

## 區塊鏈技術

ISE15/15-16

主題：[財經事務](#)、金融科技、Fintech、分布分類帳、共享分類帳

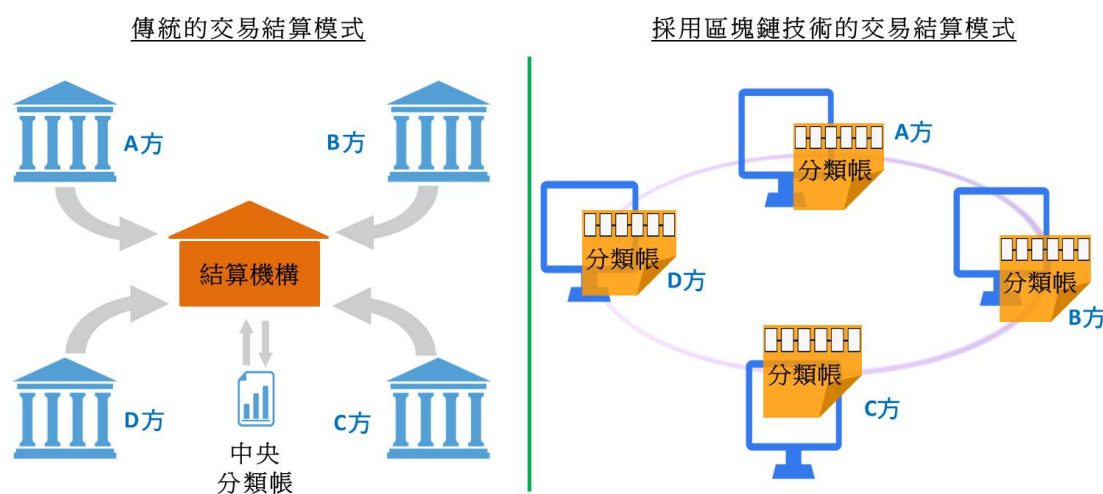
- 財政司司長在其任內發表的2016-2017年度財政預算案演辭中指出，政府會鼓勵業界和相關機構，探討區塊鏈(blockchain)技術在金融服務業的應用，發展其減少可疑交易和降低交易成本的潛力。
- 區塊鏈是一項嶄新的技術，用以建立數碼分類帳(digital ledger)，備存在網絡，從而省卻傳統上由中間人或中央機構負責處理、授權或核實交易的安排。<sup>1</sup> 區塊鏈的應用並不止於減少詐騙個案或降低營商成本。舉例而言，區塊鏈現時被應用於虛擬貨幣交易，當中以比特幣(Bitcoin)最為人熟悉。<sup>2</sup> 在貿易融資方面，區塊鏈可用於避免不同銀行為同一張貨運單據重複為客戶提供融資的漏洞。
- 根據金融科技督導小組<sup>3</sup>於2016年2月發表的報告，區塊鏈可被廣泛應用於發展低成本和具透明度交易的基礎設施。透過善用香港的金融、物流及其他專業領域的專才，香港有條件發展成為區塊鏈科技的樞紐。本期《資訊述要》旨在(a)闡述區塊鏈技術及其主要特點、(b)探討區塊鏈技術的可應用範疇和海外金融市場就發展相關技術的計劃，以及(c)說明採用區塊鏈技術所面對的挑戰。



### 何謂"區塊鏈"

- 區塊鏈一般是指用以記錄交易的數據庫或數碼分類帳。區塊鏈一詞是由"區塊"("block")及"鏈"("chain")兩個詞彙結合而成。個別的"區塊"是指在某特定時段內進行的交易。<sup>4</sup>每個區塊會透過數學運算方式與下一區塊順序地"鏈"接起來，從而形成一個區塊鏈。只要取得最新的區塊，便可讀取連結在區塊鏈上的過往區塊數據。故此，區塊鏈數據庫能夠完整保留所有過去的數據，包括資產的轉移及執行相關指令的紀錄，令所有交易得以核實及作獨立審核。這些特色使區塊鏈可用作分類帳，在相關網絡共享及供擁有權限的參與者查核。
- 一如上文所述，應用區塊鏈技術的其中一個主要特點是，可省卻由中央機構核實交易和進行結算的安排。圖1顯示了傳統模式與採用區塊鏈技術模式在交易結算安排的不同之處。在區塊鏈網絡中，每台電腦系統均備存一個相同的區塊鏈複本，此複本會自動更新每項交易，而電腦利用精密的運算程式就交易作出核實，從而確定交易金額及其他資料，令區塊鏈成為一個記載了所有交易活動的分類帳。處理交易的電腦系統一般分布於不同位置，並且不由任何一個機構／參與者單獨擁有或控制。由於區塊鏈是分布於網絡而非備存在中央伺服器，故此區塊鏈有時亦被稱為分布分類帳(distributed ledger)。

圖1 - 兩類不同的交易結算模式



資料來源：Oliver Wyman (2015)及IBM Corporation (2016)。

- 在實際操作上，區塊鏈系統可分定為公開或私人系統。公開的區塊鏈系統開放予所有使用者，可自由讀取或核實分類帳數據，這與虛擬貨幣交易系統相類似。私人區塊鏈網絡只限於一羣預先選定的參與者使用，而這些參與者擁有權限更新分類帳。參與者可來自同一機構，或某一行業的不同機構，他們簽訂非正式協議、正式合約或保密協議釐定彼此之間的權責。<sup>5</sup>
- 總結上文所述，採用區塊鏈系統的主要特點如下：<sup>6</sup>

- (a) 能按照數學運算方式核實交易，無須牽涉第三方機構；
- (b) 交易近乎實時執行及結算；
- (c) 交易紀錄完整齊備，可供追查讀取；
- (d) 區塊鏈所儲存的數據一經加入，便難以修改或移除；及
- (e) 可嵌入指令(例如"如果.....則.....否則.....")，以規定須在符合若干條件的情況下，才可執行交易或其他指令。

## 區塊鏈技術的應用

- 根據一家會計師事務所在2016年進行的調查，[7](#) 提供資金轉移及支付服務的機構曾接觸區塊鏈技術，當中30% 的受訪機構對區塊鏈技術非常熟悉。除了付款交易之外，區塊鏈技術的其他應用範疇可包括(a)打擊洗錢活動，用以追蹤資金交易及其目的地；[8](#) 以及(b)貿易發票融資，[9](#) 用以避免不同銀行為同一張貨運單據重複為客戶提供融資的漏洞。[10](#)
- 區塊鏈技術亦可以應用於證券發行及交易，藉以簡化相關的交收程序。[11](#) 舉例而言，納斯達克(NASDAQ)的NASDAQ Private Market在2015年10月成立了名為"Nasdaq Linq"的平台，應用區塊鏈技術於私人公司的股份發行、分類，以及轉讓紀錄備存。[12](#) 其他證券交易所亦計劃引進區塊鏈技術，當中，澳洲證券交易所(Australian Securities Exchange)正計劃開發區塊鏈技術，把交易後的結算及交收加快至近乎實時進行。日本交易所集團(Japan Exchange Group)正研究應用有關技術在低成交量市場的可行性，而韓國交易所(Korea Exchange)亦據報正計劃為非上市證券開發一個採用區塊鏈技術的平台。[13](#)
- 在國際層面上，金融科技公司R3與來自世界各地超過40家金融機構合作組成夥伴，探討區塊鏈的技術應用，在達到銀行安全性、可靠性、可擴展性、營運和審計要求的前提下，研究、測試、設計和策劃應用分布分類帳的方案。

## 採用區塊鏈技術所面對的挑戰

- 區塊鏈技術被認為有潛力革新傳統金融交易的運作，因此備受金融機構的重視。[14](#) 然而，要發展區塊鏈成為金融界的應用主流，必須克服多項挑戰，其中包括：

- (a) **所需資源**：區塊鏈系統的每台電腦系統均會備存一個相同的分類帳，每當有新交易時，電腦便會核實及更新該交易。與中央系統比較，這個分布式的系統可能會耗用更多運算及網絡資源。鑒於區塊鏈會隨着數據的新增而連結更多區塊，操作有關系統所需的資源或會越來越多，這令人關注到區塊鏈技術是否適用於大規模的應用範疇；
- (b) **私隱**：區塊鏈中的交易紀錄會以加密方式在網絡中儲存。儘管機構可把區塊鏈的應用限制在私人網絡，但數據私隱方面仍然存在問題。舉例來說，系統使用者可根據交易紀錄或透過擁有數據解密的權限不恰當地推敲出交易者的身份。一如歐洲證券及市場管理局(European Securities and Markets Authority)所指出，私隱問題將會是應用區塊鏈技術其中一個須予妥善管理的範疇；[15](#)
- (c) **保安**：區塊鏈的規程(protocols)常被視為具安全性，但其保安架構是利用公開密碼匙加密技術(public key cryptography)來保障資訊的。在過去20年間，各界亦曾討論若較大型的量子電腦能達到足夠的"量子位元"("qbits")時，能否入侵運用公開密碼匙加密技術的系統。[16](#)

此外，把不斷延長的區塊鏈分布於不同網絡位置，亦會帶來安全問題。國際刑警組織(International Criminal Police Organization)曾經警告，虛擬貨幣現時採用的區塊鏈技術很容易受到網絡威脅侵害，例如把惡意軟件及其他非法數據嵌入交易中，並在區塊鏈中散播；[17](#) 及

- (d) **監管**：在金融市場，現時尚未設有法律框架以保障區塊鏈技術使用者的權益，或規管金融機構使用相關技術。[18](#) 一如英國的金融市場行為監管局(Financial Conduct Authority)所指出，創新可能是一個需要反覆進行的演進過程，而為了給予創新者"空間"以研究及建立方案，該局在區塊鏈的應用範疇未趨清晰之前，不會對此持有既定立場。雖然如此，該局相信隨着區塊鏈技術不斷發展成熟，將有許多涉及規管和消費者的事宜須予釐清。[19](#) 事實上，要讓區塊鏈技術的應用取得成功，便必須建立有效的規管機制以確保區塊鏈技術穩妥，以避免網絡受到衝擊或被利用進行犯罪活動。[20](#)



- 區塊鏈技術在近年備受廣泛關注，被視為可改變現行紀錄備存及金融交易結算的模式。具體而言，區塊鏈技術可使交易無需透過第三方進行核實，加快交易的結算，甚或完全革新現有程序。世界各地許多金融機構及服務提供者已相繼投入研究，探討該技術的可應用範疇。然而，儘管區塊鏈技術被認為甚具潛力，但該技術的應用依然存在多項挑戰。
- 根據金融科技督導小組表示，透過善用匯聚香港的行業領域專家，以及金融、物流及其他專業服務機構，香港有潛力發展成為區塊鏈科技的樞紐。然而，其他亞洲經濟體亦正積極探討開發區塊鏈技術，其中，新加坡政府的資訊通信發展管理局 (Infocomm Development Authority of Singapore)，以國家科技發展部門的身份，聯同兩家商業銀行，首次應用區塊鏈技術以提高貿易發票融資的安全性，為應用區塊鏈技術發揮示範作用。[21](#)

立法會秘書處

資訊服務部

資料研究組

吳穎瑜

2016年4月20日

#### 附註：

1. 請參閱PricewaterhouseCoopers (2016)。
2. 比特幣是於2009年推出的首種建基於互聯網系統的虛擬貨幣，其付款系統無須經由第三方進行對帳及結算。現存的其他虛擬貨幣包括Litecoin及Peercoin。這些貨幣一般被稱為"加密貨幣"(cryptocurrencies)。請參閱Bank of England (2014)。
3. 政府於2015年4月成立金融科技督導小組，就發展及推動香港成為金融科技中心，向其提供建議。督導小組曾於2016年2月發表報告，就金融科技作分析及建議。
4. 區塊的重要組成部分為：(a)區塊的標題(header)，所載的資料包括獨一無二的區塊參考號碼、區塊的建立時間，以及可追蹤上一個區塊的數據碼等；及(b)區塊的內容，通常包括經過核實的數碼資產(digital assets)及指令資料，例如買賣交易、交易金額，以及參與交易的各方。請參閱Deloitte (2016)。

5. 請參閱Deloitte (2016)。
6. 請參閱例如Oliver Wyman (2015)、Deloitte (2016)及DTCC (2016)。
7. 請參閱PricewaterhouseCoopers (2016)。
8. 銀行可運用區塊鏈技術追溯過往的交易紀錄，包括資金來源、最終目的地及用途。此舉有助於加強銀行在查找可疑客戶方面的能力。請參閱White & Case (2016)。
9. 貿易發票融資讓企業可於客戶付款之前，憑藉貨運單據套現應收賬款，以改善現金流。企業一般向銀行和金融機構提供尚未付款的單據作為抵押品，從而獲得貸款。
10. 銀行只能夠查察其曾否就同一張貨運單據在過去一段時間內提供過融資，但同一張單據若是經由另一家銀行提供融資，銀行便不能查出。應用區塊鏈技術後，銀行將可從單一的來源取得資料，以查察客戶曾否以相同的單據向多家銀行獲取融資。
11. 舉例來說，參與者A與參與者B的交易指示在證券交易平台上獲得配對，區塊鏈系統可核實參與者A是否持有相關證券，而參與者B是否持有足夠資金。經核實的交易將分別自動記錄於資產分類帳及現金分類帳，無須經由中央結算系統處理。請參閱Oliver Wyman (2016)。
12. NASDAQ Private Market協助私人企業物色潛在買家，並就股東可出售的持股量訂定合適的百分比。參與的企業股東可藉此取得流動資金，而又可以在公開招股之前，將股權轉移至長期機構投資者手上。
13. 請參閱Australian Securities Exchange (2016)、Japan Exchange Group (2016)及Korea Times (2016)。
14. 根據一份業界報告，資本市場在2015年投資於區塊鏈技術的金額達7,500萬美元(5億8,400萬港元)，並預期在2019年，有關投資額將會大幅增加至4億美元(31億1,000萬港元)。請參閱Aite Group (2015)。
15. 請參閱European Securities and Markets Authority (2016)及Morrison & Forerster (2016)。

16. 請參閱Long Finance (2014)。
17. 請參閱International Criminal Police Organization (2015)。
18. 儘管如此，有少數地方(例如巴西及美國的紐約州)已制定規管使用／買賣虛擬貨幣的規例。請參閱BBVA (2016)、CFA Institute (2016)及Commodity Futures Trading Commission (2016)。
19. 根據Financial Conduct Authority (2016)，相關事宜包括個別人士如何連接到分布式的網絡系統、由何方人士／單位控制有關程序，以及使用者在數據保安方面有何保障。
20. 請參閱UK Government Office for Science (2016)。
21. 請參閱Infocomm Development Authority of Singapore (2015)及Coindesk網站。

#### 參考資料：

1. Aite Group. (2015) *Demystifying Blockchain in Capital Markets: Innovation or Disruption?*
2. Australian Securities Exchange. (2016) *Media Release: ASX Selects Digital Asset To Develop Distributed Ledger Technology For The Australian Equity Market.*
3. Bank of England. (2014) *Innovations in payment technologies and the emergence of digital currencies.*
4. BBVA. (2016) *Bitcoin and blockchain: threats and opportunities for the financial industry.*
5. CFA Institute. (2016) *Are Bitcoin and Blockchain Technology the Future?*
6. CoinDesk. (2016) *Official website.*
7. Deloitte. (2016) *Blockchain - Enigma. Paradox. Opportunity.*
8. DTCC. (2016) *Embracing Disruption - Tapping The Potential Of Distributed Ledgers To Improve The Post-Trade Landscape.*
9. Evry. (2015) *White Paper - Blockchain: Powering the Internet of Value.*

10. European Securities and Markets Authority. (2016) *Financial Innovation: towards a balanced regulatory response. Speech by Verena Ross, Executive Director*. 7 March.
11. Financial Conduct Authority. (2016) *UK FinTech: Regulating for innovation. Speech by Christopher Woolard, FCA Director of Strategy and Competition, delivered at the FCA's event on UK FinTech: Regulating for innovation*. 22 February.
12. IBM. (2016) *On the Blockchain nobody knows that you're a fridge?*
13. Infocomm Development Authority of Singapore. (2015) *Media Releases: Singapore demonstrates World's First Application of distributed ledger technology in Trade Finance*.
14. International Criminal Police Organization. (2015) *INTERPOL cyber research identifies malware threat to virtual currencies*.
15. Japan Exchange Group. (2016) *News Release: Commencement of Proof of Concept Testing for Blockchain Technology*.
16. Long Finance. (2014) *Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance*.
17. Morrison & Foerster LLP. (2016) *Demystifying Blockchain and Distributed Ledger Technology - Hype or Hero?* 5 April.
18. NASDAQ. (2015) *Press Releases: Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology*.
19. Oliver Wyman. (2015) *The Fintech 2.0 Paper: Rebooting Financial Services*.
20. Oliver Wyman. (2016) *Blockchain in Capital Markets*.
21. PricewaterhouseCoopers. (2016) *Blurred lines: how FinTech is shaping Financial Services*.
22. Sutardja Centre for Entrepreneurship & Technology of the University of California Berkeley. (2015) *Blockchain technology beyond Bitcoin*.
23. The Financial Times (2015) *Technology: Banks seek the key to blockchain*. 2 November.
24. The Korea Times. (2016) *KRX seeks share trading through blockchain*. 29 February.



25. UK Government Office for Science. (2016) *Distributed Ledger Technology: beyond block chain*.
26. U.S. Commodity Futures Trading Commission. (2016) *First, Do No Harm. Special Address of CFTC Commissioner J. Christopher Giancarlo Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium: Regulators and the Blockchain*. 29 March.
27. White & Case. (2016) *Beyond Bitcoin: The blockchain revolution in financial services*.