

Libra XS 去中心化穩定幣系統

白皮書

目錄

一、背景.....	- 1 -
二、Libra XS 概述.....	- 2 -
Libra XS 穩定幣.....	- 2 -
三、Libra XS 網路.....	- 2 -
BFT 共識機制.....	- 3 -
四、穩定幣的獲取.....	- 3 -
1、抵押物.....	- 3 -
2、抵押生成穩定幣.....	- 3 -
3、穩定幣的使用.....	- 3 -
4、抵押物的贖回.....	- 3 -
五、雙層穩定幣模型.....	- 4 -
1、抵押債倉.....	- 4 -
2、基於匯率的互換機制.....	- 4 -
六、價格穩定機制.....	- 5 -
七、Libra XS 穩定幣通證經濟.....	- 7 -
八、網路治理.....	- 8 -
1、改變抵押物類型.....	- 8 -
2、修改風險參數.....	- 8 -
3、穩定費率的調整.....	- 8 -
4、預言機的選取.....	- 9 -
5、其它參數的調整.....	- 9 -
九、穩定幣的清算.....	- 9 -
1、部分清算.....	- 9 -
2、全域清算.....	- 9 -
免責聲明.....	- 10 -
風險提示.....	- 11 -

一、背景

貨幣作為一般等價物，具有價值尺度、流通手段、支付手段、貯藏手段和世界貨幣這五種職能。以比特幣為代表的加密貨幣由於其匿名性以及無國界性，在國際轉帳等方面承擔了部分流通手段的職能。但是因為加密貨幣劇烈的價格波動，它們在價值尺度、支付手段、貯藏手段方面，幾乎起不到任何作用。因此，穩定幣應運而生。作為數字貨幣的一種，它既保留了加密貨幣簡單易用、自由流通等特徵，又與法幣掛鉤，是一種理想的交易媒介。

截至 2020 年 6 月，穩定幣市值已經超過 110 億美元。根據是否有抵押資產，穩定幣可以分為有抵押型穩定幣和無抵押型穩定幣。其中，有抵押型穩定幣又分為法幣抵押型穩定幣（USDT、GUSD、TUSD、PAX 等）和數字資產抵押型穩定幣（DAI、EOSDT、USDJ 等）。



由中心化機構 Tether 公司發行的 USDT，市值已經達到 92 億美元，佔據穩定幣市場的 82%，Tether 公司刪除了白皮書中持有 100%抵押資產的承諾。2019 年 10 月，Tether 及其關聯公司、附屬實體因涉嫌操縱加密貨幣市場而被紐約州總檢察辦公室起訴，檔中稱 Tether 通過欺詐性的增發，從而操縱加密貨幣市場，引發了數十億美元的損失。Tether 可以在沒有美元支撐的情況下自行發行 USDT，並轉移到 Bitfinex 帳戶中買入加密貨幣，使 USDT 成為加密貨幣市場的不穩定因素之一。

除了在國際貨幣體系中占主導地位的美元之外，歐洲各國、日本、韓國等發達國家，也存在對於穩定幣的市場需求。但已發佈的穩定幣專案，幾乎都選擇錨定美元，在國際匯款中確實可以部分代替 swift 國際資金清算系統。但在國際化進程中的今天，除美元外的其它法幣在跨境貿易結算、建立離岸市場、跨境投資等方面也取得了巨大進展。因此，錨定其它法幣的穩定幣專案的發展已經迫在眉睫。

二、Libra XS 概述

為了實現“讓資產在全世界範圍內自由流通”的願景，非盈利組織 Libra Xs Foundation 決定發行一類錨定法定貨幣的去中心化穩定幣，其價值與法幣 1:1 錨定。抵押資產、抵押率的確定以及資產清算等治理過程，都由持幣者共同投票決定，並由區塊鏈上的智慧合約自動完成。因為市場上已經有很多種錨定美元的數字貨幣，但錨定人民幣、日元、韓元等法幣的穩定幣卻很少，因此 Libra XS 將首先開發針對 CNY、JPY、KRW 的穩定幣。在白皮書中，我們將說明 Libra XS 區塊鏈是怎樣實現穩定幣的發行、贖回、治理以及穩定幣的價值穩定等核心功能。

Libra XS 穩定幣

Libra XS 的目標是成為可在全世界自由流通的穩定幣系統，以減少交易摩擦，讓全球支付更方便、快捷，實現法幣與法幣、法幣與數位貨幣、數位貨幣與數位貨幣之間的互相轉換，它包含以下應用場景：

- 1). 數位貨幣與法幣的出入金橋樑
- 2). 以穩定幣定價的數位貨幣交易對
- 3). 穩定幣避險
- 4). 線上、線下支付消費
- 5). 跨境支付及大宗交易
- 6). 儲值、投資理財

三、Libra XS 網路

隨著比特幣的減半和以太坊網路中應用的增加，比特幣和以太坊網路中的轉帳手續費不斷提升，網路擁堵與高昂的手續費已經對網路的繼續發展造成限制。要想開發可在全世界自由流通的去中心化穩定幣，Libra XS 首先要打造一種新的區塊鏈基礎設施，其中的穩定幣也是建立在 Libra XS 區塊鏈安全、可擴展以及可靠的基礎之上的。初期，Libra XS 區塊鏈起初將由 Libra XS Foundation 管理、開發和運營。隨著時間的不斷發展，逐漸向公共節點開放，最終實現完全去中心化。

BFT 共識機制

Libra XS 區塊鏈採用基於 Libra XS 共識協議的拜占庭容錯 (Byzantine Fault Tolerance, 簡稱 BFT) 機制。

假設分散式系統擁有 n 台節點, 並假設整個系統拜占庭節點不超過 m 台 ($n \geq 3m + 1$), 拜占庭容錯系統需要滿足如下兩個條件:

所有非拜占庭節點使用相同的輸入資訊, 產生同樣的結果。在區塊鏈系統中, 可以理解為, 亂數相同、區塊演算法相同、原帳本相同的時候, 計算結果相同。

如果輸入的資訊正確, 那麼所有非拜占庭節點必須接收這個消息, 並計算相應的結果。在區塊鏈系統中, 可以理解為, 非拜占庭節點需要對客戶的請求進行計算並生成區塊。

BFT 機制不要求所有節點都能正常工作, 只要故障節點不超過 $1/3$, 網路即可正常運行。

四、穩定幣的獲取

1、抵押物

價值穩定的抵押物是專案安全的前提。在項目初期, 抵押物只包括市值前三的加密貨幣, 即 BTC、ETH、USDT。為了獲得 Libra XS 中的穩定幣, 投資者需先持有 BTC、ETH、USDT 中的至少一種。

2、抵押生成穩定幣

以 BTC 和 ETH 為例, 首先發送一個交易到區塊鏈網路中創建抵押債倉 (Collateralized Debt Position, 簡稱 CDP), 然後將抵押資產託管到特定的區塊鏈位址中, 按照符合條件的抵押率生成穩定幣, 抵押率需大於投票決定的最低抵押率。

3、穩定幣的使用

Libra XS 發行的是一種可程式設計的去中心化穩定幣, 用戶持有穩定幣可用於抵押借貸、跨境支付、線上線下支付等場景。

4、抵押物的贖回

贖回抵押資產時需保證帳戶中的穩定幣數量大於等於借出的數量, 並使用抵押物支付相

關費用。

五、雙層穩定幣模型

大多數去中心化穩定幣專案都會發行兩種代幣，例如 Maker DAO，一種為穩定幣 DAI，另一種為治理代幣 MKR。這樣的多幣系統操作起來將會比較複雜，而且其中的穩定幣將沒有任何價值捕獲能力。為了簡化區塊鏈的應用，Libra XS 在穩定幣機制上創新性的採用了一種雙層穩定幣機制，僅通過一種穩定幣實現網路治理與價格穩定。

1、抵押債倉

大多數數位貨幣抵押型穩定幣都採用 CDP 機制生成，該機制下生成的穩定幣已成功運行多年（例如 Maker DAO 的 DAI），下面我們將先介紹 Libra XS 的 CDP 穩定幣系統。

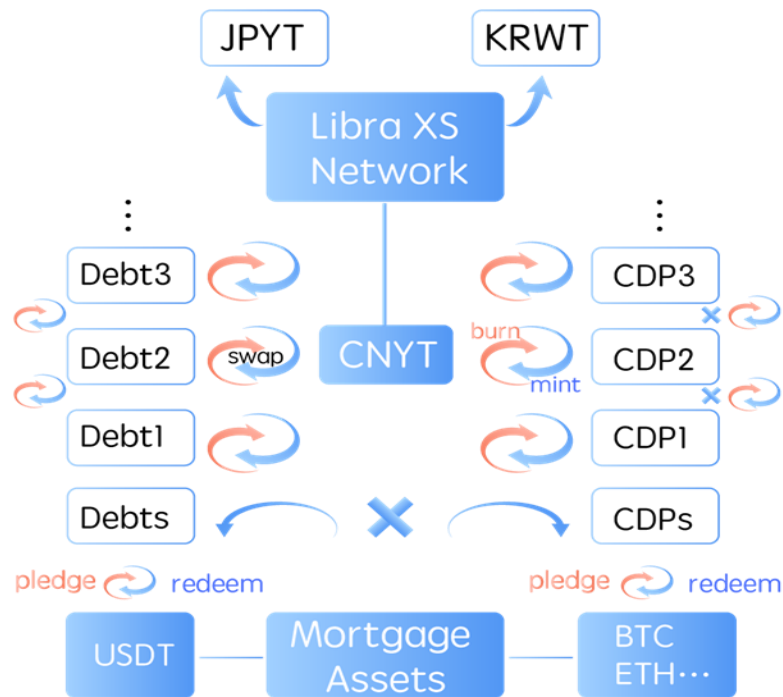
CDP 是區塊鏈網路上的一種智慧合約，用戶可以將自己的抵押資產託管到智慧合約中，從而生成穩定幣，在歸還穩定幣時贖回自己的抵押資產。為了保證有足額的抵押資產，抵押品的價值將始終高於債務本身，也就是超額抵押。穩定幣系統的最低抵押率由投票決定，但不得低於 120%。在 Libra XS 網路中，BTC、ETH 的初始最低抵押率為 150%，隨著抵押品價格的下跌，抵押率將下降，用戶可以隨時補充自己的抵押資產。當抵押率小於最低抵押率時，債務將被清算，執行清算將繳納部分罰金，以促使使用者自行維護其 CDP。

抵押資產生成穩定幣實際上是一種借貸過程，因此需要支付一定的穩定費，穩定費率由節點共同投票決定。穩定費的一部分將用於維持網路運行，剩餘部分將分發給持幣用戶。

2、基於匯率的互換機制

BTC 與 ETH 的價格波動較大，為了保證債務能夠足額償還，因此需要採用 CDP 機制進行超額抵押。但對於主流國家的法定貨幣，匯率出現大幅波動的概率不大。為了在保證安全的情況下，盡可能的擴大網路的使用範圍，抵押 USDT 將借出 100% 的穩定幣，但需支付一筆一次性的兌換費用。任何人在二級市場上買入的穩定幣都可以用於償還其他人用 USDT 借出穩定幣生成的債務，這將有利於穩定幣的價格始終趨近於法幣，下一章將詳細介紹項目的這一優勢。

在本系統中，抵押債倉機制可以借用 BTC、ETH 較大的市值，吸引更多的用戶參與，做大穩定幣規模；匯率互換機制將有利於吸引外部參與者，並自我實現穩定幣價格的穩定，如下圖所示。



六、價格穩定機制

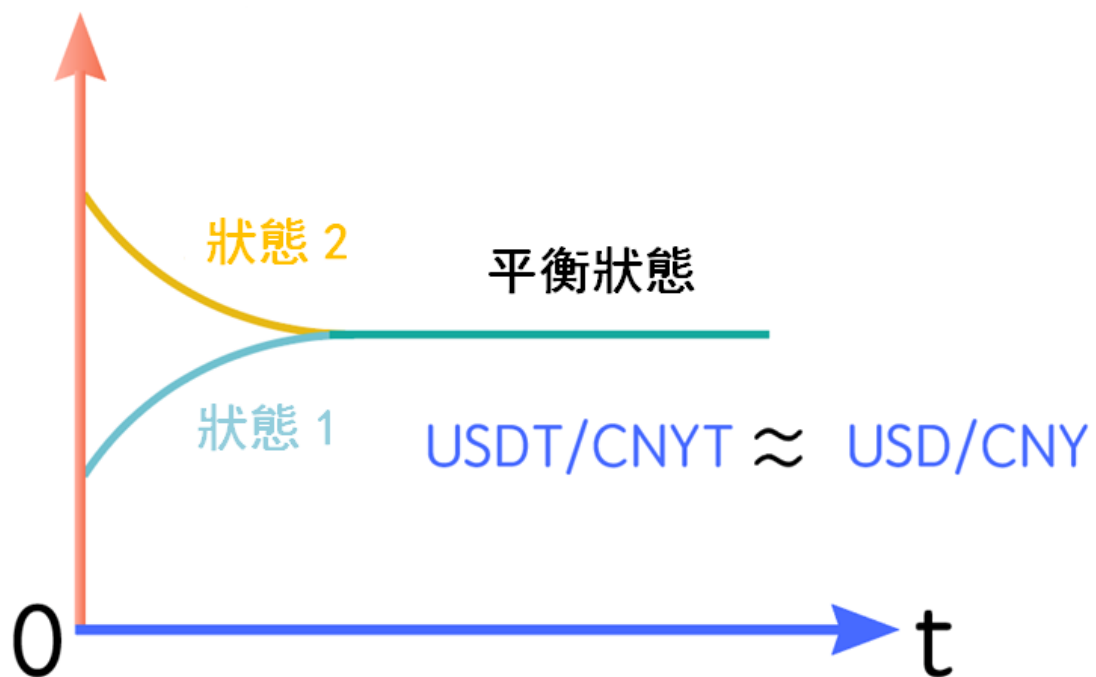
Libra XS 協議創新性的通過對不同的抵押物採取不同的償還機制的方式，以使系統中的價格自行穩定在法幣附近，下面以錨定人民幣的 CNYT 來說明。

對於比特幣和以太坊，穩定幣系統採取 CDP 機制，抵押率 > 150%。用戶借出 CNYT 後，償還債務時也將返還抵押資產。

而以穩定幣 USDT 為抵押物，在 CNYT 協議中可以生成近乎等值的 CNYT，任何人都可以用 CNYT 贖回他人抵押的 USDT。

CNYT 的彈性供應/贖回機制使系統中只有一種代幣，但仍能保持穩定幣價格接近於 1 人民幣。當 CNYT 的價格明顯低於 1 元人民幣時，用戶有動力在二級市場中購買 CNYT，並用 CNYT 以真實人民幣的價格贖回 USDT，以減少 CNYT 的供應量，推升 CNYT 的價格。當 CNYT 的價格明顯高於 1 元人民幣時，使用者可以在 CNYT 協議中以 USDT 按 USD/CNY 的匯率抵押借出 CNYT，並在二級市場上賣出，增加 CNYT 的供應，降低 CNYT 價格。

我們以一種動態平衡過程來說明 USDT 和 CNYT 的價格關係，如下圖所示。假設 USD/CNY 的匯率是 7.05，理論上 USDT/CNYT 的匯率也應該是 7.05，但在實際中匯率將圍繞這一值上下波動。當 CNYT 高估的時候，CNYT 可以在市場上換取更多的 USDT，會促使用戶以 USDT 借出 CNYT，並在市場上賣出，以賺取額外的 USDT。這樣可以增加流通的 CNYT，降低 CNYT 的價格。同理，當 CNYT 價值低估時，用戶可以在市場上以 USDT 買入 CNYT，在系統中償還他人的債務，獲得更多的 USDT，降低 CNYT 的



流通量，提升 CNYT 的價格。最終，USDT 與 CNYT 的價格將達到動態平衡，並使

USDT/CNYT \approx USD/CNY，即 1 CNYT 對應 1 CNY。

無論 CNYT 價格過高還是過低，CNYT 的價格都將通過與 CNY 直接聯繫，而穩定在 1 人民幣附近。因此，CNYT 協議可以通過 CNYT 本身實現價格的穩定。

為了使抵押資產中有足夠的 USDT，可以調低 USDT 與 CNYT 的兌換費用，以爭取更多的做市商。

七、Libra XS 穩定幣通證經濟

在 Libra XS 網路中，任何穩定幣都是通過在智慧合約中抵押代幣獲得的。基於的雙層穩定幣模型，只要一種穩定幣可以同時起到價值穩定、治理與價值捕獲的作用。最終，可能實現真正的零費用借貸。

穩定幣系統中費用的來源：

1. 穩定費用。以 BTC 和 ETH 為抵押物生成穩定幣的過程相當於借貸，因此需向系統支付一筆穩定費，穩定費由債務餘額、穩定費率、債務償還週期共同決定。
2. 兌換費用。以 USDT 為抵押物生成 Libra XS 中的穩定幣的過程類似於兩種法幣間的互換，不需要支付隨著時間變化的穩定費，但需要支付一筆固定比例的兌換費用，任何人以系統中的穩定幣償還該筆債務時都將再次支付兌換費用。
3. 罰金。當用戶的抵押率小於最低抵押率時，將觸發清算。雖然剩餘的抵押資金將還給使用者，但需要繳納一筆罰金，促使用戶維持好自己的 CDP。
4. 抵押資產生息。抵押在系統中的都是流動性非常好的 BTC、ETH、USDT 等數位資產，因此以後可能通過投票授權將部分抵押資產通過智慧合約轉移 Uniswap 等去中心化應用中獲取額外收益。

所有的費用都將以一定比例計入風險準備金，風險準備金的上限由投票決定，風險準備金的可能花費：

1. 匯率波動的影響。因為 USDT 與系統中穩定幣基本按照 1:1 兌換，如果在系統產生債務後法幣升值，則需要償還借款人更多的 USDT。但最近幾年法幣匯率的波動都很小，這一項風險很小。當匯率波動加大時，可以考慮限制兌換比例。
2. 應對系統故障。如預言機的報價更新不及時等，系統清算不及時將導致損失，這部分費用也將由風險準備金支出。

持幣用戶的收入：

當系統收到的費用減去風險準備金後有剩餘時，收入將給到持幣用戶，在償還債務時將額外獲得這一部分收益。

由於持幣使用者可能需要支付穩定費，在收益等於穩定費時，相當於免費借出穩定幣，當收益大於費率時，還會額外獲得一筆補貼，從而實現穩定幣的價值捕獲。

八、網路治理

Libra XS 發行的是一類去中心化穩定幣，允許其持有者通過投票來修改治理協議。網路治理是持幣者權利與義務的結合，持幣者將獲得穩定費等收益，同時積極行使自己的治理職能也將促使網路穩定。網路中的各項參數由持幣節點共同投票決定。治理流程包括提議、投票、執行三個階段，每兩個階段之間都有一定間隔時間。在提議發起後，社區需要時間來考慮是否應該通過，而在投票後也需要一段時間的等待來防止惡意治理協議。

1、改變抵押物類型

在專案初期，為了抵押資產價格的穩定，只選取了 BTC、ETH、USDT 三種加密貨幣。但隨著項目的完善，越來越多的加密貨幣將被增加到抵押資產中，同時不符合條件的抵押物也將被剔除。

2、修改風險參數

一開始，BTC、ETH 的最低抵押率將被設置為 150%，當抵押率 < 150% 時，將觸發清算。不同的抵押資產可能需要設置不同的抵押率，在不同時期可能也需要不同的抵押率，這些都將通過投票完成。

3、穩定費率的調整

通過 CDP 借出穩定幣後，在償還債務時需額外支付穩定費用。通過調整穩定費率也將直接影響債務規模，當債務規模過高時可以調高穩定費率來促使用戶贖回抵押物，當債務規模較低時可降低穩定費率。穩定費的一部分將獎勵給穩定幣的持幣者，另一半將計入風險準備金，以應對黑天鵝事件。

4、預言機的選取

平臺通過去中心化的預言機來獲取抵押物的內部價格，穩定幣的持有者可投票控制預言機的節點數量，或指定可信任的預言機。

5、其它參數的調整

債務規模上限、全域清算者的選舉等其它治理過程皆由投票結果產生。

九、穩定幣的清算

1、部分清算

當抵押率小於最低抵押率時，將觸發清算機制，系統將抵押的 BTC 或 ETH 進行拍賣，募集穩定幣償還債務。整個清算過程分為兩步，競標和發貨。在第一步中，將通過公開招標確定抵押資產的價格。第二步，成功競標者將穩定幣轉入智慧合約，以換取拍賣所得的抵押資產。剩餘的抵押資產將還給使用者，但需要收取部分罰金，罰金將計入風險準備金。

2、全域清算

當穩定幣系統受到惡意攻擊出現故障，導致預言機獲取的抵押資產價格與實際相差較大，超過系統風險承受能力時，持幣者投票選定的全域清算者可授權進行清算。全域清算步驟如下：

1). 啟動

在全域清算觸發後，債務的創建及償還等操作都將被禁止，系統以固定的價格凍結報價，方便所有用戶兌換。

2). 拍賣

系統中的債務將以去中心化的形式進行公開拍賣，以此來償還抵押借貸用戶的索賠。

3). 兌換

當拍賣階段完成後，穩定幣持有者可以在平臺上發出兌換請求，以目標價格兌換抵押資產。

免責聲明

本白皮書僅作為傳達資訊之用，內容僅供參考，不構成在 Libra XS Foundation 及其相關公司中出售股票或證券的任何買賣建議、教唆或邀約。本白皮書不提供任何買賣行為，也不是任何形式上的合約或者承諾。

鑒於不可預知的情況，本白皮書列出的目標可能發生變化。雖然團隊會盡力實現本白皮書的所有目標，但參與 Libra XS 專案的個人和團隊需自擔風險。白皮書的部分內容可能隨著專案的進展在也會隨之進行一定調整，團隊將通過在網站上發佈公告或新版白皮書等方式，將更新內容公佈於眾。投資人在置換穩定幣過程中遭受的損失與 Libra XS Foundation 團隊無關。

Libra XS Foundation 團隊將努力實現白皮書中所提及的目標，但基於不可抗力的存在，團隊不能完全做出承諾。在適用法律允許的最大範圍內，對因參與穩定幣專案所產生的損害及風險，包括但不限於直接或間接的個人損害、商業盈利的喪失、商業資訊的丟失或任何其它經濟損失，本團隊不承擔責任。

Libra XS Foundation 明確向投資人傳達了可能的風險，投資人參與資產抵押生成穩定幣，代表其已確認理解並認可細則中的各項條款說明，接受置換過程中的潛在風險，後果自擔。

風險提示

在 Libra XS 網路的開發、維護和運營過程中存在著風險，這其中很多都超出了開發方的控制和預期。除本白皮書所述的其他內容外，投資人還請充分知曉並同意接受下述風險。

市場風險

Libra XS 被設計成一種去中心化穩定幣系統，其穩定幣價格不應有大幅波動，且在設計階段已經給出了保持穩定幣價格穩定的措施。但由於流動性等問題，在實際交易過程中仍可能高於或低於法幣價格。

監管風險

Libra XS 區塊鏈網路是一個去中心化專案，其中的穩定幣是通過抵押資產在智慧合約上生成的穩定幣，任何個人和組織都不能憑空發行額外的穩定幣，但匯率是一個敏感話題。區塊鏈項目已經成為世界上主要國家的監管對象，如果監管主體插手或施加影響，Libra XS 可能受到其影響。

專案技術風險

密碼學的加速發展或者科技的發展諸如量子電腦的發展，或將破解的風險帶給平臺，這可能導致穩定幣的丟失。專案更新過程中，可能會出現漏洞，漏洞發現後會及時修復，但不能保證不造成任何影響。當網路出現擁堵時，可能出現由於預言機價格的延遲導致的風險。

目前未可知的其他風險

除了本白皮書內提及的風險外，此外還存在著一些創始團隊尚未提及或尚未預料到的風險。此外，其他風險也有可能突然出現，或者以多種已經提及的風險組合的方式出現。請參與者在做出參與決策之前，充分瞭解團隊背景，知曉專案整體框架與思路，理性參與。