區塊鏈技術之發展現況與趨勢

2018/05

IBM Taiwan　Jack Hsiao 蕭俊傑

何謂價值? 如何衡量、呈現、儲存？

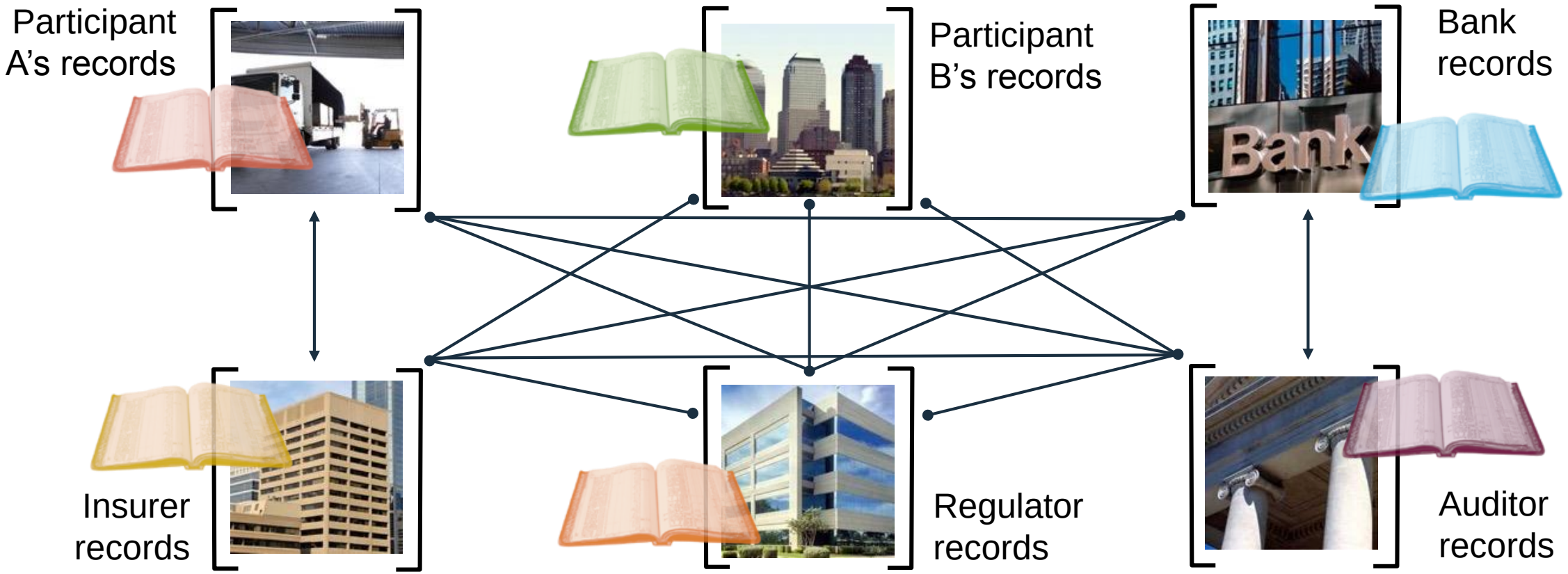
資料來源：台新金控孫一仕資訊長, 金融研訓院<價值網>

何謂價值？

三星公司估算該照片價值10 億美元
這都要歸功於數百萬推特用戶上網觀賞該照片。一個免費且即時的事件可以成就一個10 億美元價值的效應，明確的顯示了網際網路的價值

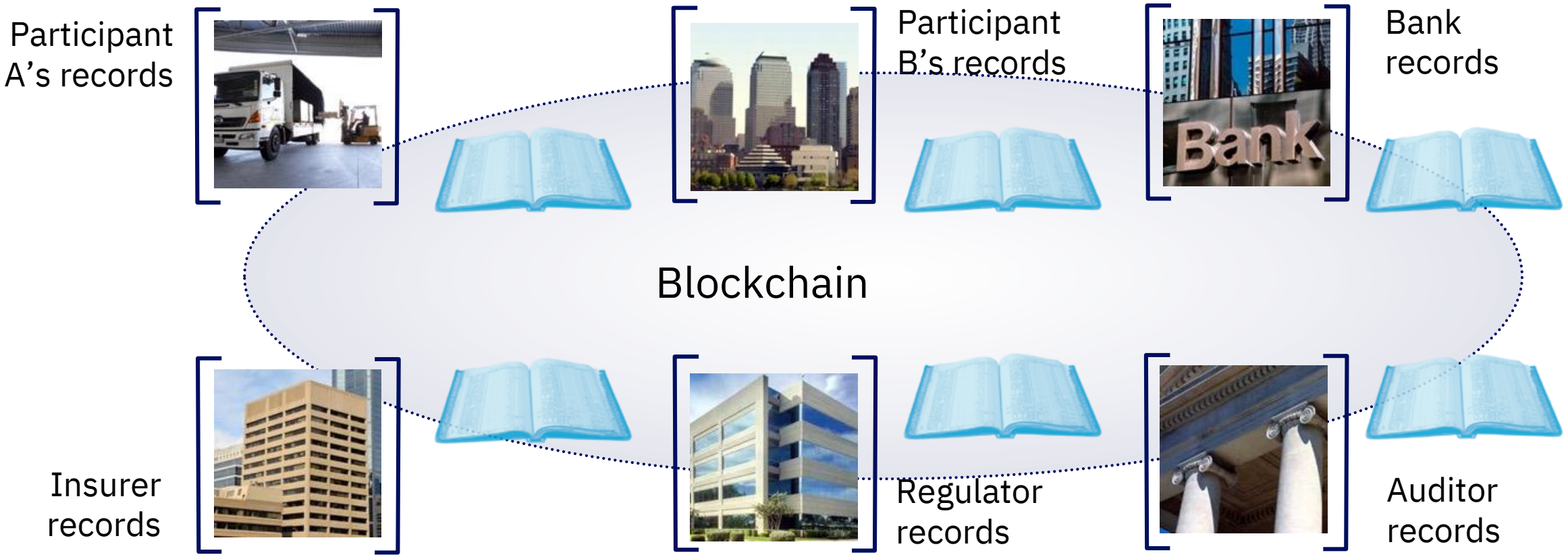
資料來源：台新金控孫一仕資訊長, 金融研訓院<價值網>

現今商業流程，資產交易仍是各個參與方自行記帳



… inefficient, expensive, vulnerable

透過區塊鏈分享式帳本可以讓交易更有效率



... with consensus, provenance, immutability and finality

(共識) (溯源) (不可否認) (最終性)

商用區塊鏈應具備的四大特性

基於商業網路的，
只能添加的
分散式記錄系統

將商業條款做為合
約執行條件
嵌入在交易過程中
自動執行

在保障安全、可信授權、
可驗證的前提下，
對相關參與方，
合理透明化資訊

交易由相關的參
加人背書

LINUX基金會區塊鏈超級帳本計畫Hyperledger 會員

Premier

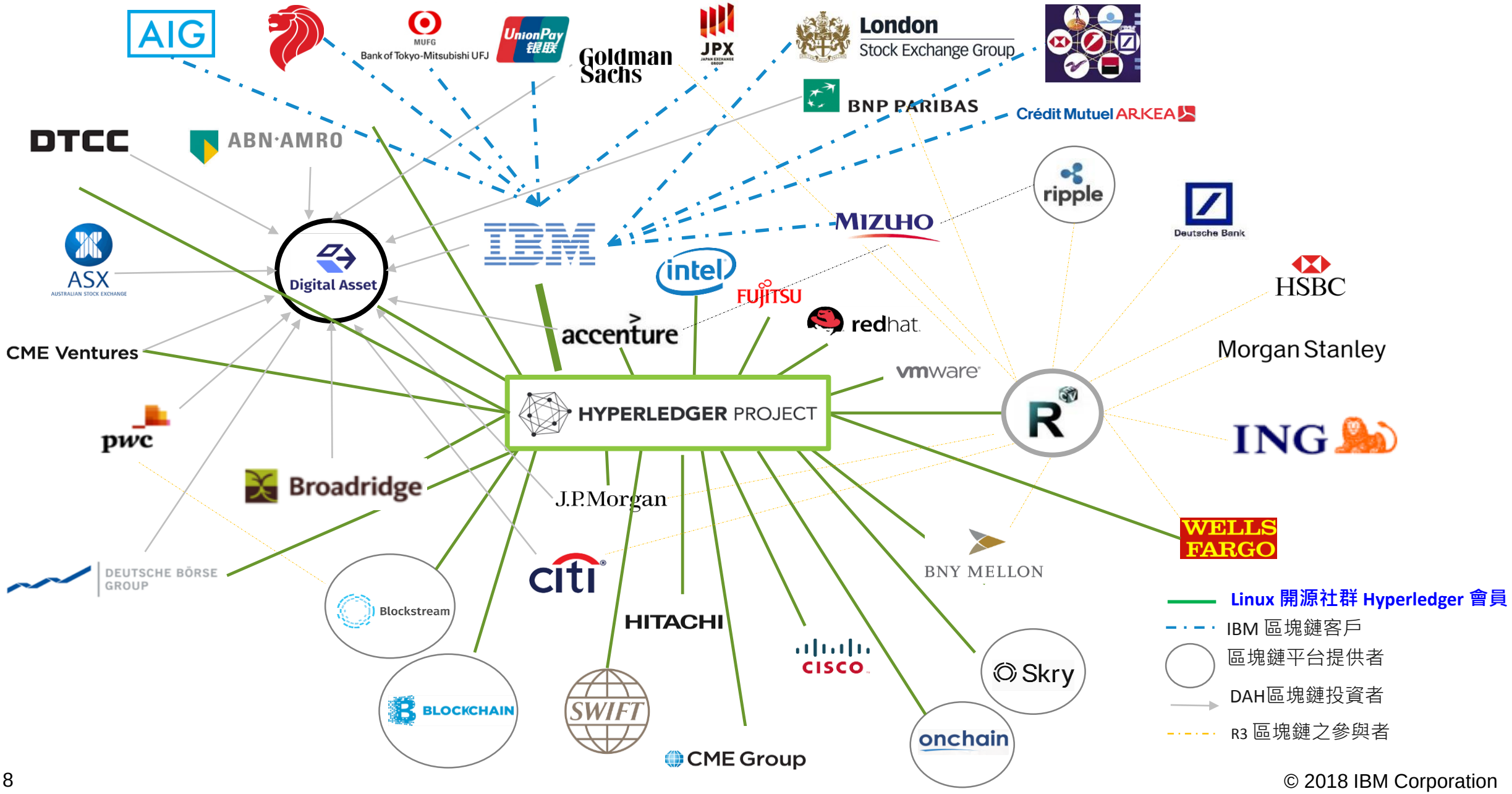
Associate

General

Associate (Academia)

Source: https://www.hyperledger.org/members Updated: 3 April 2018

Hyperledger 已成為全球最大聯盟區塊鏈平台生態體系



IBM在全球已有超過400個 Hyperledger 的案例

Trade Finance	Pre and Post Trade	Complex Risk Coverage
Digital Trade Chain, MIZUHO, NATIXIS, TRAFIGURA	DTCC, CLS Fundamental to FX, JPX, Bolsa Comercio Santiago	AIG, Standard Chartered
Identity/ Know your customer (KYC)	**Unlisted Securities/ Private Equity Funds**	**Loyalty Program**
SECURE KEY, Crédit Mutuel ARKEA, DIACC	NORTHERN TRUST, BORSA ITALIANA, SBI GROUP SBI証券	UnionPay 銀联
Medicated Health Data Exchange	**Fraud/ Compliance Registry**	**Distributed Energy/ Carbon Credit**
FDA	دبي الذكية SMART DUBAI	TenneT, ENERGY BLOCKCHAIN LABS
Supply Chain	**Food Safety**	**Provenance/ Traceability**
MÆRSK, PSA The World's Port of Call	Walmart, Driscoll's, Tyson, McLANE, Dole, Kroger, Nestlé, Unilever, gsf golden state foods	everledger

三菱東京日聯(BTMU/MUFG)攜手IBM 將Hyperledger區塊鏈用於合約管理(Case Management)

- 三菱東京日聯銀行（The Bank of Tokyo-Mitsubishi UFJ，BTMU）攜手IBM，欲將區塊鏈技術應用於商業夥伴之間的合約設計、管理和執行。兩家公司已經簽約，將使用超級帳本項目的開源平台來共同自動執行IBM雲上的商業交易
- 二者已經建立了一個基於區塊鏈的智能合約原型，他們表示此舉能為多方業務交互的服務水平協議大大提高效率和可靠性
- 三菱東京日聯銀行（BTMU）是日本最大的銀行，它計劃在2017財年開始使用區塊鏈技術來管理內部業務合同
- 為提高效率，二者將會使用傳感器來監管設備的交付和使用，此傳感器會把信息嵌入區塊鏈當中。這樣就可以在兩家公司之間實現開發票和支付過程的自動化

資料來源：https://kknews.cc/zh-tw/tech/9gmqrj.html

IBM融資部門 (IBM Global Financing, IGF)

提供4000多家上下游供應商、經銷商、業務夥伴間的訂單、庫存、應收帳款等供應鏈金流服務，總金額超過440億美元，2016年九月已上線

痛點

- 每年有兩萬五千筆爭議的交易，一旦有爭議發生，平均需要四十四天來解決爭議，隨時因爭議而被凍結的金額超過一億元美金

What?

- 藉由在安全與具透明度的區塊鏈中分享數據, 以改善融資業務的效率

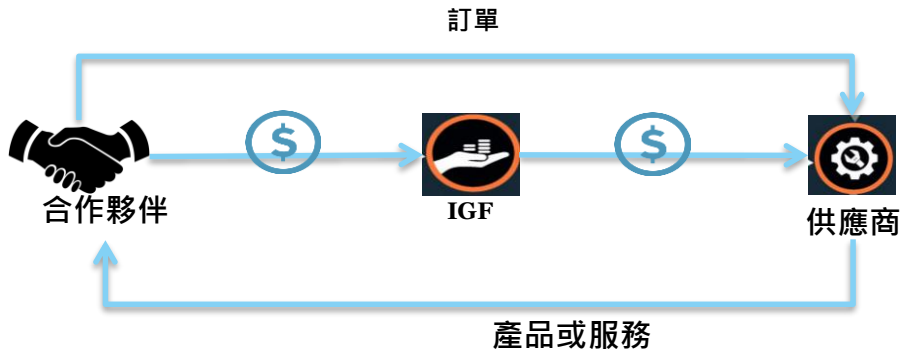
How?

- 區塊鏈提供供應鏈流程間關鍵性營運資料的全面性觀點
- 採購訂單 > 交易核准 > 出貨 > 寄送發票 > 匯款

Benefits

- 更少的爭議和更快的結算速度
- 將爭議解決的時間由四十四天降低為十天
- 增加資本效率；提高資本自由度

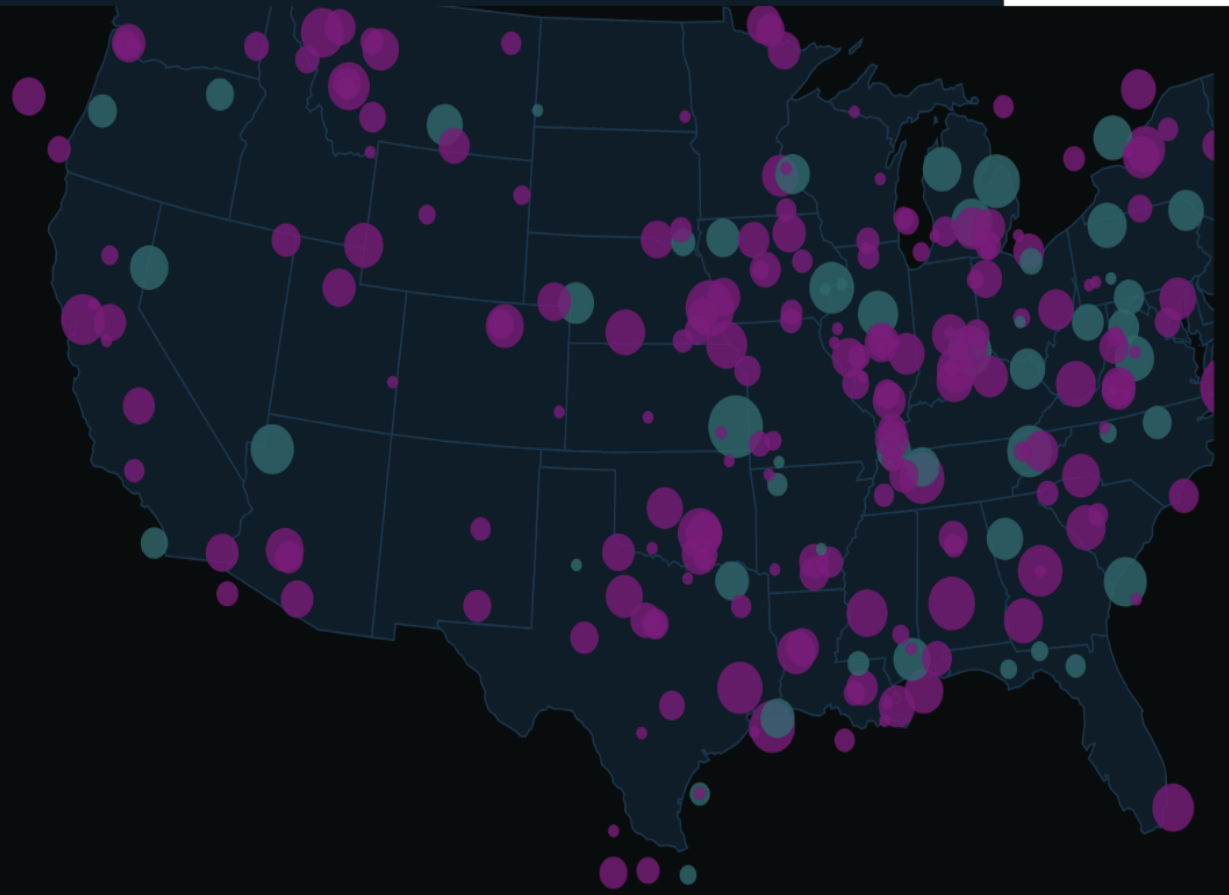
IGF 統計數據			
4000多家供應商和夥伴	每年兩百九十萬筆發票		每年440億元美金的交易金額
1億美金 因爭議而凍結的金額	2萬5000筆 每年爭議數	3萬1000元美金 每個爭議平均金額	44天 目前平均爭議處理時間



Partner 945

Number of Transactions

Supplier	Jul	Aug	Sep	Oct	Nov	Dec	Total	Total $
Supplier 307							89	55398448
Supplier 308							5	60600
Supplier 3574							103	7136289
Supplier 389							2	62000
Supplier 2201							66	19023152
Supplier 2849							2	455328



There were 17 transactions between **Partner 945** and **Supplier 3574** in August 2015

Information Available in the Current System

No Information Available in the Current System

Order Placed	Transaction Approval Request	Approved / Rejected	Shipment Sent	Invoice to IGF	IGF Remittance to Supplier Initiated	Proof of Delivery	Payment Due to IGF from Partner	Partner Remittance to IGF Initiated
							⚠	

Partner 945
Business Partner

Dispute: Proof of Delivery / Not Received

Dispute ID:	279283
Invoice / Loan:	11679040
Amount:	$ 1088.36

IBM與國際銀行、Fintech夥伴KlickEx, Stellar 共創高效率的區塊鏈跨境支付體系

本解決方案已在太平洋群島、澳大利亞、紐西蘭和英國間的12條貨幣走廊中處理實時交易。通過區塊鏈分布式帳本，所有合適的參與方都能訪問並了解財務交易的清算和結算情況

打造數位貿易鏈 歐洲7大銀行找上IBM

歐洲7大銀行委任IBM打造以Hyperledger區塊鏈為基礎的貿易融資平台 - 數位貿易鏈（Digital Trade Chain；DTC），旨在促進中小企業國際貿易。

在高科技產業爭相為華爾街提供區塊鏈技術服務之際，這紙合約對IBM可謂一大勝利。由德意志銀行、匯豐銀行、比利時聯合銀行（KBC）、法國外貿銀行（Natixis）、法國興業銀行、荷蘭合作銀行（Rabobank），和義大利裕信銀行（UniCredit）組成的聯盟，於1月宣布建立DTC

IBM表示，該聯盟挑選IBM為其打造DTC，協助參與貿易者進行國際性的追蹤、管理和交易。DTC將利用區塊鏈連接所有參與貿易的當事人，從買家、賣家、運輸方，再到提供融資的銀行等。

KBC資訊長彼德斯（Rudi Peeters）表示：「IBM的區塊鏈和金融產業專家將為聯盟打造新的平台，旨在簡化和加速中小企業進行國際貿易，並降低貿易交易成本。」

資料來源：https://ctee.com.tw/News/ViewCateNews.aspx?newsid=153694&cateid=omsc

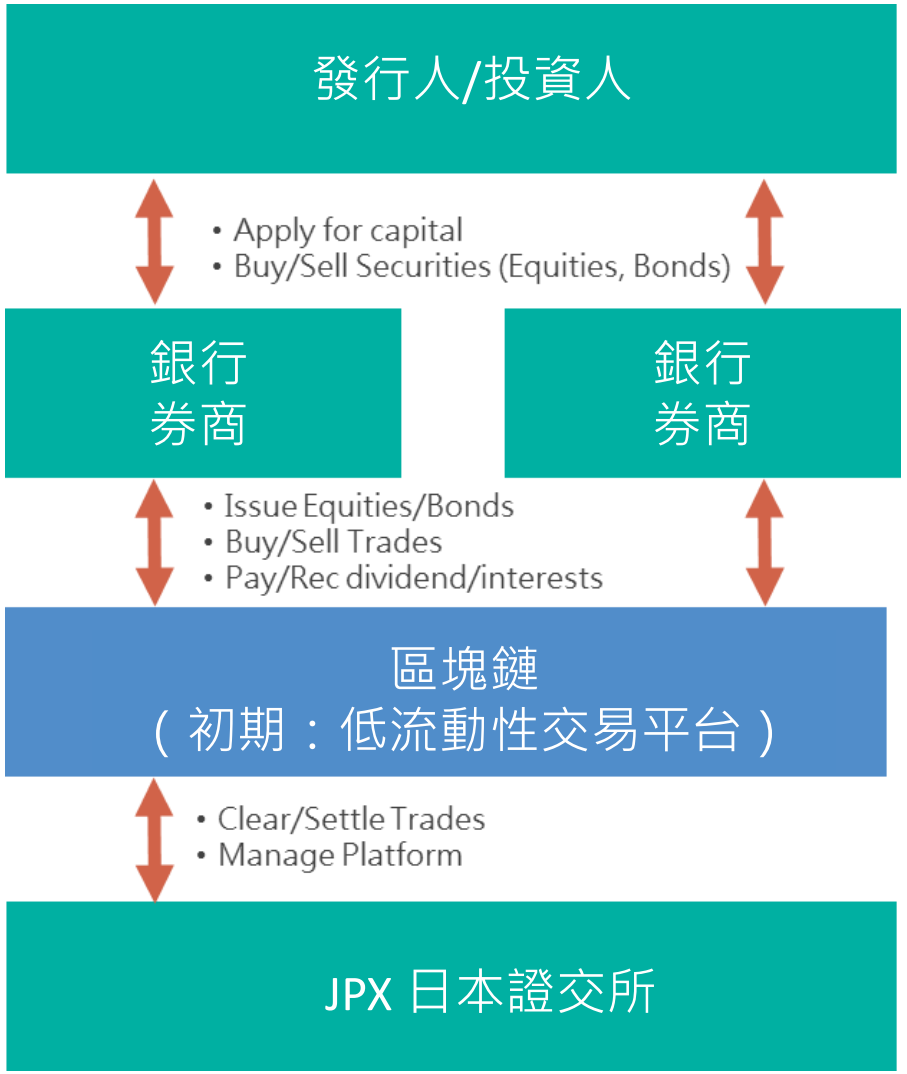
歐洲7大銀行DTC(Digital Trade Chain)計畫選擇IBM Hyperledger 的主因

- 本創新計畫源自於2016年比利時聯合銀行(KBC)在乙太坊(Ethereum)架構上的一個驗證計畫，當時IBM還沒有參與。2017年1月歐洲七大銀行簽署了合作備忘錄並組成聯盟，五個月後，**經過全球選商的競爭評選過程，IBM從七家科技廠商中脫穎而出，成為DTC平台的獲選廠商**。
- KBC負責貿易融資的總經理 Hubert Benoot 說：
  - 獲選進入最後一回合選商過程的兩家廠商是Hyperledger和Corda。Corda是一個共享帳本平台，由R3將七十家金融機構組成一個聯盟。R3主要是為Transaction Banking提供智慧合約，讓交易對象間能更好地管理合同，降低交易間的成本和風險。相對的，**Hyperledger並不侷限於特定產業，它可為貿易融資的各方打造解決方案**。
  - 雖然DTC大部分的聯盟成員也是R3的會員，但他們也都同時在Hyperledger平台開發區塊鏈應用，聯盟最後選擇採用“較成熟”的平台。**我們採用 IBM Hyperledger 的主因，是IBM除了貿易融資以外，在各行各業還有許多上線的成功案例，所以 IBM Hyperledger 是實證可行的科技方案。對照起來，Corda 還沒有實績**。
- IBM金融市場副總裁Keith Bear 說：Hyperledger v1.0 多通道(Channel)提供的隔離機制滿足聯盟銀行對隱私的高度要求。透過通道機制，比方說 KBC 和 Rabobank 進行交易時，其他聯盟銀行將看不到這筆交易。因此，**成員銀行在Hyperledger 可以享有區塊鏈信任和透明的好處，但又不像比特幣等其他平台必須把一切資料揭露給所有區塊鏈的參與者。通道機制更適合金融服務，因為交易的資料隱私是無法妥協的重點。**

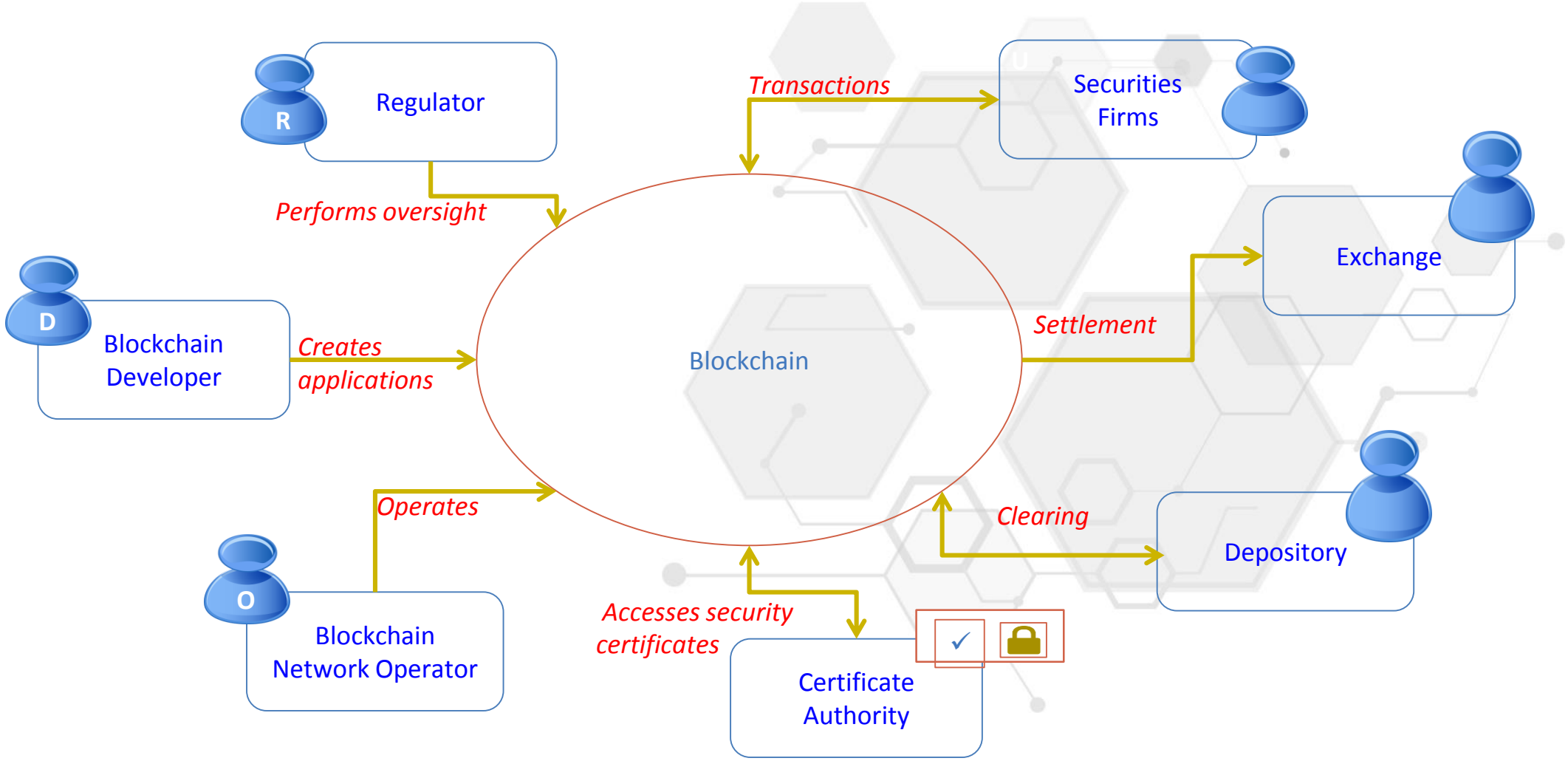
資料來源：https://www.gtreview.com/news/europe/seven-banks-to-go-live-with-hyperledger-blockchain-trade-finance-platform-in-2017/

日本證交所以Hyperledger進行在低流動性交易和結算過程中的用途

- **業務架構:** 三百個參與者以上的交易平台，由銀行、券商、交易所組成的點對點架構
- **業務價值:** 降低營運成本和清算時間，藉由分散式的架構提高可用度
- **如何做到業務轉型:** 藉由除去中間層的費用與流程來降低成本
- **End Game未來擴充:** 上市產品的交易、清算與結算

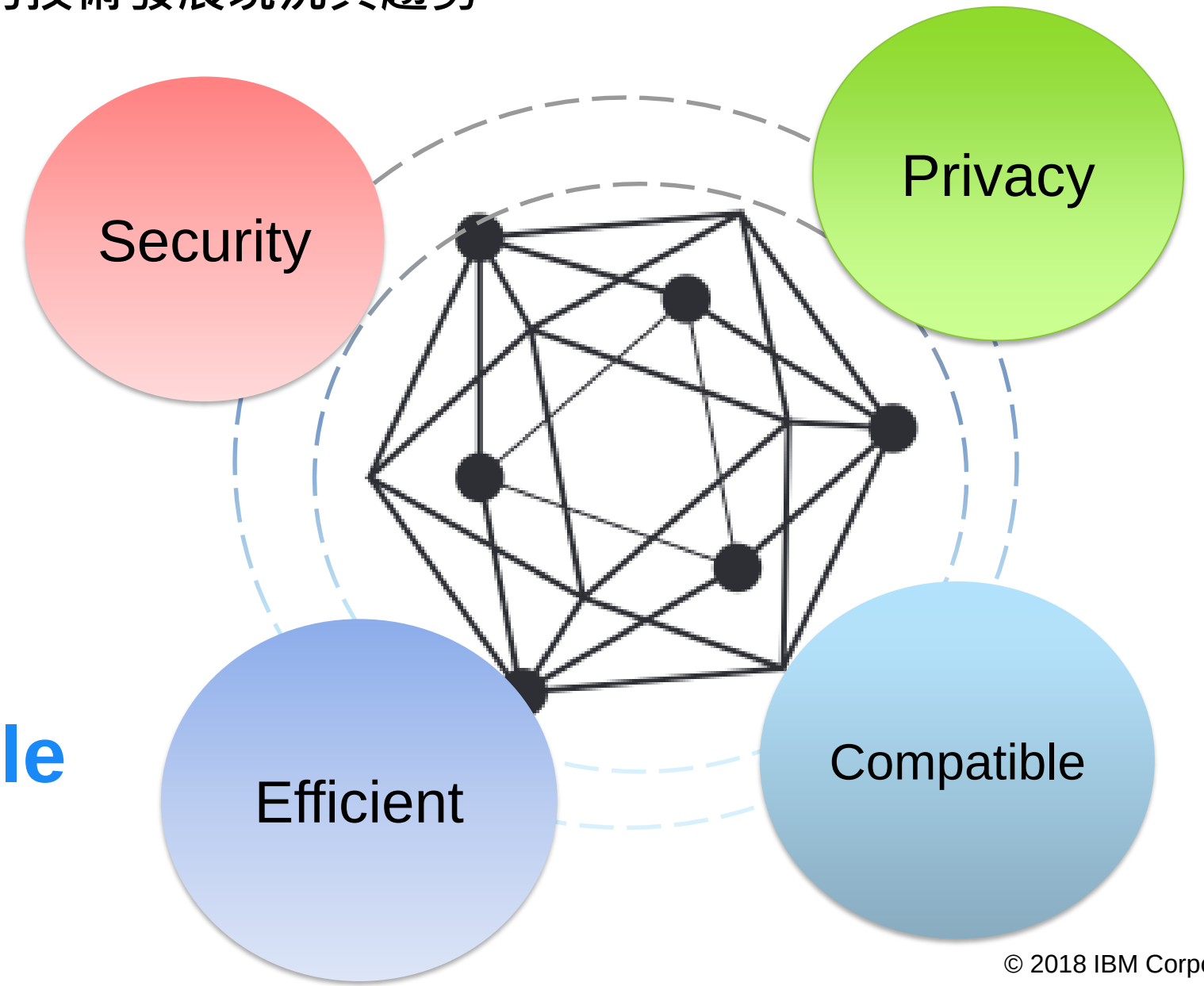


商業體系需要特別的B2B聯盟區塊鏈，以支援網路上多個不同的角色和職掌



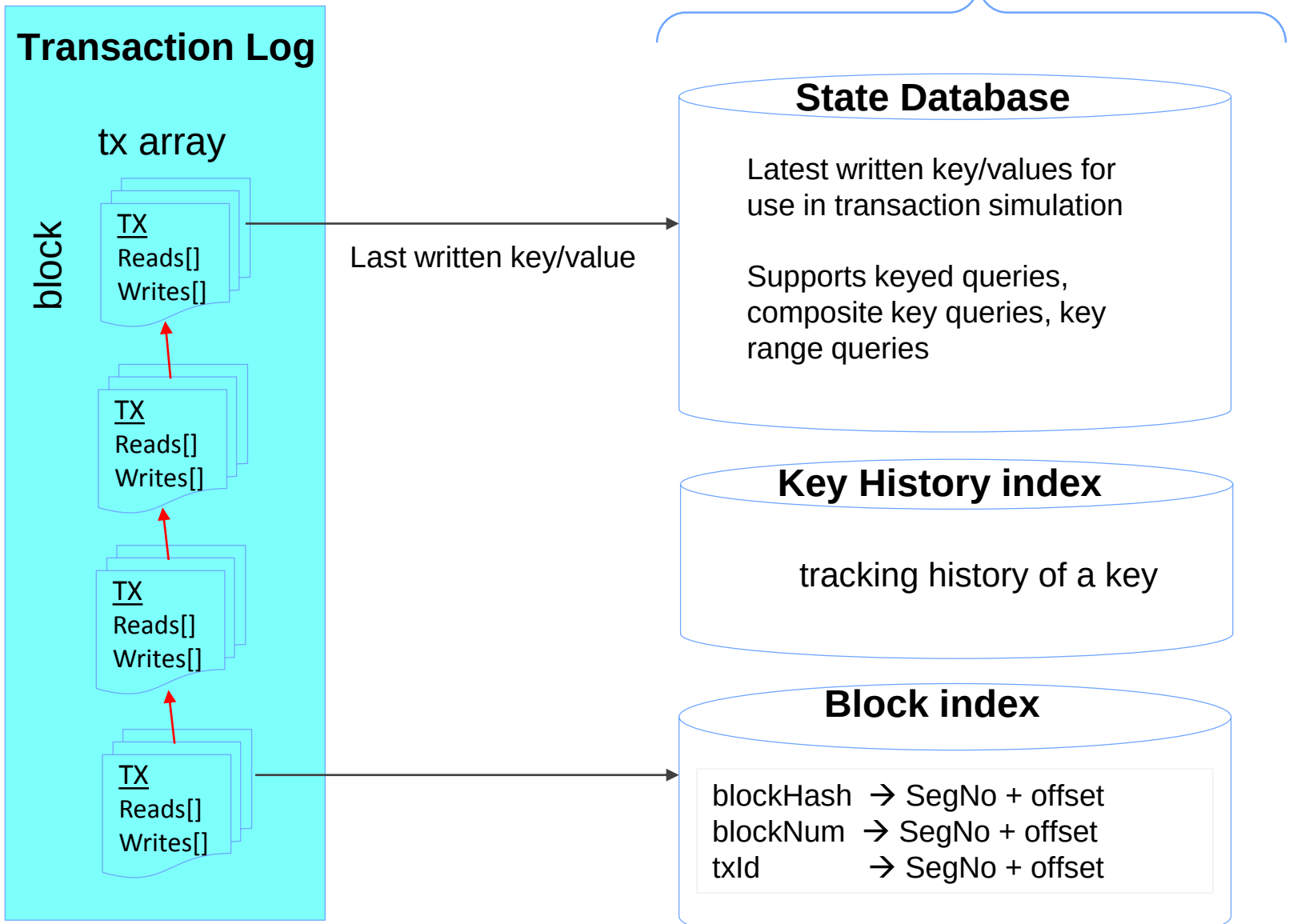
滿足資本市場對區塊鏈要求的技術發展現況與趨勢

- More **Efficient**
- More **Security**
- More **Privacy**
- More **Compatible**



More Efficient, Less waste

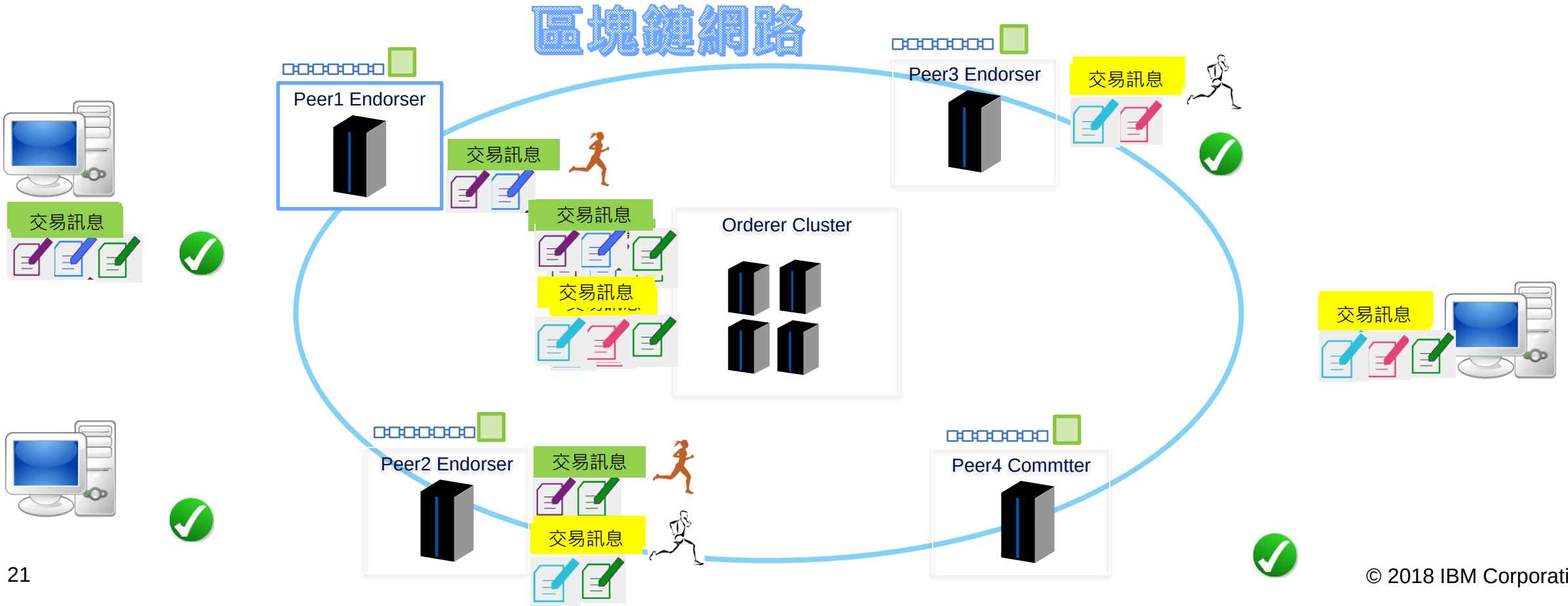
帳本區塊實體記錄檔及資料庫設計



CouchDB (external option) supports keyed queries, composite key queries, key range queries, plus full data rich queries (beta in 1.0)

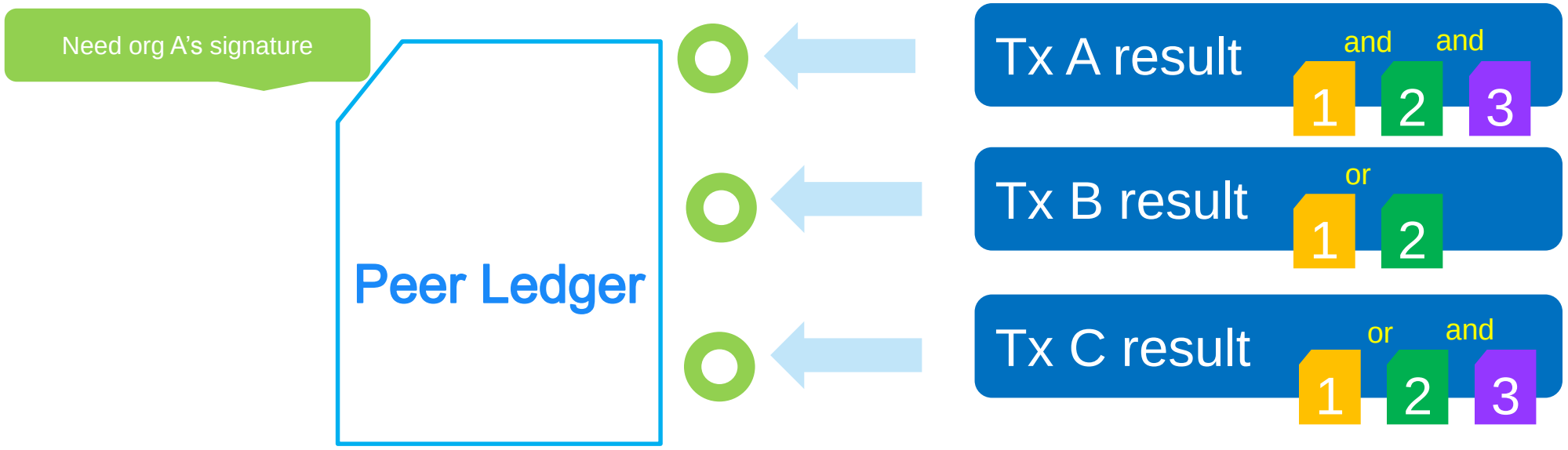
More Efficient, Less waste

- 用戶端發送的交易，透過共識機制 (背書 Endorsement、排序及確認)，將交易以相同的順序打包寫入各節點帳本，確保各節點帳本資料是同步的。
- Hyperledger Fabric 提供可插拔的共識機制接口， 目前支援 Solo、Kafka(CFT) ，未來可擴充 SBFT 、XFT。



More Efficient, Less waste

利用背書原則(Endorsement Policy)來決定一個交易在提請共識寫入帳本前，要取得認可的節點及節點數

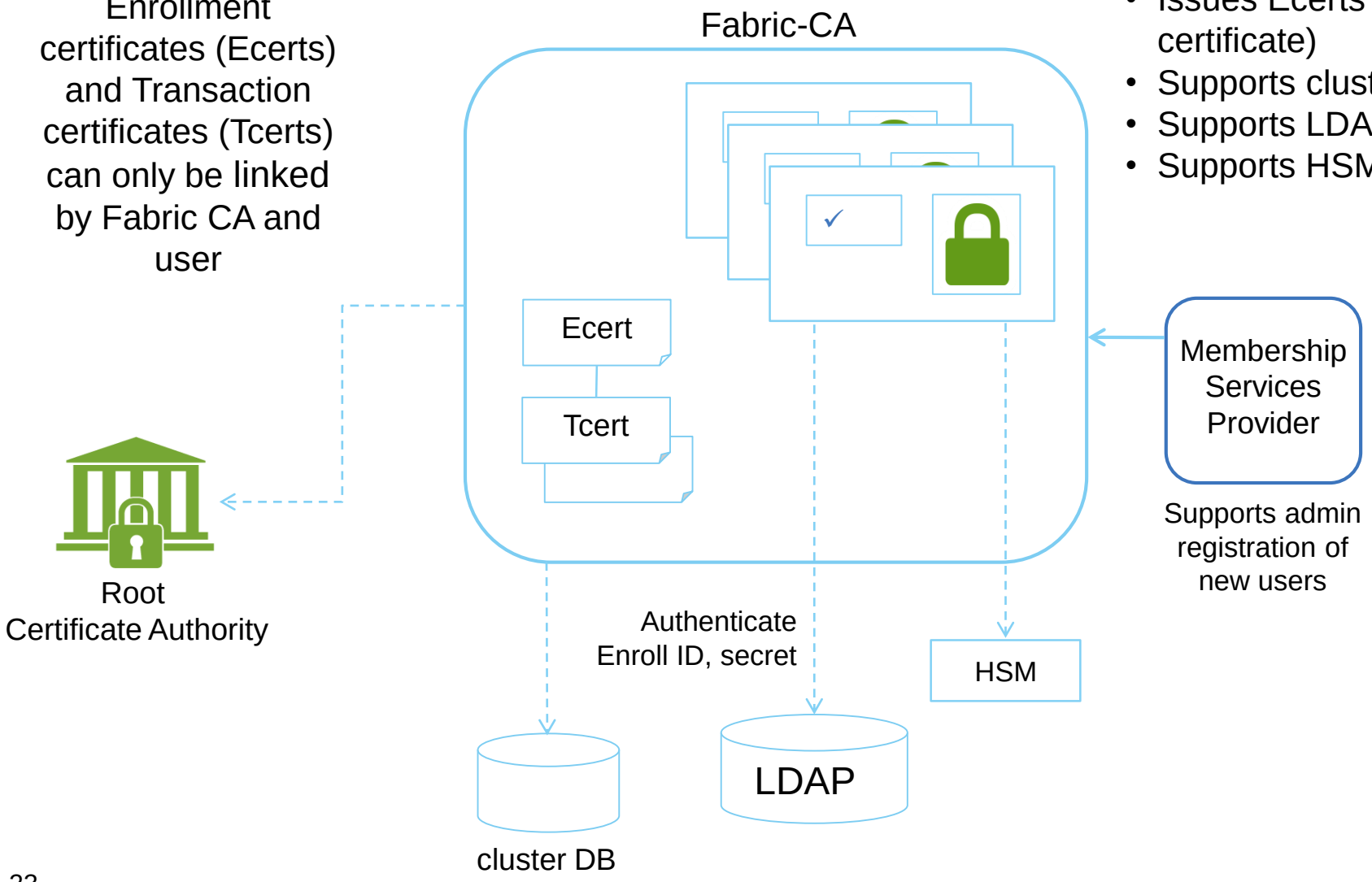


Examples of policies:

- Request 1 signature from all three principals
  - AND('Org1.member', 'Org2.member', 'Org3.member')
- Request 1 signature from either one of the two principals
  - OR('Org1.member', 'Org2.member')
- Request either one signature from a member of the Org1 MSP or (1 signature from a member of the Org2 MSP and 1 signature from a member of the Org3 MSP)
  - OR('Org1.member', AND('Org2.member', 'Org3.member'))

More Security, Less Deception

Enrollment certificates (Ecerts) and Transaction certificates (Tcerts) can only be linked by Fabric CA and user



Fabric-CA

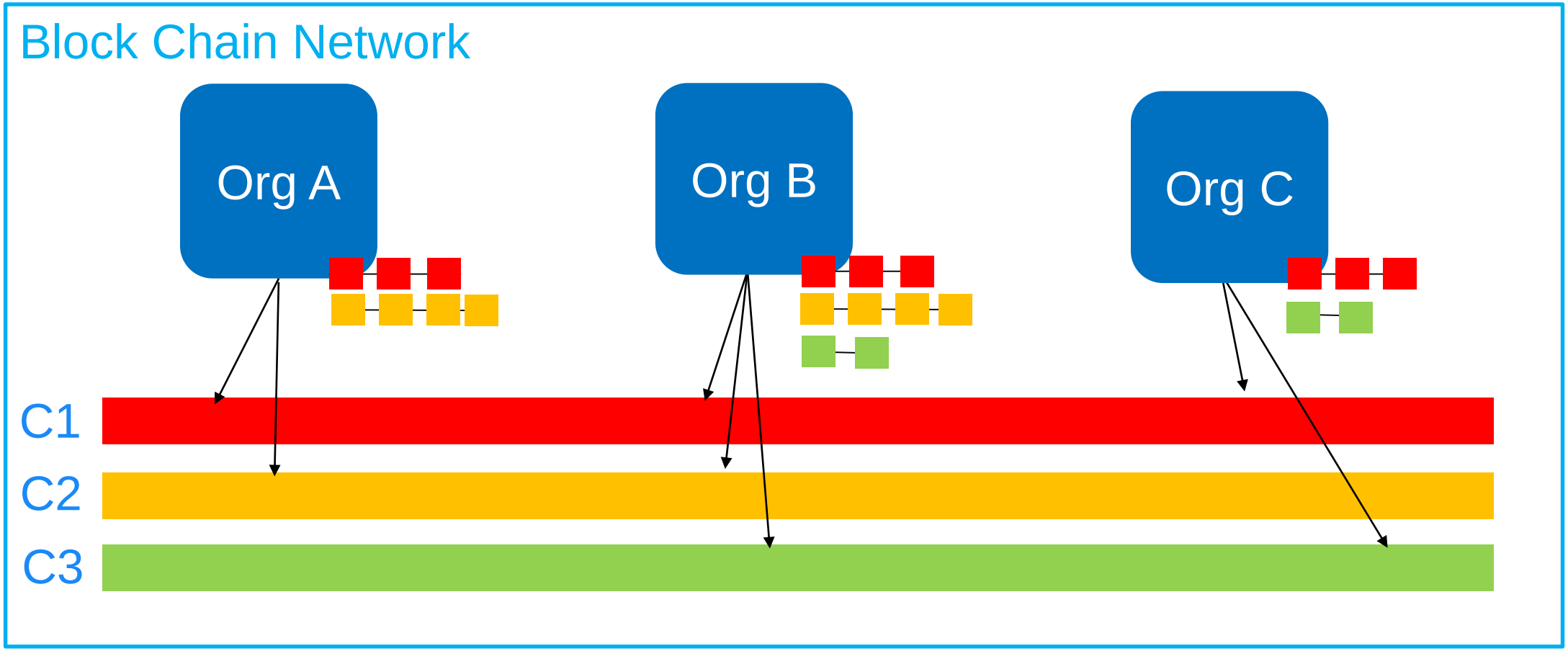
- Default implementation of the Membership Services Provider Interface
- Issues Ecerts (long-term identity) and Tcerts (disposable certificate)
- Supports clustering for HA characteristics
- Supports LDAP for user authentication
- Supports HSM

Membership Services

- Pluggable interface supporting a range of credential architectures
- Governs identity for Peers and Users.
- Provides:
  - User authentication
  - User credential validation
  - Signature generation and verification
  - Optional credential issuance
- Additional offline enrollment options available.

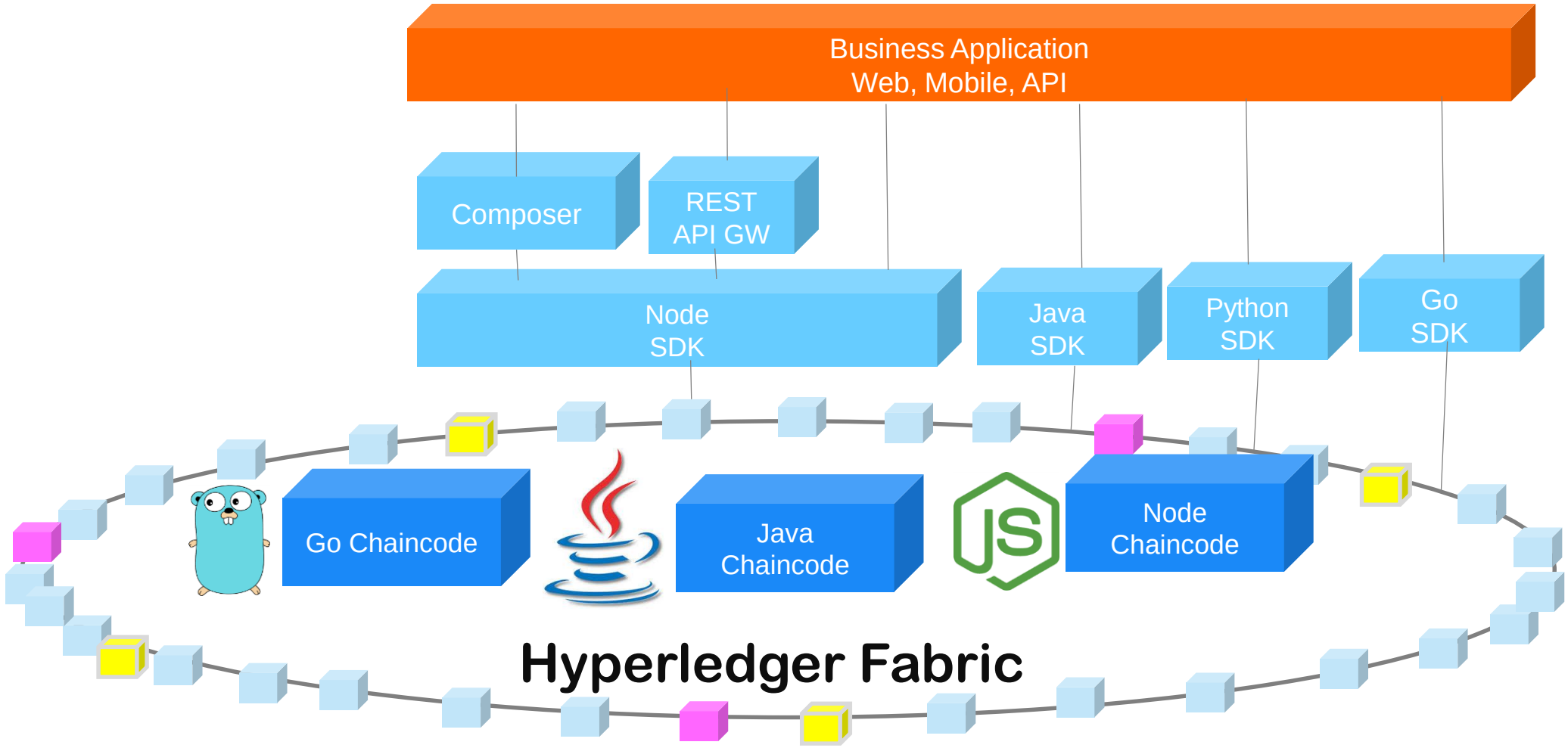
More Privacy, Less Consume

Hyperledger Fabric channel 是一種在區塊鏈網路上，任選節點之間建立的私有 “子鏈 (Subnet)” , 其目的是在建構一個私有及保密的交易通道



More Compatible, Less Learning curve

提供更多種常見的開發語言來開發智能合約及SDK



區塊鏈技術發展現況與趨勢總結 - 以Hyperledger Fabric為例

Category	Description
Member Management	Support PKI mechanism, use certification implement ACL
Multiple Channel	Have multiple channel to keep data privacy.
Consensus	Support multiple consensus model (Solo, kafka, PBFT, Xft)
Scalability	Dynamic adjust amount of nodes, endorsing policy.
Data base	Support pluggable data base interface (go level, couch Db)
Smart contract	Support multiple popular programming language.


Thank You!