[PDF Database Document] - BTCC Cryptocurrency Exchange

原文:
https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-lightning-network

BTC教學丨什麼是閃電網路 Lightning Network?

當我們想要清楚地了解「比特幣」時，必定要掌握有關「閃電網路」的有關知識。

閃電網路是比特幣的開發者為了解決比特幣交易過慢問題而提出的解決方案，它對比特幣的發展起著非常重要的促進作用。

本文將為您介紹有關閃電網路的知識，讓我們一起來看看吧！

什麼是閃電網路？

閃電網路(LightningNetwork)是應用於比特幣的第二層技術，它使用小額支付渠道來擴展其區塊鏈的能力，從而更加有效地進行交易。同時，在閃電網路上進行的交易比直接在比特幣區塊鏈上進行的交易更快、成本更低、更容易確認。

透過將交易從主區塊鏈中取出並使其脫鏈，閃電網路旨在消除比特幣區塊鏈的擁塞並降低相關的交易費用。閃電網路還可用於進行其他類型的涉及加密貨幣之間交換的鏈下交易。

簡單來說，閃電網路是一種技術解決方案，旨在通過引入賬本外交易來解決比特幣區塊鏈上的交易速度問題。

閃電網路是如何進行工作的？

閃電網路(Lightning Network)使用智能合約在用戶對之間建立鏈下支付渠道。一旦建立了這些支付渠道，資金幾乎可以立即在它們之間轉移。

巧妙的是，網路不需要在所有用戶之間創建配對。例如，如果用戶 A 與用戶 B 有一個通道，而用戶 C 與用戶 B 有一個通道但沒有用戶 A，則資金仍然可以在所有聯網方之間自由轉移。閃電地址看起來像典型的比特幣地址，用戶的支付過程非常相似。

在任何時候，用戶都可以關閉他們的支付渠道並在核心區塊鏈上結算他們的最終餘額。因為核心區塊鏈上只記錄了支付通道的開啟和關閉，所以整個比特幣網路可以移動得更快。

此外，閃電網路交易可以比在主區塊鏈上進行的交易更加私密（因為第 1 層交易都會出現在公開且透明

的分類賬上）。

從技術層面上分析，閃電網路使用智能合約和多重簽名腳本來實現其願景。當一方或雙方為渠道提供資金時，會創建稱為資金交易的初始交易。在典型的多重簽名環境中，最初會交換兩個主密鑰（一個公鑰，另一個私鑰）。其中交易所促進了資金的獲取和支出。

然而，在閃電節點的情況下，不會交換簽名。這樣做是為了防止資金交易的支出被主區塊鏈識別。相反，雙方交換一個密鑰，用於驗證他們之間的支出交易（也稱為承諾交易）。

雙方可以在自己和閃電網路上的其他節點之間進行無休止的承諾交易。僅當它們之間的通道關閉時，它們才交換主密鑰。

閃電網路的起源和發展

2015年，研究人員 Thaddeus Dryja 和 Joseph Poon 在論文「比特幣閃電網路」中提出了閃電網路(Lightning Network)的概念。該論文是基於比特幣的匿名創造者中本聰之前對支付渠道的討論。

該論文的摘要描述了一種由支付渠道組成的鏈下協議。在支付渠道中，兩個不受信任的方可以在不阻塞主網的情況下轉移價值，因為渠道存在於鏈下。鏈下渠道旨在解決比特幣的可擴展性問題。

2016 年，Dryja 和 Poon 創立了 一家致力於開發閃電網路的公司 Lightning Labs，閃電實驗室一直努力使該協議與核心比特幣網路兼容。在 2017 年比特幣基於 SegWit 的軟分叉之後，突破成為可能，它為更多交易騰出了空間以適應每個區塊，並消除了一個長期存在的比特幣漏洞，稱為交易延展性。

由於發布前的測試，開發人員可以立即在閃電網路上構建應用程式。應用程式包括簡單的用例，例如錢包和賭博平台，它們利用了閃電網路微交易的力量。

2018 年，閃電實驗室終於在比特幣主網上推出了閃電網路實施的測試版，而Twitter 創始人傑克・多爾西等公眾人物也開始參與該項目。

閃電網路的用例

在閃電網路(Lightning Network)上線後，Twitter 成為第一批參與該項目的公司。推特允許用戶透過閃電網路發送和接收比特幣提示。透過名為 Strike 的與閃電網路兼容的支付應用程式，許多推特用戶都可以立即免費向其他推特用戶的帳戶發送比特幣付款。

第一個將比特幣作為法定貨幣的國家——薩爾瓦多也在很早前就使用了閃電網路。政府創建的錢包 Chivo 與閃電網絡兼容，旨在實現無縫跨境支付。

如何使用閃電網路？

了解了閃電網路(Lightning Network)的定義和工作原理之後，我們應該如何使用閃電網路進行交易呢？

如果您想要使用閃電網路進行交易，那麼需要將一些比特幣從您的帳戶中發送到與閃電網路兼容的比特幣錢包中。

目前與閃電網路兼容的錢包主要分為託管和非託管兩種。

如果您是一個新手，那麼建議您選擇託管錢包，這些錢包將會透過管理您的私論來簡化發送和接受加密。

如果你丟失了你的密碼，你將能夠重置它。常見的託管錢包包括 Strike、Blue Wallet 和 Wallet of Satoshi 等。

如果您是一名有經驗的交易者，那麼建議您選擇非託管錢包，他們將完全由用戶控制。但需要注意的是，你需要保護好自己的私論，如果您丟失/損壞自己的錢包或忘記了密碼，你將可能無法動用錢包中的資金。