

# 去中心化金融 (DeFi)

陸裕豪

# DeFi

去中心化金融(Decentralized Finance, DeFi)

- 利用自動化取代中介

Source: <https://www.blocktempo.com/defi-101-renewed/>

2020/12/14

DeFi (陸裕豪)

2

# 穩定幣

# 穩定幣

- 去中心化金融的重要組成模塊。
- 比特幣或以太幣的價格經常大起大落<sup>1</sup>,非常波動,而穩定幣可以被設計成了錨定一單位法幣的價值。
- 大部分的穩定幣都錨定美元,市面上也存在一部分錨定人民幣的穩定幣。

# 法幣支持的穩定幣

- Coinbase 發行的穩定幣 USD Coin (USDC) ，  
每發行一枚 USDC，Coinbase 都會相應在銀行帳戶中存入 1 美金
- 有發行機構承擔責任
- 有法幣作為擔保品
- 非所有用戶都有資格使用中心化穩定幣。USDC 的用戶條款就聲明只支持部分國家和地區的用戶使用，並且嚴格限定了 USDC 的使用範圍和場景。

# 去中心化數位資產支持的穩定幣

- 沒有法幣的擔保，因而需要加密資產的超額擔保
- 無需取得某個公司或政府的許可
- 例子：構建在以太坊上的 Maker 系統就發行了去中心化穩定幣 DAI
- DAI 的目標是 1:1 錨定美金
- 將加密貨幣（通常是以太幣）作為擔保品鎖定在 Maker 系統中，然後才能借出一筆 DAI。擔保品的價值必須高於貸款額，因此是超額擔保貸款。

# DAI

- 借 DAI 主要是為了加槓桿
- 如果原本價值 200 美金的以太幣暴跌，擔保率跌至清算比率以下，那 Maker 的智能合約就會沒收你的擔保品並在市場上出售，以償付借出的 100 美金。這樣一來，Maker 系統就不會出現任何壞帳。

# 去中心化演算法實現的穩定幣

- 沒有任何資產支持，僅僅依靠演算法維持價格穩定。
- 演算法穩定幣的代表包括 Basis，它在上線前夕就宣告失敗。
- 有些人質疑財力雄厚的惡意機構能夠攻擊演算法穩定幣，造成市場的恐慌和穩定幣脫錨，最終引發死亡螺旋，穩定幣價值歸零。



# 去中心化貸款

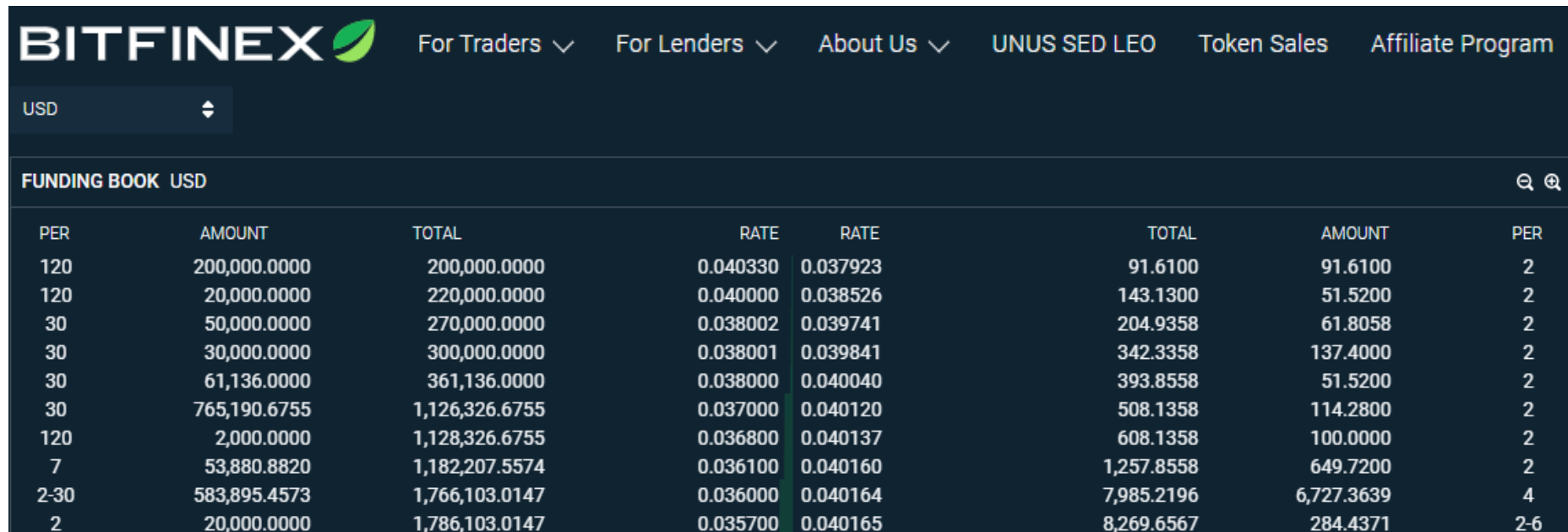
# 去中心化貸款

- 通過編寫好的程式碼從區塊鏈上獲取一筆貸款，不需要通過任何銀行帳戶。
- 利用 USDC 以及 DAI，就能通過自動化智能合約進行各種金融活動。
- 借貸是很合適的應用。

# 去中心化貸款

- 目前有許多直接通過智能合約實現以太幣借貸的 DeFi 平台，比方說 Compound、dYdX 以及 Dharma。
- 這些智能合約讓借貸雙方都不需要主動尋找交易對手。
- 事實上，智能合約替代了中介商的功能，借貸產生的利息則由演算法根據供需關係自動計算。

# 中心化借貸委託簿



The screenshot shows the Bitfinex website's 'FUNDING BOOK' for USD. The table lists various loan orders with columns for PER, AMOUNT, TOTAL, RATE, and a corresponding output column. The interface includes a dark blue header with the Bitfinex logo and navigation links like 'For Traders', 'For Lenders', 'About Us', 'UNUS SED LEO', 'Token Sales', and 'Affiliate Program'. A dropdown menu shows 'USD' as the selected currency.















PER	AMOUNT	TOTAL	RATE	RATE	TOTAL	AMOUNT	PER
120	200,000.0000	200,000.0000	0.040330	0.037923	91.6100	91.6100	2
120	20,000.0000	220,000.0000	0.040000	0.038526	143.1300	51.5200	2
30	50,000.0000	270,000.0000	0.038002	0.039741	204.9358	61.8058	2
30	30,000.0000	300,000.0000	0.038001	0.039841	342.3358	137.4000	2
30	61,136.0000	361,136.0000	0.038000	0.040040	393.8558	51.5200	2
30	765,190.6755	1,126,326.6755	0.037000	0.040120	508.1358	114.2800	2
120	2,000.0000	1,128,326.6755	0.036800	0.040137	608.1358	100.0000	2
7	53,880.8820	1,182,207.5574	0.036100	0.040160	1,257.8558	649.7200	2
2-30	583,895.4573	1,766,103.0147	0.036000	0.040164	7,985.2196	6,727.3639	4
2	20,000.0000	1,786,103.0147	0.035700	0.040165	8,269.6567	284.4371	2-6

- Bitfinex 提供這樣的訂單簿服務來撮合用戶，然後從中抽成。

# 去中心化借貸委託簿

- 一些去中心化借貸平台則更進一步，沒有採用委託簿來撮合借貸雙方，而是讓用戶直接通過智能合約借貸，動態調整利率以撮合訂單。
- 例如有人從智能合約中借出了一大筆錢，貸款利率就會提高。此外，借款人必須在智能合約內鎖定擔保品才能借款，且擔保品的價值要高於借款金額，以實現超額擔保。
- DeFi 能夠提供比傳統銀行更高的儲蓄利率，且風險更低，在理論上能吸引數十億資金入場。Compound 已經管理了 1.2 億美金的資產，而其他的平台也勢頭正旺。

# 去中心化借貸委託簿

Platform	 USDC	 DAI	 USDT	 sUSD	 BUSD	 TUSD	 PAX	 GUSD
USD Price	\$1.00	\$1.01	\$1.00	\$1.01	\$1.00	\$1.00	\$1.01	\$1.00
24h change	—	—	—	—	—	—	—	—
 Linen App ★join!★	2.31%	.	.	.	.	.	.	.
 Compound	2.31%	2.97%	4.49%	.	.	.	.	.
 dYdX	5.38%	9.12%	.	.	.	.	.	.
 Dai Savings Rate	.	0.00%	.	.	.	.	.	.
 Aave	3.53%	3.79%	5.51%	1.30%	1.80%	1.15%	.	.
 Curve Compound**	3.01%	3.01%	.	.	.	.	.	.

- LoanScan 的數據，顯示了在不同平台上借出穩定幣可獲得的利率

# 去中心化交易所

# 去中心化交易所

- 在區塊鏈上買賣密碼學貨幣，而不是通過 Coinbase 這種中心化交易所。原則上，支持腳本接入實現自動化的交易。



# 去中心化交易所

- 去中心化加密貨幣交易所試圖把 Coinbase Pro 之類的服務搬到區塊鏈上，意即促成不同數位貨幣之間的交易。
- 中心化交易所: 以 Coinbase Pro 為例，它是買賣雙方之間的中介和託管方，可以託管資產並撮合交易。
- 雖然中心化交易所促成了數十億美金的交易，但它依然存在駭客攻擊引起的單點故障（Single Point of Failure）、交易審查以及交易壁壘等弊病。

# 去中心化交易所

- 去中心化交易所最理想的形態是支持所有數位資產、完全點對點的交易所。
- 目前有很多支持基於以太坊代幣的去中心化交易所，如 Uniswap、0x 以及 Kyber.....。
- 以 Uniswap 為例，它採用了被稱為自動做市商（automated market maker，AMM）的算法來為代幣提供流動性。
- 買賣雙方直接從智能合約裡取得流動性，價格則根據代幣需求量以及智能合約中提供的流動性計算得出。Uniswap 在計算價格時不考慮買單的大小，而是根據買單量逐步提高代幣的價格。

# 擔保品

# 擔保品

- 借方必須質押數位資產才能借出去中心化貸款，確保在借方違約的情況下，依然能償還貸方。

# 去中心化身分

# 去中心化身分

- 智能合約裡採信的身分，用於去中心化貸款中評估用戶的信用。

# 去中心化身分

- 去中心化借貸的一大痛點，是需要提供大量的擔保品。這種超額擔保機制會造成資金利用效率太低
- 去中心化身分和聲譽系統能提供類似的服務，通過綜合社交媒體聲譽、歷史還貸記錄、其他信譽良好的用戶的擔保等數據，為用戶信用評分。在落地應用之前還需要就具體的數據點進行許多實驗和試錯，也許還要加入質押系統，可以說我們目前仍然處在早期探索階段。

# 可組合性



# 可組合性

- 和軟體開發中的各種庫類似，將不同的 DeFi 函數組合，實現複雜的功能。舉例來說，如果已經有一個智能合約能存幣生息，你可以實現另一個合約來自動複投利息（不需要經過第一個合約許可）。

# 可組合性

- 比如一個結合了 DeFi 和社交媒體概念的新項目 2100，可以讓參與者利用自己的推特帳號「鑄造」新的代幣，利用自己的社會資本生成數位美元。
- KOL 能把一些優質內容設置成僅代幣持有人可見，從而實現粉絲經濟變現。將個人帳戶代幣化之後，人們甚至能構建預測市場，競猜哪些帳戶會變得更流行。
- 另一個傳統金融從沒有出現過的概念是 PoolTogether，它把 DeFi 和彩券結合，創造了一種「無損失」彩券。用戶購買鏈上的彩券，然後將所有購買彩券的資金都存入 Compound 中賺取利息。在每一期彩券開獎時，每個購買人都能拿回自己的錢——不過有一個幸運兒能把彩券獎金池產生的利息全部抱回家。從本質上來說，這就是在利用彩券機制增加儲蓄並創造財富！

# 風控

- **風控**—— DeFi 的高回報通常伴隨著高風險。萬幸當下湧現出許多新工具，能盡量降低投資的風險。

# 風險

- 智能合約風險
- 擔保品和價格波動風險
- 法律與政策性風險
  - 在 DeFi 領域，Nexus Mutual 以及 Convexity 等去中心化保險能有效對沖上述風險。而 Augur 之類的預測市場可以讓用戶對其正在使用的智能合約存在漏洞的概率下注，以此對沖風險。

# 智能合約

# 智能合約

- 是一段部署 (Deploy, 即發佈) 到區塊鏈上的程式碼，因為區塊鏈上的程式碼 (嚴格來說是二進位碼) 可以被檢視，所以具備公開透明的特性。