JIBREL NETWORK

2017 年 5 月

第二版草稿

YAZAN BARGHUTHI
yazan@jibrel.network

VICTOR MEZRIN
victor@jibrel.network

摘要

Jibrel Network 旨在促進貨幣、債券和其他金融工具等傳統資產在區塊鏈上的數位化、上市與交易。Jibrel DAO可讓平台使用者存入現金、貨幣市場工具或創造自己的「密碼編譯存託憑證 (CryDR)」，從區塊鏈上 / 區塊鏈外套利交易獲益。過度暴露在數位貨幣的去中心化機構與資金，可透過穩定資產對沖持倉並保護資金。此外，Jibrel 會為開發人員提供完整平台，建構運用資產擔保的代幣憑證進行交易、投資與對沖的工具和應用程式。

另外，Jibrel 還能透過點對點 (P2P)、企業對企業 (B2B) 或消費者對商家 (C2M) 等管道，以法定貨幣 (Fiat) 對法定貨幣交易的形式做到即時、幾乎零手續費的全球付款與匯款。

本白皮書概述了 Jibrel 的組成核心元件、元件間互動的方式，並意圖展示如何使用現有基礎架構高效建構網路。

1.介紹

在 2009 年因為比特幣 (Bitcoin) 而為人所熟知之後[1]，區塊鏈 (Blockchain) 已展露巨大的價值。我們能夠透過這項新科技，在無法變更的去中心化帳本中驗證並認可交易，還能更廣泛的應用，以達成去中心化一致性。

這項令人難以置信的創新目前正逐漸讓我們擺脫對全球各產業內中介機構、結算/清算公司與仲介服務供應商的需求，一步步改變著這個世界。

話雖如此，但由於僅能在機構層級採行，因此加密經濟的大部分價值仍僅限定於特定使用案例或地理區域。此外，也由於這些經濟孤島 (Silo) 在傳統資產與數位資產之間轉換的挑戰與限制帶來瓶頸，而普遍有著體系風險。

即使傳統經濟與加密經濟之間有著差異，但前者所遭遇的難題仍困擾著後者。希望在各種傳統貨幣之間互相轉換的使用者，當合併使用加密貨幣兌換、傳統金融機構以及付款處理單位時，同樣會面臨一樣的時間延遲與應支付的手續費。

此外，能夠促進傳統資產在區塊鏈外快速流動的傳統個人與機構投資者，也由於現有的基本不相容性（尤其是缺乏透明度與極端的市場波動）而不想參與[2]。

最後，透過眾售、去中心化資金和密碼編譯投資人籌資的去中心化組織過度暴露於數位資產與加密貨幣，限制了往傳統持有形式多元拓展的選項。

數位貨幣扮演多重角色這件事讓風險進一步加劇：數位貨幣被用來獎勵促進交易的礦工，是轉讓價值的手段、是投機性的投資工具，最近也被用於群眾集資與去中心化組織和應用程式的營運（例如去中心化運算[3]、去中心化儲存[4]）。

在傳統金融中，上述各功能都使用不同的工具，且受到相應的監管。這樣有助於管理體系風險。在充分建立去中心化監管共識協議之前，加密經濟面臨未受監管匯兌方面的安全性與詐騙風險，也由於這種極度波動的貨幣被用於設計目的以外的用途而產生市場風險，更由於透過這種高波動性數位貨幣進行群眾集資以及後續受到智能合約的約束而衍生出體系風險[1]。

本報告分析了目前環境的限制與挑戰，並提出運用現有基礎架構為所有利害關係人提供解決方案的方法。

2.傳統資產擔保代幣憑證

Jibrel 生態系統的核心利害關係人有：希望獲得加密貨幣與區塊鏈技術所創造價值（例如低匯款手續費和及時轉帳等）益處的非投資型使用者；希望從新興加密經濟獲得高報酬的傳統投資者；希望以穩定的低收益資產擴展其加密持股的去中心化組織 / 基金和密碼編譯投資者。

讓區塊鏈獲得傳統金融工具的穩定性，能成功滿足所有利害關係人的需求。以他們所代表的基本傳統資產一對一支持打造栓式憑證，就能達到這個目的。透過這種方法，可將栓式憑證用來表示貨幣[5]甚至商品[6]。

1 專案有著無法實質化的風險，因為若資金由於市場低迷而減少，可能導致無償償能力

只要開發出能夠持有傳統資產同時核發基礎資產擁有權憑證的「擔保人」，就能讓貨幣、商品、貨幣市場工具和其他金融工具廣泛的在區塊鏈上公開交易。

3.系統架構

下節概述了 Jibrel Network 的關鍵元素，以及有助於將傳統資產放到區塊鏈上的必備因素。

3.1公開區塊鏈
雖然對另一個區塊鏈的依賴會帶來大量新的挑戰與限制，但直到完全跨鏈通訊可行之前，早期版本的 Jibrel 仍需要公開而安全的區塊鏈。

3.2加密貨幣匯兌
加密貨幣匯兌為一般使用者提供了使用當地貨幣的法定貨幣帳戶，以及持有加密貨幣的數位錢包。使用者可購買、交易或傳輸數位貨幣，在加密貨幣與法定貨幣之間輕鬆轉換。

3.3栓式憑證
若要建立傳統資產擔保代幣憑證，需要栓式憑證。對於所持的每一筆傳統資產，必須打造一個栓式憑證。基礎資產售出時，憑證就會銷毀。

3.4擔保人
為確保栓式憑證有相應價值，需要擔保人。擔保人會持有傳統資產並核發相應的栓式憑證，同時也會在基礎傳統資產的擁有權被釋出 / 移轉時，對憑證進行贖回或銷毀的操作。

3.5應用層、程式庫與範本
一旦奠定栓式憑證，就能運用其功能開發一系列應用程式，包括付款處理工具、匯款錢包與交易平台。為利於迅速的應用程式開發，需要一個專屬應用層，提供易用程式庫與程式碼範本。

3.6擁有權移轉
核發栓式憑證後，就能以與所有加密貨幣類似的方式，輕鬆交易其基礎資產。高階流程概述如下：

1. 使用者將法定貨幣 (FIAT) 傳給擔保人
2. 擔保人給使用者 jFIAT
3. 使用者以 jFIAT 付款給商家
4. 商家兌換 jFIAT
5. 擔保人將法定貨幣轉到商家帳戶

有了擔保人支持栓式憑證，保證基礎資產能於未來時間點兌換，憑證就能維持在系統內，運用於區塊鏈上與區塊鏈外的付款。

3.7費用與收費
數位與傳統資產的擁有權移轉都會產生費用與收費，應予考慮。

3.8監督 / 監管
代表區塊鏈外擁有權或價值移轉的所有區塊鏈上交易，都必須滿足國際與當地法規，且必須受到相應的管理。

應擬妥法規協議 / 管理工具，確保正確的管理與監督。

所有交易必須滿足 KYC / AML 規範。

4.JIBREL NETWORK 實施方式

本節概述 Jibrel Network 中實施各元素的方式。

4.1乙太坊 (Ethereum) 區塊鏈
所選區塊鏈必須與採礦獎勵以及系統參與者之間的基礎交易拖鉤。因此，乙太坊很適合構成 Jibrel 基本架構的基礎。採礦獎勵會採用乙太坊「Gas」（燃料，工作量衡量單位）的形式提供，而任何栓式憑證都不會與採礦流程有關[7]。

雖然 Jibrel 也適合以比特幣的 Omniprotocol 當作基礎來打造，但這已超出本文討論的範圍。

4.2密碼編譯存託憑證 (CryDR)
CryDR 是代表 Jibrel 所持有基礎傳統資產擁有權的栓式憑證。在本文中會以 jAsset 表示（例如 jUSD、jEUR、jGBP）。發行當時，Jibrel 會支援六種法定貨幣以及兩種貨幣市場工具，日後規劃新增其他金融工具。

4.2.1貨幣 / 法定貨幣
Jibrel Network 的第一個開發時程旨在支援美元、歐元、英鎊、俄羅斯盧布、人民幣和阿聯酋迪拉姆，且會在整合策略性匯兌合作夥伴時逐漸新增其他貨幣的支援。

4.2.2貨幣市場工具
穩定的低收益資產是 Jibrel 的核心產品服務，密碼編譯投資人可購買「美國國庫券」與「零息存款證明」的栓式憑證。在 Jibrel Network 的第一個開發時程中，所有貨幣市場工具都會包含*自動轉倉*或*累積*機制。也就是說，從期滿投資中收到的法定貨幣會自動重新配置到相似資產中。同樣的，紅利或利息也會累積到基礎資產期滿或售出為止。在日後版本中，將可配置貨幣市場工具。

4.2.3其他金融工具
在未來，隨著傳統金融機構整合到 Jibrel 平台，將能充分支援其他金融工具，包括上市與私募股權投資。

4.2.4智能循規
由於 CryDR 可充分編寫，因此可嵌入監管成份。法定貨幣將不受限制，但其他資產的購入與轉售將受到類別與地理區域的限制，以充分符合規定。每份 CryDR 都嵌有這樣的邏輯。

4.3Jibrel DAO
Jibrel DAO 會代表傳統資產的擁有者接收 / 持有資產，並核發相應的 CryDR。之後立即傳送到擁有者的錢包。贖回憑證後，憑證會遭到銷毀，其基礎資產會移轉給憑證持有人。

雖然 Jibrel DAO 以完全去中心化為目標，但在傳統金融機構充分整合到區塊鏈上之前，系統的大型元素仍必須位於區塊鏈外。區塊鏈外的活動需要當地與國際監管機關的投入與監督。

因此必須妥善管理利害關係人互動，確保徹底遵守法規且不致犧牲透明度與可靠性。這一點會透過*資產入口網站 (Asset portal)* 達成，也就是於各自地理區域營運、充分合法的專屬實體。

4.4資產入口網站
在將傳統資產轉換為區塊鏈上數位資產的過程中，資產入口網站用來進行必要的法律與金融步驟。

法定貨幣入口網站將會是簡單的加密貨幣匯兌。可以就現有交易所建立起策略性合作關係，亦可打造充份分佈於各地理區的 Jibrel 專屬匯兌網路。此外，將一部分的 Jibrel 法定貨幣儲備金保留在現有交易所中，能大幅降低轉帳時間與費用，同時為交易所提供所需的流動性。

非法定貨幣入口網站必須位於區塊鏈外，才能進行必要的盡職調查，取得非法定貨幣存款的擁有權。

在大部分的地理區域，資產入口網站需要經紀人與資金撥付執照。若涉及管制嚴格的司法管轄區或更細微的金融資產，可能需要監管機關的全面介入與監督。

隨著法規的演進，資產入口網站將能夠去中心化並由社群主導。機構投資者與其他金融機構將能使用 jibrel 平台將其傳統資產上市到區塊鏈上。

4.5Jibrel Network 憑證 (JNT)
雖然非法定貨幣入口網站會以法定貨幣收取*離線費用*，但 Jibrel DAO 的區塊鏈上費用與佣金將以 Jibrel Network 憑證 (JNT) 的形式收取。

5.基礎架構

使用者餘額和交易等關鍵資料會儲存於區塊鏈，其他資料則寄存於開發伺服器上。

現在已開發出多種開發環境、工具與架構，能做到去中心化應用的迅速開發[8]。Jibrel 必須研發類似的開發人員元件、工具與架構，以廣泛採用與散佈 CryDR。

基礎架構必須跨兩大主要領域：區塊鏈上 API 與區塊鏈外 API / Utils。

5.1區塊鏈上基礎架構
網路只需要四份金鑰智能合約就能有效運作。

5.1.1CryDR 智能合約
在 Jibrel DAO 註冊的每筆資產，都具備一份以智能合約形式核發的 CryDR。CryDR 智能合約會符合 ERC-20 標準。在使用者帳戶之間轉送 CryDR，會類似於在錢包之間轉送其他 ERC-20 憑證。

5.1.2Jibrel DAO智能合約
會有一份專屬 Jibrel DAO 智能合約規範 CryDR 智能合約的運作。

5.1.3董事會智能合約 (BODC)
董事會智能合約 (BODC) 是互動 / 影響 Jibrel DAO合約的唯一機制。

BODC 會受到投票系統管理，其中董事會成員可使用自己的乙太坊帳戶就 BODC 行動進行投票。成員必須對私密金鑰的儲存與使用負責。在理想狀況中，董事會將由密碼編譯思想領導者和金融服務專家所組成。

圖 1密碼編譯存託憑證——一般流程

5.1.4助理 / 公用程式（輔助智能合約）
我們也必須建立許多輔助智能合約才能提供輔助功能，例如在執行不同版本的合約之間轉換，以及啟用其他 API 功能等。

其詳細描述超出本文討論範圍。

5.2區塊鏈外基礎架構

為了促進將 CryDR 廣泛採用於交易、投資與對沖工具上，會發行適用於應用程式開發人員的易用程式庫與程式碼範本。

圖 2 Jibrel DApp API 工作流程

5.2.1程式庫與範本
我們希望開發人員使用現有程式庫與乙太坊區塊鏈 (例如 JS web3) 互動。我們會發行這些程式庫與程式碼樣本的包裝函式，簡化與 Jibrel DAO 和 CryDR 智能合約的互動方式。

5.2.2CryDR 檔案總管
我們會建立開放源碼檔案總管，讓使用者檢視 CryDR 中繼資料、與 BODC 互動，以及手動驗證 Jibrel DAO 基礎資產的擁有權。

5.2.3董事會工具組
我們會建立工具，作為 CryDR Ltd 內部 IT 基礎架構與乙太坊區塊鏈之間的介面。尤其會用於董事會成員與 BODC 互動的籌劃，以及系統狀態的運作狀況監控。

6.智慧型監管的實施

本節概述 Jibrel Network 內 CryDR、智慧型監管與法規遵循的實施方式

6.1CryDR 架構

CryDR 本身就是部署至乙太坊區塊鏈的智能合約。為了做到穩健而可擴充的系統，CryDR 應滿足多項需求：

高相容性：應使用與現有憑證管理工具相容的 ERC20 介面
可更新的商業邏輯：應可輕鬆更新，以跟上不斷演進的實際規則與規範
不變性：部署之後就不應改變
可移轉：事件與儲存內容應分開存放
互動功能：CryDR 之間應能彼此互動

6.2現有方法
這些技術需求很難使用乙太坊生態系中目前能使用的工具達成。智能合約的升級難以實施，而雖然目前已有特定工具和方法，但各有其限制。

6.2.1EVM DELEGATECALL
第一種可能的方法運用乙太坊虛擬機器 (EVM) 中的「DELEGATECALL」運算碼。

這雖然是更新商業邏輯的強大工具，卻有許多缺點。具體而言，一旦部署，整個更新過程中都必維持原始智能合約的儲存架構。因此，這種方法只能用於簡易可升級合約的實施，無法用於 Jibrel 的使用案例。

6.2.2智能合約刪修
另一個可能的解決方案是刪修合約並部署另一份新合約到相同的位址，保存事件與狀態。雖然這對於 Jibrel Network 可能會是理想的解決方案，但 EVM 中尚未實施。

6.3Jibrel Network 方法
在打造 Jibrel 時，我們運用一套更加繁瑣但全面化的解決方案——我們將整個系統解構為多份可彼此互動、提供流暢升級與更新的細緻智能合約。

這樣的實施複雜度更高，但能為 Jibrel DApp 提供強大的後端。

6.3.1CryDR 3 層系統
CryDR 可解構為其關鍵元件：

儲存（Storage）：放置所有資料
視圖（View）：第三方合約與網路應用程式的介面
控制器（Controller）：實施法律合規與商業邏輯，協調儲存與視圖合約

圖 3階層式架構

6.3.1.1更新法規遵循性
有了這個架構，我們就能輕鬆部署全新 CryDR 控制器合約，配置要使用這個新控制器的視圖與儲存。

這樣能讓我們有效的輕鬆更新支持 CryDR 的基礎法律合規與商業邏輯，我們稱之為智慧型監管。

圖 4控制器更新

Jibrel Network 藉由促進讓商業邏輯得以更新的流程，能夠隨著實際法規的變革一起演進，確保憑證能夠充分合法。

6.3.1.2升級介面
使用此架構，還能讓我們流暢升級憑證介面，例如可提供新憑證標準（如 ERC223）的其他支援。

圖 5視圖升級

進行這類升級時，CryDR 儲存會維持不變 / 不受影響。

因為視圖的階層在控制器之前，因此所有事件在更新過程中都會維持不變。實施完善的控制器會觸發所連線的所有視圖，讓用戶端可以接收到所有事件。

圖 6觸發事件

6.3.2智慧型監管的架構

實施 KYC/AML 措施需要嚴格而詳盡的帳戶許可控制。
智能合約有著先天限制，主要是這種合約只能存取區塊鏈上的資料，原始設計禁止合約呼叫第三方服務。

為了存取區塊鏈外資料，必須先以交易形式將資料推送到區塊鏈上。

簡單來說，所有法規遵循措施都必須透過智能合約實施於區塊鏈上。

為了實施 KYC/AML 措施，我們必須實施兩種解決方案：

資料儲存：將使用者資料儲存於區塊鏈上
規則實施：在各交易上套用 KYC / AML 規則

許多專案都處理第一項任務，如 Civic 和 uPort 等。但這些解決方案是專為適應性與多用途而打造，所以只能儲存一般使用者資訊，不足以滿足機構等級的 KYC / AML 處理需求。

因此，Jibrel 會建立專用的法規遵循 API，在專用 Jibrel KYC / AML 模組與目前可用第三方解決方案之間扮演聯繫功能。

圖 7Jibrel 法規遵循 API

6.3.3Jibrel Network 憑證 (JNT) 的角色

Jibrel Network 的其中一項關鍵商業需求，就是所有的 CryDR 都必須栓定於某筆基礎資產。為了達到這一點，區塊鏈外資產必須先進行證券化，這也是需要虛擬兌換貨幣的原因。除了要與網路進行交易，還要促進區塊鏈外費用的付款。

比特幣 (BTC)、以太幣 (ETH) 等現有貨幣並不適合，因為這些貨幣的價格波動與 Jibrel Network 中的效用無關。這樣的脫節帶來了市場與信用風險。此外，Jibrel Network 旨在於未來提供專屬區塊鏈，須有專屬憑證才能促進流暢的移轉過程。

CryDR 本身由於必須一直栓定實際資產，不適合用於此解決方案。在付款流程中運用 CryDR 會導致另一方面的脫節，造成系統失衡。

Jibrel Network 憑證 (JNT) 會當作網路的「燃料」或稱為「Gas」。JNT 會為 Jibrel Network 及相關 Jibrel DApp 提供的所有功能給予通用存取權。

JNT 會確保所有 CryDR 始終都栓定個別的基礎資產，增加額外一層法規遵循性。

圖 8Jibrel Network 憑證互動

7.充分去中心化的運作

在短至中期內，會需要區塊鏈外活動，以進行必要的法律與金融盡職調查，將實體資產轉換為數位資產。此外，也需要董事會成員監督 Jibrel DAO，確保充分透明度與遵循法規。

長期來看，法規應會演進而能夠促進資產擁有權的區塊鏈上驗證，讓 Jibrel 成為去中心化自治組織。

7.1自助式入口網站

區塊鏈上運算能力、實施複雜零知識證明的可行性[2][9]、取得相關授權的法規障礙等技術限制一旦獲得克服，Jibrel 就能營運自助式入口網站網站（即託管於區塊鏈上、與 Jibrel Network 通訊的傳統兌換平台）。

這些入口網站的建立對於 Jibrel 達成充分去中心化非常重要。

7.2區塊鏈上數位身份 / KYC / AML

雖然目前有許多區塊鏈上數位身份與 KYC 解決方案，但其功能仍然有限。需要更先進的身份解決方案，才能做到自助式入口網站。

7.3董事會去中心化自治組織

一旦營運達到穩定狀態，就能解散董事會，以自治監管實體取代董事會的功能來監督 Jibrel DAO 的營運。

8.使用案例

可輕鬆匯兌的傳統資產擔保憑證提供了廣泛的使用案例

8.1傳統 / 數位資產匯兌

讓傳統資產和數位資產得以自由互相交換，本質上就能將傳統投資工具大規模銷售給尋求穩定數位資產的投資者與實體，為機構投資者開發出一個促進低風險、高報酬的平台。

8.1.1投資平台

客户可將貨幣市場工具或商品存進 Jibrel DAO，再將這些產物 (CryDR) 以較高價格銷售給去中心化組織與基金，從*區塊鏈上 / 區塊鏈外套利* 獲益。

8.1.2對沖憑證

去中心化自治組織與基金可購買貨幣市場 CryDR 並存放於區塊鏈上，有了充分透明度，可讓投資者安心確認自己的資金安全無虞。去中心化自治基金可從廣泛的傳統資產中選擇，以補足其數位產品組合，並防止加密經濟衰退。

8.2全球轉帳

提供資產擔保憑證可讓平台得以提供同時具備傳統資產（尤其是穩定性與全球採用）與數位資產（不變的特性、易於移轉與可靠）優點的憑證。

有了這些憑證，就能實施付款閘道、匯款管道與其他金錢轉帳等使用案例。

8.2.1匯款

Jibrel 能夠讓法定貨幣和法定貨幣間使用密碼編譯基礎架構執行交易而進行轉帳，做到匯款功能。使用者可運用數位貨幣提供的低廉費用新增資金並轉帳給世界上任何一個人，同時享有傳統貨幣的穩定性與安全性。

8.2.2通用錢包

可建立貨幣不可知錢包，讓使用者自由轉換貨幣，並以任一種貨幣轉帳給任何地點的任何人，不致被收取這類交易一般需要的高額手續費。

8.3跨境付款

同樣的，Jibrel 也能提供跨境付款功能。

8.3.1貨幣 API

有了基礎憑證，Jibrel 就能提供貨幣 API，讓使用者在各種貨幣間自由轉換。

8.3.2商家 API

Jibrel 可為商家提供簡單易用的付款閘道，接受任何貨幣的款項，並以當地貨幣對外支付。無須匯兌或轉帳費用。

一旦建立起網路，商家就能使用 Jibrel 的易用程式庫和 API，設定貨幣不可知付款閘道。

---

2 雖然目前在改善可能性核對證明 (probabilistically checkable proof) 的效率方面，已經花費了很大努力，但這種方式仍高度不實用

9.引用

[1] Nakamoto, Satoshi, *Bitcoin: A peer-to-peer electronic cash system*, 2008 - URL - {https://bitcoin.org/bitcoin.pdf}

[2] Brennan and Lunn, Credit Suisse Equity Reports - *Blockchain - The trust disruptor: Shared ledger technology and the impact on stocks*, 2016 - URL {http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf}

[3] Golem, *The Golem Project: Crowdfunding White Paper*, 2016 - URL {http://golemproject.net/doc/DraftGolemProjectWhitepaper.pdf}

[4] Wilkinson, Shawn, *Storj Project: A Peer-to-Peer Cloud Storage Network*, 2014 - URL {https://storj.io/storj.pdf}

[5] Tether Ltd, *Tether: Fiat currencies on the Bitcoin blockchain*, 2016 - URL {https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf}

[6] Eufemio, Chng and Djie, *Digix: The Gold Standard in CryptoAssets*, 2016 - URL {https://dgx.io/whitepaper.pdf}

[7] Buterin, Vitalik, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2013 - URL {http://ethereum.org/ethereum.html}

[8] Solidity, *Solidity: A contract-oriented, high-level language for the Ethereum Virtual Machine*, Release 0.4.10 Documentation - URL {http://solidity.readthedocs.io/en/v0.4.10/}

[9] Ben-Sasson, Chiesa, Garman, Green, Miers, Troma and Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 - URL {http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf}