



金融科技的美麗與哀愁

Ieta Chi 紀孟宏

2005



Luca Bruno / AP

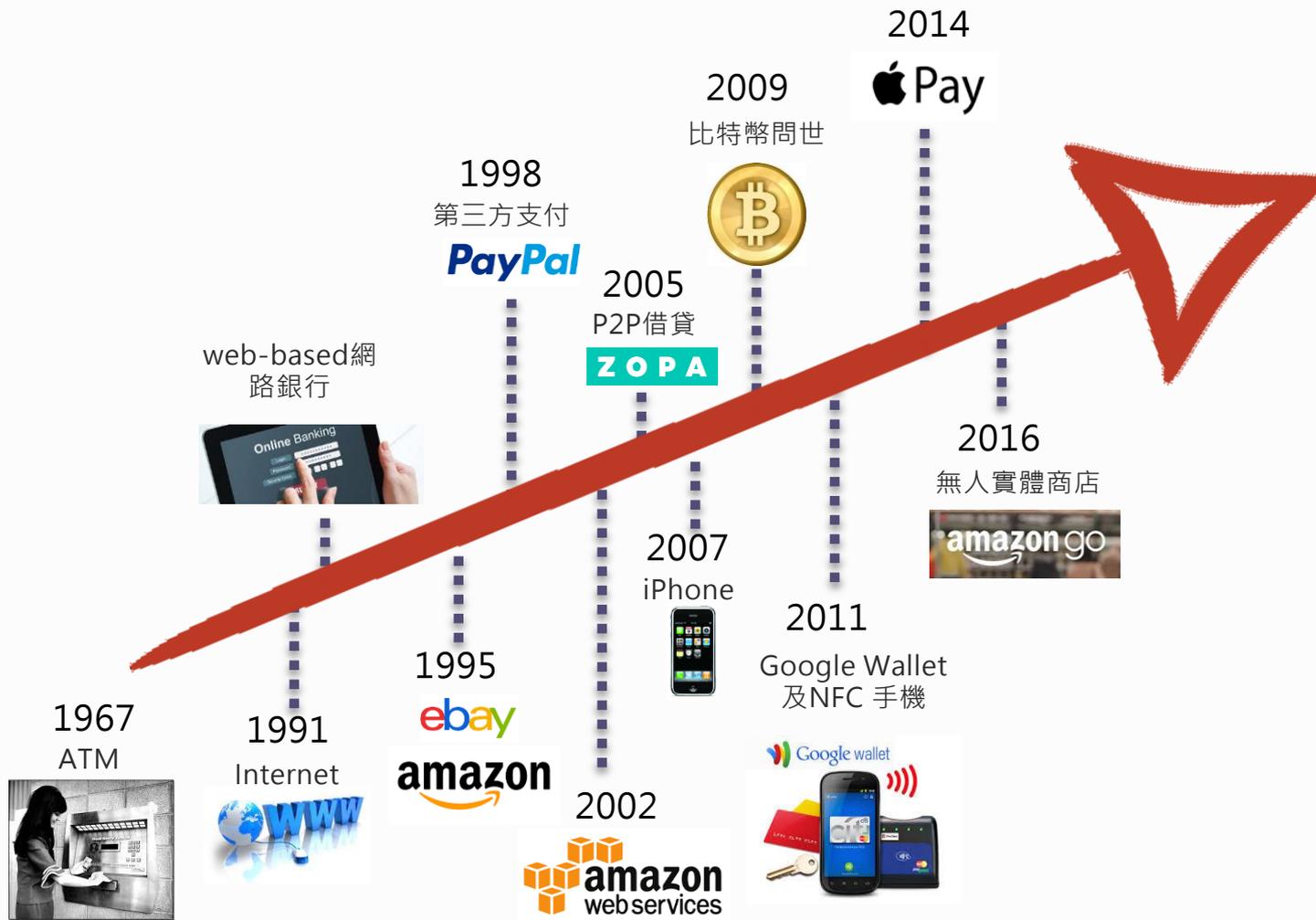
2013



NBC NEWS

Michael Sohn / AP

Fintech Evolution



World FinTech Report 2017



Over 50% of all customers globally are using at least one **FinTech Firm**

Rise of FinTech driven by **customer expectations**,
VC funding, **ease of entry**, **pace of technological evolution**



China India

Highest levels of FinTech usage seen in **China (84.4%)** followed by **India (76.9%)**



Gen Y, tech-savvy consumers lead adoption; open to new products but less likely to stay with current providers

Mobile emerges as the 2nd most important channel for Gen Y (47.6%) and tech-savvy customers (56.5%)

FinTech 概況

國內FinTech概況

	銀行是否跨入	實際做法
行動支付	各銀行均有推出電子錢包及與各家業者合作	<ol style="list-style-type: none"> 2016/8萬事達卡攜手台灣行動支付公司，推出T Wall plus，首波約十一家銀行合作。 玉山Wall。 預期行動支付短期回歸信用卡市占競爭。
跨境支付	已有多家銀行分別與支付寶及微信合作	<ol style="list-style-type: none"> 玉山銀行最早投入，則做通路較廣也較佳。 台新與新光取得新光三越通路。 元大與第一取得台北101通路。
P2P借貸	短期無法直接貢獻太多手續費收入，但可將傳統無法接觸到的客戶，導入p2p平台籌資，成功茁壯後再拉回正規銀行體系，提共各種金融服務。	市場傳出富邦及中信積極研究與業者洽談合作計畫。
群眾募款	銀行已有創投部門，市場小較無利可圖。	第一證、元富證，較無成功案件。
P2P匯款	受法規保護，換匯屬銀行特許業務	無
虛擬貨幣	央行定義為非合法貨幣，屬商品投資	無
機器人理財	為降低理財對理財專員的衝擊，金管會2016/1表示，2016年底前不會開放。	<ol style="list-style-type: none"> 瑞士銀行推出"智慧財富管理服務"，由IT系統搭配理專的現場服務。 台灣機器人理財顧問新創公司Kuchi，進入新加坡StartupBootcamp FinTech計畫。

那裡有錢，駭客就會往哪裡去

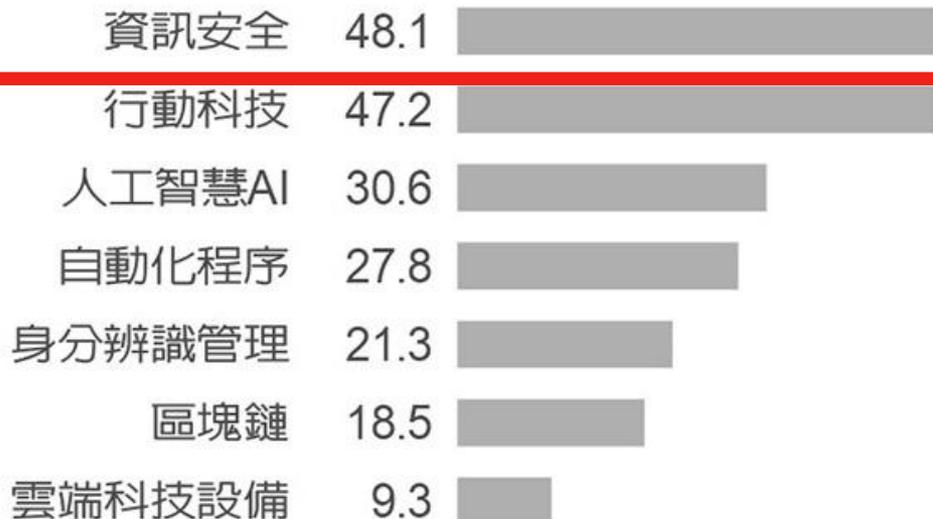


2017台灣FinTech業界大調查

表4 逾五成企業，未來一年將積極發展數據分析領域

問 因應金融科技未來發展，貴公司未來1年將增加人力與資金發展以下哪些項目？（可複選，%）

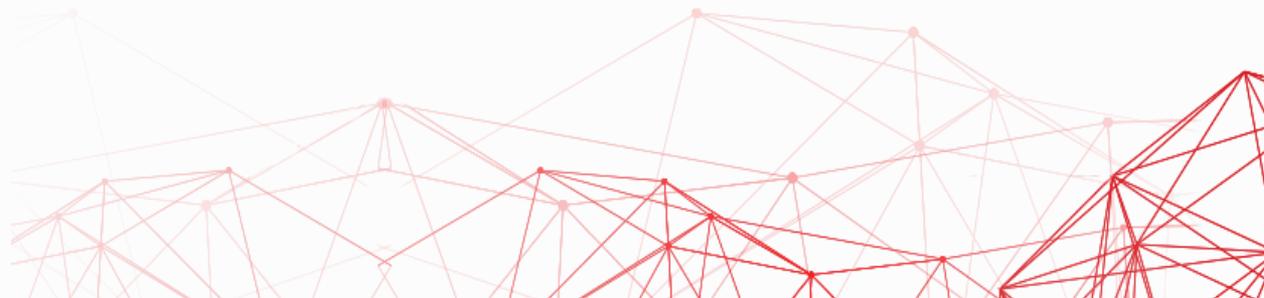
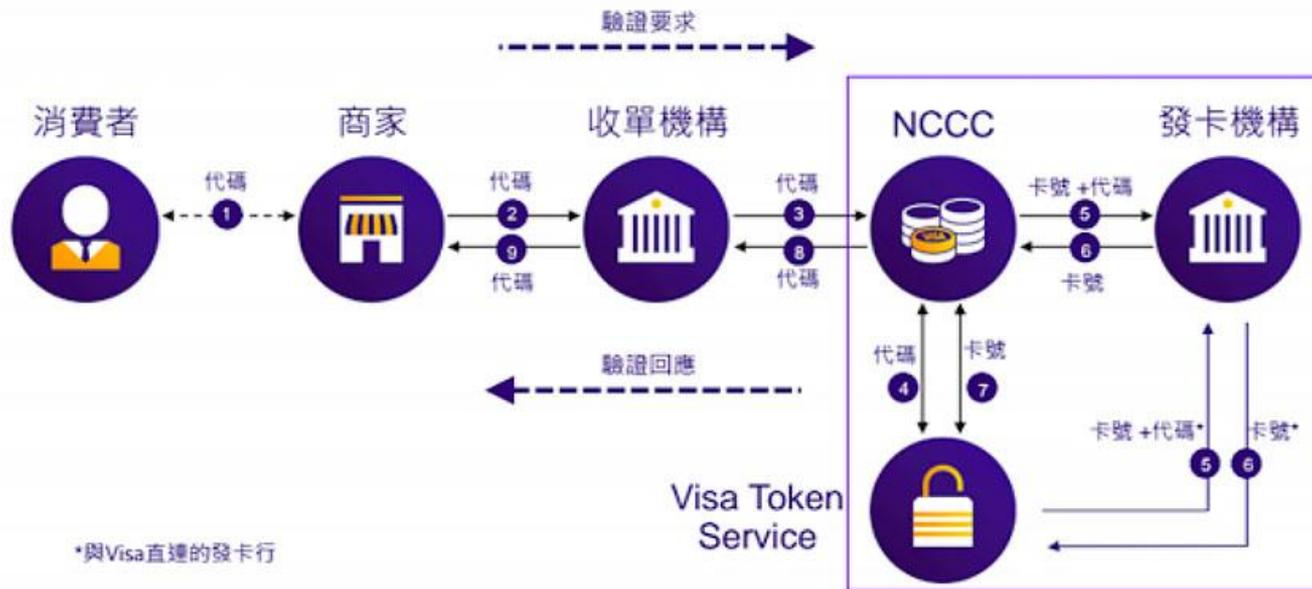
數據分析 51.9



Apple Pay 的代碼化 (tokenization) 技術

商家和收單機構都不會知道消費者的信用卡資訊。 

Visa代碼化技術服務如何處理國內交易



用了 Apple Pay 後沒有盜刷問題？

Apple Pay首遭盜刷 詐騙犯又是黃琪



2017-08-26



〔記者邱俊福、陳慰慈、王孟倫 / 綜合報導〕Apple Pay行動支付服務今年三月二十九日在台推出後，我國發生首例盜刷案，涉案人是國內知名的騙子黃琪。



辯稱沒錢 無交保金走出地檢署

本名黃照岡的二十五歲黃琪，今年初才因詐欺案獲得交保，四月間取得他人信用卡個資，矇騙銀行核發授權碼後，利用Apple Pay不用實體信用卡即可刷卡的功能，冒稱自己是息影影后林青霞的助理四處盜刷購物、住飯店等，至少涉案三十四筆，他雖揮霍享受，但落網後表示沒錢付三萬元交保金，最後不用保金改成限制住居及責付律師，昨晚七時悄悄從新北地檢署法警室側門離開。

刑事局表示，黃琪取得至少兩名被害人個資、信用卡號，打電話給銀行通過徵信，將Apple Pay認證電話變更為自己手機及獲發授權碼，開始盜刷。



信用卡測錄裝置 (card skimmer) 二秒鐘安裝完成



QR Code 支付

偷換店家支付QR code 賊輕易盜收500萬

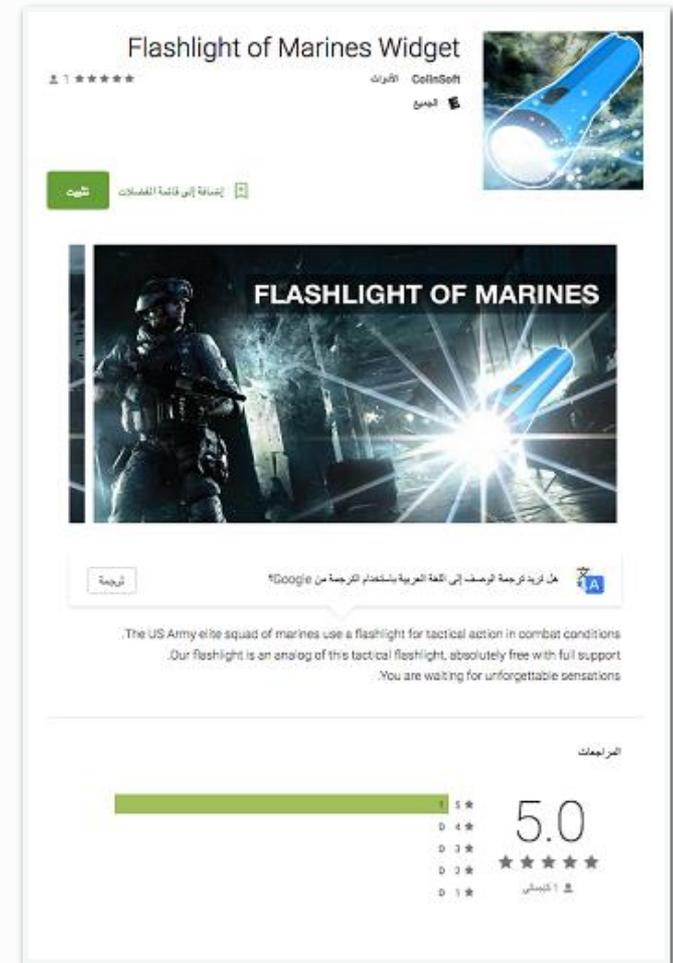
🕒 2016/12/22 12:30

記者 高嘉甫 / 攝影 盧宏昌 報導

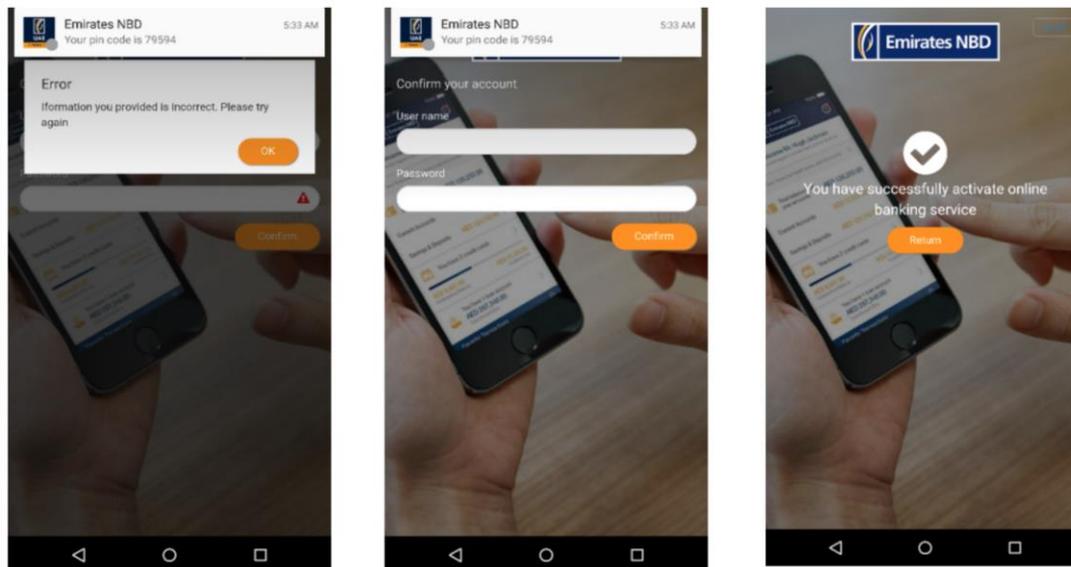
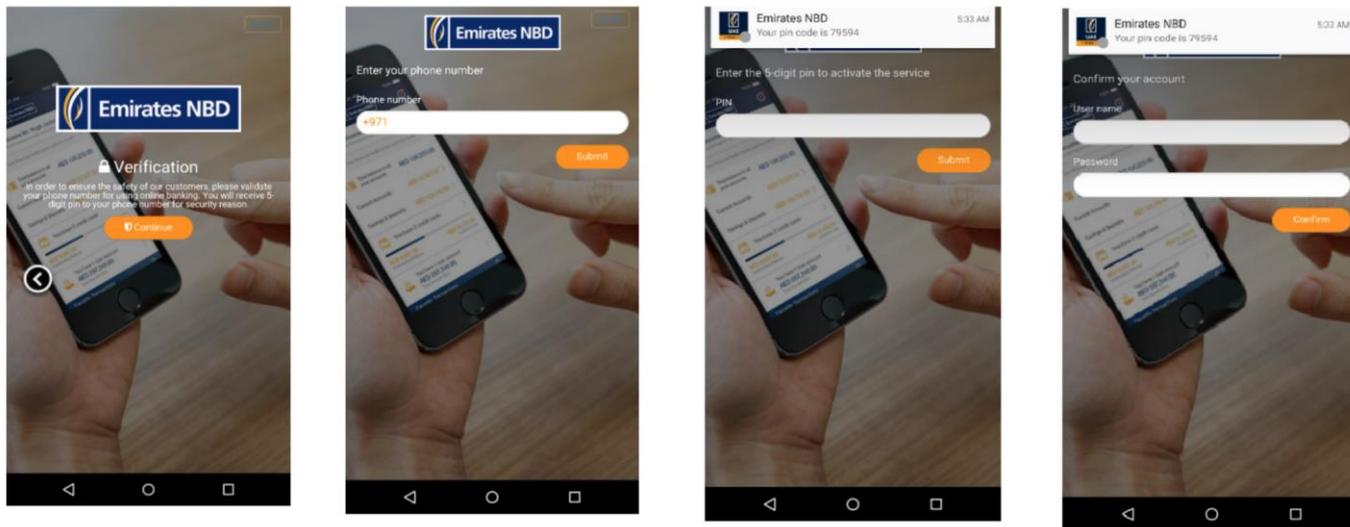


行動銀行 (Mobile banking) 惡意 APP -- bankbot

- Google Play 商店上出現了含有 Bankbot 惡意程式, 偽裝成正常的應用程式到處散佈。
- 至2017年9月為止, 總數就超過 20 個以上。
- 利用假網頁覆蓋在正常行動銀行App上方, 以盜取使用者所輸入的帳號密碼。再使用偷來帳密從網路銀行登入, 進行轉帳。
- 惡意程式還會攔截手機的簡訊雙重認證, 讓受害者無法察覺。



Bankbot 利假網頁覆蓋在正常行動銀行App 上方, 來騙取銀行的帳號密碼



SWIFT 系統金融犯罪

自由時報

Liberty Times Net

即時新聞 ▾

報紙總覽 ▾

影音

娛樂

汽車

時尚

體育

3C

評論

玩咖



臺北市 26°C

駭客入侵遠東銀行SWIFT系統 金管會：損失由銀行承擔



2017-10-06 20:39



〔記者王孟倫 / 台北報導〕針對遠東銀行發生電腦病毒入侵，金管會今天表示，該行清查此事件屬於虛偽交易，並非從個別客戶帳戶匯出資金，因此，客戶沒有損失；金管會也強調，未來若有損失，全額由該行承擔，故客戶權益不受影響。



遠東銀行發生電腦病毒入侵。(資料照，記者李靚慧攝)

金管會表示，於10月5日接獲遠銀通報，經該行檢視發現疑似駭客入侵SWIFT系統產生虛偽交易之情形，已立即要求該行立即強化網路安全防禦。

經查，遠銀遭駭事件並未造成客戶損失，而金管會接獲遠東銀行通報SWIFT系統異常後，也請其他各銀行進行全面清查；根據其他銀行回報結果，SWIFT系統均屬正常。

為加強金融機構資訊安全維護，金管會並要求各銀行

SWIFT 系統遭攻擊盜領事件回顧



2013 : 孟加拉 Sonali Bank (被盜 25 萬美元)

2015/01 : 厄瓜多銀行 Banco del Austro (被盜 1,200萬美元)

2015/10 : 菲律賓某銀行 (損失數目未知)

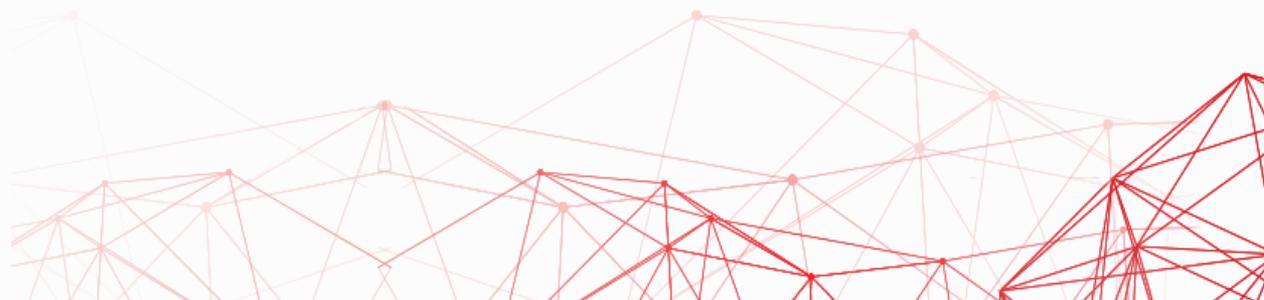
2015/12 : 越南先鋒銀行 (險遭竊 120萬歐元)

2016/02 : 孟加拉央行 (被盜 8,100萬美元)

2016/06 : 烏克蘭銀行 (被盜1,000萬美元)

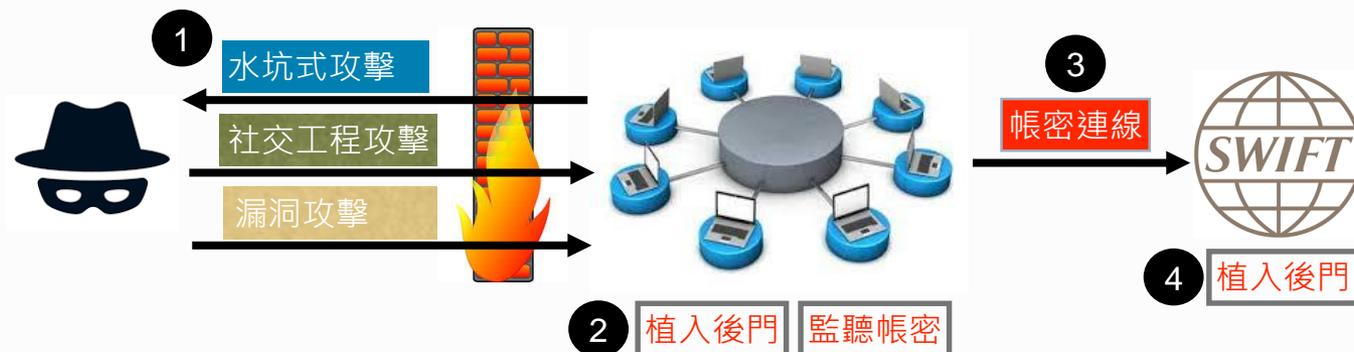
2017/10 : 台灣遠東銀行 (遭轉帳 6,000 萬美元)

2018 : 俄羅斯銀行 (被盜 600 萬美元)



SWIFT 入侵事件的共通點

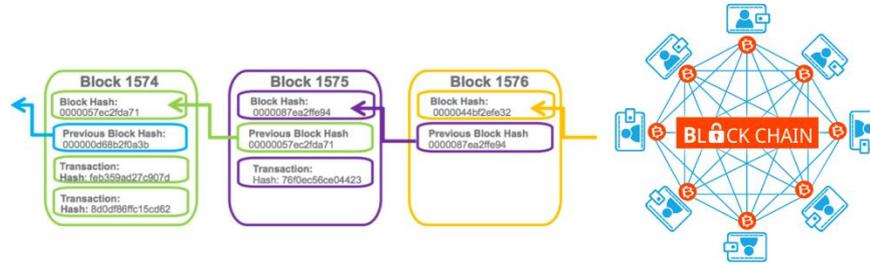
- 銀行內部網路被佔領
- SWIFT network 伺服器被佔領
- 駭客可以從Internet遠端進入SWIFT伺服器
- 駭客對於SWIFT messages type很熟(對整個SWIFT系統 Alliance Access軟體也很熟)
- 惡意程式可將其所有活動痕跡刪除
- 惡意程式內的英文, 常會拼錯..... (例如: already 拼成 alreay)





數位貨幣 與區塊鏈

區塊鏈的特性



1. 資料無法篡改

- 使用「區塊」與「鏈結」確保交易資料在合理時間內無法篡改
- 篡改一個區塊要把所有的鏈結區塊都一起篡改

2. 可驗證的匿名制

- 使用公開金鑰驗證機制，確認這筆交易的真實性

3. 去中心化的信任機制

- 同一份交易帳本會被複製到每一個結點 (Node)
- 篡改單一帳本是沒有任何意義的，系統默認擁有相同帳本數量相對較多的節點的版本才是真實的帳本。無需藉助任何第三方中心的介入就可以使參與者達成共識，以極低的成本解決了信任機制

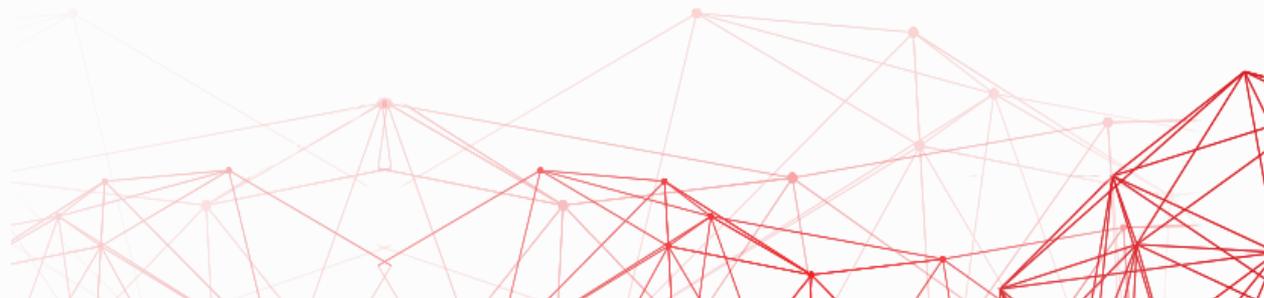
概念上 = 低成本的分散式資料庫(帳本)



智能合約 (Smart Contract) 開啟區塊鏈的無限應用



- 區塊鏈的特性給「合約」提供可信賴的執行環境
 - 無法篡改、可驗證性、分散式的真實帳本(合約保存)
- 智能合約：一個可以自動執行合約的電腦程式。這個程式可以回應、接收、保管數位資產，並按照事先約定好的規則執行操作。



區塊鏈的應用

- 各式交易記錄
 - 結算系統、國際匯款、跨境支付、行動支付、供應鏈追蹤
- 可數位化的資產或物品
 - 虛擬貨幣
 - 保險契約及理賠
 - 有價證券發行及交易
 - P2P融資



區塊鏈應用的 資安風險

交易所：駭客眼中的肥羊

Cryptocurrency exchange Coincheck has \$500m Nem coins STOLEN in biggest hack in history

A CRYPTOCURRENCY exchange had £350MILLION (\$500m) wiped from its listings after hackers stole NEM coins from Coincheck in possibly the biggest crypto hack in history.

By LAURA MOWAT

PUBLISHED: 12:21, Sat, Jan 27, 2018 | UPDATED: 13:53, Sat, Jan 27, 2018



NIKKEI ASIAN REVIEW

Log in | Subscri

Search articles

| Home | Spotlight | Politics & Economy | Business | Markets | Tech & Science |

Spotlight > Cryptocurrency

February 6, 2018 4:08 am JST

North Korea suspected in Coincheck cryptocurrency heist

Hack on Japanese exchange provider follows similar thefts in South last year

SOTARO SUZUKI, Nikkei staff writer



1億美元的以太坊智能合約 (Smart Contract) 漏洞

智能合約是一段邏輯程式碼，只要是程式碼就會有一定 Bug
、也可能會有安全漏洞

The screenshot shows a news article on the iThome website. The article title is "The DAO專案遭駭客盜走360萬個以太幣，價值暴跌逾40%". The sub-headline reads: "駭客利用了The DAO專案中潛藏的遞歸呼叫漏洞，將逾360萬個以太幣移轉到child DAO中。由於The DAO要求投資人先把資金轉到child DAO中，要經過27天之後才能提領，這筆虛擬貨幣目前仍在child DAO中。". The author is listed as "文/ 陳曉莉" and the date is "2016-06-20 發表". There is a link to "按讚加入iThome粉絲團". Below the article is a banner for "The DAO" with the text "THE DAO IS REVOLUTIONARY." and a "CREATION STATISTICS" button. A small caption at the bottom right of the banner says "圖片來源: The DAO".

基於Ethereum（以太坊）公共區塊鏈平台的分散式自治組織（the Decentralized Autonomous Organization，The DAO）專案在上周五（6/17）遭到駭客入侵，駭客盜走了逾360萬個以太幣（Ether），以上周五每個以太幣價值20美元來計算，總價約7200萬美元。不過，駭客盜走以太幣後導致價值暴跌，已跌至11.2美元。

ICO第一天駭客就用很簡單的修改網頁方式 盜走價值 770萬美元以太幣

\$7 Million Worth of Ethereum Stolen During CoinDash ICO

July 30, 2017

126 0



Hackers hijacked cryptocurrency trading platform CoinDash last week just as it was in the middle of its initial coin offering, or ICO. It's the first known breach of an ICO, this season's hottest fundraising method.

ICO (Initial Coin Offering) 是目前最熱門也是爭議最多的金融科技，令不少新創公司選擇透過 ICO 進行募資，並鼓勵投資人利用數位貨幣以換取該公司的代幣 (Token)，取得代幣就等於握有公司股權。



Christian Montoya [Follow](#)

Views expressed here do not represent those of my employer.

Sep 26 · 11 min read

How one hacker stole thousands of dollars worth of cryptocurrency with a classic code injection hack on EtherDelta and what you can learn from it



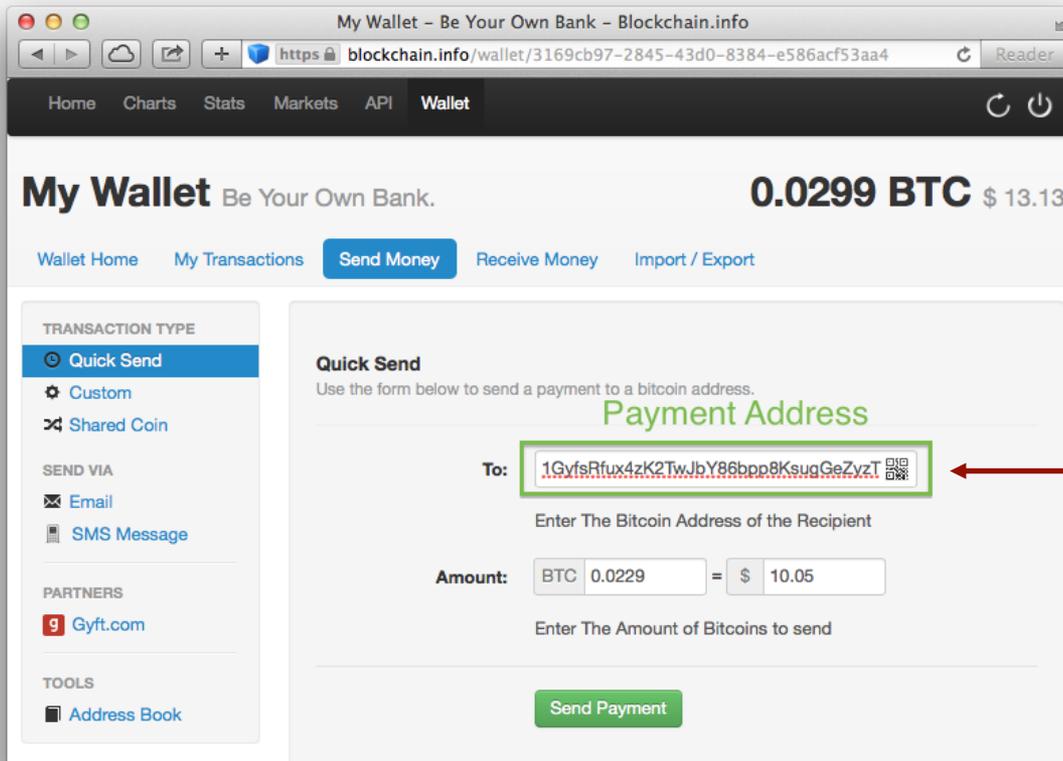
針對加密貨幣的惡意程式



By William Suberg

JUN 07, 2017

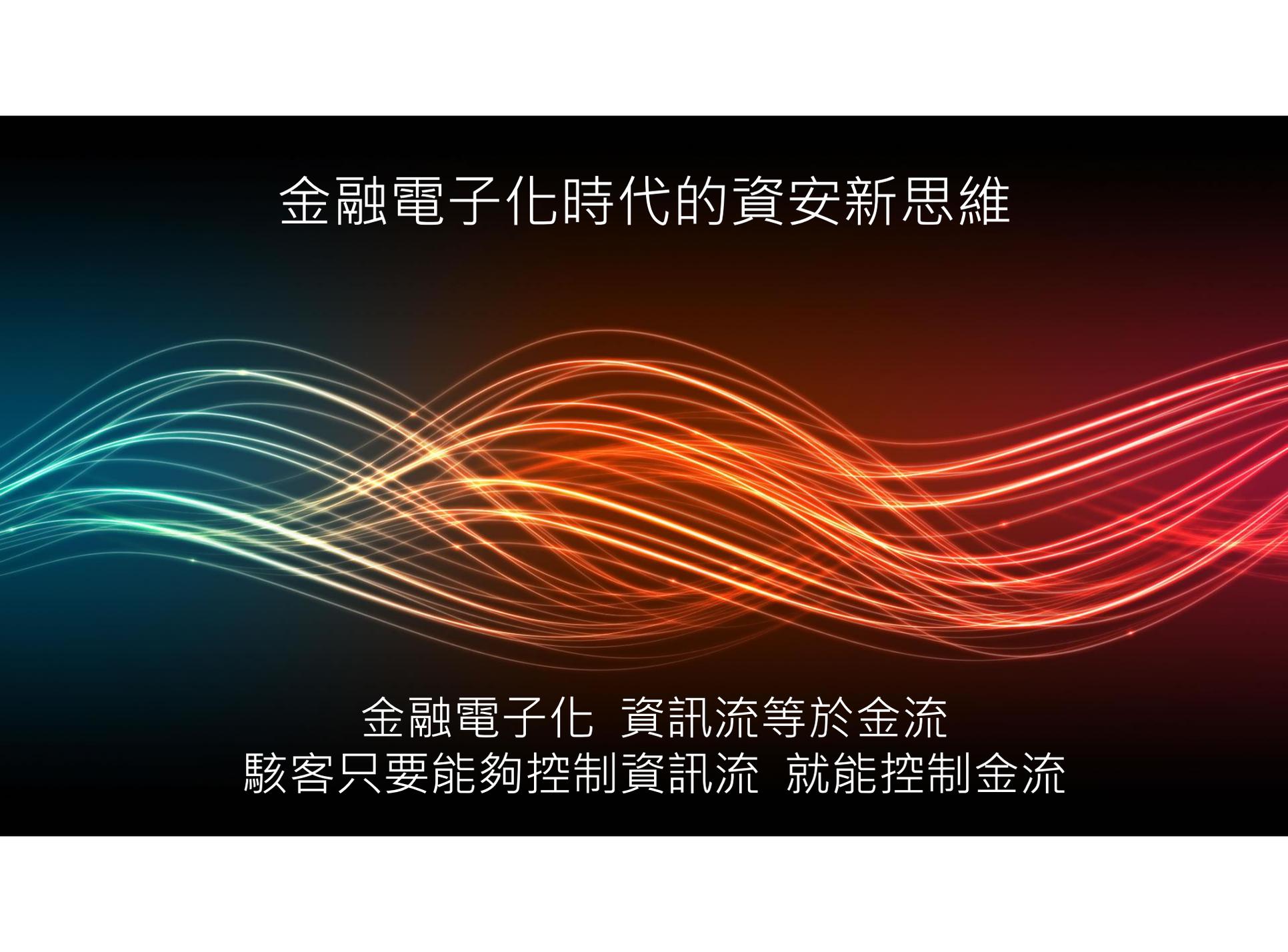
Bitcoin Malware Changes Destination Wallet To Steal 13 BTC



受感染的電腦，其中的惡意程式在 Copy & Paste 過程，自動置換付款地址



金融電子化時代的資安新思維



金融電子化 資訊流等於金流
駭客只要能夠控制資訊流 就能控制金流

資安思維：Fintech 服務提供者



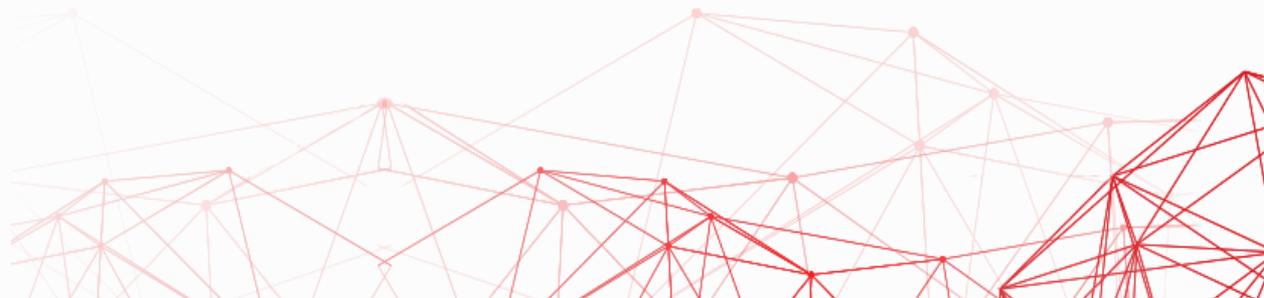
- 提升人員的資安意識
 - 避免 Targeted Attack 最常見社交工程手法
 - 加強程式開發人員、系統維運人員資安能力
- 強化資安控管 (包含內賊監守自盜及協力廠商VPN連線)
 - 定期做原始代碼掃描、軟體安全更新、弱點掃描、滲透測試, 避免程式、系統遭受已知弱點攻擊
 - Access Control (連線控管, 存取控制, 帳密管制, 特權帳號管理、實體隔離)
 - Application Control (建立應用程式白名單)
 - Audit log (稽核紀錄與監控)



資安思維：Fintech 服務提供者 (續)

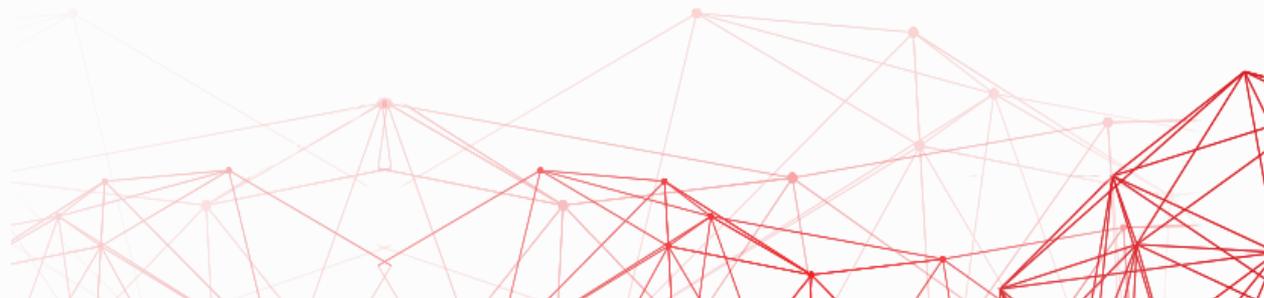


- 做好被駭客入侵的準備 (bad but true)
 - 建立資安事件響應程序 (Incident Response Process), 並定期演練, 以期將可能損失減至最低



資安思維：用戶端

- 主要問題
 - 帳號、密碼被盜
 - 個資外洩
- 如何預防
 - 不安裝來路不明的 App
 - 安裝並定期更新防毒軟體
 - 使用金融服務時，儘可能用手機的行動網路(3G/4G), 避免使用公共或不明 Wifi
 - 妥善保管機密資料 (如: 私鑰、個資、信用卡資料、帳號/密碼 ...)
 - 啟用雙重驗證 (Two-factor Authentication) 登入遠端服務



Thank You