「數碼港元」先導計劃第二階段

摘要

香港金融管理局（金管局）於2024年9月啟動「數碼港元」先導計劃第二階段，以深入探討個人及企業在使用新型數碼貨幣過程中的創新用例。

為支持央行探索央行數碼貨幣（CBDC）及數碼貨幣，香港上海滙豐銀行有限公司（滙豐）亦加入了先導計劃第二階段，並以代幣化資產結算為主題。

憑藉我們深厚的金融專業知識、第一階段的參與以及進行中的研究項目的發現，我們專注於評估「數碼港元」在數字資產交易中的可行性，並解決在設計、實施和運營數字貨幣生態系統時可能遇到的實際問題。其中包括私隱和安全考慮因素，以及探索 「數碼港元」如何在公共和私有分佈式賬本技術 （DLT）環境中安全並大規模地運行。

我們的研究框架結合了定量數據和定性分析，在幾種DLT環境中模擬了不同類型的「數碼港元」交易，並於2025年3月至4月期間進行了一項有關評估客戶對「數碼港元」認知和態度的調查。

滙豐進行了三項試驗，以探索「數碼港元」擴展至個人及企業使用時可能面臨的機遇和挑戰。

問題陳述1：
提供有限的鏈上結算便利

試驗

研究「數碼港元」是否可以在公共區塊鏈環境中安全可控地運行，作為穩定幣和加密貨幣的替代品，用於儲存和轉移貨幣價值，並作為代幣化資產的結算工具。

調查結果

- 驗證了數碼港元的原子化結算能力，最大限度地降低交易對手風險。
- 即時結算提高交易效率。

問題陳述2：
使用「數碼港元」的潛在私隱及安全問題

試驗

解決與「數碼港元」相關的私隱和安全問題，因為這些問題對於擴大公眾採用非常重要。調查是否可以透過使用隱私增強技術 (PET)、去中心化身分識別 (DID) 和拒絕清單 (Deny List) 來緩解這些擔憂。

調查結果

- 經過驗證的身份和隱私控制，使用 DID 和 PET 以 「數碼港元」結算虛擬代幣化資產，維護安全和私隱。
- 經過驗證的拒絕清單功能，該功能將凍結錢包並阻止轉帳。
- 有成本的保障：使用 DID 和 PET 的交易成本分別增加 12 倍和 80-320 倍。

問題陳述3：
大規模營運「數碼港元」

試驗

確定公共和私有區塊鏈網絡樣本中採用「數碼港元」的獨特優勢和限制。

調查結果

- 選擇進行實驗的公共和私有區塊鏈在高流量負載期間都面臨性能挑戰。
- 批次處理功能可以減少了操作時間和交易複雜性。

總結

「數碼港元」可以在公共和私有的區塊鏈上進行擴展，每種區塊鏈都有其自身的優點和限制，均支持運用授權協議解決方案（如 PET、DID 和拒絕清單）來管理安全和私隱問題。同時，「數碼港元」為代幣化資產交易提供了新的結算工具。

「需要重點注意的是，滙豐第二階段的結果及發現應該在試驗的背景下和調查的固有局限性來解釋。這些試驗是使用具有假設的「數碼港元」和代幣化資產的滙豐錢包進行的。試驗 1 運用了公共區塊鏈，而試驗 2 和 3 則在私有區塊鏈和「測試網 」公共區塊鏈環境中進行。儘管存在這些限制，這些發現旨在支持圍繞 CBDC 和數碼貨幣的持續討論和試驗。這些見解和經驗教訓僅用於教育目的，並不反映滙豐在香港實施數字貨幣的政策立場。」

收穫與發現

假設 1：「數碼港元」可以運用許可協議在公有區塊鏈上安全運行，作為儲存和轉移價值的替代方案，並作為代幣化資產的結算工具。

- 「數碼港元」的原子化結算能力，最大限度地降低了交易對手風險並增強了結算時實行： 我們的研究證實，「數碼港元」在結算「假設」代幣化資產方面表現可靠，實現了原子化結算和不可逆交易。其原子化結算功能讓「數碼港元」能夠有效地處理常規和零碎交易。此功能對於減少結算時間和最大限度地降低交易對手風險特別有利，從而優化整體用戶體驗。

假設 2：使用隱私增強技術 （PET）、去中心化身份 （DID） 以及拒絕清單 (Deny List) 和允許清單（Allow List)可能會增強零售用戶的私隱（以及對私隱的信心），從而減輕區塊鏈生態系統中非法行為者的威脅。

- 經過驗證的 PET、DID 和拒絕/允許清單功能雖然有助於維護安全和私隱，但需要考慮成本：我們的研究驗證了使用 PET、DID 和允許/拒絕清單可以解決安全和私隱問題，有可能增強用戶信任，同時解決區塊鏈生態系統中非法行為者的威脅。 然而，這些技術和解決方案導致交易複雜度增加從而導致成本增加。因此，需要進一步完善 PET、DID 和允許/拒絕清單，以平衡安全性和私隱性與成本效益。
- 假設 3： 在私有和公共區塊鏈環境中進行假設「數碼港元」和代幣化資產交易，將呈現出不同的好處和限制。 選擇進行試驗的公共和私有區塊鏈在高流量負載期間都面臨了容量挑戰：我們試驗中使用的公共和私有區塊鏈環境的性能各不相同，與私有區塊鏈相比，公共區塊鏈顯示出更高的每秒事務處理（TPS） 能力，隨著節點數量的增加，私有區塊鏈在交易壓力增加的情況下面臨挑戰。值得注意的是，這一觀察結果只反映我們試驗期間測試的區塊鏈環境。因此，必須避免對區塊鏈環境的功能作出普性的歸納陳述。公共區塊鏈網路本質上可能無法實現更高的 TPS，因為它們的效能是可變的並且取決於其特定功能。
- 因此，在選擇區塊鏈平台時考慮容量限制至關重要。我們還得出結論，批次處理（Batch processing）功能和默克爾分發（Merkel Drop）機制可以顯著減少操作時間和複雜性，尤其是在零售環境中為增強可擴展性提供可行的解決方案。

透過我們的客戶調查，我們還獲得了以下見解：

一. 對「數碼港元」有認識的個人使用「數碼港元」的意願較高：雖然整體使用「數碼港元」的意願為中等，介乎17%至31%，但在有數字資產交易經驗或對「數碼港元」有認識的個人中，使用「數碼港元」的意願顯著增加。年輕和富裕人士對「數碼港元」的認識明顯較高，這與採用「數碼港元」的意願較高有關。

二. 解決私隱和安全問題是「數碼港元」採用的關鍵：約70%的受訪者擔心「數碼港元」的安全性，這種認知部分是由於意識有限而非實際風險所驅動，這凸顯了提高意識以推動採用的必要性。私隱也是一個關鍵問題，71% 的受訪者將其視為一個重要考慮因素。對私隱方案（如PET）的了解，可能有助紓緩其中一部分疑慮，並促進「數碼港元」的採用。

三. 很少有受訪者願意為私隱支付額外費用：儘管私隱很重要，但很少有受訪者願意支付與可以增強私隱和合規性的技術相關的額外費用。他們希望此類解決方案成為任何標準產品的一部分，就像現有支付解決方案經常出現的情況一樣。

建議與未來

雖然我們的研究結果為「數碼港元」在擴展到零售用例時的設計和運作提供了重要見解，但也強調了央行數碼貨幣和其他形式數碼貨幣的出現需要進一步研究。比如：

- 交易監控：檢查誰應該負責監控數碼貨幣交易。考慮中央當局、金融中介機構或其他實體是否以及如何管理監控、交易限制或凍結能力。
- 基礎設施所有權和成本框架：探索誰擁有和維護數碼貨幣基礎設施並支付相關費用，包括開發和執行私隱和安全增強技術所需的費用。在公共區塊鏈或混合環境的情況下，考慮應由誰持有加密貨幣並支付區塊鏈交易手續費（Gas 費）。
- PET：繼續調查 PET 在區塊鏈上的運用，探索接受程度更高的用途、包括參與者控制和政策考慮因素，以增強用戶私隱保護和合規性。進一步探索新的 PET 解決方案，因為它們不斷發展。
- DID 和可驗證憑證：研究如何在整個市場建立起信任框架，幫助 KYC、客戶盡職調查和打擊洗錢和恐怖分子資金籌集。識別誰可以發行和維護 DID 和可驗證憑證，尤其考慮到個人資訊會隨時間而變化等因素。
- 允許列表和拒絕列表的管理： 確定更新允許和拒絕列表的角色和職責劃分，以及如何處理數字錢包生態系統內的爭議以保持合規性。

有關滙豐假設「數碼港元」先導計劃的詳情，請瀏覽：

https://www.about.hsbc.com.hk/news-and-media/phase2-e-hkd-pilot-factsheet-en.pdf

有關本文件的中文版本，請瀏覽：

https://www.about.hsbc.com.hk/zh-HK/news-and-media/phase2-e-hkd-pilot-factsheet-cn.pdf