本文件包含五張流程圖，輔助說明投稿中雜湊時間鎖與混和模式的文字內容。以下流程圖將以 Alice、Bob 分別為以太坊和 Corda 的使用者。場景為 Alice 要用美元(cash)，交換 Bob 在 Corda 上的汽車(car)。

圖 1 為雜湊時間鎖的作法，理論上，若兩個 timeouts 的值(T1,T2)設定適當，HTLC 方法是可以順利執行原子交換（atomic swap）。

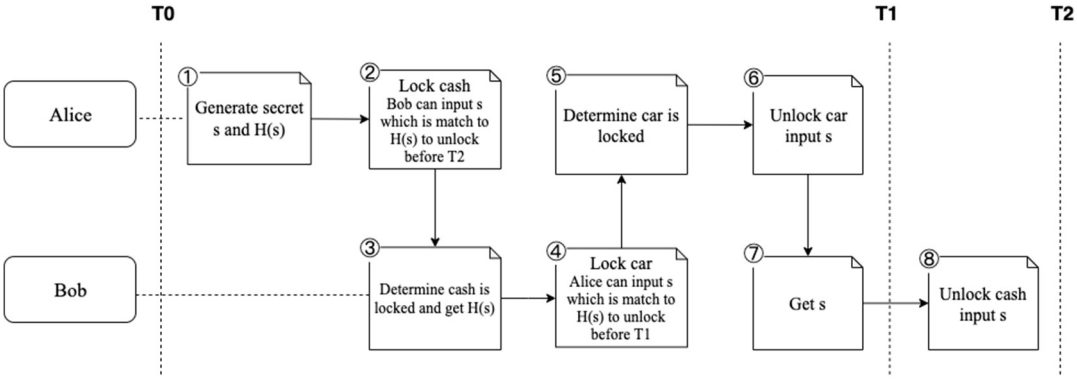

圖 1：雜湊時間鎖作法

為了確保交換應用的雙方能達成銀貨兩訖，在我們的實作架構中，兩個區塊鏈平台都透過智能合約(下圖的 Asset SC)實現資產的雜湊鎖與時間鎖的功能，並設立仲裁人服務(下圖的 Arbitrator)。若先被上鎖的資產其鎖定時間長度需足以讓新擁有人能夠成功解鎖資產，即使新擁有人嘗試解鎖失敗後，仍可通知仲裁人介入，並有足夠時間進行仲裁，執行資產之強制交換，如圖 2；若先被上鎖的資產時間鎖長度非常長，如果對方對應的資產已經 timeout 而 rollback，則其單一資產鎖定就失去了意義。這時可以請仲裁人介入處理，讓先被上鎖的資產得以提早 rollback 回原擁有人，如圖 3。

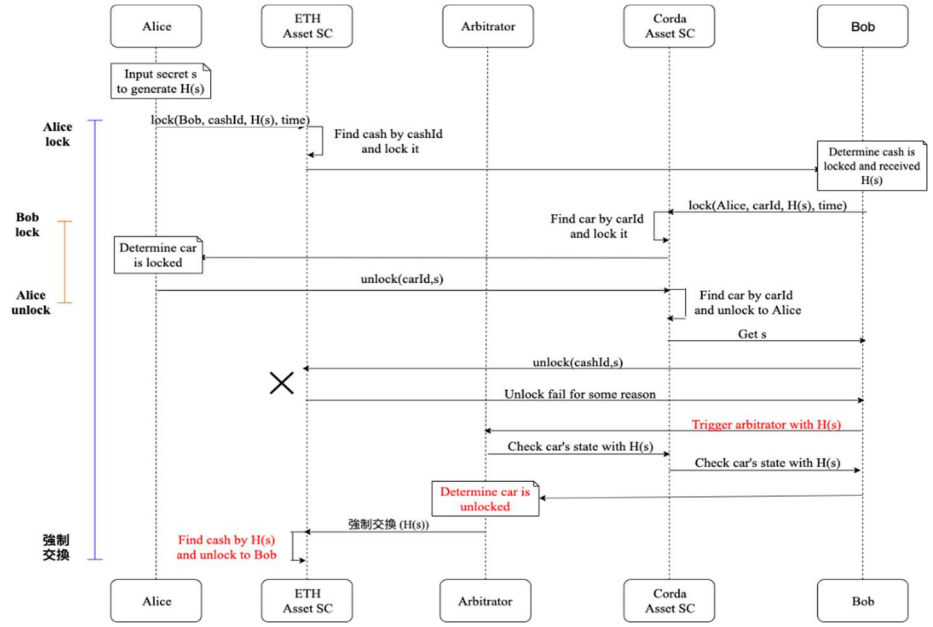

圖 2：雜湊時間鎖 - 強制交換

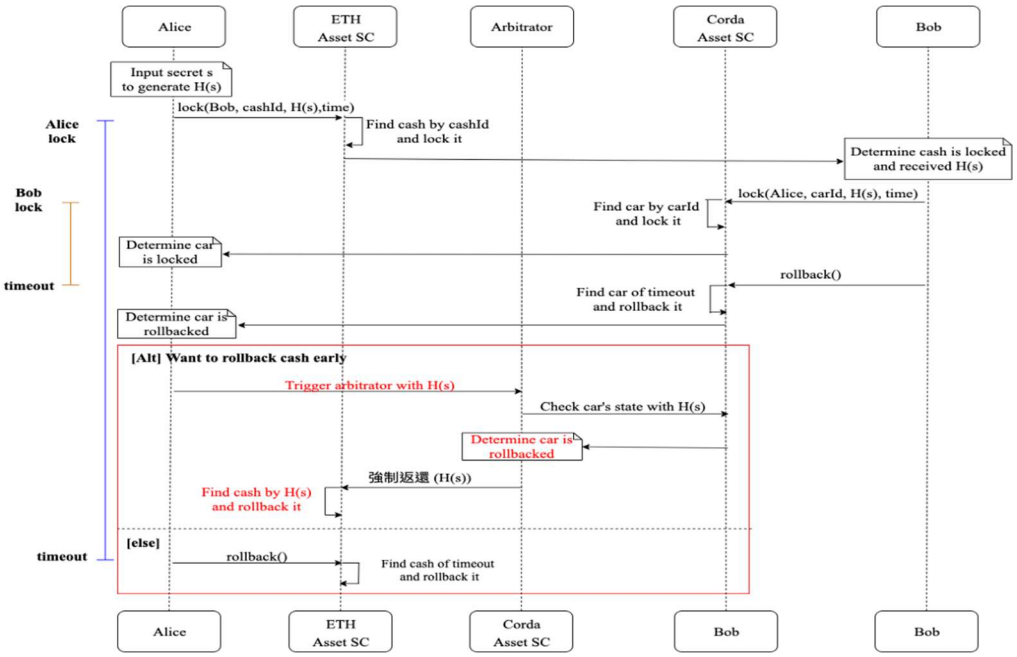

圖 3：雜湊時間鎖 - 強制返還

最後，我們提出一種新的混合模式來支援：以雜湊時間鎖為基礎，加入搭配中繼模式舉證程序的有限度仲裁功能。舉例而言，仲裁人應使用者要求介入時，除了查詢 Corda 上紀錄之資產狀態外，也需請求 Corda 公證人就查詢結果簽署數位簽章。接著仲裁人方能附上此交易證據，對以太坊智能合約提出執行強制處理的要求；以太坊端的智能合約配合修改，僅在驗證過仲裁人所附的數位簽章後，才會尊循其強制處理資產（返還或交換）的指令，如圖 4、5。

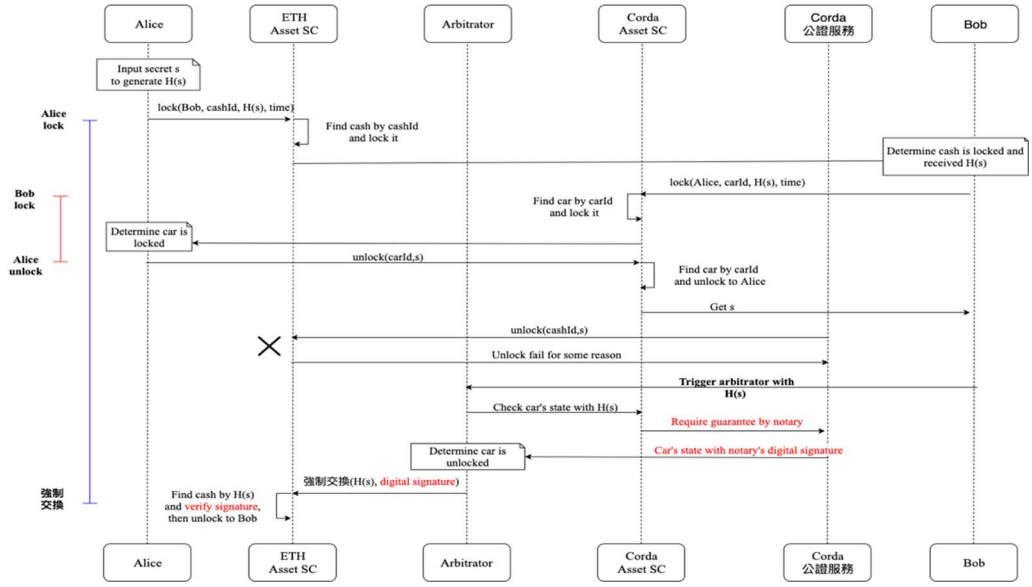

圖 4：混合模式 - 強制交換

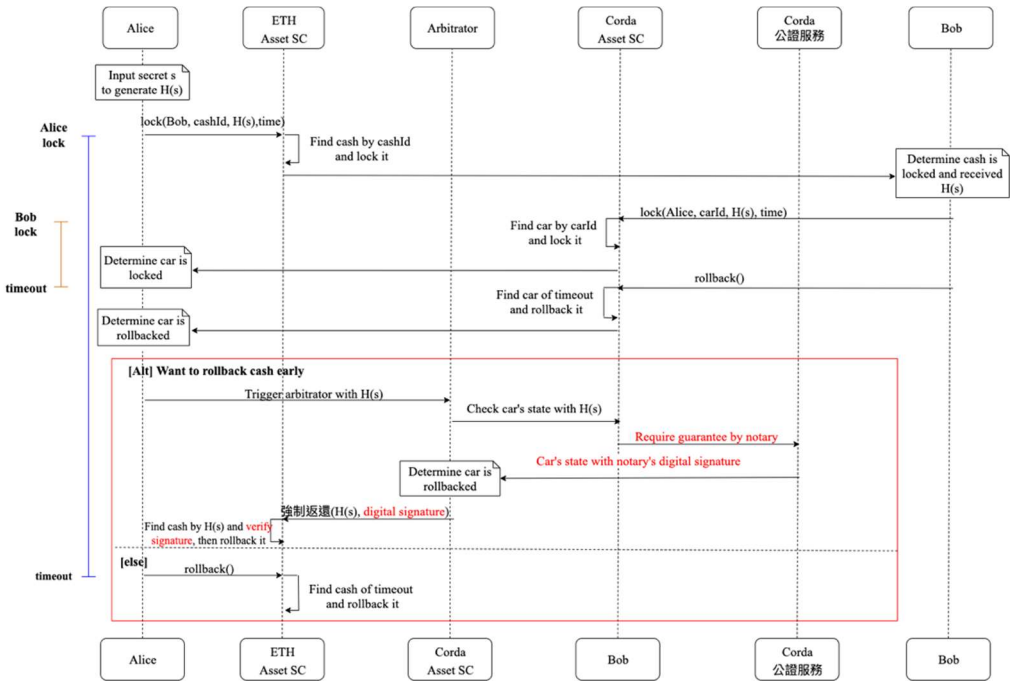
Alice
ETH Asset SC
Arbitrator
Corda Asset SC
Corda 公證服務
Bob
Input secret s to generate H(s)
Alice lock
lock(Bob, cashId, H(s),time)
Find cash by cashId and lock it
Determine cash is locked and received H(s)
Bob lock
lock(Alice, carId, H(s), time)
Find car by carId and lock it
Determine car is locked
timeout
rollback()
Find car of timeout and rollback it
Determine car is rollbacked
[Alt] Want to rollback cash early
Trigger arbitrator with H(s)
Check car's state with H(s)
Require guarantee by notary
Car's state with notary's digital signature
Determine car is rollbacked
強制返還(H(s), digital signature)
Find cash by H(s) and verify signature, then rollback it
[else]
timeout
rollback()
Find cash of timeout and rollback it
Alice
ETH Asset SC
Corda Asset SC
Bob
Corda 公證服務
Bob

圖 5：混合模式 - 強制返還