關於虛擬資產中心化交易 去中心化監管的建議函

鯽魚湧華蘭路18號港島東中心54樓

敬啟：證券及期貨事務監察委員會

發函日期：2023年03月27日

函件編號：TDB202303000003

主旨：從區塊鏈技術觀點，提供「關於適用於獲證券及期貨事務監察委員會發牌的虛擬資產交易平臺」監管規定建議，基於零知識證明的即時審計技術，推廣適用於政府、服務商、客戶三方的去中心化監管理念和實踐。去中心化帳本記錄的虛擬資產之儲存、流通、支付、交易、公權力監管乃是全新的生態，根本有別于傳統的中心式帳本；傳統與現存的社會關係和治理模式必然面臨挑戰。只有以互聯網和區塊鏈技術與邏輯，創新社會關係與治理模式之技術、契約、法規，適應並推動社會進步。

說明：

泰德比特是自2017年起、由香港登記的公司 ISunCrowd Limited 經營的項目，是一個虛擬資產的中心化的現貨交易所，只提供現貨交易，無杠杆、無融資、無合約、無做空。 我們致力於大宗虛擬資產（如：比特幣和乙太坊）的科普、交易、流通、支付，採取去中心化監管的方式以保障客戶之權益。自泰德比特提供服務以來，平臺和客戶平等互利，實行符合區塊鏈精神的去中心化監管，創新技術與商業模式，並考慮了公權力介入監管的多方角色和治理體系，具備領先業界之理念和技術實踐。

虛擬資產的中心化交易所，具備高頻交易24/7/365不間斷運營的特性，故而交易所的資產情況是隨著連續運營的情況在即時變動的。 然而在審計上，傳統會計師事務所一般過一段時間（例如每個月底）計算一次，故而不能很好的體現這段時間中的每個時間的切片瞬間的資產組成情況，無法應付如今瞬息萬變的金融市場，亦无法及早發現各種帳務流動異常並提出市場警告。

交易所的商業模式不同於銀行的商業模式。銀行出於承貸業務的需要，會借出使用者資產給借貸方以支付儲戶利息，故銀行永遠是"部分儲備金"系統 。 而中心化交易所撮合買賣雙方的交易需求以賺取交易手續費，交易所本身並不依賴承貸業務而盈利； 故而交易所必須在任何時刻，都能夠有效的隔離自有資產和用戶資產，且能夠隨時應對KYC用戶的合規大額即時的資金流入、流出的需求，即為"全部儲備金"系統。

2022年11月虛擬資產行業迎來至暗時刻，FTX交易所因挪用巨額客戶資產，在擠兌浪潮下，一周內轟然倒塌。 行業中的大型交易所了自證清白，紛紛開始儲量證明。 儲量證明的概念雖然好，卻有兩個邏輯漏洞： 1， 由於儲量＝淨資產＋用戶資產， 儲量＝鏈上資料，然而使用者資產等於交易所負債，是一個資料庫裡的、交易所可隨時修改的資料，並無鏈上資料能夠自證； 2， 因為沒有即時的儲量證明，交易所之間可以互相拆借達到需要的數位。

我們在此建議推動一種基於即時審計的去中心化監管技術，可以做到：

儲量證明即時更新：即中心化交易所的資料庫，經過人工智慧取證存證的機器審計，並上鏈到乙太坊公鏈，這三本帳本可以高頻快速地對比、匹配，以便確認記載使用者資產的資料庫未經篡改；每一次的自動即時對比記錄匹配，一旦察覺異動可以報警，每一次的對比匹配的結果，系統可存證、取證，做成符合會計標準的檔範本，供合規使用，這樣可以大幅度的降低合規的難度和成本； 交易所高頻定期地，例如每天來更新儲量證明來增加透明度。這樣，用戶可以隨時瞭解交易所的資金狀況，並確保交易所擁有足夠的資產來滿足用戶提現需求。

即時風控：通過即時監控交易資料、資金流動和風險狀況，交易所可以確保資金安全，並及時發現和解決潛在問題。這可以提高用戶對交易所的信任度，並降低資產丟失的風險。基於區塊鏈的去中心化監管技術可以在保護資料隱私的情況下，以演算法審計帳務中是否出現可疑金流、異常餘額變化、並比對實際區塊鏈上的虛擬資產金流是否與帳務一致，與交易行為完全零時差，達到適時即時審計。

即時審計：區塊鏈技術基於數學、密碼學與演算法運作，專業的區塊鏈技術公司可以從公開的帳本中追蹤所有虛擬資產流動軌跡，也因此所有區塊鏈上的虛擬資產都可以由世界各地的專業團隊二十四小時不間斷共同執行去中心化監管。這將是劃時代的金融革新，有望帶來更安全且高效的金融服務。我們在此建議推動一種基於零知識證明區塊鏈的去中心化監管技術，包括虛擬資產交易平臺在內的所有企業，藉由泰德比特的建議方式，即可以安全地將財務報表等公司營運資訊保存于區塊鏈上，徹底杜絕審計過程可能出現的錯誤和欺詐，提升審計的準確性。

我們相信，隨著區塊鏈技術的不斷發展和普及，區塊鏈審計與去中心化監管將成為未來主流審計與監管方法。如今香港在虛擬資產的政策發展已領先世界，我們希望證券及期貨事務監察委員會能夠在這一領域中發揮領導作用，推動去中心化監管的應用和發展，持續維持香港的世界金融中心地位。

提供泰德比特技術白皮書說明區塊鏈審計以及去中心化監管概念，我們期待能與證券及期貨事務監察委員會攜手合作，共同推動這一重要領域的發展。

建議人：iSunCrowd Limited

連絡人：

聯絡電話：

聯絡地址：

附件1：泰德比特技術白皮書

附件2：有關適用於獲證券及期貨事務監察委員會發牌的虛擬資產交易平臺營運者的建議監管規定的諮詢文件的意見回復

意見回復：

有關適用於獲證券及期貨事務監察委員會發牌的

虛擬資產交易平臺營運者的建議監管規定的諮詢文件

問題 1：你是否贊同，持牌平臺營運者在採取所建議的妥善投資者保障措施的前提下，應獲准向零售投資者提供服務？請說明你的看法。

回復 1： 贊同，應獲准向零售投資者提供服務，因為他們有投資虛擬資產的需求。

1. 投資者保障：區塊鏈和 Web3 是目前市場最有發展潛力的方向之一，虛擬資產作為這些平臺的基礎資產，有巨大的投資價值。讓投資者可以在合規交易所接觸到有價值的虛擬資產，對於投資者理解和學習最新的科技有巨大幫助。讓投資者可以較早的投資有價值的虛擬資產，可以更好的保護投資者的利益。
2. 市場發展：允許持牌平臺營運者向零售投資者提供服務，有助於市場的繁榮和發展。零售投資者可以通過平臺更容易地獲得投資機會，從而增加市場活躍度，提高資金流動性。這有可能促進創新和經濟增長。
3. 風險與責任：零售投資者往往缺乏專業知識和經驗，可能在面對市場波動和風險時做出不理智的決策。因此，在允許持牌平臺營運者向零售投資者提供服務時，應確保投資者充分瞭解投資風險，並願意承擔相應的投資損失。

若持牌平臺運營者無法向零售投資者提供服務： 那麼零售投資者為了滿足自己的需求，必將在不持牌的平臺運營商，或者在去中心化交易平臺（即“ DeFi”）上操作，如 Uniswap、Curve 等。這些服務交易量已經高達數百億美元，暫時不被政府監管。 因此，若受到政策阻攔，零售投資者無法在持牌平臺交易，那麼勢必轉向無法被監管的服務，使得零售投資者暴露在更大的風險中。

問題 2：對於有關一般代幣納入準則及特定代幣納入準則的建議，你是否有任何意見？

回復 2：參考泰德比特技術白皮書去中心監管原則，持牌平臺營運者應設立分析研究團隊，週期性的分析其平臺所有代幣，具體包括：

1. 代幣信息：包括但不限於項目背景、近期新聞、發展計畫、治理結構、收益分配、總發行量、新增發行量、當前市值等。平臺應向投資者披露代幣的資訊，公開于區

塊鏈流覽器上，提供投資者檢閱。這有助於投資者更好地瞭解項目的價值和風險，從而做出明智的投資決策。

2. 技術基礎設施：代幣應基於可靠、安全的區塊鏈技術，以確保交易的安全性和專案的穩定性。代幣應有足夠的開發和維護支持，以及一個活躍的開發者社區。
3. 流動性：代幣應具有良好的流動性，以確保投資者能夠在需要時輕鬆買入和賣出。這可以通過在主要交易所上市代幣來實現。同時，流動性也是評估專案成熟度和市場接受程度的一個指標。
4. 風險管理：投資者應充分瞭解代幣專案的風險，包括市場風險、技術風險和法律風險。平臺應對於代幣有著風險評級管理，例如設立量化指標為高、中、低三種風險，連續一段時間高風險之產品應予下架；另應設立特殊風險指標，資產觸發特殊風險，應即刻暫停交易一段時間。

問題 3：如證監會有意允許零售投資者使用持牌虛擬資產交易平臺，那麼從投資者保障的角度來看，你認為應要實施甚麼其他規定？

回復 3：參考泰德比特技術白皮書，為保障投資者資產安全以及市場公平公正，持牌虛擬資產交易平臺應該要實現去中心監管機制，其具體原則如下：

1. 資料披露：交易平臺內的統計資料，包含但不限於總交易量、成交資料、平臺資產總進出入金數量等，應於 24 小時內公開于區塊鏈流覽器上，供零售投資者檢視，並於交易平臺內醒目位置提供檢閱方法。此外，交易平臺還應披露與虛擬資產相關的重要資訊，如專案背景、總市值、交易量等。
2. 投資者教育：加強對投資者的教育和培訓，讓他們瞭解虛擬資產的特性、風險以及投資策略，提高投資者的風險意識和辨別能力。
3. 風險管理：交易平臺應建立完善的風險管理體系，對投資者進行風險提示和風險評估，對高風險投資者採取限制性措施。
4. 保護隱私：對於投資者的個人資訊，交易平臺使用零知識證明等技術在確保 KYC、AML 的基礎上，也會保護投資者的個人隱私。

問題 4：對於允許結合使用第三者保險及持牌平臺營運者或與其屬同一公司集團旗下法團撥出的資金的建議，你是否有任何意見？你是否有任何其他建議？

回復 4：應採取有前提允許的方法。

參考泰德比特去中心監管原則，應將相關資金流動訊息公開於具備流覽器的區塊鏈上，且確保交易平臺恪守禁止任意調動用戶資產原則。所有虛擬資產須接受公開檢視是否有調用、於市場上質押借貸之情事，以保障用戶的資產安全，不受該集團其他業務風險影響。

1. 協力廠商保險公司：許多虛擬資產交易平臺已經開始尋求與保險公司合作，為用戶資產提供保險。這種做法可以降低投資者在交易所遭受損失的風險。保險公司可以為交易所提供盜竊、駭客攻擊等方面的保險覆蓋，保障用戶資產安全。此外，保險公司會對交易所的安全措施進行評估，確保其符合一定的安全標準。
2. 同一公司集團旗下法團撥出的資金：加密資產交易平臺也可以考慮從同一公司集團旗下的法團撥出的資金來為用戶提供保障。這種做法的優勢在於，交易平臺可以利用集團內部的資源和支援，更靈活地為用戶提供保障。然而，這種做法可能存在潛在的利益衝突，因此需要確保透明度和合規性。應將相關資金流動訊息公開於具備流覽器的區塊鏈上，以保障用戶的資產安全，不受該集團其他業務風險影響。

問題 5：對於持牌平臺營運者應如何劃撥該等資金，你是否有任何提議（例如，撥入持牌平臺營運者的公司帳戶，或設定代管安排）？請詳細說明你所建議的安排，及有關安排所提供的保障如何能提供與第三者保險相同的保障水準。

回復 5：

持牌平臺劃撥該等資金應確保，其一、交易平臺內使用者資產皆無受到調用，其二、該等資金並非來自非法來源。參考泰德比特去中心監管原則如下：

1. 撥入持牌平臺營運者的公司帳戶：將資金撥入持牌平臺營運者的公司帳戶是一個可行的選項。這種方式可以讓持牌平臺營運者直接管理和監控資金，並確保資金的合規使用。為了提供與協力廠商保險相同的保障水準，可以採取以下措施：
   a. 保持資金隔離：將客戶資金與公司自有資金分開存放以降低資金被挪用的風險。
   b. 設立專項帳戶：為客戶資金設立專項帳戶，以確保資金的安全和透明度。

c. 即時審計與風險管理：交易平臺應及時提交其資產儲備狀態，于區塊鏈流覽器上公開於眾，確保資金的安全與合規使用。

2. 設定定代管安排：通過與信譽良好的協力廠商金融機構建立代管安排，可以將資金的管理和監督委託給協力廠商，提高資金的安全性。這種安排可以通過以下方式提供與協力廠商保險相當的保障水準：
   a. 選擇合適的託管機構：與信譽良好、具有豐富經驗的託管銀行或金融機構合作，確保資金的安全管理。
   b. 簽訂明確的代管協議：明確雙方的權利和義務，確保資金的安全和合規。
   c. 資金隔離：確保託管機構將客戶資金與其他資金進行隔離管理，降低資金被挪用的風險。
   d. 即時審計與風險管理：定期對託管機構進行審計和監督，以確保資金的安全和合規使用。

綜上所述，持牌平臺營運者可以根據自身需求和監管要求選擇合適的資金劃撥方式。無論採用哪種方式，關鍵是確保資金的安全、透明度和合規性，並通過相應的保障措施提供與協力廠商保險相當的保障水準。

問題 6：對於哪些技術方案能夠有效地紓減與保管客戶虛擬資產（尤其是以線上儲存方式持有虛擬資產）有關的風險，你是否有任何提議？

回復 6：

區塊鏈上的虛擬資產因其技術的特殊性，無法針對其存放狀態與移轉狀態進行藏匿。參考泰德比特技術白皮書，我們建議：

1. 即時審計： 所有交易平臺應使用區塊鏈即時審計技術，達成即時存證（Real-Time Evidence）與即時審計（Real-Time Audit），即時掃瞄出交易平臺現有資產是否能夠全部完成使用者的提現需求，藉此紓減客戶虛擬資產之風險。建立即時監控和報警系統，以檢測和應對異常活動和潛在攻擊。一旦發現異常，及時採取措施以防止損失。
2. 私密金鑰管理： 2a. 多重簽名技術（Multisig），要求多個私密金鑰才能進行交易。這種技術可以提高虛擬資產安全性，因為攻擊者需要同時獲得多個私密金鑰才能盜

取資產；2b. 分散式金鑰管理：將私密金鑰分割成多個部分，並將這些部分分別存儲在不同的設備或地點。這樣可以防止單點故障，並增加攻擊者盜取全部金鑰的難度。

3. 冷錢包存儲：儘管線上錢包（熱錢包）方便使用者進行即時交易，但其安全性相對較低。為降低風險，可以將大部分虛擬資產存儲在離線錢包（冷錢包）中，只保留少量資產（不超過 2%）在熱錢包以滿足日常交易的運營需求。

問題 7：如持牌平臺營運者可提供虛擬資產衍生工具交易服務，你會建議採納哪一種業務模式？你建議推出哪類虛擬資產衍生工具供投資者買賣？目標將會是哪類投資者？

回復 7：

在選擇適合的業務模式時，持牌平臺營運者應考慮其目標市場、客戶需求、法規要求以及自身的運營能力。以下是一些建議採納的，適用於機構投資人和零售投資人的虛擬資產衍生工具交易服務業務模式：

1. 常規交易所模式：作為一個中心化的交易所，平臺方為用戶提供虛擬資產衍生工具（如期貨、期權、互換等）的交易服務。在這種模式下，交易所需要維護一個高度安全和可靠的交易系統，並提供清晰的交易規則、費用結構和風險管理措施。

2. 交易所指數基金（ETF）：加密貨幣交易所指數基金（ETF）是一種以加密貨幣為基礎的交易所指數基金。投資者可以通過購買 ETF 來獲得多樣化投資。

以下是一些建議採納的，適用於機構投資人，但暫時不建議面對零售投資人的虛擬資產衍生工具交易服務業務模式：

1. 杠杆交易平臺：提供杠杆交易服務，允許使用者借入資金進行虛擬資產衍生工具交易，從而提高收益的可能性。然而，這種模式也會增加使用者的風險，因此需要強調透明度和風險管理。加密貨幣交易所通常提供杠杆交易，這意味著交易者可以通過借入交易所的資金來增加自己的交易頭寸，從而提高交易收益；然而，杠杆交易也帶來了更高的風險。杠杆倍數表示交易者可以借入多少倍的資金來進行交易。這

樣的交易使得交易者可以更快地獲得收益，但同時也增加了虧損的風險。杠杆交易的風險在於，如果市場價格不利於交易者，他們將承擔更大的虧損。如果價格下跌，交易者的損失可能會超過他們的保證金，導致他們的頭寸被強制平倉。在這種情況下，交易者不僅會失去他們的投資，還可能會因為杠杆交易而欠下債務。因此，交易者應該非常小心地使用杠杆交易，並確保他們有足夠的瞭解和經驗來管理這種風險。建議交易者在使用杠杆交易前，首先進行充分的市場分析，確定自己的風險承受能力和投資目標，同時使用適當的止損策略來最大限度地限制風險。

2. 去中心化交易平臺：採用去中心化的方式，使用智慧合約進行交易撮合和清算。這種模式可以降低中心化交易所的信任和安全風險，但可能會面臨更多的技術挑戰和監管問題。所有虛擬資產衍生交易都應採用公開並具備流覽器的區塊鏈，使用鏈上智慧合約進行。所有智慧合約應提交其設計原理以及程式碼交由三家以上區塊鏈技術公司執行審計，確認其設計原理內容無誤，以及不存在交易漏洞，公佈 30 日後方可上線，公佈期間若任何區塊鏈技術公司提出錯誤通報且屬實，則予以撤回重審，除此之外證券及期貨事務監察委員保留其審查權力，若其設計存在巨大市場風險或系統風險則予以駁回。虛擬資產衍生工具屬於金融科技先進技術，尚在發展階段，現階段並不適合以法規限制其運作範疇，但可保留其風險等級評核權力。

3. 對沖基金和專業投資者服務：為對沖基金、機構投資者和高淨值個人投資者提供專門的虛擬資產衍生工具交易服務。這種模式需要提供更高的客戶服務水準，包括對接、執行、報告等功能，並為客戶提供投資策略和風險管理建議。

在選擇業務模式時，平臺營運者需要權衡各種因素，包括潛在的市場規模、利潤空間、競爭環境以及監管風險。虛擬資產衍生品交易涉及較高的風險，交易者應該根據自己的風險承受能力和交易策略選擇適合自己的交易方式，並採取適當的風險管理措施。在現階段，某些有極大風險的虛擬資產衍生工具，例如高倍杠杆交易，應該面對有著良好風險控制意識的機構投資者和合資格投資人為宜。

問題 8：對於如何在將《虛擬資產交易平臺條款及條件》中的其他規定納入《虛擬資產交易平臺指引》內的同時對其加以改良，你是否有任何意見？

回復 8：金融本應是透明的、公正的、普惠的，但過去受限於技術，以及企業的不可控性而無法落實，如今區塊鏈技術的發展將帶來了金融服務的革新，從新實現金融服務應有的樣貌。參考泰德比特技術白皮書，我們建議所有的金融服務平臺，皆應該使用區塊鏈審計技術，達成即時存證（Real-Time Evidence）與即時審計（Real-Time Audit）；以及去中心化監管原則，在保護用戶的隱私前提下公開一切營運資訊，在人人都是投資者的同時，也實現人人都是監管者，嚇阻一切不法情事發生。

問題 9：對於《適用於持牌法團及獲證監會發牌的虛擬資產服務提供者的打擊洗錢指引》第 12 章當 中有關虛擬資產轉帳的規定或任何其他規定，你是否有任何意見？請說明你的看法。

回復 9：參考泰德比特技術白皮書，所有交易平臺具有責任義務瞭解其客戶虛擬資產來源以及最後虛擬資產的去向，需做到基於區塊鏈錢包的用戶身份盡職調查，並使用區塊鏈資產來源分析或相似技術追蹤虛擬資產是否涉及國際公開之打擊洗錢及資助恐怖活動之高風險名單，至此即可在最低管理成本下確保相關法規遵守。

問題 10：你對《證監會紀律處分罰款指引》是否有任何意見？請說明你的看法。

回復 10：無意見。