電子金融及支付工具

第四堂　區塊鏈及「加密貨幣」

視像文字稿

大家好。歡迎收看由港島區長者學苑聯網提供的「電子金融及支付工具介紹」網上課程。今堂為大家介紹電子金融項目下在的區塊鏈及「加密貨幣」的知識。

區塊鏈

簡單來說，區塊鏈是一種公開、去中心化的分散式資料庫。你可以把資料庫理解成商店擁有的一本大賬簿，記錄了商店的所有交易紀錄。而區塊鏈就是一不依賴第三方，通過自身分散式節點進行這些交易紀錄的存儲、驗證、傳遞和交流的一種交易系統方案。

去中心化

到底去中心化是甚麼意思？我們先簡略講解中心化是指怎樣的一回事。中心化的交易系統在日常生活中很常見，例如我們把款項轉帳給其他人時，我們需要通向銀行發出轉帳指示，然後由銀行核實轉帳雙方的身分，以及確認你的帳戶內有足夠的金額，才會執行轉帳。「中心化」中的「中心」就是指像銀行這種存在於交易雙方中間，擔當核實和紀錄交易的中間人角色。而區塊鏈的去中心化就是指交易系統裡並不是由任何權威人士、機構、政府等持分者處理，而是由系統內每一個參與者（稱為節點）去核實和紀錄交易。參與區塊鏈的每一個節點都會有一份由區塊鏈開設至今的完整交易紀錄。在一筆交易發生之後，每一個節點都會收到這一筆交易的細節，例如交易雙方的身分和交易金額，然後核算這項交易是否正確無誤，核算完成後，這一筆交易就會正式於所有節點加入交易紀錄內。因為區塊鏈技術中每一筆交易都會直接連接著上一筆的交易，這種一筆接一筆的鏈狀紀錄亦是得其名「區塊鏈」的原因。

不可竄改性

區塊鏈的另一大特色是他的「不可竄改性」。區塊鏈中的每一筆資料都會加入一個由高強度雜湊演算法產生的簽名，這種高強度演算法產生的簽名很容易可以被驗證，但同時非常難以偽造。如果區塊鏈中的資料遭到竄改，區塊鏈中的各個節點就會發現遭竄改的資料與簽名不符，從而阻止惡意刪改資料，保障區塊鏈資料正確完整。

區塊鏈的用途

區塊鏈技術不需要可信任的中間人，本身已經可以確保數據的完整性及提供有效的核查機制。因此，區塊鏈技術不但可以用在各種金融交易上，也可用在商務契約、稅收、投票、醫療記錄、數碼護照及數碼貨幣發行等各種公私領域，幾乎遍及日常生活的各個層面。

「加密貨幣」

區塊鏈的一個最著名的應用方式就是「加密貨幣」。「加密貨幣」是一種以密碼作保障資料的一種「虛擬貨幣」，並使用區塊鏈記錄「加密貨幣」的所有產生和交易情況。著名的「加密貨幣」有比特幣（Bitcoin）、以太幣（Ethereum）、瑞波幣（Ripple）等。

「加密貨幣」的去中心化

基於區塊鏈技術的「加密貨幣」的其中一個主要特徵當然就是去中心化，但是「加密貨幣」的去中心化除了區塊鏈有的特性之外，還有一個非常獨特的特點：就是「加密貨幣」的發行是不受政府、金融機構、財政部門及某特別群體所直接控制。這種發行方式可以在最大程度上防止人為干預和市場操縱。但是與實體貨幣不同，「加密貨幣」沒有銀行、政府、發行人或者實物支持，它們的現實價格可以有很大幅度波動，如果要投資「加密貨幣」，記緊要考慮清楚啊！

「加密貨幣」如何運作？

儲存「加密貨幣」需要類似電郵信箱的「加密貨幣錢包」。「加密貨幣錢包」包含了一個位址和私鑰，只有擁有私鑰的人才可以從錢包領取「加密貨幣」。而在付款時，你需要輸入收款人的錢包位址，將「虛擬貨幣」直接支付給對方。我們可以簡單的把「加密貨幣」位址理解成為銀行卡號，而私鑰則是銀行提款卡和密碼。只有在持有提款卡和知道密碼的情況下才能動用銀行帳戶中的錢。

「加密貨幣」交易

在使用「加密貨幣」進行轉帳時，交易記錄將記錄在區塊鏈的公共交易賬簿中，交易中所有細節，包括金額、時間、支帳和收帳戶口都是公開的。如果你知道「加密貨幣錢包」位址，你甚至可以查到該錢包內擁有的「加密貨幣」數量。

總結

像區塊鏈和「加密貨幣」這些技術在未來或會為世界很多產業帶來改變。區塊鏈和「加密貨幣」去中心化和公開的特徵，可以使交易更加迅速；而區塊鏈的不可竄改性亦可以使交易本身變得更安全可靠。

今次就分享到這裡，多謝你的收看。再見！
本影片由港島區長者學苑聯網提供內容及製作。