些差額之反向沖抵補足作業。

【0042】 接著，清算交割模組144接收至少一買賣搓合資訊，在本實施例中，清算交割模組144接收至少一買賣搓合資訊的過程中，得加密亦得不對買賣搓合資訊進行加密。清算交割模組144用以對各買賣搓合資訊，依據各交易條件指令與各參與者帳戶124進行一清算程序與一交割程序，此清算程序與交割程序合稱結算。結算完成後將產生相對至少一買賣搓合資訊之一交易紀錄，其中各

交易紀錄包含一交易收據與一結算餘額。在本實施例中，清算交割模組144進行清算程序與交割程序，不分別對清算程序與交割程序的交易紀錄中交易收據或結算餘額進行加密。在其他實施例中，亦可分別於先清算程序與交割程序的交易紀錄中交易收據或結算餘額進行加密。詳細而言，清算程序係為清算交割模組124清算各買賣搓合資訊之對應基金種類與交易單位數量及對應之金額。交割程序係為各參與者帳戶124交割各買賣搓合資訊之基金種類與對應基金種類之交易單位數量與對應之金額。清算交割模組144依據各買賣搓合資訊，使各交易條件指令之參與者帳戶124之間移轉至少一基金種類與對應基金種類之交易單位數量以取得交易收據，並傳輸各交易收據至對應交易條件指令之參與者帳戶124，且依據各交易收據中至少一基金種類之金額與對應基金種類之交易單位數量取得對應之結算餘額。需說明的是，前述加密方式包括但不限於非對稱加密，採取的演算法包括但不限於不可逆的加密演算法。

【0043】 接著，加密打包模組146用以接收各交易紀錄對應之交易收據或結算餘額，依據各交易紀錄之時序，藉由加密打包模組146分別將各交易紀錄對應之交易收據或結算餘額紀錄到至少一帳本資訊。接著，加密打包模組146對複數個帳本資訊進行一加密程序以取得一總專屬加密值。詳細而言，加密程序包括以下步驟。加密打包模組146依據至少一帳本資訊之數目，分別對各帳本資訊加密成一專屬加密值，專屬加密值僅對應帳本資訊內之各交易紀錄對應之交易收據或結算餘額，換言之，每個帳本資訊有對應之專屬加密值，若有參與者帳戶124或其他帳戶篡改某一帳本資訊內之任一交易紀錄或對應之交易收據或結算餘額，則專屬加密值會無法對應篡改後某一帳本資訊內之交易紀錄。接著，加密打包模組146將各專屬加密值視為一莫克樹(Merkle Tree)的葉節點(Leaf Node)，加密打包模組146將繼續對至少二個以上之各專屬加密值再次加密，依此循環加密直到專屬加密值的數目等於1，取得總專屬加密值，換言之，加密打

包模組146使用一演算法從葉節點依序進行每個階層葉節點之演算加密，直到剩下最後一個，得到根節點的總專屬加密值，前述加密方式包括但不限於非對稱加密，採取的演算法包括但不限於不可逆的加密演算法。若有參與者帳戶124或其他帳戶篡改某一帳本資訊內之任一交易紀錄或對應之交易收據或結算餘額，則專屬加密值會跟隨變動，進而此變動總專屬加密值，使得總專屬加密值無法對應到原本之總專屬加密值，此舉透過本發明之分帳管理、紀錄與加密過程使得帳本資訊具有完整性(Integrity)、加密性(Encrypted)、不可篡改性(Incorruptible)、不可否認性(Non-repudiation)與可追溯性(Traceability)，做到公信驗證及交易資料的持續正確性。

【0044】 在一實施例中，加密打包模組146會持續接收上述各交易紀錄對應之交易收據，並將每筆交易紀錄對應之交易收據透過上述莫克樹(Merkle Tree)儲存起來產生一交易收據樹(Receipt Transaction Tree)，並將總專屬加密值傳輸至前述符合雙邊預設條件可自動執行之電腦代碼協定的網路，以利後續參與者帳戶124進行驗證稽查；同理，加密打包模組146會持續接收上述各交易紀錄對應之結算餘額，透過上述莫克樹(Merkle Tree)儲存起來產生一結算餘額樹(Receipt Balance Tree)，當收到每筆交易紀錄對應之交易收據的同時，依據每筆交易收據動態更新結算餘額樹，並將總專屬加密值傳輸制前述符合雙邊預設條件可自動執行之電腦代碼協定的網路，以利後續參與者帳戶124進行驗證稽查。

【0045】 接著，藉由稽核系統16對基金處理系統14之至少一帳本資訊中之交易收據或結算餘額進行驗證稽查，做到公信驗證及交易資料的持續正確性，降低徇私或錯帳而導致參與者之損失。在一實施例中，稽核系統16係供各參與者帳戶124相對應之專屬加密值與其循環加密過程中關聯之專屬加密值，進行驗證稽查，透過不可逆且高度困難被篡改的總專屬加密值驗算結果一致，代表驗證結果之莫克樹(Merkle Tree)的資料正確無誤。詳細而言，各參與者帳戶124提

出交易條件指令被接收與完成後，會取得交易收據，其對於自己的交易條件指令對應之交易紀錄、交易收據均有自行稽核權限，並且，參與者帳戶124在調閱與自己帳務相關之專屬加密值時，也要同步調閱其他參與者帳戶124的相關加密資料，故該位參與者帳戶124作驗證稽核，等同幫其他參與者帳戶124也進行了稽核。一旦任何葉節點資料有被篡改，推導出的總專屬加密值就會不一致。

【0046】 接著，公有區塊鏈30接收加密打包模組146傳輸之總專屬加密值，總專屬加密值將被紀錄至公有區塊鏈30中第j個區塊之一數位標籤值，其中j大於1，且數位標籤值依區塊鏈特性公開且高度困難被篡改，並恆久等於該總專屬加密值。在本實施例中，稽核系統16係依據公有區塊鏈30中數位標籤值，以對總專屬加密值進行驗證，但前述加密打包模組146僅接收加密打包模組146傳輸之總專屬加密值，而所有具體的交易紀錄均在本發明之弱中心化基金交易系統10中，因此，任何人無法藉由僅有公有區塊鏈30被記錄之總專屬加密值去窺得投資交易雙方與其具體交易內容，而若任何人在前述傳輸協定(Protocol)中進行資料篡改，則得到的總專屬加密值則無法與公有區塊鏈30之數位標籤值一致，故本發明可透過公有區塊鏈進行分散式儲存，在可公示稽核的特色下，達到對本發明之弱中心化基金交易方法之公眾監督與參與者監督之效，不但保護參與者個資與交易隱私，又提升公眾對本發明之弱中心化基金交易系統10及其方法建立起交易的安全性、公正且易於證明真實性。

【0047】 綜上所述，本發明提供一種弱中心化基金交易系統及其方法，提供一門檻低的環境，不需合格中介者介入，進而省去中介者對於每筆交易所收取手續費或管理費之費用，參與者帳戶能在本發明之弱中心化基金交易系統上進行基金交易以物易物交換，任何交易過程透過本發明之分帳管理、紀錄與加密過程使得帳本資訊具有完整性(Integrity)、加密性(Encrypted)、不可篡改性(Incorruptible)、不可否認性(Non-repudiation)與可追溯性(Traceability)，做到公信

驗證及交易資料的持續正確性，進一步可透過公有區塊鏈進行分散式儲存，達到對本發明之弱中心化基金交易系統及其方法之公眾監督與投資者監督，進而提升公眾對本發明之弱中心化基金交易系統及其方法建立起交易的安全性、公正且易於證明真實性。

【0048】 雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，故本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【符號說明】

【0049】

10	弱中心化基金交易系統
12	金流資料庫
122	調節者帳戶
124	參與者帳戶
14	基金處理系統
142	基金媒合模組
144	清算交割模組
146	加密打包模組
16	稽核系統
20	外部交易機構
30	公有區塊鏈
40	參與者裝置

I656496

108年1月18日 修正本

【發明摘要】

公告本

【中文發明名稱】弱中心化基金交易系統及其方法

【英文發明名稱】LEAST DECENTRALIZED FUND TRADING SYSTEM AND METHOD THEREOF

【中文】

一種弱中心化基金交易系統，包括金流資料庫及基金處理系統。基金處理系統包括基金媒合模組、清算交割模組及加密打包模組。基金媒合模組媒合配對金流資料庫中各參與者帳戶之交易條件指令成買賣搓合資訊。清算交割模組對買賣搓合資訊進行清算程序與交割程序，以產生交易紀錄。加密打包模組將交易紀錄對應之交易收據或結算餘額紀錄到帳本資訊，並對帳本資訊進行加密程序以取得總專屬加密值。總專屬加密值將被紀錄至公有區塊鏈中第j個區塊之數位標籤值，且數位標籤值等於總專屬加密值。此外，一種弱中心化基金交易方法亦被提出。

【英文】

A least decentralized fund trading system is provided. The least decentralized fund trading system includes a money pool database and a fund transaction processing system. The fund transaction processing system includes a fund matching module, a clearing and settlement module and an encrypted packaging module. A plurality of trading condition instruction of counterparty in the money pool database is matched into the trading information by the fund matching module. The trading information is performed a clearing process and a settlement process by the both modules and is generated a plurality of transaction record information. The encrypted packaging module records a receipt transaction and a receipt balance according to the transaction record information into ledger information, and the ledger information is

encrypted to obtain a total exclusive encryption value. The total exclusive encryption value is recorded into digit tag value of the j-th block in the public blockchain, and the digit tag value is equal to total exclusive encryption value. In addition, a least decentralized fund trading method is provided.

【指定代表圖】圖1

【代表圖之符號簡單說明】

10	弱中心化基金交易系統
12	金流資料庫
122	調節者帳戶
124	參與者帳戶
14	基金處理系統
142	基金媒合模組
144	清算交割模組
146	加密打包模組
16	稽核系統
20	外部交易機構
30	公有區塊鏈
40	參與者裝置

108年1月18日 修正本

【發明申請專利範圍】

【第1項】 一種弱中心化基金交易系統，包括：

一金流資料庫，包括一調節者帳戶以及複數個參與者帳戶，其中各該參與者帳戶係能提出一交易條件指令，各該交易條件指令包含一申購需求或一賣出需求，該申購需求及該賣出需求分別包含至少一基金種類與相對應之交易單位數量；以及

一基金處理系統，連接於該金流資料庫，該基金處理系統包括一基金媒合模組、一清算交割模組以及一加密打包模組，其中：

該基金媒合模組媒合配對各該交易條件指令，於第N個時間單位內產生至少一買賣搓合資訊，其中該基金媒合模組將能相互沖抵的該申購需求與該賣出需求配對成該買賣搓合資訊，所述能相互沖抵係指該申購需求與該賣出需求分別為同一該基金種類且對應該基金種類之相同該交易單位數量；而該基金媒合模組對無法相互沖抵的該申購需求與該賣出需求之一差額，由該調節者帳戶對該些差額反向沖抵補足作業成該買賣搓合資訊，該些差額係指不同之該基金種類或同一該基金種類但該基金種類之該交易單位數量不同而買賣相互沖抵後有餘額，其中N大於或等於1；

該清算交割模組接收該至少一買賣搓合資訊，該清算交割模組用以對各該買賣搓合資訊，依據各該交易條件指令與各該參與者帳戶進行一清算程序與一交割程序，以產生相對該至少一買賣搓合資訊之一交易紀錄，其中各該交易紀錄包含一交易收據與一結算餘額；及

加密打包模組用以接收各該交易紀錄對應之該交易收據或該結算餘額，依據各該交易紀錄之時序，分別將各該交易紀錄對應之該交易收據或該結算餘額紀錄到至少一帳本資訊，該加密打包模組對該至少一帳本資訊進行一加密程序以取得一總專屬加密值；

該基金處理系統連接一公有區塊鏈，該公有區塊鏈係以一區塊鏈技術使複數個區塊鏈接，且該公有區塊鏈接收該加密打包模組傳輸之該總專屬加密值，該總專屬加密值將被紀錄至該公有區塊鏈中第j個區塊之一數位標籤值，其中j大於1，且該數位標籤值等於該總專屬加密值。

【第2項】 如申請專利範圍第1項所述之弱中心化基金交易系統，其中該調節者帳戶係與一外部交易機構進行交易以取得對應該些差額之該基金種類及對應該基金種類之該交易單位數量，以施行對該些差額之反向沖抵補足作業。

【第3項】 如申請專利範圍第1項所述之弱中心化基金交易系統，其中該清算程序係為該清算交割模組清算各該買賣搓合資訊之對應該基金種類與該交易單位數量及對應之金額；該交割程序係為各該參與者帳戶交割各該買賣搓合資訊之該基金種類與對應該基金種類之該交易單位數量與對應之該金額，其中該清算交割模組依據各該買賣搓合資訊，使各該交易條件指令之該參與者帳戶之間移轉該至少一基金種類與對應該基金種類之該交易單位數量以取得該交易收據，並傳輸各該交易收據至對應該交易條件指令之該參與者帳戶，且依據各該交易收據中該至少一基金種類之金額與對應該基金種類之該交易單位數量取得對應之該結算餘額。

【第4項】 如申請專利範圍第1項所述之弱中心化基金交易系統，其中該加密程序係為依據該至少一帳本資訊之數目，該加密打包模組分別對各該帳本資訊加密成一專屬加密值，該專屬加密值僅對應該帳本資訊內之各該交易紀錄對應之該交易收據或該結算餘額，該加密打包模組將繼續對該至少二個以上之各該專屬加密值再次加密，依此循環加密直到該專屬加密值的數目等於1，取得該總專屬加密值。

【第5項】 如申請專利範圍第4項所述之弱中心化基金交易系統，更包括：

一稽核系統，連接該基金處理系統以及該公有區塊鏈，該稽核系統係對該基金處理系統之該至少一帳本資訊中之該交易收據或該結算餘額進行驗證稽查。

【第6項】 如申請專利範圍第5項所述之弱中心化基金交易系統，其中該稽核系統係依據該公有區塊鏈中該數位標籤值，以對該總專屬加密值進行驗證。

【第7項】 如申請專利範圍第5項所述之弱中心化基金交易系統，其中該稽核系統係供各該參與者帳戶相對應之該專屬加密值與該專屬加密值循環加密過程中關聯之該專屬加密值，進行驗證稽查。

【第8項】 一種弱中心化基金交易方法，其運用如第1項至第7項所述之弱中心化基金交易系統，該弱中心化基金交易方法包括以下步驟：

各該參與者帳戶分別提出該交易條件指令，各該交易條件指令包含該申購需求或該賣出需求，該申購需求及該賣出需求分別包含該至少一基金種類與相對應之該交易單位數量；

藉由該基金媒合模組媒合配對各該交易條件指令，於第N個時間單位內產生該至少一買賣搓合資訊，其中N大於或等於1；

藉由該清算交割模組用以對各該買賣搓合資訊，依據各該交易條件指令與各該參與者帳戶進行該清算程序與該交割程序，以產生相對該至少一買賣搓合資訊之該交易紀錄，其中各該交易紀錄包含該交易收據與該結算餘額；

依據各該交易紀錄之時序，藉由該加密打包模組分別將各該交易紀錄對應之該交易收據或該結算餘額紀錄到該至少一帳本資訊；

藉由該加密打包模組對該至少一帳本資訊進行該加密程序以取得該總專屬加密值；以及

該公有區塊鏈接收該加密打包模組傳輸之該總專屬加密值，該總專屬加密值將被紀錄至該公有區塊鏈中第j個區塊之該數位標籤值，其中j大於1，且該數位標籤值等於該總專屬加密值。

【第9項】 如申請專利範圍第8項所述之弱中心化基金交易方法，其中所述媒合配對各該交易條件指令的步驟中，包括以下步驟：

該基金媒合模組將能相互沖抵的該申購需求與該賣出需求配對成該買賣搓合資訊，其中所述能相互沖抵係指該申購需求與該賣出需求分別為同一該基金種類且對應該基金種類之相同該交易單位數量；以及

該基金媒合模組對無法相互沖抵的該申購需求與該賣出需求之該些差額，由該調節者帳戶對該些差額反向沖抵補足作業成該買賣搓合資訊，該些差額係指不同之該基金種類或同一之該基金種類但該基金種類之該交易單位數量不同而買賣相互沖抵後有餘額。

【第10項】如申請專利範圍第9項所述之弱中心化基金交易方法，其中所述反向沖抵補足作業的步驟中，包括以下步驟：

該調節者帳戶係與該外部交易機構進行交易以取得對應該些差額之該基金種類及對應該基金種類之該交易單位數量，以施行對該些差額之反向沖抵補足作業。

【第11項】如申請專利範圍第8項所述之弱中心化基金交易方法，其中所述產生相對該至少一買賣搓合資訊之該交易紀錄的步驟中，包括以下步驟：

該清算交割模組依據各該買賣搓合資訊，使各該交易條件指令之該參與者帳戶之間移轉該至少一基金種類與對應該基金種類之該交易單位數量以取得該交易收據；

該清算交割模組傳輸各該交易收據至對應該交易條件指令之該參與者帳戶；以及

該清算交割模組依據各該交易收據中該至少一基金種類之金額與對應該基金種類之該交易單位數量取得對應之該結算餘額。

【第12項】如申請專利範圍第8項所述之弱中心化基金交易方法，其中所述進行該清算程序與該交割程序的步驟中，包括以下步驟：

該清算程序係為該清算交割模組清算各該買賣搓合資訊之對應該基金種類與該交易單位數量及對應之金額；以及

該交割程序係為各該參與者帳戶交割各該買賣搓合資訊之該基金種類與對應該基金種類之該交易單位數量與對應之該金額。

【第13項】如申請專利範圍第8項所述之弱中心化基金交易方法，其中所述藉由該加密打包模組對該至少一帳本資訊進行該加密程序以取得該總專屬加密值的步驟中，包括以下步驟：

依據該至少一帳本資訊之數目，該加密打包模組分別對各該帳本資訊加密成一專屬加密值，其中該專屬加密值僅對應該帳本資訊內之各該交易紀錄對應之該交易收據或該結算餘額；以及

該加密打包模組將繼續對該至少二個以上之專屬加密值再次加密，依此循環加密直到該專屬加密值的數目等於1，取得該總專屬加密值。

【第14項】如申請專利範圍第8項所述之弱中心化基金交易方法，更包括以下步驟：

藉由該稽核系統對該至少一帳本資訊中之該交易收據或該結算餘額進行驗證稽查；以及

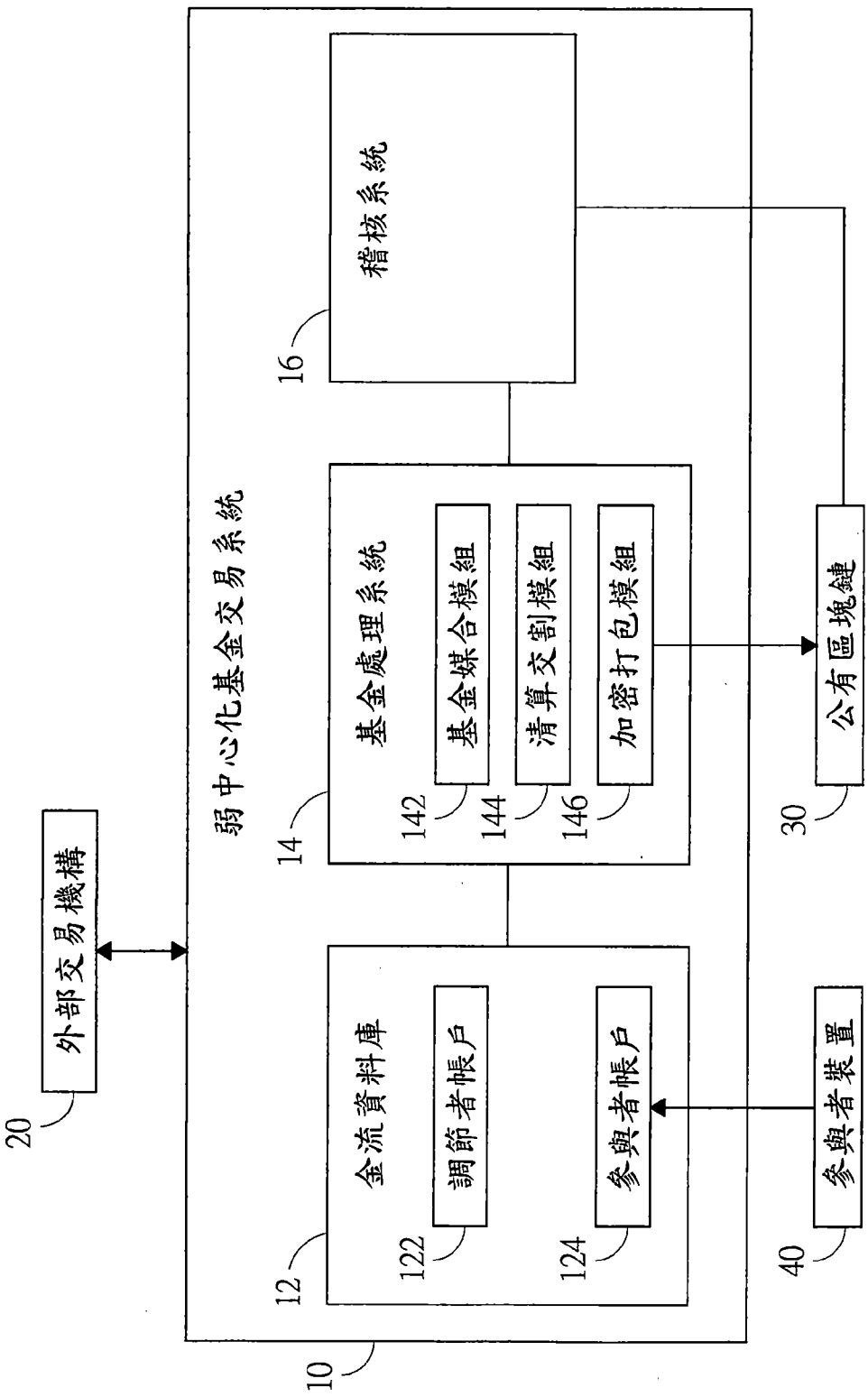
該稽核系統係供各該參與者帳戶相對應之該專屬加密值與該專屬加密值循環加密過程中關聯之該專屬加密值，進行驗證稽查。

【第15項】如申請專利範圍第8項所述之弱中心化基金交易方法，其中所述藉由該加密打包模組對該至少一帳本資訊進行該加密程序以取得該總專屬加密值的步驟中，包括以下步驟：

該稽核系統係依據該公有區塊鏈中該數位標籤值，以對該總專屬加密值進行驗證。

【發明圖式】

108年1月29日 修正頁



【圖 1】