區塊鏈技術與資產數位化

資本市場交易結算架構新範式

February 2016

For Discussion Purposes

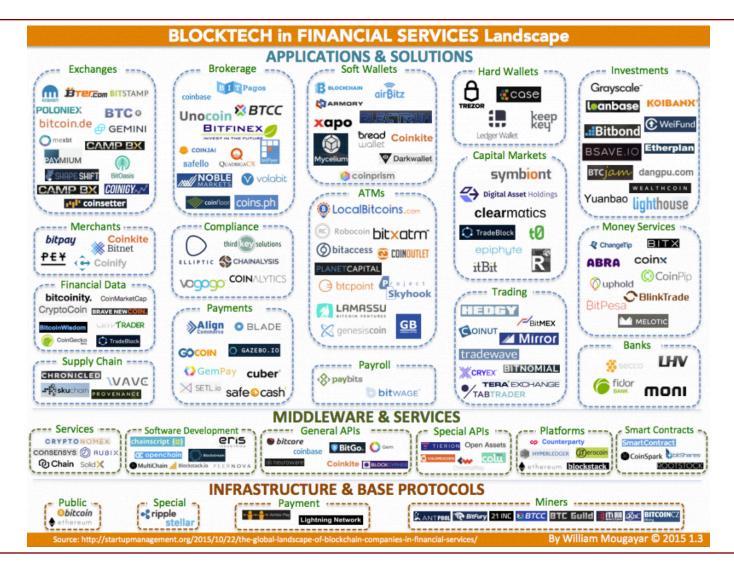
新型態信用基礎建設是金融變革的新希望



Blockchain Overview:

- An automated <u>workflow</u> process in which a disparate group of entities comes to majority consensus on the state of a shared ledger via non-hierarchical, peer to peer communication.
- A <u>mathematically irreversible</u> verification and authentication process which embedded in the network protocol.
- Ability to facilitate transactions between counterparities without a trusted central authority.
- A powerful new tool for implementing <u>cross-entity, multi-asset</u> clearing and settlement in market infrastructure.
- Potential as a viable <u>alternative liquidity venue</u> during liquidity crunch and credit crisis.
- Enabling technology for financial inclusion.

總計高達十億美元的創投資金已投入相關的新創企業



華爾街與矽谷精英:錯過區塊鏈就好比二十年前錯過互聯網

MARKETS

Ex-J.P. Morgan CDS Pioneer Blythe Masters To Head Bitcoin-Related Startup

Wall Street veteran will become CEO of Digital Asset Holdings, which formally launches Wednesday



Blythe Masters, shown in Denver in April 2012, helped pioneer the credit-derivatives markets in the 1990s. PHOTO: DENVER POST VIA GETTY IMAGES

By MICHAEL J. CASEY
March 11, 2015 12:41 a.m.

2 COMMENTS

Former J.P. Morgan Chase & Co. executive Blythe Masters has become one of the most high-profile Wall Street bankers to join the burgeoning digital-currency sector, taking on the leadership of a new platform for settling trades in bitcoin and other digital assets.

"How seriously should you take this blockchain technology? About as seriously as you should have taken the concept of the Internet in the early 1990s."

- Blythe Masters CEO, Digital Asset Holdings







Mark Andreessen – Tim Draper – Fred Wilson: Bitcoin today is like the Internet in 1994

華爾街與矽谷精英:錯過區塊鏈就好比二十年前錯過互聯網

JPMorgan Chase

Blythe Masters and JPMorgan trial blockchain project

Bank working with Digital Asset Holdings in efforts to cut trading costs

Goldman Sachs Group

Goldman Sachs files patent for virtual settlement currency

US bank files patent application for bitcoin-like ledger system



© EPA

DECEMBER 3, 2015 5:05 PM

Blytne Masters © Bloomberg

by: **Ben McLannahan** in New Yor

Less than a year after Blythe joining DAH!

全球知名金融機構已積極加速佈局投資

- Goldman Sachs part of \$50M investment into Circle (US) and has filed US patent for SETLcoin
- NASDAQ enabled first-ever private security issuance via its blockchain platform Linq
- New York Stock Exchange (NYSE), BBVA, USAA, Westpac part of \$75M investment into Coinbase (US)
- CME, Euroclear, LCH.Clearnet, LSE formed blockchain settlement group
- R3CEV, a permissioned Blockchain pilot program with broad support from 42 leading global banks
- Mitsubishi UFJ Capital & Mitsui Sumitomo Insurance \$4M investment in bitFlyer (Japan)
- Bank of England also proposed to study the feasibility of "digitizing" GBP onto Blockchain.
- People's Bank of China considered launching its own digital currency.

區塊鏈技術與相關法規挑戰

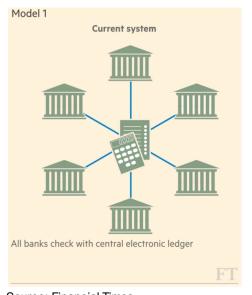
先進國金融監管機關持審慎開放態度支持金融創新

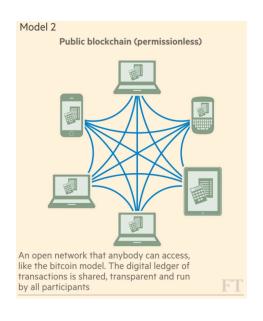
- UK Treasury, HM Revenue & Customs, Bank of England have put together the most comprehensive set of policies (http://www.thenewslens.com/post/141218/)
- NY State has begun collecting applications for BitLicenses (http://www.coindesk.com/nydfs-22-bitlicense-applications/)
- European Court of Justice Rules Bitcoin Exempt from VAT (http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/)
- Japan is still in deliberation mode and widely expected to promulgate constructive policy (http://www.japantimes.co.jp/news/2014/12/04/business/bitcoin-policymaker-tries-gain-converts-election/)
- Russia remains conservative due to ideology (http://www.coindesk.com/russian-president-vladimir-putin-addresses-bitcoin/)

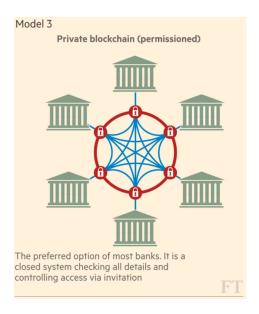
區塊鏈技術概覽

從單中心到多中心清算網絡的新型態信用基礎建設

- 區塊鏈結合先進密碼學與網絡通信科技,實現了「共享帳簿」(shared ledger)或「帳聯網」此一新型態信用基礎建設。
- 單一中心信用架構:效率最高,但若該中心節點被攻陷,整個支付系統也就隨之癱瘓,且發展受限於經濟體的先天限制。
- 多中心化信用架構:同儕節點均保有一份經最新密碼技術保護的交易帳簿達成清算共識,創新快速但監管較為不易。
- 經監管機關**認許**(permissioned)的多中心化清算網絡是可在效益與效率之間取得平衡,又能與既有系統兼容並蓄的新方案。





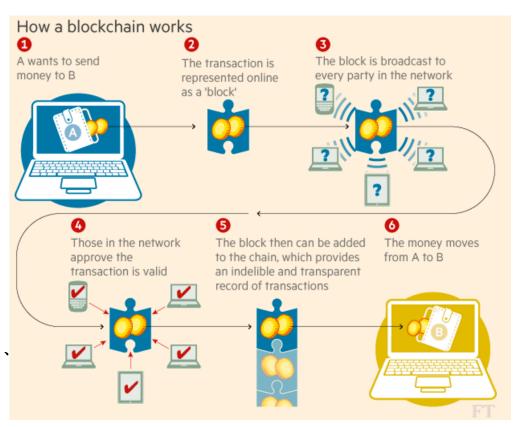


Source: Financial Times

區塊鏈技術概覽(續)

從單中心到多中心清算網絡的新型態信用基礎建設

- 想像一個連結不同支付與交易平台紀錄資料庫的「帳聯網」。
 - 經監管機構認許的帳聯網節點如同電子郵件伺服器。
- 「價值」傳遞應該如同電郵傳遞一般方便。
 - ▶ 網內互打 vs.網外漫遊
- 支付平台之間應該達成無障礙互通互聯(interoperability)。
 - 範例一:用戶手機號轉換電信商;
 - ➤ 範例二:金融卡ATM跨行轉帳;
 - ➤ 範例三:小額點對點移動支付;
- 區塊鏈技術可立即實現支付平台,消費者與商家之間傳遞價值、 紀錄交易的金融基礎建設。
 - 共享帳簿互聯網是繼複式簿記以來金融界的根本創新。



區塊鏈技術平台效益與風險

多中心化架構較能發揮網絡效益

單一中心清算架構	多中心化網絡架構
 優勢: 每秒處理交易量較高 單一監控節點易於監管 高資本門檻建立市場秩序 勞: 單一失敗環節 高額前期資本投入 	優勢: 僅需聯網節點傳遞訊息 無單一弱點癱瘓網絡風險 基於互聯網的軟體通訊協定 對 一 同儕節點須守望相助 網絡共識仰賴同儕節點多數決
所有用戶均須與中心節點連結大者恆大不利創新	

區塊鏈技術平台效益與風險 (續)

帳聯網發展須努力兼採認許與非認許架構的長處

非認許帳聯網 (Permissionless)

<u> 長處:</u>

- 多中心化架構無須信用機構存在
- 可在金融基礎不足的經濟體迅速佈建
- 有效抗衡極權管控
- 開放系統促進跨境聯網(例:bitcoin)

短處:

- 網絡共識能源耗費高("mining")
- 容易出現監管漏洞

認許帳聯網 (Permissioned)

長處:

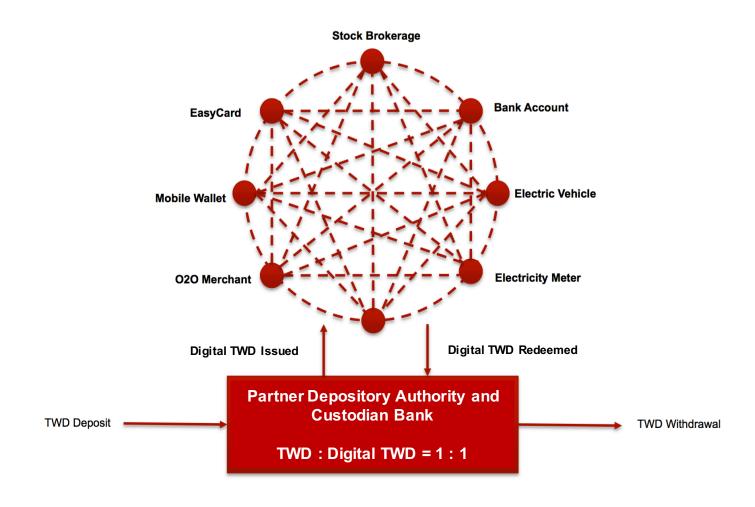
- 容易管理與換代升級
- 網絡共識較有效率
- AML/KYC程序較易落實

短處:

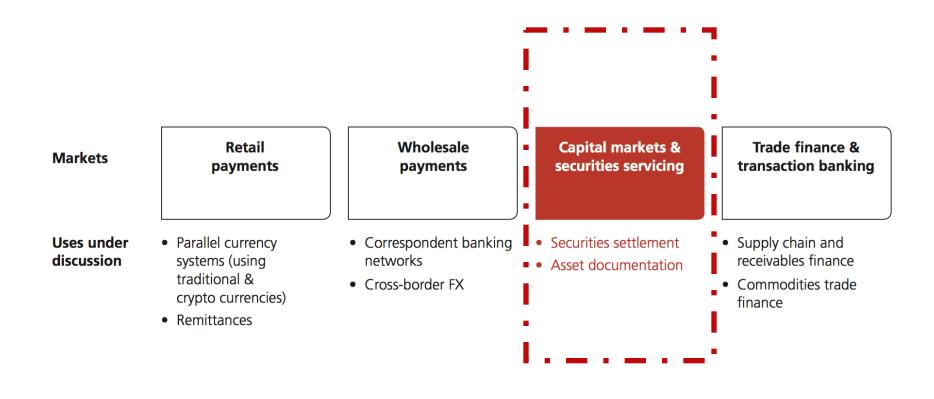
- 同儕節點必須有信用
- 跨境聯網不易無縫對接

認許區塊鏈架構實施策略

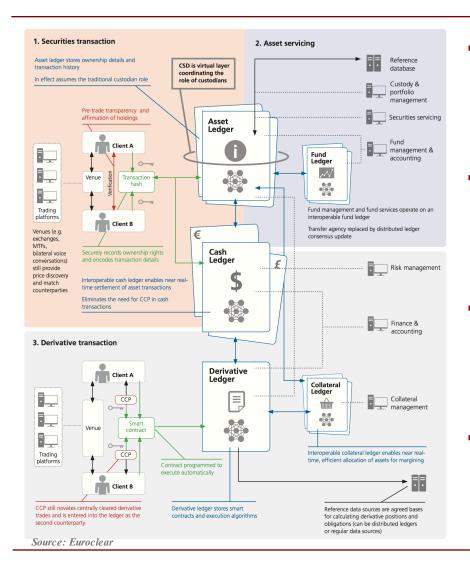
帳聯網營運架構示意圖



帳聯網信用基礎建設平台能力的自然延伸



帳聯網2.0:數位資產交易結算大平台



- Assets digitally natively created and/or registered on a decentralized ledger via blockchain technology.
 - 5 private blockchains to implement vital functions of the existing market utilities.
- Settlement is a ledger update confirmed by the permissioned network participants.
 - Almost instantaneous trade settlement that significantly reduces capital cost and operating risk.
- Financial intermediaries that create little value-add in the trade lifecycle might become redundant.
 - However, links to existing trading systems and market infrastructure shall be preserved.
- A trusted central authority continues to provide critical clearing and depository functions.
 - Centralized & Decentralized systems serve as back-up capacity with respect to each other.

帳聯網數位資產交易結算大平台的架構效益

Pre-trade Post-trade Custody & securities servicing

- Transparency and verification of holdings
- Reduced credit exposures
- Mutualisation of static data
- Simpler KYC/KYCC¹ via look through to holdings
- Secure, real-time transaction matching, and immediate irrevocable settlement
- Automatic DVP on a cash ledger
- Automatic reporting & more transparent supervision for market authorities
- Higher AML² standards

- No central clearing for real-time cash transactions
- Reduced margin/ collateral requirements
- Faster novation and efficient post-trade processing
- Fungible use of assets on blockchains as collateral
- Auto-execution of smart contracts

- Primary issuance directly onto a blockchain
- Automation and deduplication of servicing processes
- Richer central datasets with flat accounting hierarchies
- · Common reference data
- Fund subscriptions/ redemptions processesed automatically on the blockchain
- Simplification of fund servicing, accounting, allocations and administration

Source: Euroclear

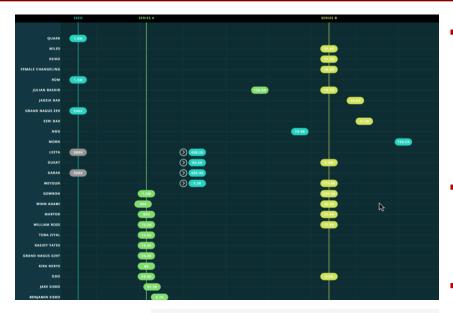
¹ KYC – Know Your Customer, KYCC – Know Your Customer's Customer

² AML – Anti-Money Laundering

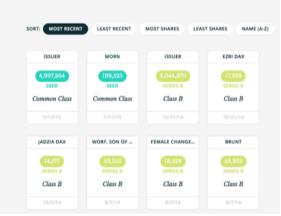
帳聯網數位資產交易結算架構的建議實施策略

Туре	Use case	Capital markets examples	Other industry examples	Rationale for adoption		
First order adoption – works as standalone	• Tokenising assets not currently on a common ledger (new blockchains on tokens on Bitcoin)	Pre-IPO equitiesSyndicated loansDepository receipts	Physical objects e.g.diamonds, paintings	Proof of ownership/ provenanceSettlement efficiency	•	
	 New blockchains to share data between participants KYC data sharing Collateral ledger to support efficient margining Reference and market data Supply chain data invoicing Trade finance Collection 	Multiple opportunities for capital market leaders to initiate pilot				
	New blockchains to process transactions	 Corporate finance bookrunning Fund portfolio management 	 Inter-bank blockchain to support cross- border banking payments Intra-bank blockchain to support cross- bank accounting 	 Disintermediation of actors Simplified data and infrastructure 	programs before disruption occurs	
Second order adoption – reliant upon critical mass of assets on blockchains	Monitoring of richer datasets	Concentration monitoringMarket surveillancePricing data	Trade flows, transit data	 Powerful understanding of data 		
	Processing using blockchains	Securities servicingRegulatory reporting	•	Efficient processing capabilities		
Source: Euroclear	•					

案例研究: NASDAQ Private Markets with Linq

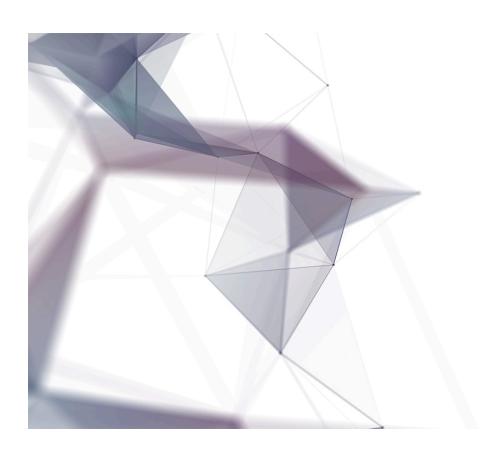






- The first platform from an established financial services firm to demonstrate how digital asset trading on blockchain-based platforms.
 - Part of Nasdaq's product suite of services for entrepreneurs and venture investors.
- Potential to remove operational pain points (mostly due to human errors) by providing immutable recordkeeping and a chain of custody for users.
- Cap table management dashboard with equity funding timeline monitoring toolkits.
 - Big implications for corporate finance and M&A activities.
- Startups using the platform can also view stock certificates by date of issuance and by overall ownership, drilling down into which investors hold the most shares in the company with a single click.
 - Look-through transparency offers multiple benefits.

案例研究:Smart Contract via Ethereum





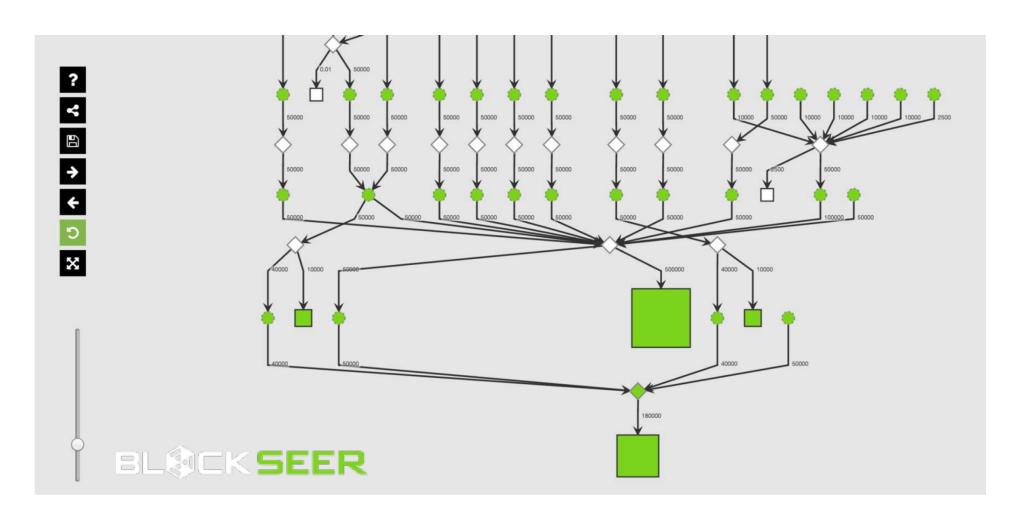
ethereum

- Just as assets can be represented on blockchain ledgers, so can business logic enforcing contracts.
- These smart contracts, once embedded into a blockchain through consensus, cannot be modified.
- With a blockchain protocol such as Ethereum, the full range of logic that can be represented by a Turingcomplete programming language, can also be embedded into a blockchain.
- Profound implications for security collateral lending, cross-margining provisioning, portfolio risk management, exotic financial derivatives structuring & execution. asset securitization, regulatory compliance monitoring, etc.

案例研究: Crowdfunding via Smart Contract

```
contract token { mapping (address => uint) public coinBalanceOf; function token() {} function sendCoin(address)
contract Crowdsale {
    address public beneficiary;
    uint public fundingGoal; uint public amountRaised; uint public deadline; uint public price;
    token public tokenReward;
    Funder[] public funders;
    event FundTransfer(address backer, uint amount, bool isContribution);
    /* data structure to hold information about campaign contributors */
    struct Funder {
        address addr;
        uint amount;
    /* at initialization, setup the owner */
    function Crowdsale (address beneficiary, uint fundingGoal, uint duration, uint price, token reward)
       beneficiary = beneficiary;
        fundingGoal = fundingGoal;
        deadline = now + _duration * 1 minutes;
       price = price;
        tokenReward = token( reward);
    /* The function without name is the default function that is called whenever anyone sends funds to a con-
    function () {
        uint amount = msg.value;
        funders[funders.length++] = Funder({addr: msg.sender, amount: amount});
        amountRaised += amount;
        tokenReward.sendCoin(msg.sender, amount / price);
        FundTransfer(msg.sender, amount, true);
    modifier afterDeadline() { if (now >= deadline) }
```

案例研究:AML/KYC視覺化即時監控平台



區塊鏈技術平台投資策略

支持帳聯網新創企業可協助台灣金融業開創新藍海

- 帳聯網技術架構可以更有效地實現金融科技創新的發展願景:
 - Regulated Interoperability, Cyber Security & Consumer Protection
 - ▶ 加強推動Bank 3.0革新方案,實現互聯互通、可管可控的用戶體驗。
 - 整合跨領域資源,讓台灣成為亞太區領先的區塊鏈金融商品與服務創新的研發與投資平台。
 - ▶ 發揮台灣既存優勢,掌握領先全球的關鍵契機,提升台灣金融業的全球競爭力。
 - 創造經濟新動能與新希望,立足亞洲,進軍全球。

區塊鏈技術平台投資策略 (續)

支持帳聯網新創企業可協助台灣金融業開創新藍海

- 帳聯網技術架構可為台灣金融業帶來的利益:
 - ▶ 移動社群支付平台:創造互聯互通、可管可控的移動支付體驗,讓消費者與商家「信」而樂「用」。
 - ▶ 信用評級機構:全行業共享底層用戶大數據,提升信用風險預警及控管能力。
 - ▶ 商業銀行:自主創建信用卡/現金卡結算網絡,無須支付境外網絡服務費即可跨境支付,有利打「亞洲盃」。
 - 證券承銷商與投資銀行:提升中後台跨資產級別的交易與清算能量,提升資本運用效率。
 - ➤ 保險公司:從帳聯網到金融物聯網的自然演進,增強風險定價能力與管理水平。
 - 基金管理公司:資產數位化創造具流動性的多元投資工具,實現金融商品大市集。
 - ▶ 法律會計服務業:文件託管、公證、記帳等傳統業務的服務模式革新。
 - ▶ 其他:食品安全認證機制,跨國企業金流即時監控、新型金融資訊犯罪預防服務,網絡聲譽防護。

區塊鏈技術平台投資策略 (續)

以帳聯網打造金融科技開放市集大未來



區塊鏈技術平台投資策略(續)

以帳聯網打造金融科技開放市集大未來



■▶新支付趨勢》

要實現這個關景,可從台灣所有銀行與第三方支付平台的手機錢包 诱過共享經復技術形成經際網失業主,推而實理全職物際網

摺文:劉世偉、胡一天、管中間、際世偉

前的第三方支付系統正在面臨新的變革。
□ 20年前互聯網剛剛開始發展時,電子頭 訊系統(何如電子郵件、BBS站)有許多家營運 商、每一家都經營自己的主機、每台主機都被保 護在各種防火牆後集中管理,彼此之間不直接共

今天的第三方支付系統很類似當年的電子通訊 系統;目前全球知名的第三方支付平台,例如阿 里巴巴的支付實、騰訊的微信支付,及剛從eBay 分拆覆立上市的PavPal,本質都是封閉系統,不 同亚台的田戶之間無法百途轉載。田寮住高的祭 海縣才來比擬, 这些大刑支付至台的田戶網內石 打很方便,但要網外漫遊時就很昂貴。這樣的封 閉系統顯然有改進的空間。

台灣如今正在發展第三方支付系統,尤其應該 注意新的發展方向。因為奠基於中國大陸或美國 等大型經濟體的主要支付平台的用戶數都已經破 億,規模經濟使得增加一名新用戶的邊際成本只 會線性增加,但隨著用戶增長與支付應用的拓 展,平台的網絡效益卻會呈現指數性上升。這意

味著大型支付平台運營商已經有足夠的臨界質量 來維持大者恒大的競爭優勢。反觀台灣,本土市 場較小、且金融業過度競爭、單打程門的銀行或 第三方支付業者較難累積足夠的臨界質量來創造 规模經濟與網絡效益。因此,台灣不應侷限於傳

在目前的技術發展中·共享帳簿(shared ledger)是最受矚目的一種技術。受惠於此一技 術在移動支付、個資保護與反洗錢等面向的迅速 孙屋街全球大刑会励楼梯的重组,新世代古村区 終非常有可能將依据常都系統在過去20年的發展 軌跡,向開放協定、平台互通、以網絡聯盟而非 單一機構為清算主體的範式快速演進。

第三方支付平台將走向「多中心化」

(centralized) 架構(詳見圖1) · 所有消費者 與商家均須與一個受信任的中心節點連結,讓價 值的傳播誘過該單一節點清算與紀錄。中心化架 構的效率最高,但若該中心節點被攻陷,整個支 付系統也就隨之瘧瘅。在實際世界中,由於市場 競爭、地理侷限與反壟斷法規的限制。單一支付 平台不可能獲霸天下。

對台灣這樣外向型的島嶼經濟體而言,地緣政 治與國安考量很可能會限制非本土大型支付平台 在台灣的發展。但若監理法規的制定與詮釋太過 審慎、很容易造成本土大、國際小的台灣第三方 支付業者與金融機構各自為改、使得這些系統無 法實現網絡效益,陷入過度競爭又無法累積用戶

相對於中心化的系統,多中心化 (decentralized)的「帳聯網」架構(詳見圖 2) ,是既可在網絡效益與清算效率之間取得平 衡,又最能發揮台灣相對優勢的替代方案。每一 個紅色節點可以是商業銀行、第三方支付平台或 是想分享清算網絡效益的非金融機構(何知電訊 育) ,都是受法規認許及市場信任的清算主體。 每個清算主體都可以是中心節點。

單一清算中心節點的效率

最高,但風險也高

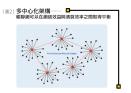
(圖1) 中心化架構─

每一個黑點代表消費者或是商家,均可以與-個或多個紅色節點對接 (開戶), 也可以直接诱 過紅色節點實現不同平台用戶之間的對接。從 平台A轉帳到平台B,就如同自Gmail街電部到 Yahoo電箱一般便捷。便捷的理由,是因為每個 紅色的點都保有一本相同帳簿的副本。

每份副本的內容雖然相同,但都使用最先進的 公開秘輸 (public key) 加密技術保護,只有持 有到應解密金鑰的黑點才能修改對應內容。帳簿 副本之間的同步,如同電彩伺服器之間的連結 是透過共享帳簿技術中先進的加密通訊協定實 现。我們將這樣的清質架構構為「帳聯網」。

「區塊鏈技術」將創造巨大商機

帳聯網技術最為知名的應用,就是承載比特幣 的「區塊鏈」(Blockchain)。區塊鏈技術的核 心、既可允许多中心化、無需信用中介機構的比 特幣,亦可容許一群通過認許、值得信賴的同價 節點,例如領有牌照的第三方支付業者與商業銀



向全球金融科技新創公司開放金融基礎建設

圆代工商業模式的時代,而

一群有遠見的投資人在1987

年成立了台籍電。來到2015

年,全球半導體產業的競爭格

局已經發生了巨大的變化。根

據2015年上半年統計(詳見

品種競爭的能力,最終陷入被

表2) , 日資企業在全球前20

如同台積雷惠注品圖製程的精進與研發、打造變世無匹的半導體製造業用戶體點 台灣金融業也有絕佳的機會在此刻藉由帳聯網,創造金融科技的台積電

撰文:劉世偉、胡一天、管中間、廖世偉

動物 , 往往偏重在金融面 或科技面的技術性議題,鮮少 從新科技與新商業模式促推產 業結構範式移轉的角度來理解 這個趨勢的意義。本文參考全 球半導體產業在過去30年的變 化、對台灣金融科技以及金融 產業的發展方向提出新的觀察

從半導體業國衰看全融業

不到30年前,日本企業在 全球前20大半導體廠商總營 收规模中的占比超過55%。 研究「菊花與劍」是美國商學 院的顯學,好菜塢電影中的日 本形象是且未來感的高科技島 托邦,日資企業在全球大學擴 世界。當時全球半導體產業的 競爭格局(詳見表1)。

自外部遵應性和生存能力高的

大坐填棚窗面由僅占有4個名 額,在前10大中僅有1個名 (表1)1987年 全球半導體營收規模 額,且在前20大總營收規模 占比僅約10%,與1987年 前20名排行榜 的學譽相去其读。在此同時, (百萬美元・米松遠景図製 台積電已崛起為排名第三,發 收占比近10%的領導廠商。 2 東芝 日本 3,029 日本在全球半導體業與消費性 電子產業中大幅敗退的原因, 6 富士通 日本 1,801 有人歸咎於擁抱封閉標準的島 三菱 日本 1,492 國心鄉, 即所謂「加拉巴哥症 三洋 日本 852 候群」,意指在孤立的環境下 OKI 日本 651 霜自進行優化,而喪失面對來

企業文化不利創新,有人說是

泡沫經濟破滅後整體經營策略

大規約。但是一個非常重要約

不常被討論的原因,就是台稿

在1990年代以前,半導體

夏普 日本 590 新力 日本 571

堂流行垂直整合。從設計、生 超其他大企堂一較短長、發揮 勘堂现行孕期的缺憾。好如同 產到行銷,通通自己來。即使 到了21世紀,一些最成功的半 導體企業,如英特爾或三星, 仍然堅持结個模式。但在只有

垂直整合的世界中,沒有自建 品圆廠的品片設計公司不可能 在高達2,500億美元產值的 半導體業中占有超過15%的 份額。從這個角度看,無廠坐 導體產業的「得」,是日資半 導體業的「失」,這是台積電 以及品圖代工業的巨大成就。 透過台積電晶圖設計的開放標 準 (Process Design Kit) / 沒 有資力自建品圖的新創公司。

例如當年的高通、博通與聯發

營收規模前20名排行榜 (百萬州元・大田諸原調) 英特爾 美國 23,578 51,400 3 3 台積電 台灣 13,624 24,976 5 4 高通 美國 8,287 19,291 8 8 東芝 日本 5,500 11,040 9 9 博通 美國 4,154 8,428 13 12 聯發料 台灣 3,034 7,032

(表2)2015年上半年全球半導體

| 15 | 11 | Renesas | 日本 | 2,909 | 7,307 | 16 | 17 | 奈尼(新力) | 日本 | 2,652 | 5,292 |

19 21 勝電 台灣 2,320 4,350

20 23 直普 日本 2,223 3,515

創意,執行策略,赚取鉅額利

帳聯網具開放標準的精神

局, 应1980年代後期的半導 體產業有許多相似之處。一些 巨大的全型機構不力型投速好 股關客戶資產與審慎承作貸款 的角色,反而捨本逐末,想要 「垂直整合」金融服務的用戶 體驗。從分行裝潢到移動支付 App的設計, 乃至開發組售各 式各樣叫人眼花撩亂的理財產 品。殊不知以如此資本密集的 科,才有機會在全球市場上 經營模式,已經難以來彌補金

成本,又競爭不過快速挟代的 新创公司,消费者缓不一定领 情,但要自己開發AppStore 為例,無論是阿里巴巴的支付 寶、騰訊的微信支付、乃至蘋 果邸谷歌的支付平台, 目前都 看起來巨大無比。1987年的 日本半導體產業・亦復如是 鋭意進取的台灣金融業者無需 遵循資本密集的競爭選輯,也 不無理首台灣事食市占率,而 應學習當年台積電創造品圓代 工業的厳略思維・積極開創新

不久之前「輸人不輸陣」的電

信業者・從埋光纖到賣手機到

預裝移動應用程式,「彼一能

フ・己士之:被士能之・己百 之。」 直到iOS與Android橫

空出世、電信業者才認知到

自以為是的垂直整合只會增加

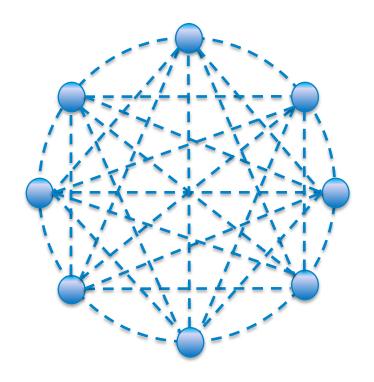
市場,重新制定遊戲規則。 在2015年11月號的《台 澄銀行家) 雜誌專文中,我們 提出了帳聯網這個新範式。在 互聯互通、可管可控的帳聯網 上,共享帳簿的資訊安全是透 過自顯聯網的同僚節點維護。 此一基於區塊鏈技術的多中 心化架構,將用戶對「帳戶」 的產權概念轉化成一組公開。 私密金鑰:所有帳戶的加密內 容是由所有帳腦網同傳節點井







Q & A



We Build the Internet of Value With You.