DeBi .com

人工智能數字資產交易中心

白皮書

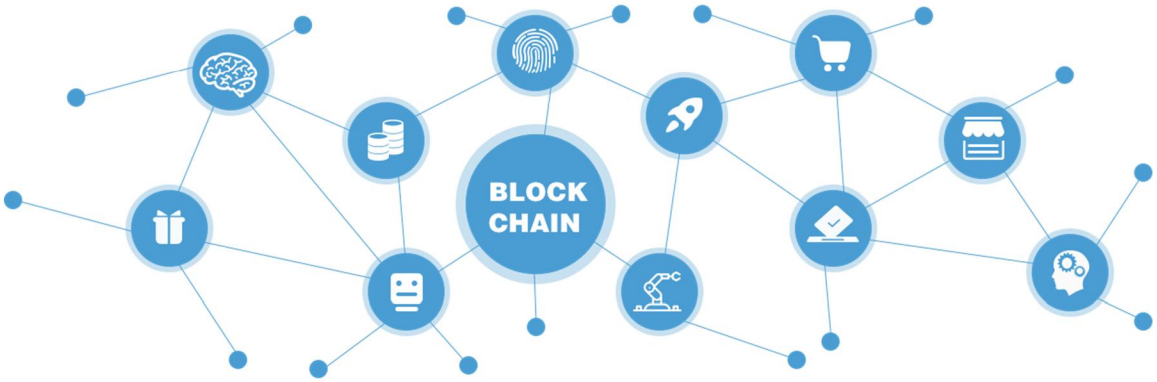
V1.1

目錄

前言

世界正走向去中心化時代

區塊鏈作為 BTC 和 ETH 為代表的底層技術，已經發展成為一種新的金融體系，數據即資產，未來基于區塊鏈的新金融會有一個明顯趨勢，即資產代幣化（Tokenization），資產代幣化的目標之一就是低成本、全球化、全天候的高流動性，而流動性則主要通過數字交易所得以實現。



去中心化

現階段市面上的數字交易所以中心化為主，其集中式的數據管理，安全問題尤為凸顯，雖然去中心化數字資產交易中心在安全方面有保障，但其交易效率低一直是得不到市場認可的主要原因。

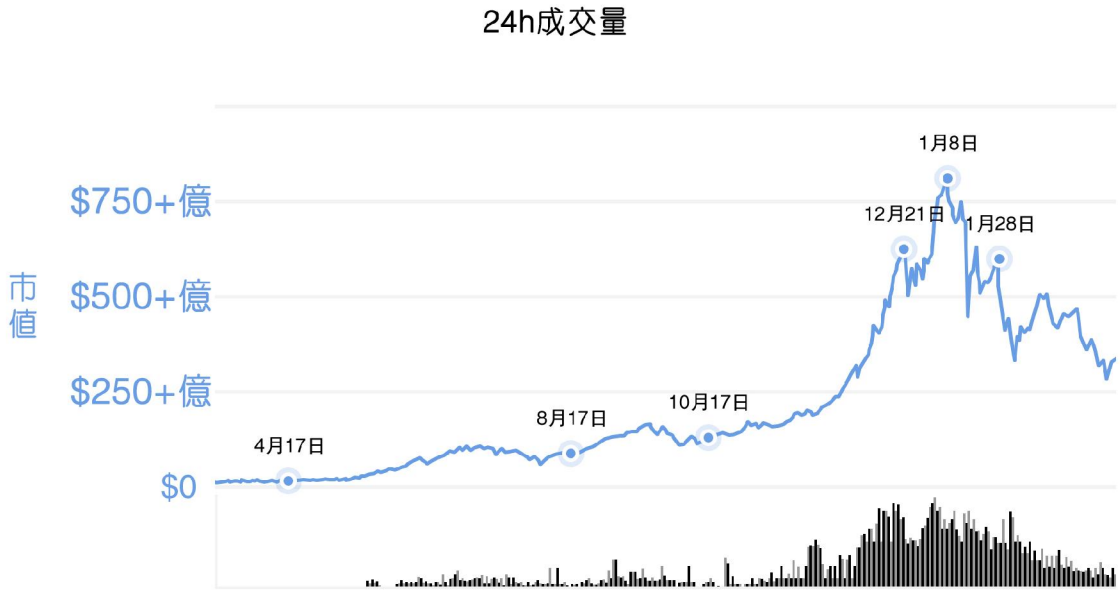
在這樣的一個大環境下，DeBi 推出數字資產交易中心人工智能化的概念，同時利用了中心化與去中心化的優勢，將鏈上與鏈下相結合，把重要的數據，比如清算成功的交易放在鏈上，而非必要的，比如交易的撮合放在鏈下處理。這樣做的好處是可以解決主鏈性能低下、網絡擁堵的狀況，從而降低交易成本和提高用戶的使用體驗。不僅具有去中心化數據安全和隱私特性，更有中心化數字交易所快速且便利的體驗。

項目背景

現狀分析

2017 年，比特幣價格上漲了 1100%，12 月份單個比特幣的價格一度高達 20000 美元，全球加密貨幣日交易額也隨着大幅度的提升，2018 年 1 月 5 日全球加密貨幣日交易額達 700 億美元（約 4430.65 億元），根據數據分析，自去年 11 月以來，全球加密貨幣日交易額平均在 250 億美元以上（約 1585.25 億元）。

在未來，當現實資產代幣化之后，會有更大的市場因運而生，從現在市場就知道想象空間，6000 億美元的加密貨幣市場、5 萬億美元的全球外匯市場、75 萬億美元的全球股票市場、120 萬億美元的全球債券市場。

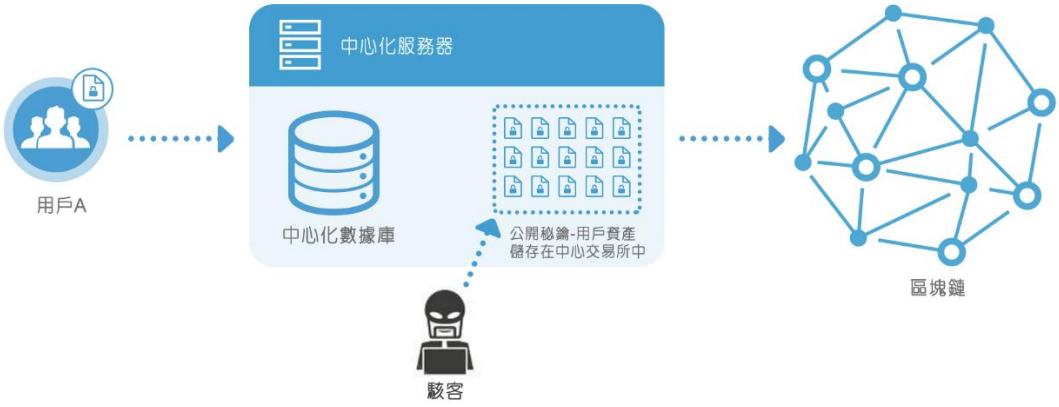


全球數字貨幣總市值走勢圖

市場痛點

中心化數字交易所

隨着全球加密貨幣關注度的提高，脆弱性也隨之而來，現階段承接如此龐大交易量的中心化交易所首當其冲成為黑客攻擊的重點對象，特別是韓國的交易平臺更是黑客的熱名單。前稱為 Yapizon 的 Youbit 在 2017 年 4 月份損失了 3816 個比特幣。黑客攻擊時其價值為 500 萬美元，現在市值超 5000 萬美元。更糟糕的是，Youbit 在去年 12 月再度遭受重創，迫使其在損失 17%的資金后申請破產。此外，在 7 月份，有消息傳出韓國最大的交易所 Bithumb 的 3 萬個用戶賬戶遭到數據泄露，導致數十億韓元被盜，按目前的市場價格計算，客戶至少損失 1000 萬美元。



中心化數字交易所

雖然中心化數字交易所在技術實現上是有傳統成熟解決方案，即使面對海量大幵發實時交易，依舊可以給用戶提供很好的服務體驗，也帶來了足夠的交易深度，提供了充分的流動性和便利性。但是中心化數字交易所的劣勢也是顯而易見：

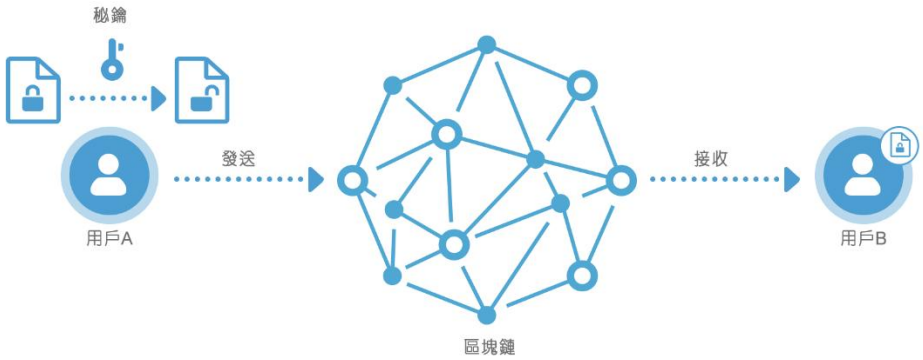
- 不安全：由于中心化的特點，資產控制和系統管理過于集中，中心化交易所是用戶資金的看護人，具有法律責任。73%的中心化交易所管理着用戶的私鑰，只有23%是由用戶自己掌握私鑰。平臺每天負責數以十億計的交易量，而其中大多數存儲在服務器上，這對黑客來說極具吸引力。

- 缺乏流動性：數額特別巨大的訂單很難匹配，即使是最繁榮的活躍期，對比傳統市場而言，交易量也不高。
- 分裂的市場：把全球的流動性分成幾個主要的市場，交易量上沒有明確的市場領先者，這會加劇用戶資產碎片化，不利于市場有序發展。
- 用戶面臨着高級別的風險：潛在的操作問題、市場操縱、硬件故障、等待時間過長，以及其它因為交易量巨大所引發的各種潛在問題。
- 缺乏信任和透明性：交易進程和實際成本不透明，包含高昂的交易費用，通常是遠遠大于宣布的費用，同時在流量高峰時不當的運營導致交易所的高延遲。
- 缺乏教育的用戶：市場中充斥着純粹的投機者，沒有意識到交易加密代幣的安全方法。

解決思路

去中心化數字交易所

以目前市場來說，雖然中心化數字交易所是市場主流，然而其弊端明顯，促進了眾多去中心化數字交易所的誕生，如 0xProject、AirSwap、IDEX (Aurora Labs)等。去中心化數字交易所模式簡單，它只需要承擔主要的資產托管、撮合交易及資產清算，而不需要像中心化數字交易所需要承擔非交易的功能像賬戶體系、KYC、法幣兌換等。用戶在區塊鏈上的賬戶公鑰就是身份，不需向交易所注冊個人信息，因此就不存在個人信息安全問題也不需要 KYC。



去中心化數字交易所

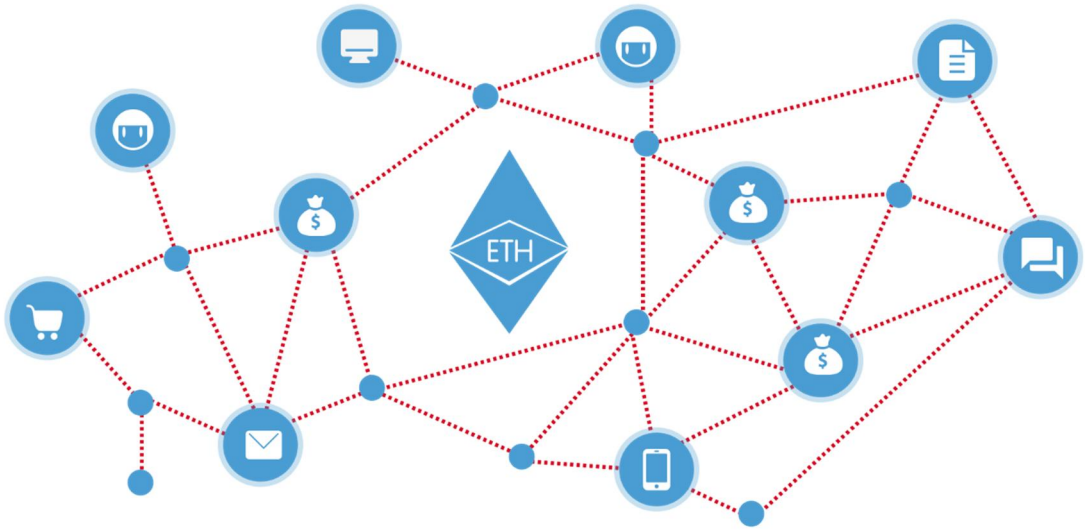
去中心化數字交易所最大的特點是所有交易通過智能合約來實現，將資產托管、撮合交易、資產清算都放在區塊鏈上，完美解決了用戶資料、資產信息集中在交易所的弊端。然而去中心化數字交易所在現階段技術上也存在明顯的劣勢：

- 用戶在去中心化數字交易所的一切資產和交易操作是以區塊鏈交易來驅動的，因此即時性上就受到區塊鏈本身的確認速度的影響，在目前以太坊上交易確認大約需要幾十秒的時間，這對用戶體驗而言并不友好。

- 交易成本也會受到區塊鏈本身交易費用的影響，因此對于小額交易而言交易成本會變得很高。

- 由于區塊鏈網絡交易處理性能低下，并不能處理大并發的實時交易，所以在交易量和交易深度上遠遠不如中心化數字交易所，流動性上有所受限。

- 用戶本身需要對賬戶公私鑰有足夠的安全操作知識才能保障足夠安全，否則賬號遺失、被盜也是會經常發生的。



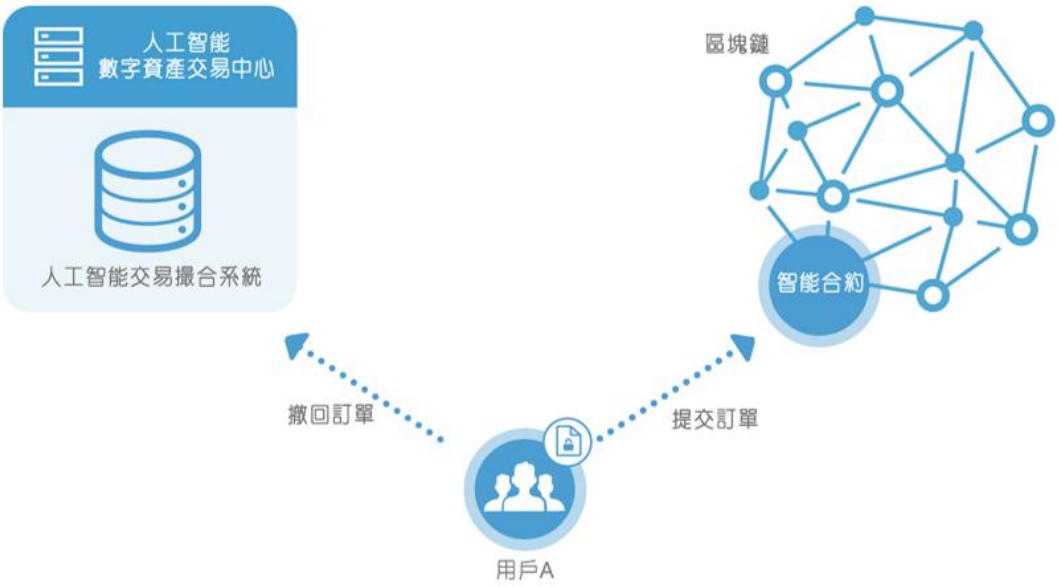
以太坊網絡擁堵

人工智能數字資產交易中心

綜合以上原因，可發現中心化數字交易所與去中心化數字交易所各有其優缺點，如何兼顧中心化與去中心化的優點幷去除兩邊的缺點，人工智能模式將會是未來數字資產交易中心發展的趨勢。

一個理想的人工智能去中心化架構，由人工智能交易撮合系統進行訂單撮合，當訂單撮合成功且系統對雙方的智能合約進行驗證，交易結果將廣播至區塊鏈上，幷進行最后的交易。人工智能模式的交易中心不單單實現訂單快速撮合，同時還能在短時間內匹配到更好價格。

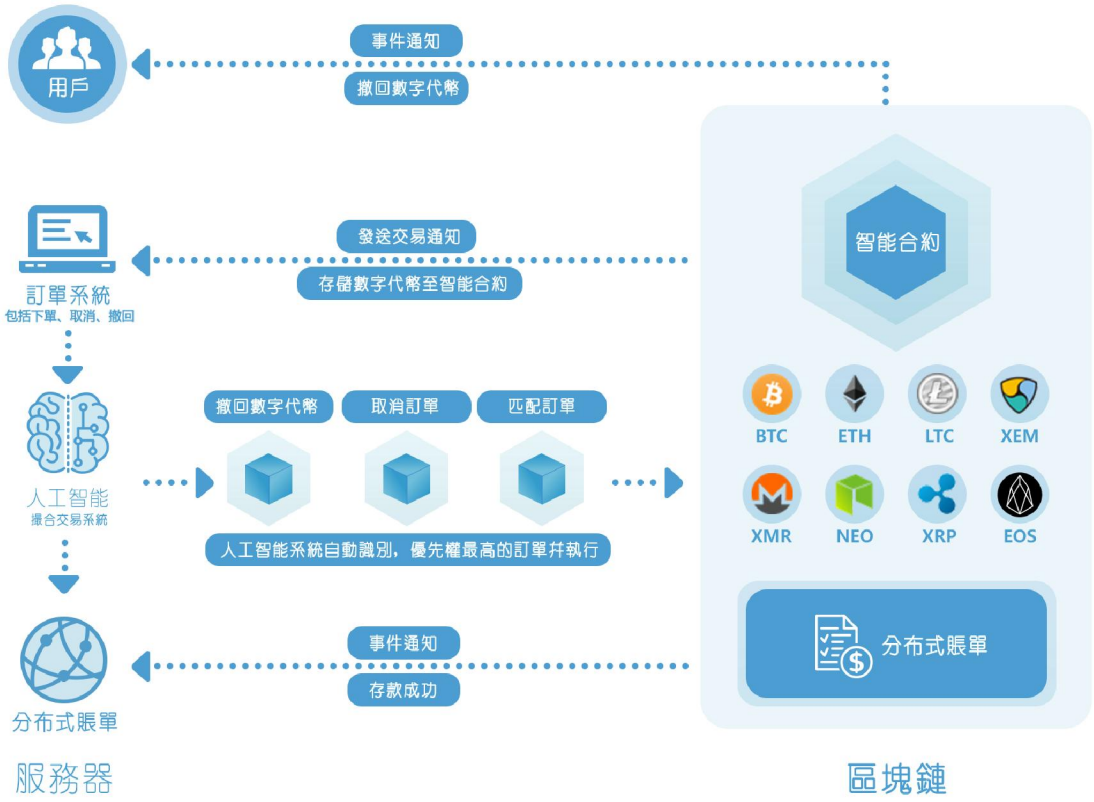
因為用戶的數字資產是存放在智能合約上，即使黑客攻擊交易中心的服務器，用戶的數字資產也會安好無損。交易中心上的所有訂單均在智能合約上，通過智能合約發送到區塊鏈，因此任何交易信息將是透明化且可追溯的。



人工智能數字資產交易中心

DeBi 人工智能數字資產交易中心

交易中心架構圖



人工智能數字資產交易中心架構

DeBi人工智能數字資產交易中心（本文統一簡稱：DeBi），結合了中心化交易所的效率和去中心化交易所中智能合約的安全與隱私性。

交易程序主要分為三部分：

1. 用戶首先將數字代幣存入智能合約，向 DeBi 發送訂單交易請求。

2. DeBi 通過人工智能交易撮合系統進行撮合，一筆交易訂單能同時配對多筆需求交易訂單，使用戶成交在較優價格。在交易中心中，所有訂單都通過鏈下傳輸，因為撮合效率得到保障。

3. 撮合系統將會對雙方的智能合約進行檢查，確認無誤后，系統將把成功撮合的結果公布至區塊鏈上，若在撮合完成前，雙方任意一個想取消交易，交易中心不能進行任何干預。（交易中心任何權限的管理員均無法修改用戶智能合約內容，更無法動用客戶的資金，由于用戶的每一筆交易均通過智能合約進行且發送至區塊鏈為公開賬本，因此所有交易透明且可追溯。）

智能合約是一套以數字形式定義的承諾，包括合約參與方可以在上面執行這些承諾的協議。

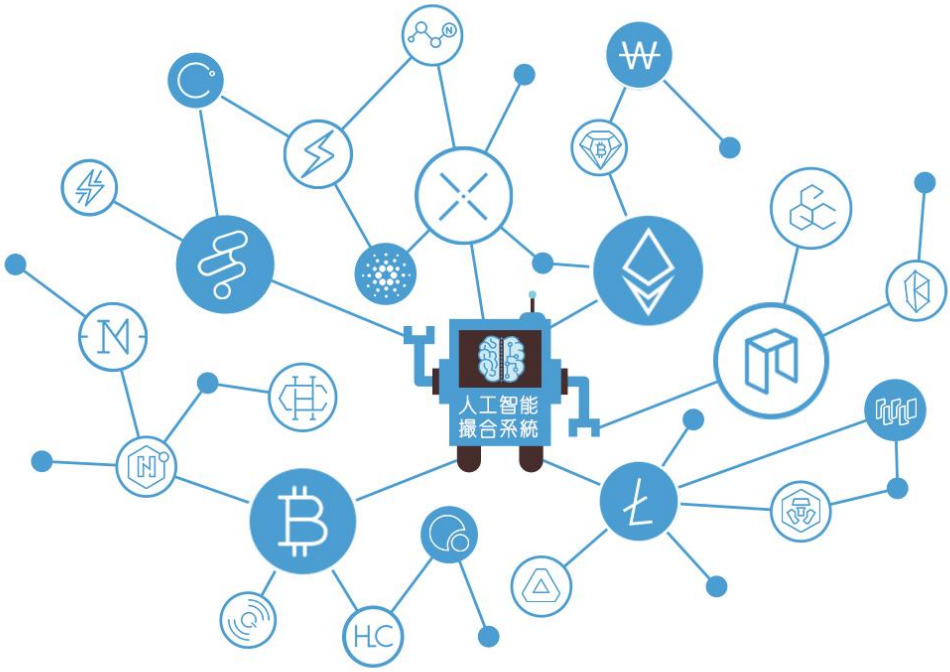
區塊鏈技術給我們帶來了一個去中心化的，不可篡改的，高可靠性的系統，在這種環境下，智能合約才大有用武之地。

DeBi正是利用智能合約這個特性，結合中心化高效率的撮合系統，打造出一個結合了中心化交易所的效率和去中心化交易所中智能合約的安全與隱私性的新平臺。

人工智能交易撮合系統

現在主流的中心化交易所主要采用集中式一對一的訂單撮合系統，DeBi的人工智能數字資產交易中心則采用人工智能交易撮合系統。

人工智能交易撮合系統，把訂單混合式分散在交易中心和區塊鏈上進行匹配。當用戶需要進行交易時，系統會把用戶的代幣存放在智能合約上，然后按照一對多的模式排列在人工智能交易撮合系統中，不單單實現訂單快速撮合，同時還能在短時間內匹配到更好的價格。



人工智能交易撮合系統

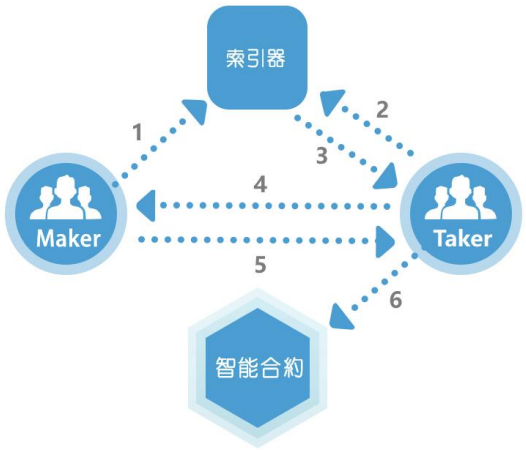
交易中心交易邏輯

市場訂單可以“鏈上”或“鏈下”存儲，鏈上存儲意味着它們被存儲在智慧合約中，鏈下則意味着存儲在第三方如中央服務器中。鏈下訂單開始運轉的關鍵因素來自區塊鏈的核心算法之一：橢圓曲綫數字簽名算法（ECDSA），這是一種非對稱加密算法，對訂單信息進行簽名蓋章，確認各自的身份，保證交易邏輯有序執行。

- Maker 創建一個新的訂單：ERC20 代幣，它的數額，它的 ETH 金額，以及是買入還是賣出訂單
- 然后 Maker 使用以太坊私鑰為訂單散列簽名（使用 ECDSA，還有特別是在比特幣中也使用的 Secp256k1 來實現）
- Maker 在鏈下發送訂單以及簽名（在數字資產交易中心中，這一個步驟通過一組服務器用 Web Sockets 傳遞 JSON 消息來完成）
- 當 Taker 想要與該訂單進行交易時，簽名和訂單信息被發送到智能合約的交易功能
- 智能合約驗證簽名來源于 Maker
- 智能合約確認訂單沒有過期或已經履行
- 資金轉移幷收取費用

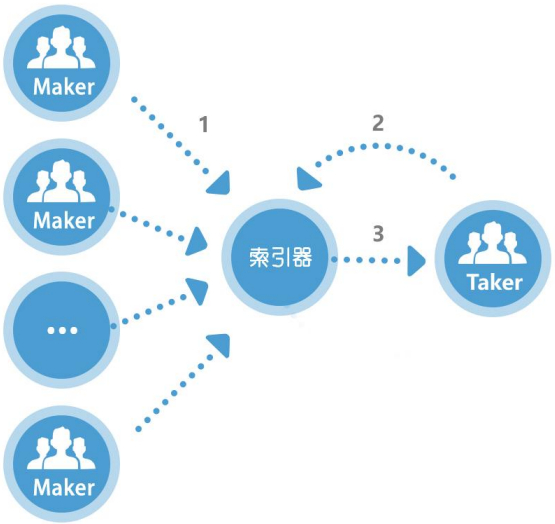
交易中心索引器協議

索引器是一種脫機服務，它聚集并匹配基于其交易意圖的對等點：潛在的Maker和Taker是否希望購買或出售代幣。索引器聚合了這種“交易意圖”，并說明匹配基于意圖購買或銷售特定代幣的對等點。接受者找到了他們想要交易的Maker，他們就開始使用上面的對等協議進行談判，一旦Maker和Taker達成了協議，訂單就會被完成交易。



1. Maker調用索引器
2. Taker使用索引器
3. 索引器匹配到相對應的Taker
4. Taker直接聯系Maker
5. Maker根據交易響應Taker
6. Taker根據智慧合約向Maker付款

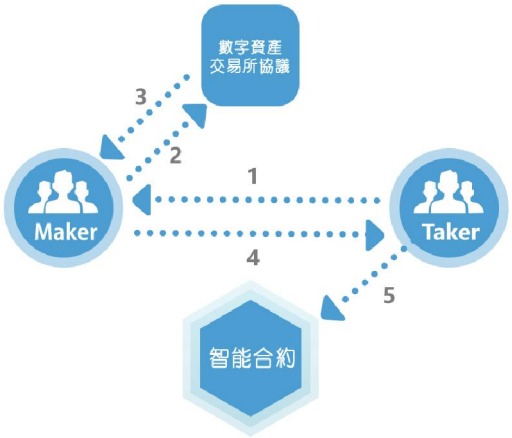
一個 Taker 對應多個 Maker，每個 Maker 都獨立地宣示他們的意圖



1. 多個 Maker 調用索引器
2. Taker 使用索引器
3. 索引器匹配到對應的 Taker

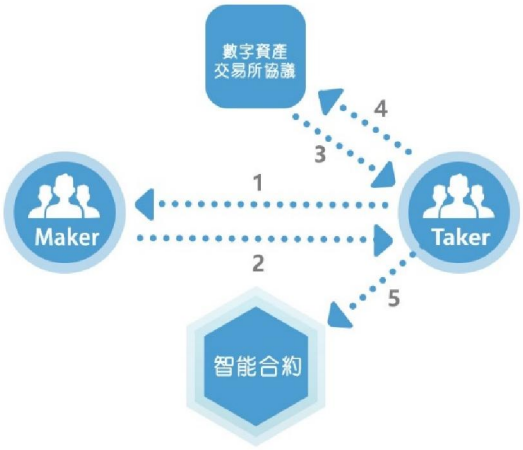
數字資產交易中心協議

數字資產交易中心協議是一個連鎖服務，為Maker和Taker提供價格信息。定價時，在提供給Taker之前，Maker可以向數字資產交易中心提出對它所認為的公平價格的建議，同樣，在接到訂單后，Taker會通過協議檢查以驗證它的公平價格。數字資產交易中心協議提供了價格信息，幫助Maker和Taker做出更明智的定價決策和順利進行貨幣交易。



1. Taker向Maker提出交易請求
2. Maker通過數字資產交易所協議協定獲取交易價格
3. 數字資產交易所協議向Maker返回交易價格
4. 分析價格信息，Maker向Taker回復

當Taker收到交易請求時，Taker和數字資產交易所協議之間會發生非常相似的交互



1. Taker向Maker提出交易請求
2. Maker回復交易請求
3. Taker通過數字資產交易所協議協定獲取交易價格
4. 數字資產交易所協議向Taker返回交易價格
5. 在分析價格信息，Taker通過智能合約付款并完成交易

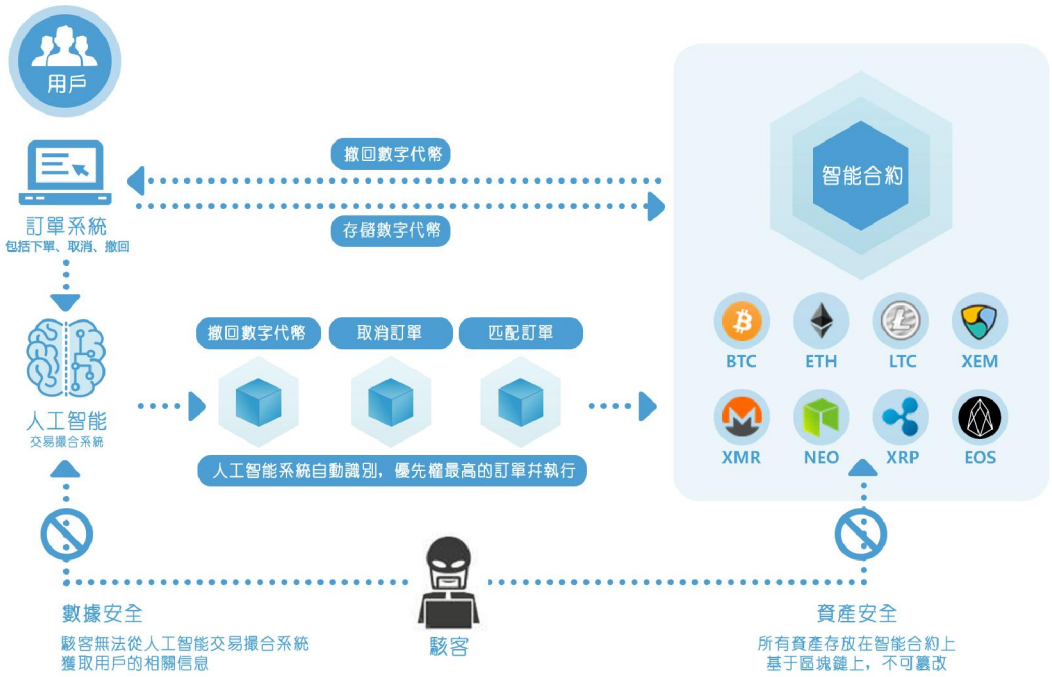
安全技術措施方案

DeBi對交易系統的安全性極其苛刻，因為任何交易都需要Smart Trade傳送到智能合約。當接收到用戶的交易請求時，交易訂單將送到人工智能交易撮合系統，撮合成功的訂單將傳送到智能合約上，驗證和進行最終交易。

金融級防入侵系統

DeBi全系統按照全球頂尖金融級系統技術要求進行開發，全面采用SSL+數字簽名通訊機制。全數據采用3DES加密，多節點分布式RSA非對稱加密雲儲存等。所有資產模塊采用公鑰層管理及綫下冷密鑰相結合的方式進行保護。

即使黑客成功入侵幷控制了DeBi，撮合系統是需要管理員的私鑰才能正常運行，當系統檢測到網站被不明來源入侵時，撮合系統將停止所有訂單的撮合進程，若要系統重新運行，則需要管理員的私鑰。若私鑰也落入黑客手中，黑客也不能改變交易訂單中的價格，因為任何的交易均在智能合約中，整個交易過程不可篡改。

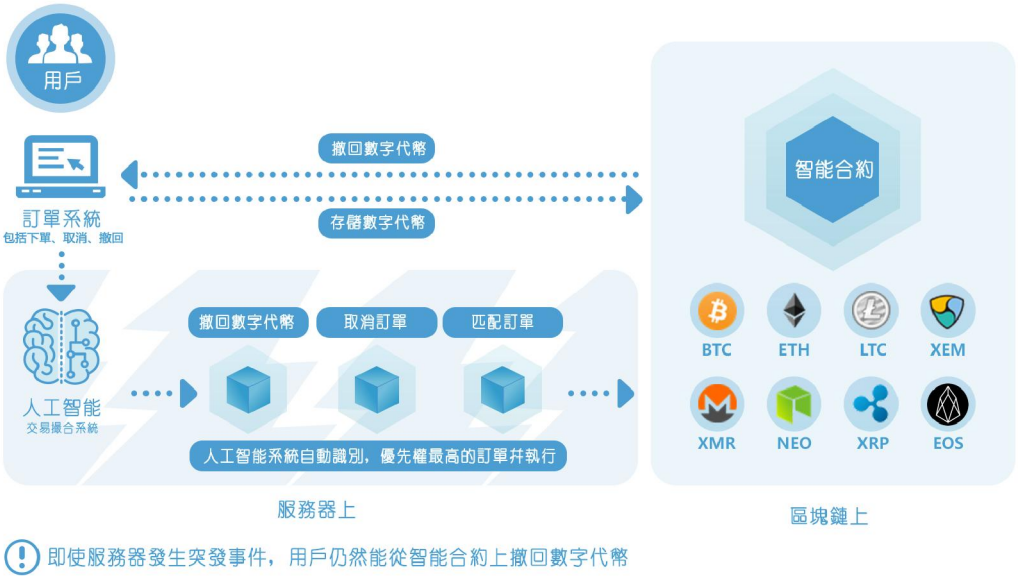


金融級防入侵系統

全球多節點回溯式復原

當DeBi服務器發生灾難，用戶無法進行訂單操作，由于用戶所有的資金都是保管于智能合約里，所以即使服務器無法立即被復原，所有的用戶仍然可以通過智能合約，將數字資產轉移至安全的地方。

交易中心服務器發生灾難時，DeBi在全球毫秒級同步的多節點服務器集群中啟動緊急停機預案，采用所有交易結果都必須能正確回溯的方式，從主備份服務節點中開始執行回溯式復原。該復原的準則是從歷史上回溯和驗證所有交易記錄，確保復原后整個交易中心的數據準確無誤。



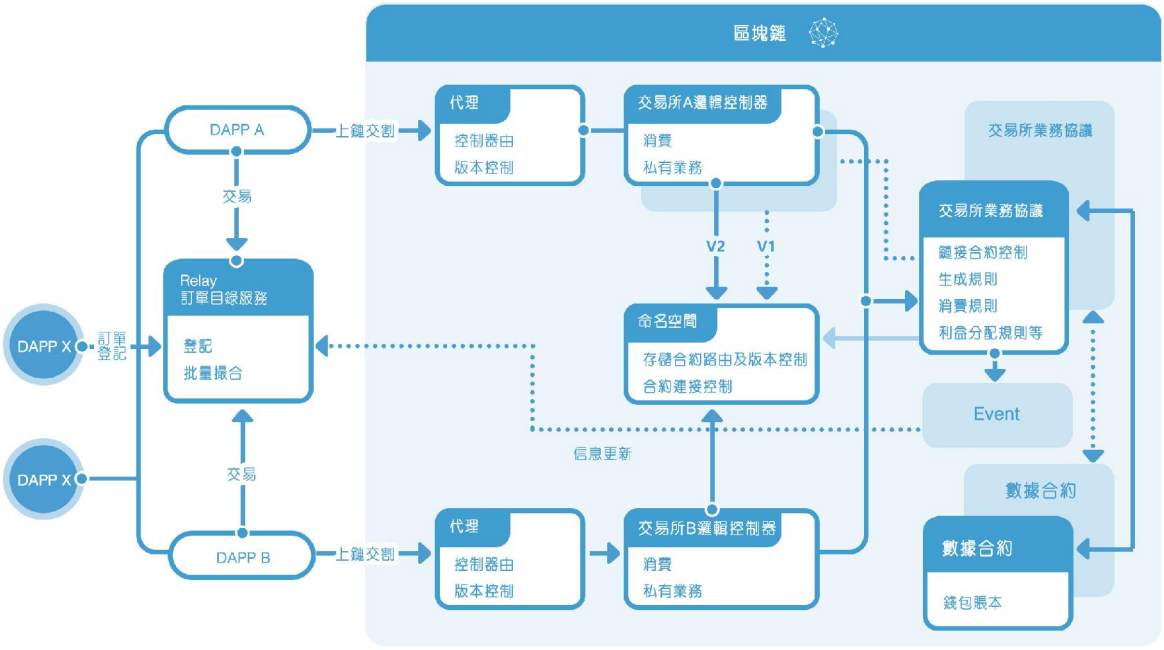
全球多節點回溯式復原

DeBi 智能合約

DeBi合約主要包括權限管控，人工智能訂單管理以及提幣等功能，只能由人工智能交易撮合系統發起。

要保證一筆交易的順利完成，第一步要對用戶的交易智能合約進行檢查，這個步驟由人工智能交易撮合系統進行，檢查合約內容是否經過用戶的同意即簽名，若該合約沒有得到用戶的同意，任何數字資產將原封不動，所以不用擔心人工智能交易撮合系統在未經過用戶的同意私下挪用用戶的數字資產。

在訂單交易的順序中，人工智能交易撮合系統將進行一對多的模式排列在人工智能交易撮合系統中，不單單實現訂單快速撮合，同時還能在短時間內匹配到更好價格。

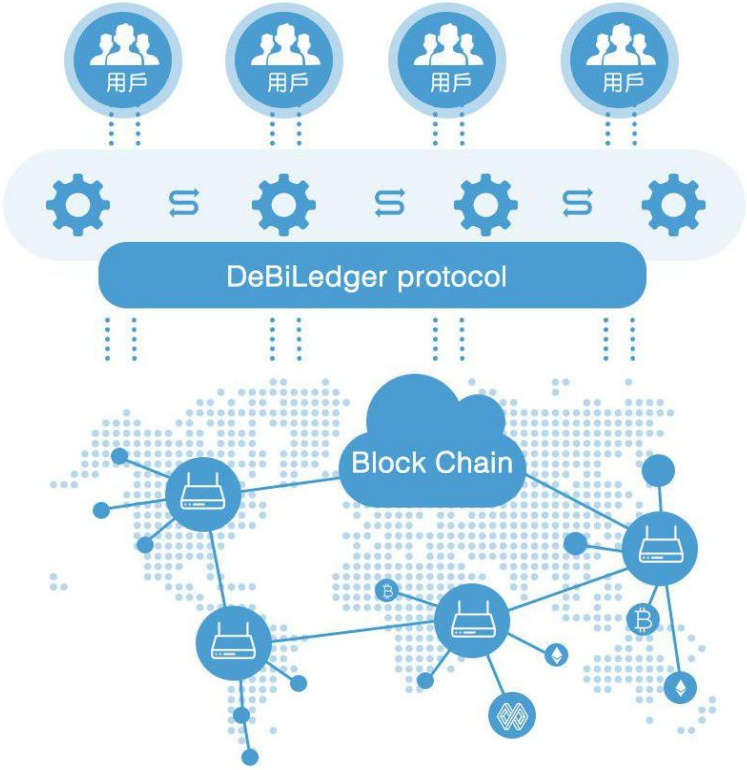


智能合約構架圖

跨鏈技術-DeBiLedger

眾所周知，側鏈是以錨定比特幣（以太坊）為基礎的新型區塊鏈，就像美金錨定到金條一樣。側鏈是以融合的方式實現加密貨幣金融生態的目標，而不是像其他加密貨幣一樣排斥現有的系統。利用側鏈，我們可以輕松的建立各種智能化的金融合約，股票、期貨、衍生品等。而跨鏈技術以智能合約的方式訪問公鏈賬戶賬本，同時建立側鏈，通過側鏈交換賬本信息，實現跨鏈交易。

舉一個最簡單的例子，目前的去中心化交易所，都存在着非常大的問題：第一，用戶基數少導致交易深度非常低；第二，去中心化交易所技術不完善，導致交易速度慢，用戶體驗糟糕；第三，無法像中心化交易所一樣實現 BTC 和 ERC20的直接交換。 但是通過 DeBiLedger 協議，可以輕松解決跨鏈交互，增加交易深度，提高交易速度，改善交易體驗，任何開發者均可以通過 DeBiLedger 協議，構建高效的跨鏈人工智能數字資產交易中心。

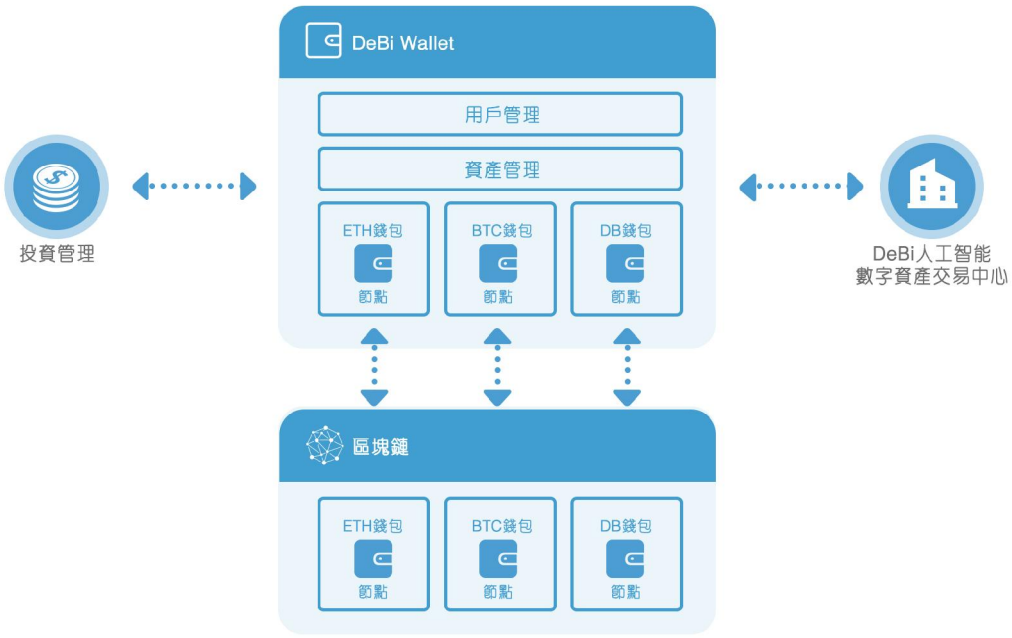


跨鏈技術

DeBi Wallet

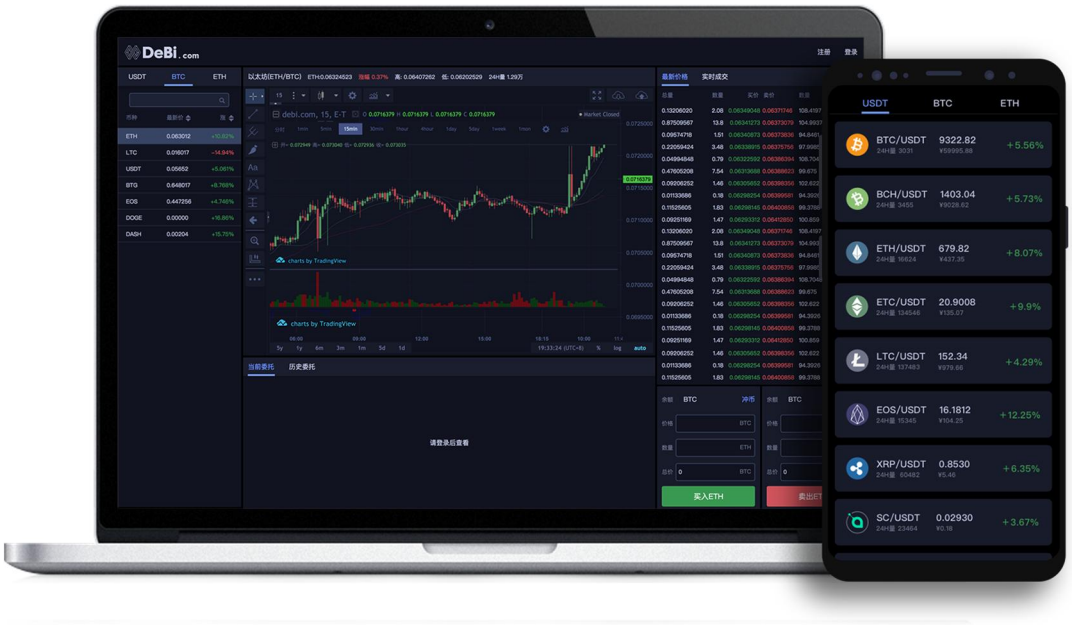
DeBi Wallet具有良好的兼容性，能夠連接多個主流公鏈，如ETH、BTC、NEO等等，為了方便用戶統一管理多種數字資產，DeBi Wallet支持基于比特幣、以太坊的加密數字資產，往后還會陸續兼容其他類型的加密資產。

同時DeBi Wallet提供了安全的加密和混淆機制，防止用戶的私鑰被盜取。每次交易用戶都需要輸入交易密碼，完成交易的簽名均發送到以太坊網絡中。



錢包架構

DeBi 優勢



低費率

激勵用戶限時免費，交易零手續費

高安全

智能合約鏈上交易，冷熱錢包分離

低門檻

行情趨勢一目了然，多終端多語言

高性能

高速內存撮合引擎，無鎖環形隊列

分布式

微服務分布式集群組件獨立部署

高可用

系統級別彈性擴容KBS容器編排

企業介紹

得幣國際集團有限公司(DeBi International Group Co., Ltd)，核心團隊源于頂尖區塊鏈、互聯網以及金融行業，公司致力于推動區塊鏈相關的應用與發展，同時也參與世界性的技術研發，推動區塊鏈和現有系統整合，改進系統效率與成本問題。

團隊構成

團隊由一群經驗豐富的專業人士組成，他們來自 Google、Citibank、Huawei、Tencent 等世界頂尖企業，專注于數字貨幣、區塊鏈、系統安全與創新應用研發等。

DeBi 致力于提供區塊鏈、數字貨幣、智能合約、撮合系統等專業技術解決方案，隨着 DeBi 的發展與市場份額的增大， DeBi 將會以開放的態度吸納願意為區塊鏈生態做出貢獻的人才。

行業背景

1：擁有 15 年從事 Linux 底層開發經驗，對分布式架構基本原理，包括分布式計算、分布式存儲、分布式緩存、分布式數據庫、分布式消息中間件，以及高性能計算、并行處理、虛擬化技術、集群部署、分布式任務調度、分布式資源管理等雲計算相關領域擁有多年實戰經驗，曾參與 IBM HPC 項目和 KVM 項目。

2：區塊鏈數字應用研發和管理，擁有自己的區塊鏈支付服務，來自麻省理工學院碩士學位，現任風險投資顧問、資本合伙人，在電子商務和網絡安全領域有超過 10 年的工作經驗，曾任美國、英國、德國等國家眾多高新技術企業及投資銀行高管。

3：曾參與過銀行、第三方式支付行業的系統設計和開發。有千萬級大數據量，分布式集群和高并發應用設計和開發經驗以及大型金融級支付系統研發和運營，每秒支持超過 10 萬筆的交易負載。

4：資深營銷團隊，投身互聯網廣告行業 10 余年，在網站運營、網站推廣、搜索引擎行銷等方面有着豐富的經驗，深諳 Google AdSense 等廣告聯盟盈利方式，運營超過 5 億的廣告訪問流量。

5：資深分布式存儲工程師，超過 15 年的 IT 從業經驗，在多家大型 IT 公司從事企業解決方案及架構設計工作。 擁有 5 年以上分布式存儲系統設計和開發經驗，掌握分布式存儲相關技術理論，部署、運維超過 1 億用戶的分布式雲存儲平臺。

聯系我們


support@debi.com


https://t.me/debicom


https://facebook.com/DeBiCenter


https://twitter.com/DeBiCenter