日期：	2018 年 9 月 1 日
媒體：	星島日報
版面：	A18. 每日雜誌
標題：	排除障礙 使區塊鏈發展得更好
內文：	區塊鏈是目前非常熱門的技術，受到廣泛的關注。從開始時因為是 Bitcoin 的原因，到目前不管是在銀行業、金融業、物流業，都有人在研究使用區塊鏈技術，甚至是政府都開始探討在土地房屋登記、交易、智慧合同等使用的可能性。區塊鏈技術確實有它的優勢，而且對很多行業都會帶來重大影響，可以說是有很大的潛在商業價值。對於新技術來說，制約它發展的不是它有多少強項，而是它有甚麼弱點。所以要推動區塊鏈的快速良性發展，令它可以產生更大的商業價值，就必須對區塊鏈技術的弱點有所瞭解了，研究如何揚長避短。 須負擔資料儲存成本 區塊鏈的優勢在媒體上已經有廣泛的介紹，但討論區塊鏈的弱點就比較少了，所以我們不如來看看區塊鏈的弱點，一起來想想如何優化，這個可能是一大商機。區塊鏈技術有幾個特點，包括管理去中心化，資料不可更改等。 區塊鏈技術的去中心化，其實是由每個參加者保存一份交易記錄所實現的。具體來說就是所有該區塊鏈的參與者都需要保存一份完整的交易記錄。所以如果有駭客要篡改交易記錄，就必須同時將所有的記錄篡改，而不被發現，這樣是不可能的。由於每個參與者都有一份完整記錄，所以這些記錄只有增加，不可能減少。參與者本身就必須負擔資料儲存的成本了，對於像一般的房產轉讓的參與者來說，可能十年交易不到一次，卻需要一直保存所有記錄，可能有些參與者會有意見。 一項交易要在區塊鏈裡被確認，是需要滿足 consensus 的要求。假如需要五成一的參與者的確認，參與者愈多，需要獲得的確認就愈多，交易能夠被確認的時間就會愈長。那能不能降低五成一的要求呢？當然可以啊，不過這樣就會降低該區塊鏈的安全性。例如房屋交易，一般的業主可能十年交易不了一次，所以自己交易完了，可能就不會連上區塊鏈系統了，如果大部分的業主都是這樣的話，可能根本不夠五成一的活躍參與者，交易可能一直無法確認。設計區塊鏈應用的人，就要好好想想如何鼓勵參與者連上區塊鏈了。

Bitcoin 的做法就是如果你連上它的區塊鏈，幫它認證交易，你就會有機會獲得 Bitcoin 了，可是像房屋轉讓，難道參與者一直連上區塊鏈就有機會獲得一套房屋？虛擬貨幣可以通過網路自己產生，可是實體資產的區塊鏈就要想想辦法了。

每個人網路安全能力不同

愈多的人連上區塊鏈，而每個人的網路安全的能力都不同，意味著參與者的機器安全性也不同。區塊鏈可以設置到很高的安全程度，可是如果參與者的機器中毒了，參與者的帳號密碼可能就被盜取了，駭客就有可能會盜取參與者的身分進行交易，並通過他控制其他人的帳號來認證他自己的交易了。雖然這是區塊鏈以外個人網路安全問題，但也應在應用區塊鏈時格外留意和考慮這情況。

雖然區塊鏈有以上的一些弱點，不過我相信集思廣益，區塊鏈的推動者們很快就會想到辦法來完善區塊鏈的技術和應用，為人類做出貢獻。

Francis Wong 黃振昌
香港電腦學會 FinTech 專家組