DeFi Ecology Protocol
去中心化金融生態協議

白皮書 V3.0

摘要：針對當前加密開放金融領域存在的問題，DeFi Ecology Protocol（其通證 DFC，以下簡稱 DFC 協議），提出了包括 DeFi 技術組件和多個通證化協議在內的解決方案，向全球用戶提供安全、普惠、創新、透明的加密開放金融服務。

目錄

1 背景

以太坊智慧合約是一項偉大的發明，它使區塊鏈不再僅僅只是一種電子現金系統，而是具備了邏輯處理能力的圖靈機。但是，基於資產安全等多種考慮，乙太坊智慧合約從一開始就被設計為不可修改不可升級的機制，這就對基於智慧合約的應用開發提出了嚴峻的挑戰。

首先，程式師都有可能犯錯，特別對於合約中的複雜邏輯，更有可能存在無法輕易察覺的問題，即使歷經嚴格反復的邏輯檢查和代碼審計，仍然無法確保所有代碼都正確無誤。潛在問題的改正和錯誤代碼的修復，勢不可免。其次，現實世界是瞬息萬變的，用戶需求也不可能一成不變。一個產品無論在事先考慮得多麼周密和詳盡，在經過運營尤其是大規模運營之後，總會發現已實現需求中的問題，以及亟待實現的全新需求。這就要求智慧合約是可持續反覆運算和升級的。

自從第一個去中心化 DApp 上線以來，資料和資產安全問題就始終是影響甚至毀滅 DApp 的最關鍵因素之一。層出不窮的資產安全事件，持續震動著整個業界。如何最大化地提升區塊鏈應用的系統安全性，全力保護好用戶資產，已經成為橫亙在每一個 DApp 開發運營團隊面前的首要問題。

2 DFC 協議定義

DFC 協定是基於主流區塊鏈系統搭建的加密開放金融服務協定，由一套 DeFi 技術元件和多個通證化協議組成。DFC 協定致力於向全球使用者提供安全、普惠、創新、透明的加密開放金融服務。

2.1 DeFi 技術組件——“The DeFi”

針對乙太坊 DApp 開發中存在的諸如合約不易升級反覆運算、資料結構固化、鏈上交互速度慢、使用者體驗差、缺乏必要基礎設施、安全問題突出等問題，DFC 協定提出基礎元件、擴展元件、金融元件等三大 DeFi 技術組件，合稱為“DFC”。最終目標是讓乙太坊金融服務類 DApp 能夠接近傳統互聯網產品的開發反覆運算速度、使用者體驗，並保留其安全特性。

- **基礎組件**：APEC，即 Assets Protected Elastic Contracts，資產安全的彈性智慧合約。
- **擴展組件**：BEAMS，即 Blockchain Enquiring, Auditing & Messaging System，區塊鏈查詢、審計和消息系統。
- **金融組件**：GEL，即 Global Emergency Lockdown，全域緊急閉鎖；CALM，即 Cooperative Automatic Lockdown Mechanism，協同自動閉鎖機制；MAK，即 Multisig Admin Keys，多重簽名的管理員金鑰。

2.2 通證化協議——“DFC-Tube”

在 DeFi 技術元件的基礎上，DFC 協定將債券融資協定、貨幣借貸協定和去

中心化穩定幣協議集成，形成 DFC-Tube 加密開放金融服務平臺，DFC-Tube 將為個人和企業使用者提供加密數字資產的投資、融資和交易服務，滿足不同使用者的加密數位金融需求。

- **DFC-Tube Bond**：債券融資協議，固定期限、固定利率的數位貨幣借貸服務；
- **DFC-Tube Bank**：貨幣借貸協定，由演算法驅動的活期、可變動利率的通證存借服務；
- **QIAN**：去中心化穩定幣協定，致力於成為加密數位領域具有影響力的穩定幣項目，QIAN 穩定幣可用於投資 DFC-Tube Bond，也可以存入 DFC-Tube Bank 獲取利息。

上述三種協議互相促進，業務間具有較高的關聯性，可以形成聚合效應，有利於業務的協同發展。

3 DeFi 技術組件

3.1 基礎組件 APEC

基於 Solidity 語言的 APEC 平臺是 DeFi 協定的主要基礎元件，APEC 即 Assets Protected Elastic Contracts，資產安全的彈性智慧合約。

3.1.1 設計理念

APEC 作為鏈上（On-Chain）核心架構，基於 Solidity 智慧合約，並且在堅守去中心化和資產所有權的前提下，對合約開發中的不便之處進行了調整和優化。

APEC 的核心理念是資產安全和元件彈性，主要包括以下 3 個方面的特性：

- 資產安全，Assets Protected
- 邏輯可升級，Logic Upgradable
- 資料可擴展，Data Extensible

3.1.2 架構圖

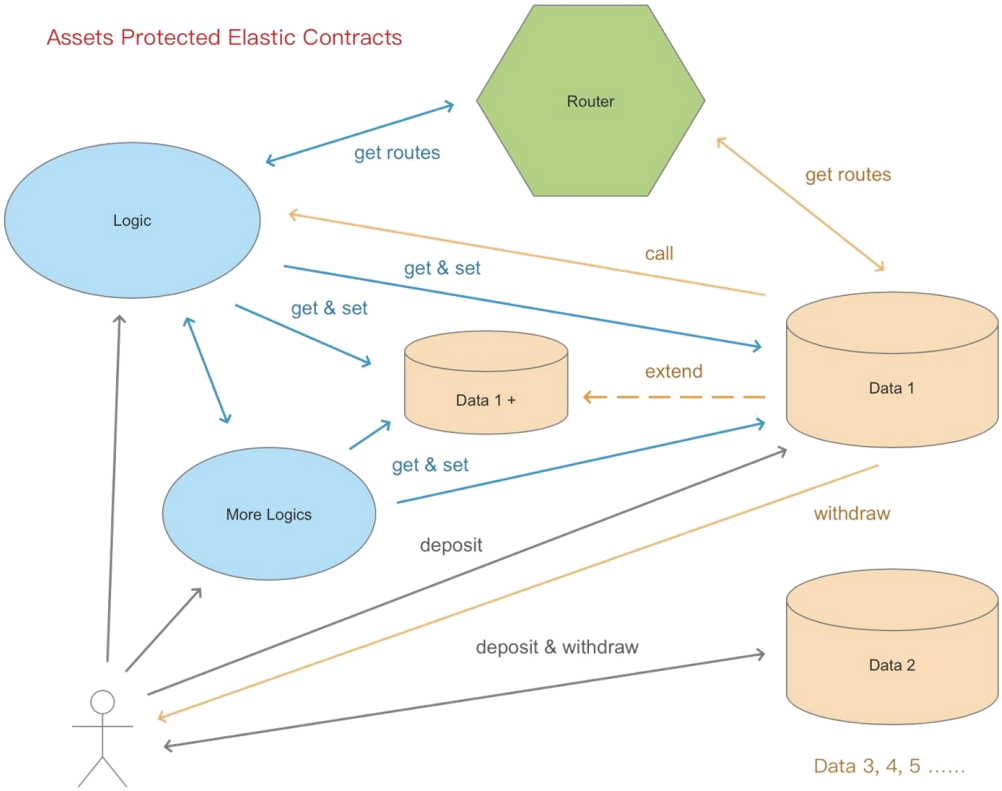

圖 1 APEC 技術架構圖

3.1.3 技術構架

APEC 在整體上可分為 3 大模組：

Ÿ 數據（Data）：把經典合約結構的資料部分獨立出來，做成一個或一組資料合約，用於存儲資料，對外只暴露必要的讀寫介面。

Ÿ 邏輯（Logic）：邏輯合約負責純粹的業務邏輯，不含業務資料。

Ÿ 路由（Router）：業務邏輯所需要讀寫的欄位資料，可根據資料模組和欄位名稱從路由表中查詢，再根據定位結果進行訪問。

路由表

路由表是一個獨立合約，內含一個路由對照表，存儲邏輯合約和資料合約位址的路由映射，可隨系統升級持續更新。

合約系統在整個部署後，各個邏輯合約的位址就會被存儲到路由表中，外部請求可訪問路由表，獲取邏輯合約的位址映射並調用其介面。資料合約也可以通過查詢路由表獲取邏輯合約位址，進行業務邏輯的調用或回檔。

對於每組資料，都會有一個屬於自己的獨立的資料合約，資料合約的位址將會在創建時被自動存儲到路由表中。邏輯合約在訪問指定的資料之前，也會首先從路由表中獲取資料合約位址，再通過位址讀寫資料合約。

邏輯可升級

邏輯合約不存儲資產，不含業務資料，因此就不存在資產安全和資料移轉等問題，所以它是可升級和可插拔的。邏輯合約的新版本在經過測試和審計後，即可部署到鏈上。

部署新合約時會同時更新路由表合約中的映射表資料，更改路由表中該邏輯合約的位址映射指向，以供其它合約或應用前端查詢和調用。

資料可擴展

作為一個可反覆運算升級的應用，它的資料結構往往也要求是可反覆運算的。但出於資料所有權和資產安全的考慮，資料合約不可升級。我們採用的解決方案是擴展。如果業務上需要添加新欄位，這些欄位會被存儲到一個全新的資料合約中。同時，這個新資料合約的位址和內含的欄位名稱，會被添加和更新到路由表中，業務邏輯通過查詢路由表，獲取新欄位的位址路由進行讀寫。

資料合約的擴展，應該是節制和有限度的。一味地增加新的資料合約，會提升整個系統的複雜度和運行效率。資料擴展機制只是把資料結構反覆運算的需求從不可能變為可能，不鼓勵頻繁和隨意地使用這個機制。

我們在設計和使用資料結構時，仍然需要遵循合約的經典設計原則和最佳實踐，設計充足和彈性的資料結構。對於資料的擴展，應始終保持克制的態度，非必要時不使用資料擴展機制。

3.1.4 資產安全

如果邏輯合約可升級，資料合約可擴展，那麼隨之而來的問題就是，使用者的資料所有權和資產安全是否能得到保障。

眾所周知，對於傳統 DeFi 應用而言，用戶的所有資產都被鎖定在合約裡。智慧合約，特別是代碼開源的合約，通過代碼公開的形式向用戶保證，除了用戶自己，沒有其它任何人或程式可以染指使用者鎖定在合約中的資產。更進一步地，合約的不可修改性使得合約一旦部署就不會有代碼的變動。

APEC 採用了職責分離的方式解決了在可升級架構下的合約資產安全問題。

業務合約是可修改和升級的，資料合約則秉承經典合約的理念，不可修改升級。在初始化時，每份資料集合會自動生成一份初始資料合約，這個合約一旦部署到鏈上就不可再修改其代碼邏輯。

- **資料合約會在內部維護一個用戶位址和資產詳情的映射表。**該映射表在資料合約內部，只提供用戶資產的入帳和出賬兩個介面，其它任何介面都無權寫入和更新該資產表。

- 使用者入帳交易，直接發往資料合約位址，調用其入帳介面。用戶資產鎖入合約後，**在資產映射表中記錄該使用者的位址和其資產詳情**。然後再調用邏輯合約，處理和記錄業務邏輯。

- 使用者在出賬交易時，仍然是直接調用資料合約上的出賬介面，**合約將校驗使用者的位址是否存在於資產映射表中**，然後調用邏輯合約，計算出賬數額，最後把資產直接轉帳給用戶的請求位址。

- **任何不在資產映射表中的位址，出賬介面將不回應其資產請求。**在邏輯上保證了任何一份出賬的資產，都屬於當初投資入帳的原始位址，確保了用戶對投資資產的所有權和用戶資產的安全。即使是運營團隊自己，也無法篡改和冒領用戶的任何鎖定資產。

通過資料合約嚴格的所有權約束，保證了用戶資產的所有權和安全性，使得 APEC 的安全哲學秉承了智慧合約的一貫理念：超越了“不要作惡”（Don't Be Evil），實現了“無法作惡”（Can't Be Evil）。

3.2 擴展組件 BEAMS

BEAMS 即 Blockchain Enquiring, Auditing & Messaging System，區塊鏈查詢審計和消息系統。

3.2.1 區塊鏈的局限性

區塊鏈對現實世界幾乎是完全割裂的，它無法主動向鏈下推送消息，如果智慧合約的邏輯出現問題或受到攻擊，現實世界是無法被動感知的。因此我們需要持續地監控合約的運行，嚴格地審計合約中的資料和資產，在出現問題時第一時間發出告警，盡最大可能保證應用的安全。

對用戶而言，區塊鏈交互體驗天然的不友好。區塊延遲導致的非同步回饋，頻繁而大量的鏈上資料讀取和業務模型重建，鏈上和鏈下的消息割裂，都造成了體驗上的緩慢甚至交互上的混亂。

3.2.2 設計理念

上述問題的存在，促使我們去構建一個連接鏈上和鏈下的系統，持續監控合約的運行，審計資料和資產，加快產品的回應速度，使回應速度的波動曲線趨向平滑，讓不可避免的非同步回饋更加順滑和流暢。各種由條件觸發的狀態提醒和消息推送，可以讓用戶在使用 DeFi 應用解決金融需求之外，獲得更為人性化的產品體驗。

BEAMS 是與合約緊密配合的鏈下（Off-Chain）系統，其核心理念主要包括以下 3 個特性：

- 查詢，Enquiring
- 審計，Auditing
- 消息，Messaging

3.2.3 BEAMS 架構圖

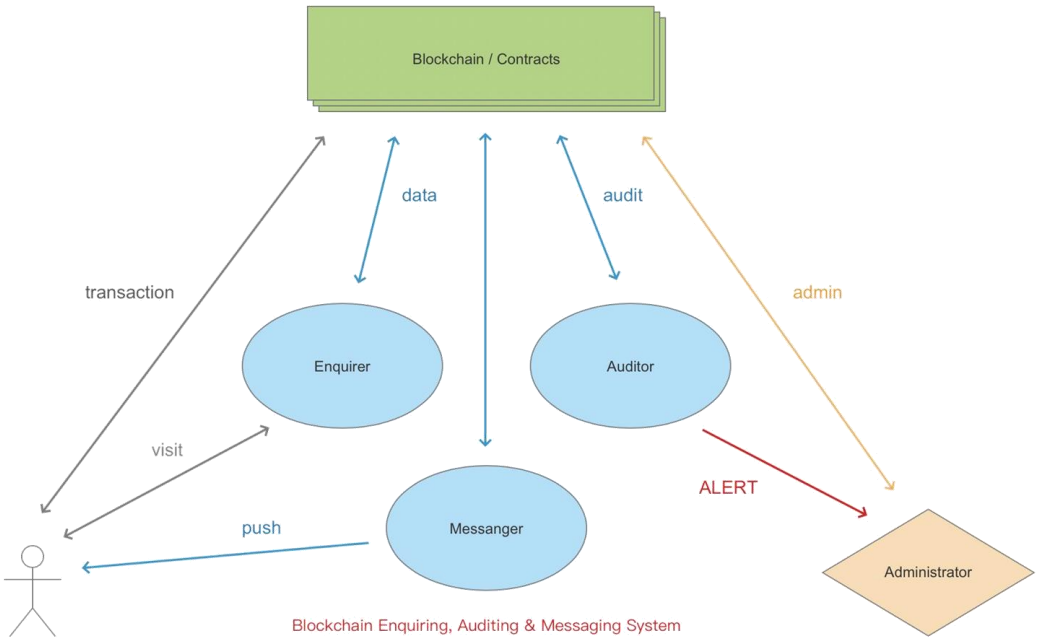

圖 2 BEAMS 技術架構圖

3.2.4 技術架構

BEAMS 由 3 個模組構成，查詢（Enquirer），審計（Auditor）和消息（Messanger）。

BEAMS 採用基於鏈上事件（Event）的輪循機制，監控鏈上合約狀態和資料的變化，基礎資料將會存儲在資料庫中，通過介面提供給前端介面。合約資料的變動會即時並行審計，並將異常情況即時上報給系統管理員。同時對抵押物價值變化和清算等狀態進行持續計算，必要時主動向相關用戶推送各種形式的通知和告警。

資料查詢

涉及資產變動的核心交易，都會觸發自訂的鏈上事件。查詢系統持續地監控新事件的產生，並根據事件內容去查詢相應的合約資料。資料合約向外部提供暴露資料的唯讀介面，查詢系統按照資料模型的要求，從合約中讀取相關資料。

讀取到的資料都將被整理和聚合到 BEAMS 的資料倉庫，並記錄其資料變動情況。資料倉庫作為整個系統的資料核心，將通過後端 API 介面向前端提供准即時的資料緩存，向消息模組提供計算和觸發的所需資料。審計模組也會使用這些資料對鏈上合約的狀態轉移和資料變動進行覆核和審計。

審計風控

審計風控模組將持續監控每個合約的狀態和資料的更改，對於涉及到的資產變動，審計風控模組會使用獨立並行的邏輯對資產變動情況進行二次覆核，如果出現異常，則即時通知系統管理員進行處理。

審計風控模組會使用資產總量、變動邏輯、狀態校驗等不同的覆核方式從各個方向對合約資料進行即時審計，以提升審計的準確性。審計模組可以對異常情況進行評級和告警，風控模組在判斷為極高風險的場景下甚至將有權對鏈上合約的運行情況進行干涉和管理。

審計風控模組還將擔負統計分析的職責，對使用者的訂單記錄，歷史收益，資產變化曲線，平臺的即時收益指標，歷史收益曲線等系統運營資料進行統計和分析，預測和控制風險點，並為產品運營方向提供資料參考。

消息推送

為了提升由於區塊鏈特性導致的非同步回饋的使用者體驗，消息推送模組將在使用者使用流程的各個環節起到重要的作用。特別是在涉及到用戶自身利益的提醒通知和警示消息等方面，缺乏基礎設施的區塊鏈更需要消息推送系統來配合工作。

在頁面一側，消息推送模組將優先使用 Websocket 長連接模式，通過前端頁面和使用者建立雙向即時鏈路，在各個需要執行鏈上交易的環節，監控鏈上交易執行情況，交易結束後，向使用者推送交易結果和鏈上狀態。

而對於資產清算、收益發放、贖回提醒等消息，則由消息推送模組對合約資料進行持續的監控和分析，達到觸發條件後，可以使用包括郵件和短信在內的各種方式，即時對使用者推送提醒通知和告警資訊。

3.3 金融組件

3.3.1 DeFi 金融安全三定律

DeFi 安全哲學可以概括為層級防禦理念的 **DeFi 金融安全三定律**：

Ÿ 保護平臺安全，不受攻擊和入侵

Ÿ 如果受到入侵，保護資產安全

Ÿ 如果資產不再安全，把損失降到最低

DeFi 金融安全體系是一個多層次全方位的體系。去中心化是核心，是基礎，但並不是唯一和全部。一個具備良好可擴展性，能夠應對未來可能存在的千萬數量級用戶，安全可靠具有完備風控能力的開放金融應用，如果僅僅依靠去中心化的基礎設施，是不可能建設成功的。

3.3.2 GEL

GEL 即 Global Emergency Lockdown，全域緊急閉鎖。

在 DeFi 體系，所有涉及到資產變動的智慧合約介面上，都有全域緊急閉鎖開關。如果合約出現問題，可以手動或自動觸發緊急閉鎖，禁止所有的出入帳調用，保護合約內鎖定的資產安全。

3.3.3 CALM

CALM 即 Cooperative Automatic Lockdown Mechanism，協同自動閉鎖機制。

CALM 是鏈下風控機制，採用金融級風控標準，使用獨立的高可用主從熱備集群，7x24 小時不間斷運行。CALM 每 5 秒檢查一次合約狀態，對合約內所有的金融資產進行嚴格的記帳和對賬，一旦發現可能的資產風險，將立即自動觸發全域緊急閉鎖，禁止受波及資產的所有出入帳介面，把資產損失降至最低。同時通知管理人員，啟動運營團隊快速反應機制，人工介入和排查問題。

3.3.4 MAK

MAK 即 Multisig Admin Keys，多重簽名的管理員金鑰。

DeFi 採用管理員金鑰機制，管理員可使用金鑰設置各級許可權，如合約路由的更新，預言機的喂價許可權，全域閉鎖標誌位元的設置許可權，等等。管理員金鑰可以添加、刪除和更新下級許可權，在下級許可權金鑰洩漏時，可迅速更換金鑰。

為了規避管理員金鑰被盜和遺失的風險，我們採用了多簽機制。目前使用的是 3-2 多簽，隨著平臺鎖定資產的增加，我們還會逐步提升至 5-3 甚至 7-5 機制。

以 3-2 多簽為例，合約中保存 3 個管理員金鑰，在進行諸如更換管理員金鑰等最高安全等級的操作時，必須使用至少 2 個管理員金鑰，同時進行多重簽名，該操作才可被執行。

管理員金鑰的多簽機制保證了：

- 如果某個管理員金鑰洩漏，攻擊者使用這個金鑰也無法完成高許可權等級的操作。而平臺管理員可以使用多簽機制將洩漏的金鑰刪除，使之失效。
- 如果某個管理員金鑰遺失，可使用剩餘的管理員金鑰添加新的管理員金鑰，並刪除遺失的金鑰。
- 管理員金鑰多簽才能生效的機制，使每一個高等級的許可權操作都依賴於集體決策和執行，有效地防範了內控風險，進一步保護了資產安全。

4 通證化協議

4.1 債券融資協議——DFC-Tube Bond

加密數位債券（Crypto Bond）是以 token 形式發行和記帳的新型債券，既能為持有加密資產的團隊或個人提供融資服務；也能給加密貨幣市場補充固定收益產品，滿足部分投資者的需求。DFC-Tube Bond 將為加密數位債券提供整套解決方案，包括信用評級、債券發行、債券清算、債券交易等。

4.1.1 債券信用評級

受限於目前加密金融服務仍然不成熟，不適合中長期債券發行，當前加密數

字債券產品類型將以短期債券為主。加密數位債券發行採用註冊制，不需要任何中心化機構審核和批准。債券發行人提交的發債基礎資訊將由 DFC-Tube 平臺自動進行必要的形式化校驗，發債資訊由 DFC-Tube 社區投票確定信用等級後，債券即可正式發行。

債券信用評級（Bond Credit Rating）是對債券違約風險的評測，為用戶的投資決策提供參考，DFC-Tube 平臺採用如下債券信用評級表。

表 1 債券信用評級表

評級	含義
A-1	為最高級短期融資券，還本付息風險很小，安全性很高。
A-2	還本付息風險較小，安全性較高。
A-3	還本付息風險一般，安全性易受不利環境變化的影響。
B	還本付息風險較高，有一定的違約風險。
C	還本付息風險很高，違約風險較高。
D	不能按期還本付息。

DFC-Tube 平臺債券信用評級由社區評級和專業評級組成。社區評級由 DFC 協議生態通證 DFC 的持有者執行，評級人瞭解債券資訊後，將 DFC 鎖倉至相應等級，評級結束後即可取回 DFC 通證。專業評級由專業信用評級機構或專業人士執行，成為專業評級人需要向 DFC-Tube 運營團隊提交申請，提供能夠證明其專業能力和資質的材料。最終評級結果將由社區評級和專業評級共同確定，社區評級權重為 60%，專業評級為 40%。參與評級將獲得評級服務費，評級服務費按同等比例分配。

4.1.2 BondTokens

債券信用評級完成後，加密數字債券即可發行。每份債券以 ERC-20 格式發行，我們稱之為 BondTokens，BondTokens 是投資債券後獲得的投資憑證。每種類型的 BondTokens 都有自己的 ERC-20 合約，包含了該債券的所有必要資訊和相關操作。BondTokens 可任意轉帳，但是不可分割，其票面價值通常為 100 USD。誰持有 BondTokens，誰即是該債權債務關係中的債權人，擁有 BondTokens 即可在 DFC-Tube 平臺兌付本金和收益。

表 2 BondTokens 主要資訊

債券資訊	舉例
發債人	乙太坊位址
債券信用等級	A-3
發行量	1,000,000 DAI
票面價值	100 DAI
發行份數	10,000 份
息票利率	15%
債券期限	30 天
債券起始日	2020-02-01
債券到期日	2020-03-02
是否可贖回	否
是否可回售	否

BondTokens 是一種新型的加密數位資產，不同質押資產、不同到期日、不同利率、不同信用等級的 BondTokens 可滿足加密數位資產市場的多樣化需求，成為其他創新金融應用的基石。

4.1.3 債券清算

若債券底層質押資產出現大幅貶值或者發債人未按時還款時，會涉及到質押資產的清算。DFC-Tube 平臺當前採用折價清算模式，即清算人可以按折扣價格兌換質押物。

為方便計算，設定如下參數：設定目標質押率為 **TCR**，當前債務總計 **CD**，當前質押率 **CCR**，折扣率 **Discount**，質押物當前價格 **Price**，清算前質押物剩餘數量 AC。其中折扣率（1-Dicount）為對清算人的清算獎勵。

債券存續期內清算

債券存續期內，當質押物價值下降 20%後，系統將向債務人發送補倉提醒，當質押物價值下降 30%後，系統觸發質押物處置，系統將清算部分質押物，使得質押率回到初始值。

當

$$CCR \leqslant 70\% \times TCR$$

時，計算清算質押物數量 X，以及清算債務額 Y

$$Y = X \times Price \times Discount$$

其中 X 的計算過程如下。若質押資產不能清償債務，即

$$AC \times Price \times Discount < CD$$

時，全額清算

$$X = AC$$

當質押資產能夠清償債務，即

$$AC \times Price \times Discount \geqslant CD$$

時，清算後質押率需等於目標質押率 PCR，即

$$\frac{(\$)\cdot}{\$\cdot\ \ \cdot} = \frac{\$\cdot}{\$\cdot}$$

求解 X，得

$$X = \cdot(\$\cdot\ \ )$$

逾期未還款清算

債券到期後，若債務人未能還款，系統將觸發質押物處置，系統將清算部分質押物以償還所有債務和手續費，剩餘質押物返還債務人。

若質押資產不能清償債務，即

$$AC \times Price \times Discount < CD$$

時，全額清算

$$X = AC$$

當質押資產能夠清償債務，即

$$AC \times Price \times Discount \geqslant CD$$

時，

$$X = \frac{}{\cdot}$$

剩餘質押物數量（AC-X），發債人可取回。

4.1.4 債券交易市場和債券衍生品

為方便債券持有人提前退出投資，收回本息，DFC-Tube 平臺未來將推出債券二級交易市場。債券持有人可在系統給定的參考定價上自由設定轉讓價格和轉讓數量。投資人可查看債券基礎資訊、信用評級資訊、預期收益等。投資人支付投資款項後即可獲得相應債券的 BondTokens，到期後即可在平臺兌付本息。隨著 BondTokens 的流行，DFC-Tube 平臺將繼續推出更多功能以支持各種債券衍生品，包括：

Ÿ 債券回購（包含逆回購）；

Ÿ 可贖回債券（指債券發行人可在債券到期日前贖回已發行的債券）；

Ÿ 可回售債券（指債券持有人可在到期日前將債券回售給債券發行人）；

Ÿ 其他符合業務需求的債券衍生品。

4.1.5 Bond 模組社區治理

DFC-Tube 致力於推動去中心化（或多中心化）債券發行和結算，系統許可權及核心參數在將來會交由社區管理。但是，在項目初期，為了快速推動項目開發和平臺發展，系統許可權和參數將由 DFC-Tube 開發者維護。DFC-Tube 開發者將秉持公正和透明原則，對系統的任何改動都將及時告知社區。當前，由 DFC-Tube 開發者維護的系統參數包括但不限於：

Ÿ 支援的加密數字資產及其質押率、最大可發債數量、清算折扣等；

Ÿ 債券發行基本參數，如息票利率、債券期限、發行費用、評級服務費等；

Ÿ 時間參數，如信用評級期限、債券發行期限、還款寬限期等；

Ÿ 債券信用等級設置；

Ÿ 可信預言機喂價程式。

4.2 加密貨幣借貸協議——DFC-Tube Bank

DFC-Tube Bank 是一個加密數位貨幣存借協定，支援隨存隨取，隨借隨還。通過部署在區塊鏈系統上的自動程式（智慧合約），出資方可以無摩擦地快速獲得資金收益，有資金需求的借款方在提供合適的抵押物之後就可以快速便捷地獲得財務支援。

4.2.1 設計思路

DFC-Tube Bank 支援使用者將其數字資產存入智慧合約獲得利息收入，同時獲得貸款額度，用戶可以在貸款額度內借出其他數位資產。不管是存款還是貸款，使用者不需要關注借款期限，隨時取回或者還款。

當借款人的未償還借款超過其抵押物限定比例時，系統將扣押使用者資產，進入清算流程。此時，允許套利者調用清算合約，按照一定的折價比例置換扣押資產。由於不同的數位資產在市場規模、流動性、價格穩定性等方面存在區別，其質押率、清算折扣等會有差異，產品相關資訊如下表。

表 3 Bank 產品資訊表

要素	規則
支持幣種	USDT(ERC-20)、USDC、DAI、ETH、WETH、HBTC、IMBTC、QIAN 等
質押率	150%
清算折扣	95%
平倉線	用戶存幣資產之和小於所有借幣資產乘以對應質押率之和時，可對用戶借幣資產進行平倉
借款年利率	1.5% ~ 20%
存款年利率	0 ~ 18%，存款年利率由借款年利率和使用率決定，計算公式：借款年利率 × 使用率 × 0.9
合約中每一幣種用戶可借最大數量	=［（所有存幣資產之和 - 所有借幣資產乘以對應質押率之和） ÷ 對應幣種最小質押率 ］ ÷ 對應幣種價格

頁面中每一幣種用戶可借最大數量	= 合約中每一幣種用戶可借最大數量 ×（1 − 幣種清算折扣）

4.2.2 利率模型

DFC-Tube Bank 採用一套演算法控制的利率模型，基於供求關係的變化，利率自動調節，從而調節借貸總規模、資金供應量等因素。

對於借貸資金的調控，Bank 遵循以下原則：當借貸資金池內的資金借出量較低時，借貸利率上漲的速度較低，以促進借款人從資金池借款；當借貸資金池內的資金借出量較高，甚至接近飽和時，借貸利率上漲的速度較快，帶動存款利率增加，以促進存款人向資金池內存入更多資產。通過演算法調節，確保整個借貸資金池的發展和增長處於健康的範圍。

對資金借出量進行量化，我們引入參數 x，代表資產 a 的資金借出比例，其公式為：

$$= \frac{\text{穩定幣的借出總額}}{\text{穩定幣的借出總額}}$$

設借款利率為 y，y 和 x 的關係可以用分段函數表示如下：

$$\begin{cases} = @ + 0.015; & 0 \le < \frac{3-\sqrt{5}}{2} \\ = N \quad \frac{3-\sqrt{5}}{2} \quad @\$P \quad 0 + 0.015; & \frac{3-\sqrt{5}}{2} \le < \frac{\sqrt{5}-1}{2} \\ = N \quad 2 \quad 0 \quad @\$P \quad @ \quad \frac{\sqrt{5}-1}{2} \quad -(1-)+0.015; & \frac{\sqrt{5}-1}{2} \le \le 1 \end{cases}$$

如公式所示，DFC-Tube Bank 將利率的變化分為了三個階段：

- 第一階段，為了刺激初始階段的借貸量上漲，利率增長模型近似指數曲線，這也符合自然增長規律；
- 第二階段，通過積累一定量的借款額，利率的增長速度進入了穩定期，其圖形為一定斜率的直線；
- 第三階段，由於借出的資金量已經較多，借貸利率的增加速率會加快，以適當的控制資金借出速度，促進存款量增加，利率增加的速度會逐漸逼近一個極值，這一階段的利率變化接近於修正指數曲線。

相對應地，存款利率 SIR 公式為：

$$_9 = \times \quad \times (1-)$$

其中，

x = 穩定幣 a 的借出比率；

y = 穩定幣 a 的借款利率；

s = 調整比率，0 ≤ s < 1，一般可取 0.1。

4.2.3 利率計算

存款年化利率和借款年化利率將轉換成每秒利率，採用連續複利計算。假定 R 為借款年化利率，則每秒利率 r 的計算公式為：

$= 365 \times 24 \times 60 \times 60$

所以，t 時刻的利率：

y = Y$P × [×ΔY

其中，Δt 是指 t-1 時刻到 t 時刻的時間間隔。

因此，假定用戶借款金額為 BA，借款時刻為 t0，還款時刻為 t1, 則到期應還本息和為

× YP / Y_

存款利率和利息計算公式類似。

4.3 去中心化穩定幣協議——QIAN

QIAN 同“乾”和“錢”。在《易經》當中，乾卦代表天，代表宇宙萬物運轉的規律，是最崇高的精神和正向能量。遵循這個重要的涵義，我們將去中心化穩定幣協議命名為 QIAN。QIAN 致力於創造一種人人皆可平等、自由、便捷參與的穩定幣系統，讓每個人都享受無差別和無歧視的金融服務。

4.3.1 QIAN 的設計理念

持有加密資產的用戶，只需要將超額的加密資產鎖定到 QIAN 的智慧合約，就可以獲得等價於法定貨幣的 QIAN 穩定幣，不需要支付任何利息。穩定幣 QIAN 被視為智慧合約對加密資產持有人的貨幣交換證明，我們將這一機制下的智慧合約命名為 CSA（即 Currency Swap Agreement，貨幣互換協議）。

持有 CSA 無利息成本

作為流動性提供者，持有 QIAN 的 CSA 不需要支付任何利息，相反有可能獲得來自于智慧合約的利息作為額外收入，這將刺激債權人長期持有 QIAN 的 CSA，使 QIAN 有了被用於跨境支付、消費支付、資產交易、借貸活動等各類經濟活動的可能。無需持有成本，QIAN 才有可能真正的參與加密開放金融生態的發展過程，與同樣無需持有成本的法幣擔保型穩定幣共同發展，服務不同需求的使用者。

支持閃電貸

目前已知閃電貸（Flash loan）是一項安全的技術，任何擁有資產的智慧合約，都可以選擇對外提供閃電貸服務，通過收取一定量的借貸利息，可以利用自身資產增加更多的收益。目前已經在乙太坊 DeFi 生態中出現了閃電貸的聚合類工具，通過將支持閃電貸的智慧合約的流量進行聚合，可提供更強大的閃電貸服務。QIAN 的智慧合約將支援閃電貸，鎖定在 QIAN 智慧合約裡的加密資產可以獲得額外的收益，QIAN 系統的運營者將定期用獲得的收益在市場上買入 DFC 通證，DFC 作為 QIAN 智慧合約收益的價值貯藏載體，將被鎖入保存 QIAN 系統收益的智慧合約。

風險控制

在 QIAN 的設計中，我們遵循如下的風險管理規則：

首先，QIAN 2.0 秉持超額儲備原則，用戶在使用 ETH 等加密資產生成 QIAN 時，需要滿足一定比例的啟動充足率，鎖定加密資產的價值與生成 QIAN 的價值比例至少要大於 120%。

其次，為了增加 CSA 內鎖定資產的安全性，避免在極端行情下產生爆倉，同時兼顧加密資產的利用率，QIAN 將根據加密資產市場價格的變化速度，引入波動率因數，調控 CSA 的資產鎖定倍數。當價格進行單邊上漲或下跌時，波動率上升，系統將上調 CSA 的啟動充足率。在市場較為平穩的時期，波動率下降，系統將下調 CSA 的啟動充足率。這種設計將有效的減輕市場波動對 CSA 鎖倉

資產的影響，鼓勵使用者在市場平穩的狀態下進行 CSA 鎖倉，增加鎖倉資產的安全性。

第三，當市場行情暴跌時，用戶的 CSA 充足率會下降，在下降過程中，CSA 有預警狀態和凍結狀態兩種變化。例如，某用戶持有 ETH 的 CSA，當其儲備資產充足率下降到 150%（ETH 的預警線）附近，QIAN 系統將會提示使用者補倉。此時，如果行情繼續暴跌，用戶來不及進行補倉，CSA 的充足率繼續下降，當低於 120%以下時，智慧合約將會凍結用戶的 CSA，直到用戶補充鎖定資產到安全水準以上才進行解凍。用戶在補充鎖定資產之前，將不能通過自己的位址發起對於鎖定物的贖回。

第四，處於凍結狀態的 CSA 可能被清算，允許非 CSA 持有者用 QIAN 按照所有處於凍結狀態 CSA 所生成 QIAN 的數值贖回凍結合約當中的資產，這部分內容將在後續平滑套利機制章節詳細闡述。

極端行情之下，QIAN 系統內某幾種或全部儲備資產的充足率可能低於 100%，導致 QIAN 的內在價值支撐不足。如果此時 CSA 持有人普遍沒有意願補充鎖定物，而且底層儲備資產的市場價格在一段時間內都沒有恢復，這將會在 QIAN 系統形成儲備缺口（債務）。在這種情況下，系統會在整體儲備充足率持續低於某一水準，且經過一定的觀察期之後，啟動全域債務拍賣。

在全域債務拍賣裡，系統將解凍由 DFC 基金會所提供的治理通證 DFC 並對外拍賣，拍賣所得的收益將用於彌補整個系統的儲備資產充足率。

總結而言，QIAN 的設計優勢如下：

表 4 QIAN 的設計優勢

對比項	QIAN 2.0	DAI
發行機制	貨幣互換	抵押借貸制
CDP 持有成本	無成本，潛在正收益	成本中到高
CDP 持有風險	中低風險	中高風險
抗極端行情能力	強，待檢驗	弱，已暴露
抵押資產是否有收益	正收益	負收益
對新技術的支援	強	待觀察
生態支持	完善中	較完善
是否有最終購買方	有	有

目標市場	DeFi、實體經濟中的跨境支付、消費支付、資產交易、借貸活動等各類經 DeFi 動	主要局限於濟活
匯率對標的法定貨幣	人民幣	美元

4.3.2 鎖定物管理

QIAN 由用戶向智慧合約鎖定加密資產生成，初期的底層資產將以 ETH、ERC-20 版本的 BTC 等加密數位貨幣為主，待系統穩定運作一定時期後，將考慮納入具備共識的線下資產 token 等加密資產作為發行抵押物。

對於每一種加密資產，系統組態的核心參數包括：

- **市場價格波動率 Vol_i**：由於加密資產的高頻交易特性，QIAN 系統將借鑒目前國際市場上常見的，反映期權價格波動的指標 RV（Realized Volatility），定義加密資產 i 的波動率為 Vol_i。在系統上線初期，Vol_i 將根據預言機的報價間隔進行更新，穩定幣和期權的概念不同，通過近期的已實現波動率即可有效調控底層資產的風險，因此 Vol_i 不涉及對未來波動率的預測。

- **啟動充足率 $Q_{i,0}$**：受到每種加密資產市場價格波動的影響，$Q_{i,0}$ 處於動態的變化中，在 QIAN 系統上線初期，$Q_{i,0}$ 將根據預言機的報價週期進行更新；

- **當前資產充足率 $Q_{i,t}$**：cd@ef@e(a,Y)；

- **最低充足率 $Q_{i,min}$**：加密資產 i 的 CSA 低於某個比例時將觸發凍結；

- **預警充足率 $Q_{i,alarm}$**：$= \frac{g_{k,m}\ n\ g_{k,okp}}{q}$，CSA 低於某個比例時將觸發預警，提示用戶為了保持健康的充足率，需要向 CSA 補充更多儲備資產，但用戶如果不補充，也能正常進行 CSA 的贖回操作；

- **最高鑄幣量**：指該類加密資產在系統中所能鑄造 QIAN 的最大量；

其中，() 為當前鎖定的加密資產 i 總體價值，報價來自預言機，定期更新。

對於特定的加密資產 i，設其可鑄幣量為 H，則有

$$0 < H \leq \frac{cd@ef@e(a) \times c[av@(a)}{q}$$

其中， ( ) 為當前加密資產的市場價格（來自預言機）。

對於系統整體，核心參數包括：

- **全域資產充足率 Q_{total}**：
- **全域最低充足率 Q_{min}**：初始階段，要求 $Q_{min} \geq 90\%$，後續會通過社區治理流程進行調整。
- **債務拍賣觀察時間 $T_{auction}$**：當 Q_{min} 出現後，距離全域債務拍賣開始的時間。

4.3.3 價格波動緩衝機制

設計理念

當前的主流加密資產質押型穩定幣缺少基於波動率指標對平倉和抵押操作進行調整的機制，導致在面對極端行情時，穩定幣系統不能有效緩衝市場波動對於質押資產的影響，在面臨 2020 年 3 月 12 日類似的市場暴跌時，就容易產生質押資產損失，從而影響整個穩定幣系統的均衡性。

因此，在設計 QIAN 系統時，我們綜合考慮了價格、波動率和時間等因素對底層儲備資產的影響。在 QIAN 穩定幣系統引入波動率參數，旨在讓資產價格對穩定幣均衡性的擾動降低，從而能夠最大化的維持系統的整體均衡。

波動率指數

QIAN 將引入波動率指數 V_i，作為衡量底層儲備資產波動率的重要指標。任何資產的價格都會有漲跌，當價格加速上漲或者下跌時，隨著回報率的加速上升或下降，穩定幣的底層儲備資產 V_i 增加，質押風險逐漸的積累增大。此時通過增加啟動充足率 $Q_{i,0}$ 和暫緩清算操作，可以有效的緩衝價格波動對底層儲備資產安全性的衝擊。當穩定幣的底層儲備資產價格變化速度逐漸趨於平穩，此時 V_i 下降，質押風險得到釋放，通過降低 $Q_{i,0}$ 和恢復清算操作，可以讓發生偏離的 QIAN 價格得以回歸。

每日間 RealVol

在傳統衍生品市場，收益率，或稱為已實現波動率（Realized Volatility，RealVol），尤其是每日間的 RealVol，已被廣泛接受作為期權波動率指數（例如 RVOL 和 RVOV 等）的基礎計算參數。由於加密貨幣的交易特殊性，需要對傳統市場的每日間 RealVol 公式進行再設計，以作為穩定幣儲備資產 i 波動率計算的基礎參數。

每日間 RealVol 公式從傳統的標準差公式開始，並在幾個關鍵的方面進行了修改：

Ÿ **年化係數：**RealVol 將年化係數設置為一個常數。由於加密市場 7×24 的交易特性，實際的交易天數應該修正為自然年的天數。由於存在月份的天數變化，最好是有一個近似的常數，而不是有幾種確切但不同的數值，因此在系統上線初期，我們將年化係數定為 360。

Ÿ **更加易讀的表示：**RealVol 的結果通常是一個小於 1.00 的值。我們選擇將 RealVol 的結果乘以 100，以使數值達到更直觀的“百分數衡量”結構。例如，一種加密資產回報率的年化波動可能是 0.20。通常情況下，我們會把這個數字乘以 100，作為 20.00 來傳播。

每日 RealVol 公式

Y= Y / Y$P

其中：

R_t = t-1 至 t 之間的連續複合收益率（Continuously Compounded Return）

ln = 自然對數

P_t = 當日 t 時的基準價（"收盤價"，根據預言機報價源確定具體時刻）

P_{t-1} = 緊接 t 日前一天的基準價（"收盤價"，根據預言機報價源確定具體時刻）

$$= 100 \times \int \sqrt{\frac{360}{n}} \sim q \; y_{Y \bullet P\ Y}$$

其中：

Vol = 日間已實現波動率

360 = 一個常數，代表一年中大約的交易天數。

t = 代表每個交易日的計數

n = 測量時間框架內的交易天數

R_t = 按公式計算的連續複利日收益率。

即時 RealVol 公式

由於加密貨幣的持續交易特性，我們在得出每日間 RealVol 之後，需要進一步計算即時 RealVol。我們將以 30 天為週期，進行即時 RealVol 的計算。

RealVol 每日公式中描述的所有設計項目都與 RealVol 即時公式相同。要將每日值轉換為即時值，需要從 RealVol 每日公式開始，然後合併當前的基礎價格和加權方案。這樣做可以在整個交易日內提供連續的更新，並向 CSA 持有者提供有用的即時指示，以即時瞭解最新的 30 日內，每日已實現的波動性。從

本質上講，即使我們處於新的最近一天（“今天”）內任一時刻，VOL 也能衡量出 30 天的恒定已實現波動率。

舉例來說，如果在當天（n + 1）的交易時間已經過了 80%，我們將使用最新的底層資產即時價格（Underlying Real-time Price，URP）來從昨天的 URP （n）中的對應（80%）部分計算當前日的收益（n + 1）。然後，取計算週期內的第一天，並將該天的收益率加權 20%（100%-80% = 20%）。通過這種方式，我們仍然可以得到 30 天內在任何時間點上實現的波動率的權重，即使實際上有 31 個回報--第 1 天的權重為 20%，第 31 天的權重為 80%，第 2 天至 30 天的權重為 100%。

注意：雖然當日的部分回報是自加權的，因此不需要額外的協同因數，但仍然需要計算當日的自加權部分，以便將適當的剩餘權重應用於第 1 天的全日回報。為了計算出當日的權重，每天的當日時間要取到最接近的一分鐘。由於一天有 1,440 分鐘，所以在 RealVol 即時公式中使用當前時間和一天中的秒數來計算要應用到第 1 天的權重。

當一天的時間等於今天的收盤時間（n+1）時，現在第 n+1 天的權重為 100%，而第 1 天的權重為 0%。因此，由於其權重為 0，原來的第 1 天的收益率從計算中刪除。原來的第 2 天現在變成了新的第 1 天，所有其他的日子也被重新編號。 RealVol 即時公式在這個時間點（我們的例子中是中國標準時間每日 0 點收盤）簡化為 RealVol 每日公式。在市場收盤後的瞬間，我們開始一個新的交易日，回報率被重新編號，這樣又只有 30 個回報率，新的交易日的加權回報率為第 31 天。

$$\mathrm{Vol}_t = 100 \times \int \sqrt{\frac{360}{n} \left(\frac{1{,}440 - m}{1{,}440} \cdot R_{n+1}^2 + \sum_{i=1}^{n-1} R_i^2 \right)}$$

其中：

1,440 = 一天中的分鐘數

n+1 = 今天

m = 從最近一次收盤時間(第 n 天)開始，截至當日的最接近時刻(n+1)的分鐘數

R_1 = 計算週期內第一天(第 1 天)的回報(從第 0 天收盤到第 1 天收盤)

R_{n+1} = 部分回報（使用當前的相關價格和前一天的相關參考價格的回報）。

注：為了澄清，花體"R"表示部分回報，其他所有回報均為全日回報。

啟動充足率 $Q_{i,0}$ 和 $\mathrm{Vol}_{i,R}$ 的關係

如果不加任何調節因數，始終保持 $Q_{i,0}$ 為一個固定值（例如 150%），則在市場波動的情況下，新開倉用戶將暴露於極大的風險之中，在擁有了即時波動率因數後，我們可以將即時波動率的變化值與啟動充足率建立如下關係式：

$$Q_{i,t} = 120\% + e^{(Vol_{R,i,n} - Vol_{R,i,n-1})}$$

其中：

n = 當前時刻

i = 特定資產種類，例如 ETH

$Vol_{R,i,n}$ = 當前採樣點資產 i 的即時波動率

$Vol_{R,i,n-1}$ = 上一採樣點資產 i 的即時波動率

上述關係式反映了波動率本身的變化值，及其對 $Q_{i,0}$ 的調節作用。我們將通過 QIAN 系統的運作對該公式進行持續檢驗，如果發現上述公式存在不足之處，DFC 協議專案團隊保留通過社區治理程式進行修改的可能性。

4.3.4 加密資產平滑套利清算機制

QIAN 系統將根據 Vol_R 的值決定是否開啟套利機制，系統鼓勵在市場波動較低的情況下進行清算，以減緩市場短期恐慌情緒對 QIAN 系統穩定性的衝擊。

在任意時間 t(i)，對於充足率 $Q_{i,t}$，QIAN 系統會存在以下幾種 CSA 狀態：

Ÿ 正常合同 CSA(normal)，$Q_{i,t} > Q_{i,alarm}$

Ÿ 預警合同 CSA(alarm)，$Q_{i,min} < Q_{i,t} \leqslant Q_{i,alarm}$

Ÿ 凍結合同 CSA(frozen)，$Q_{i,t} \leqslant Q_{i,min}$

對於不持有 CSA 的套利者，其贖回行為可能會導致 CSA 持有人的鎖定資產減少。為了兼顧公平和效率，對於平滑套利清算的參與者而言，其在時刻 t(i) 可贖回資產的來源，將被限制在 CSA(frozen)。

在套利過程中，套利者將從儲備資產 i 的整體凍結資產當中套利，具體來說，假設在 t 時刻，QIAN 系統有 100 個處於凍結狀態的 CSA，這些 CSA 一共生成了 100,000 QIAN。此時，任意一個或 n 個套利者可以用不大於 100,000 QIAN 的清算資金，按照出資額大小，從清算合約裡獲得部分/全部凍結資產。在清算過程裡，持有 CSA(frozen) 的所有使用者都會按其被凍結資產占凍結 CSA 內總資產的比例分擔損失。

所有處於 CSA(frozen) 中的儲備資產都可以被套利者贖回，為了使自己不受損失，CSA(frozen) 的持有人必須搶先補充自己 CSA 裡的儲備資產，使其脫離凍結狀態。無論是套利者的贖回操作還是 CSA(frozen) 持有人的補充鎖倉，都能夠有效的提升 QIAN 的資產儲備充足率，讓 QIAN 在儲備資產不足的情況下儘快價值回歸。

這種清算機制的設計既可以促使所有 CSA(frozen) 的持有者補充儲備資產，也平滑了凍結資產的清算速度和數量，盡可能的減緩和減少單個用戶所受的損失，因此，我們將這一機制命名為平滑套利清算。

当 QIAN 系統支援多種加密資產時，平滑套利清算機制將變得複雜。理論上，套利者可贖回系統中的任何一種符合清算條件的儲備資產，各儲備資產之間不存在清算的先後順序。當套利者贖回加密資產時，系統即時動態呈現各加密資產的可贖回量。套利者在可贖回量的範圍內贖回加密資產，將不會大幅改變整個系統加密資產的分佈情況。

各種加密資產的可贖回量始終處在動態變化中，當質押資產 i 已經達到最大贖回比例 R_i 後，客觀上提升了系統的整體儲備充足率，此時質押資產 i 的套利操作受到最大贖回量的影響而暫停，由於 QIAN 是一個多抵押系統，對其他質押資產的套利活動仍將繼續。

4.3.5 債務拍賣

在極端情況下，系統的全域資產充足率 Q_{total} 可能不足 100%，如果市場環境持續低迷，此時的清算套利過程將可能會不順利，套利者的套利意願不足。此時，系統內的儲備資產價值不足，將產生整體債務。為了維持 QIAN 系統的內在價值，系統將解鎖（unlock）治理通證 DFC 並通過拍賣的形式補齊整體各儲備資產的差額，讓系統的整體充足率回到安全線以上，恢復 QIAN 在極端行情下的內在價值。

對於債務拍賣的參與者而言，吸引他們參與債務拍賣的原因，是被解鎖的 DFC 將以低於市場價的形式折價進行拍賣，在 QIAN 的債務拍賣中，會引入最大折價率 Δr。Δr 的初始值設置為 70%，具體數值將由社區充分討論後通過投票進行修改。參與債務拍賣的 DFC 總量為：

DFC- total value in debt auction = œ•žŒžŸ-ŸŽ•

DFC 的拍賣中，起拍價 i

p(start) = ¢Ÿ¡£•Œ¤¡'•(¥¦±) × Δr

拍賣參與者以資產 i 作為報價和結算標的¢Ÿ¡£•Œ¤¡'•()，最終成交價 i(final) 為：

i(start) ≤ i(final) ≤ i(market)

拍賣所得的資產 i 將用於彌補系統債務差額，若有剩餘，則會鎖定到拍賣盈餘合約，以備未來所需。

4.3.6 全域清算

雖然我們長期看好加密資產的發展，但是我們也必須要正視這樣的一個現狀：加密資產仍然處於整體發展的早期，市場暴漲暴跌時常出現，在過往的市場記錄中也曾出現過長達數年的熊市。

雖然 QIAN 穩定幣有著一系列的穩定機制，但是仍然有可能在發生市場極端行情並且市場長期低迷的情況下，即使通過債務拍賣也仍然無法彌補整個系統的儲備資產充足率。如果發生了這種情況且持續一段時間，將意味著整個 QIAN

穩定幣系統喪失了內在價值的支撐，我們在這種情況下，將通過社區治理的流程，探討是否進行全域清算並且關閉 QIAN 穩定幣系統。一旦社區治理通過了 QIAN 穩定幣系統的關閉議案，則將會啟動全域清算。

在全域清算狀態下，QIAN 穩定幣系統將會首先凍結所有 CSA，關閉 CSA 的生成功能，其次關閉預言機喂價，並且以最後一次預言機喂價的價格作為系統全域清算的參考報價。此時，系統狀態再次發生改變，以最後一次預言機報價為准，持有 CSA(normal) 的用戶將能夠優先向合約贖回自己的鎖定資產，系統將處理這部分使用者的資產贖回操作。在 CSA(normal) 的持有用戶贖回資產完成之後，系統內如果仍然存在儲備資產的剩餘，則將允許 CSA(alarm) 的持有用戶進行贖回。

在全域清算狀態下，使用者是否能夠拿回全部鎖定資產，不受到損失，這是不確定的。能夠全額贖回鎖定資產的概率，依次為 CSA(normal) ＞ CSA(alarm)，不同的底層儲備資產的數量、市價等因素會對贖回成功的概率形成綜合影響。

4.3.7 QIAN 系統治理

QIAN 系統的主要參與者包括 QIAN 鑄造者，QIAN 持有者及治理通證 DFC 的持有者。系統治理的目的在於平衡所有參與者的利益關係，在一定權衡和取捨的基礎上，維持系統的穩定和持續健康發展。

QIAN 鑄造者在系統中主要承擔的風險是儲備資產價格下跌，系統鎖定後導致的贖回風險，享受的利益包括獲得流動性、價值貯藏、風險對沖等功能。基於對行業中類似方案的研究，我們認為，在合理的風險範圍內，QIAN 的鑄造應該是被鼓勵的，這有利於 QIAN 系統的發展，所以我們設計了可調整的利息機制。 QIAN 持有者的核心訴求在於其匯率穩定性，因此我們設計了匯率穩定調節機制。

DFC 持有者將是整個系統最後收益或風險的承擔者，平臺的管理是通過 DFC 持有者進行投票確定的，被投票選中的提案可以修改 QIAN 平臺的內部管理變數，這些變數包括但不限於：

- 增加新的儲備資產
- 選擇可信任的預言機
- 調整利息
- 調整閃電貸利率
- 風險參數：每種儲備資產的債務上限、初始鎖定比例、可贖回上限、預警線等。

5 生態擴展

當前，DFC 協定已基本完成乙太坊上的 DeFi 技術組件，以及債券融資、貨幣借貸、去中心化穩定幣等通證化協議的開發。未來，我們將擴展這些通證化協議至其他區塊鏈系統，包括 ETH2.0、幣安鏈和波卡等。

5.1 Ethereum 2.0

ETH 2.0 是新一代乙太坊。它是一個完全不同的項目，在區塊鏈的架構上採用了全新的思路。ETH 2.0 的目標是提高乙太坊的可擴展性、安全性和可程式設計性。不同於 ETH 1.0 只能達到 15 TPS 的輸送量，ETH 2.0 每秒可處理上千至上萬筆交易，同時不用降低其去中心化程度。

ETH 2.0 是一個巨大的飛躍，它的分片技術將有可能使得主流鏈錨定幣成為可能，那它事實上將成為一個連接所有區塊鏈的跨鏈系統。如果 ETH 2.0 做到了這一點，再結合它的高併發事務執行能力和 PoS 特性，也將成為跨鏈平臺的典範。

DFC 協議將會充分利用 ETH 2.0 在技術上的巨大優勢，第一時間隨著主鏈的升級，把當前應用平滑遷移到最新的穩定版本上，緊跟乙太坊升級的步伐，引領 DeFi 金融平臺業務模型和技術升級的發展趨勢。

另外，基於乙太坊 2.0 的 POS 特性，用戶的 ETH 資產鎖定到 QIAN、Bank 等智慧合約將仍能獲得 ETH 挖礦獎勵，QIAN、Bank 等合約在未來可以形成類似于礦池的功能，同時繼續提供原有的金融服務，讓使用者的 ETH 資產進行最大化利用，創造更多的價值。

5.2 幣安鏈及幣安智能鏈

幣安鏈（Binance Chain）是一個由社區驅動的區塊鏈軟體系統，由全球各地的開發者和貢獻者組成。它是一條專注轉帳和交易區塊鏈資產的公鏈，著重于性能、易用性和流動性。是一條為 DEX 量身打造的交易公鏈。幣安鏈推出了 BEP2 通證標準，可在其上發行自訂的通證。尤其是幣安鏈已支持主流通證錨定幣，如 BTC、ETH、XRP、BCH、LTC、TRX。這些錨定幣再配合幣安鏈基於 Cosmos 的跨鏈特性，就給 DFC 協定的跨鏈 DeFi 金融應用提供了無限想像空間。

2020 年，幣安鏈的開發團隊發佈了通過並行鏈擴展幣安鏈功能的方案：幣安智能鏈。該方案在保留幣安 DEX 的高性能撮合的前提下，實現對開發者友好的智慧合約功能。

結合幣安鏈的秒級事務和高 TPS 特性，BEP2 主流錨定幣，以及幣安智慧鏈的 EVM 相容性，DFC 協定在乙太坊上的 DeFi 應用可以無縫拓展到幣安鏈和幣安智能鏈生態體系中。屆時，基於幣安鏈生態，通過主流通證的價值互換，高併發的金融交易，相容良好的虛擬機器，DFC-Tube 將會成為重要的跨鏈 DeFi 金融平臺。

5.3 波卡

波卡是一個允許不同區塊鏈以一種無信任成本的方式傳輸消息、資料、價值的平臺。可以同時共用它們的獨特功能和安全性。簡單來說，波卡是一種可擴展的異構多鏈技術。波卡是獨立跨鏈技術的引領者，它的中繼鏈、平行鏈和轉接橋理念，可能將成為通用跨鏈技術事實上的標準。通過波卡跨鏈體系，主流鏈將會通過跨鏈機制進行良好的通證價值互換和事務協同。

DFC 協議將會對波卡進行持續深入的研究和實踐，基於波卡體系進行 DFC 協議應用的原型驗證和適應性開發。隨著波卡系統的完善和逐步上線，DFC 協議將考慮把 DFC-Tube 體系逐步拓展到波卡生態中，在跨鏈金融應用賽道上保證持續的競爭領先地位。

6 DFC 協定生態通證

6.1 DFC 通證用途

6.1.1 參與 DFC-Tube Bond 評級投票

社區評級人持有 DFC 協議生態通證 DFC 即可參與債券信用評級。投票人瞭解債券發行資訊後，將 DFC 鎖倉至投票等級，評級結束後即可解除 DFC 鎖定。

專業評級由專業信用評級機構或專業人士進行。成為專業評級機構或個人需要向 DFC-Tube 運營方提交申請（後期審批權將會被移交給 DFC-Tube 社區），提供能夠證明專業能力和資質的材料，並向系統鎖倉 100 萬 DFC 通證。鎖倉通證在評級期間以及所評級項目存續期間不可取回。

6.1.2 參與 QIAN 的穩定性調節

通過閃電貸，鎖定在 QIAN 智慧合約裡的加密資產可以獲得額外的收益，QIAN 系統的管理委員會將定期的使用獲得的收益在市場上買入 DFC 通證，DFC 作為 QIAN 智慧合約收益的價值貯藏載體，將被鎖入保存 QIAN 系統收益的智慧合約。當 QIAN 系統認為需要激勵鑄幣者以提升 QIAN 的流通量時，系統會支付利息給新創立 CSA 的用戶，支付的利息以 DFC 通證的價值進行計算，發放的利息也是 DFC。

6.1.3 參與 QIAN 的全域債務拍賣

在極端情況下，QIAN 系統的全域資產充足率可能不足 100%，如果市場環境持續低迷，套利者的套利意願不足，進而導致系統內的儲備資產價值不足，將產生整體債務。為了維持 QIAN 系統的內在價值，系統將解鎖（unlock）治理通證 DFC 並通過拍賣的形式補齊整體各儲備資產的差額，讓整體充足率回到安全線以上。

6.1.4 參與 DFC-Tube 的治理

DFC-Tube 平臺的治理是通過 DFC- 持有者投票進行的，被投票選中的提案可以修改和調節 DFC-Tube Bond、DFC-Tube Bank、QIAN 的系統關鍵變數。

6.2 DFC 通證分配計畫

DFC 通證總量 10 億，永不增發。在 DFC 協定發起團隊主導下，將會有 85% 的 Token 用於社區建設和社區捐贈計畫，其中社區生態建設占 30%，DFC 協議

基金會占 25%，戰略投資者及社區捐贈占 30%。剩餘 15%的 Token 將為 DFC 協議創始團隊和 DFC-Tube 開發團隊預留，作為他們在專案初期做出貢獻的獎勵，以及作為後續新團隊成員的激勵。分配給團隊的 token 鎖倉 3 年，首次公開交易后 12 個月釋放 30%，24 個月後釋放 30%，36 個月後釋放 40%。

6.2.1 社區生態建設

社區生態建設包括但不局限於:DFC 協議區塊鏈應用(DFC-Tube)生態治理和激勵、開發者社區建設、商業合作和產業合作、市場行銷推廣、學術研究、教育投資、法律法規等。

6.2.2 DFC 協議基金會

我們已經在新加坡註冊非營利性 DFC 協議基金會，該基金會主要任務是負責 DFC 生態的搭建和運營、開發戰略方向的制定、DFC 通證發行及管理等，公開透明地管理由通證捐贈而獲得的資金。

6.2.3 戰略投資者及社區捐贈

根據專案發起及運營需求，我們將會預留 30%的通證回饋戰略投資者及社區成員的資助。基石輪投資由團隊創始成員們自籌資金完成，出於對項目的長期看好和自我激勵，團隊決定在基石輪所投入的資金對應的 DFC 通證永不解鎖。

7. 研發路線圖

2020 年 4 月，專案啟動，白皮書設計，官網上線；
2020 年 8 月，推出中心化點對點借貸產品—幣幣貸；
2020 年 12 月，推出基於 EOS 的試驗性借貸 DApp；
2021 年 2 月，項目通證 DFC 在公開市場開放交易；
2021 年 3 月，上線基於 Ethereum 的點對點借貸 DApp—Pawn；
2021 年 5 月，在 Pawn 內上線 Bank 借貸功能；

2021 年 8 月，上線去中心化穩定幣 QIAN，支援 Ethereum 網路；

2021 年 9 月，推出加密數位債券 DApp — DFC-Tube Bond；

2021 年 12 月，將借貸、穩定幣、債券集成至 DFC-Tube，形成一站式 DeFi 平台；

2022 年 4 月，穩定幣 QIAN 2.0 上線；

2022 年 7 月，推出 DeFi 應用安全協定元件；

2022 年 9 月，與其他公鏈合作 DFC-Tube 業務，如 Binance Chain、Polkadot 等；

2022 年 10 月，在無法獲得銀行服務的東南亞地區使用者中推廣 QIAN 的使用；

2022 年 12 月，推出實體企業加密債券試點業務；

2023 年 3 月，QIAN 穩定幣開放技術聯盟成立，發展 QIAN 穩定幣全球合作夥伴。

參考文獻

An Introduction to Smart Contracts and Their Potential and Inherent Limitations [EB/OL].https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Implementation of Smart Contracts Using Hybrid Architectures with On- and Off-Blockchain Components [EB/OL].https://arxiv.org/pdf/1808.00093.pdf

Robert Leshner and Geoffrey Hayes. Compound: The Money Market Protocol [EB/OL]. *https://compound.finance/documents/Compound.Whitepaper.pdf*

MakerDAO. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System [EB/OL].*https://makerdao.com/en/whitepaper*

Wikipedia. Federal Reserve [EB/OL].*https://en.wikipedia.org/wiki/Federal_Reserve*

Wikipedia. United States Treasury security [EB/OL].*https://en.wikipedia.org/wiki/United_States_Treasury_security*

Fedreal Reserve Bank of New York. How Currency Gets into Circulation [EB/OL].*https://www.newyorkfed.org/aboutthefed/fedpoint/fed01.html*

Wikipedia. Quantitative easing [EB/OL].*https://en.wikipedia.org/wiki/Quantitative_easing*

Wikipedia. 香港外匯基金 [EB/OL].*https://zh.wikipedia.org/wiki/香港外匯基金*

MBA 智庫·百科. 貨幣發行制度 [EB/OL].*https://wiki.mbalib.com/wiki/貨幣發行制度*

香港金融管理局. 強方兌換保證 [EB/OL].*https://www.hkma.gov.hk/gb_chi/news-and-media/insight/2005/05/20050519*

香港金融管理局. 外匯基金資產負債表摘要及貨幣發行局帳目 [EB/OL].https://www.hkma.gov.hk/gb_chi/news-and-media/press-releases/2018/04/20180430-4/

潘攀（北京大學金融法研究中心）. 港幣的發行及其穩定機制 [J]. 金融法苑, 1999, 14（總第二十六期）: 52 頁

朱孟楠. 香港外匯基金的發展及投資策略的選擇 [J]. 國際經濟合作, 1997, No.6: 39~42 頁

Prashant Bhayani & 譚慧敏（香港首席投資策略師）. 為何我們不擔心港幣聯繫匯率制度 [EB/OL].*https://wealthmanagement.bnpparibas/asia/cns/news/hkd-peg.html*

瞿新榮. 美聯儲重啟擴表，美元發行的邏輯與油價 [EB/OL].*https://www.guancha.cn/QuXinRong/2019_10_13_521093_s.shtml*

中信期貨研究員 姜沁. 美國國債的規模管理體制、發行體制以及流通管理體制 [EB/OL].*https://finance.sina.com.cn/money/DFC-ex/DFC-exroll/2018-10-19/doc-ifxeuwws5814324.shtml*

中國金融期貨交易所. 美國國債期現貨市場研究報告 [EB/OL].*http://yjs.dwfutures.com/uploadfiles/2013/8/20130806142789838983.pdf*

DAppTotal. 穩定幣 [EB/OL].*https://dapptotal.com/stablecoins*

CEIC. 中國香港特別行政區 外匯儲備 [EB/OL].*https://www.ceicdata.com/zh-hans/indicator/hong-kong/DFC-eign-exchange-reserves*

CEIC. 中國香港特別行政區 貨幣供應 M1 [EB/OL].*https://www.ceicdata.com/zh-hans/indicator/hong-kong/money-supply-m1*