

電子商務安全 (Electronic Commerce Security)



本章內容

- 16.1 前言
- 16.2 網路行銷
- 16.3 電子折價券
- 16.4 網路交易的安全機制
- 16.5 電子付款機制
- 16.6 電子競標

16.1 前言

- 電子商務是指利用電腦或網際網路來完成交易的商業模式，諸如網路行銷、網路銀行、電子購物、及隨選視訊等，都是以電腦網路來做為其交易的平台。
- 電子商務在安全方面需滿足：
 - 身分鑑別
 - 交易資料的機密性
 - 交易資料的完整性
 - 不可否認性

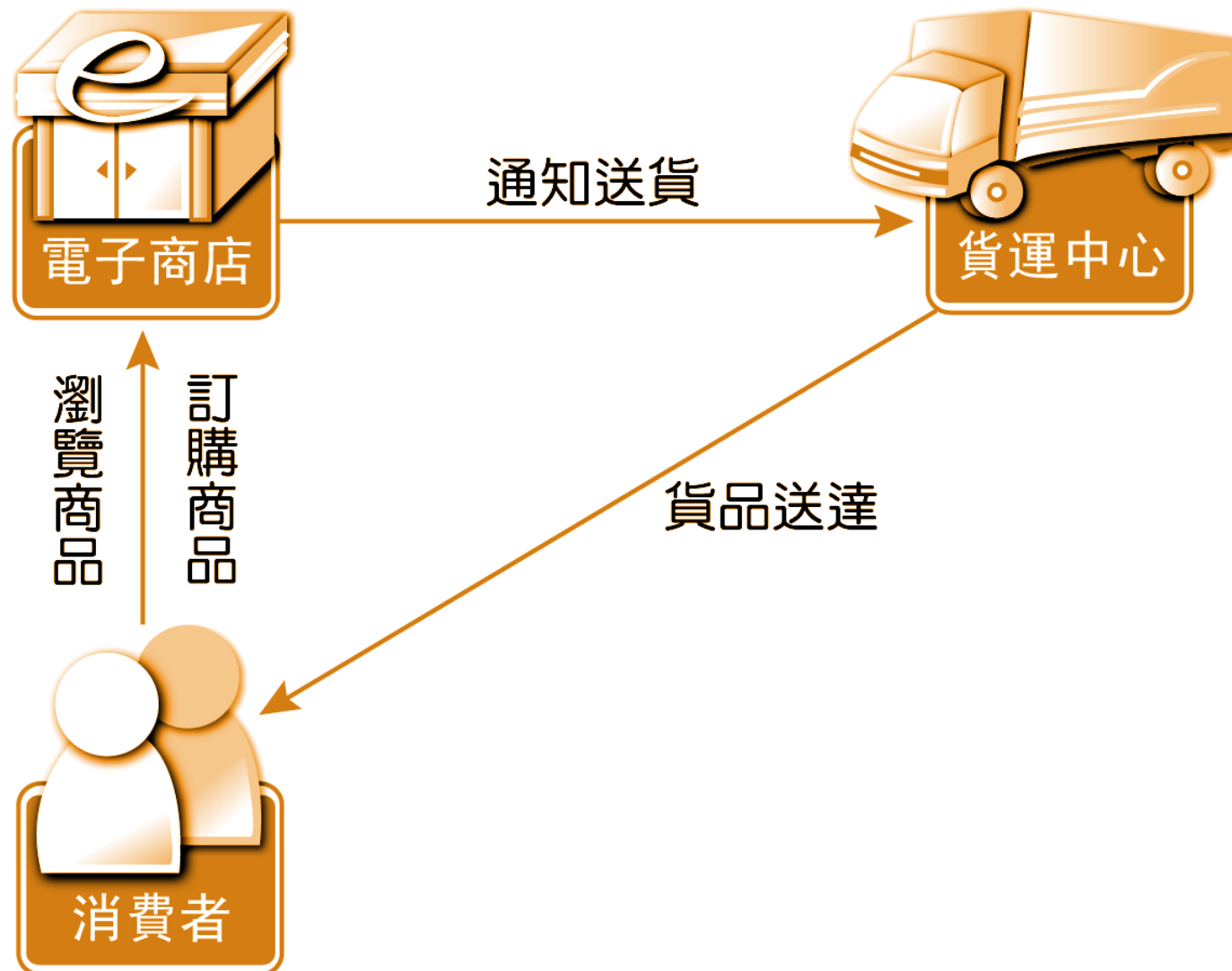
16.2 網路行銷

- 網路行銷又稱為電子行銷(E-marketing)或線上行銷(On-line Marketing)，泛指利用電腦網路來傳送廣告訊息以進行市場的推廣活動。
- 一般來說，網路行銷可分為被動行銷及主動行銷兩種。

被動行銷

- 商家藉由網站的架設來提供商品資訊。商家利用電腦網路當做媒介，在上面刊登商品資訊、定期及不定期的廣告、或促銷活動，以吸引顧客消費，進而能使顧客完成交易及付款事宜。

簡易的網路行銷示意圖



主動行銷

- 商家主動對可能的顧客進行行銷，常見的方式有寄發廣告信函或折價券等方式。
- 另外一種常見的主動行銷方式是利用折價券，其目的是希望藉由較優惠的價格來吸引消費者的購買。

16.3 電子折價卷

- 數位化的折價券可以經由電子郵件傳遞或顧客自行到商家的網站下載，收到電子折價券後，顧客再用印表機將此折價券印出，並帶到實體商店使用。

電子折價券的優點

- **經濟**：電子折價券以數位化的樣式產生，可省去大量印刷成本。
- **傳播範圍極大**：藉由網際網路無國界限制的傳播力量，可對全球的客戶進行行銷。
- **時效性高**：能夠24小時接觸顧客，超越時間及空間的限制，不會遺漏任何潛在客戶。
- **互動性高**：可搭配線上遊戲、問卷、或網頁的瀏覽，經由消費者的高度參與，業者能夠更了解顧客的需求，進而提升行銷效果。
- **容易實現一對一行銷**：可針對特定的顧客行銷，易於區別顧客的族群，並容易追蹤行銷成果，掌握顧客需求。

折價卷類型

- 商店折價券與製造商折價券(Store Coupon VS. Manufacturer Coupon)
- 有限折價券與無限制折價券(Limited Coupon VS. Unlimited Coupon)
- 特定折價券與無特定折價券(Targeted Coupon VS. Untargeted Coupon)
- 退化折價券與遞增折價券(Aging Coupon VS. Countable Coupon)

商店折價券與製造商折價券

- 商店折價券通常是由某一商家針對其販售的少數商品提供折扣。
- 製造商折價券則是由某一商品的製造商所發行，顧客可持此折價券到任何一家商店購買此一折扣商品。

有限折價券與無限制折價券

- 有限折價券是指該折價券的發行量是受到控制的，也就是說使用過的折價券便無法再使用，使用者無法自行複製折價券來使用。
- 無限制折價券便是指折價券的發行量是不受控制的，使用者可自行複製折價券來使用。

有特定折價券與無特定折價券

- 無特定折價券是指不指定特定使用者的折價券，其主要目的是在增加商品的銷售量及吸引新的顧客。
- 特定折價券則是一種指定特定使用者的折價券，商家有時為了留住某些忠實的顧客或回饋經常往來的顧客或會員，會針對這些顧客發行一些特別的折價卷。

退化折價券與遞增折價券

- 退化折價券是指該折價券所提供的折扣會隨著時間的流逝而逐漸減少。
- 遞增折價券則是具有計數特性的折價券，隨著顧客消費次數的增加，該折價券會提供更多的折扣給消費者，或者是當消費者消費滿一定的次數後，就可以兌換禮物等。

電子折價券機制角色說明

- **製造商(Manufacture)**

- 泛指產品的製造者或是服務的提供者。

- **零售商(Retailers)**

- 泛指銷售促銷商品的商店，可以是線上的商店或是實體的商店。

- **顧客(Customers)**

- 為了以較低的價格購買一項商品，顧客會先從相關的廣告商取得該項產品的折價券，然後再拿此折價券到零售商購買該項產品。

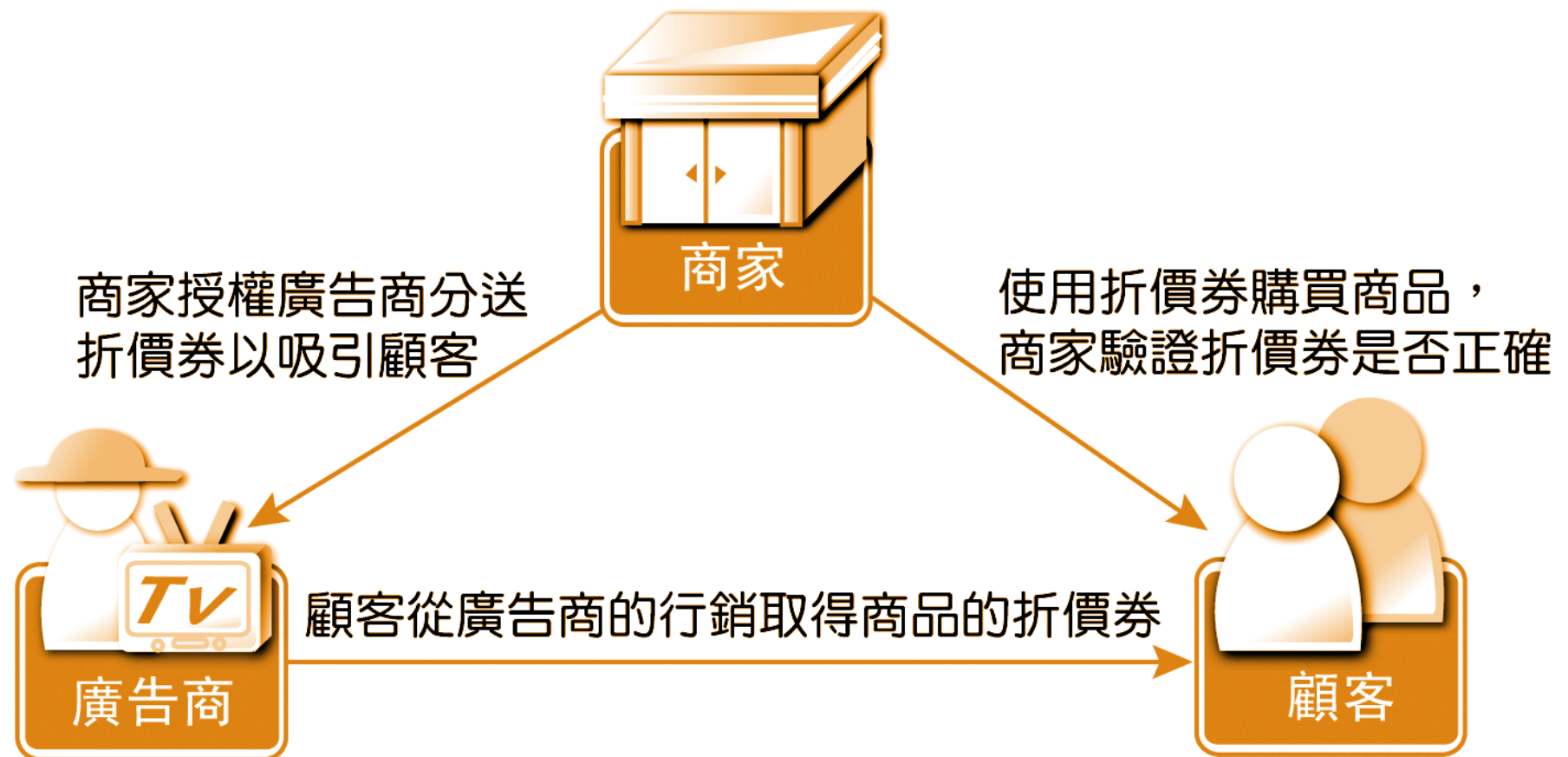
- **廣告商(Advertisers)**

- 幫製造商做相關產品的促銷活動，廣告商可以透過網頁的瀏覽、線上遊戲、或電子郵件等媒介發送電子折價券給特定族群的顧客，來吸引這些顧客消費。

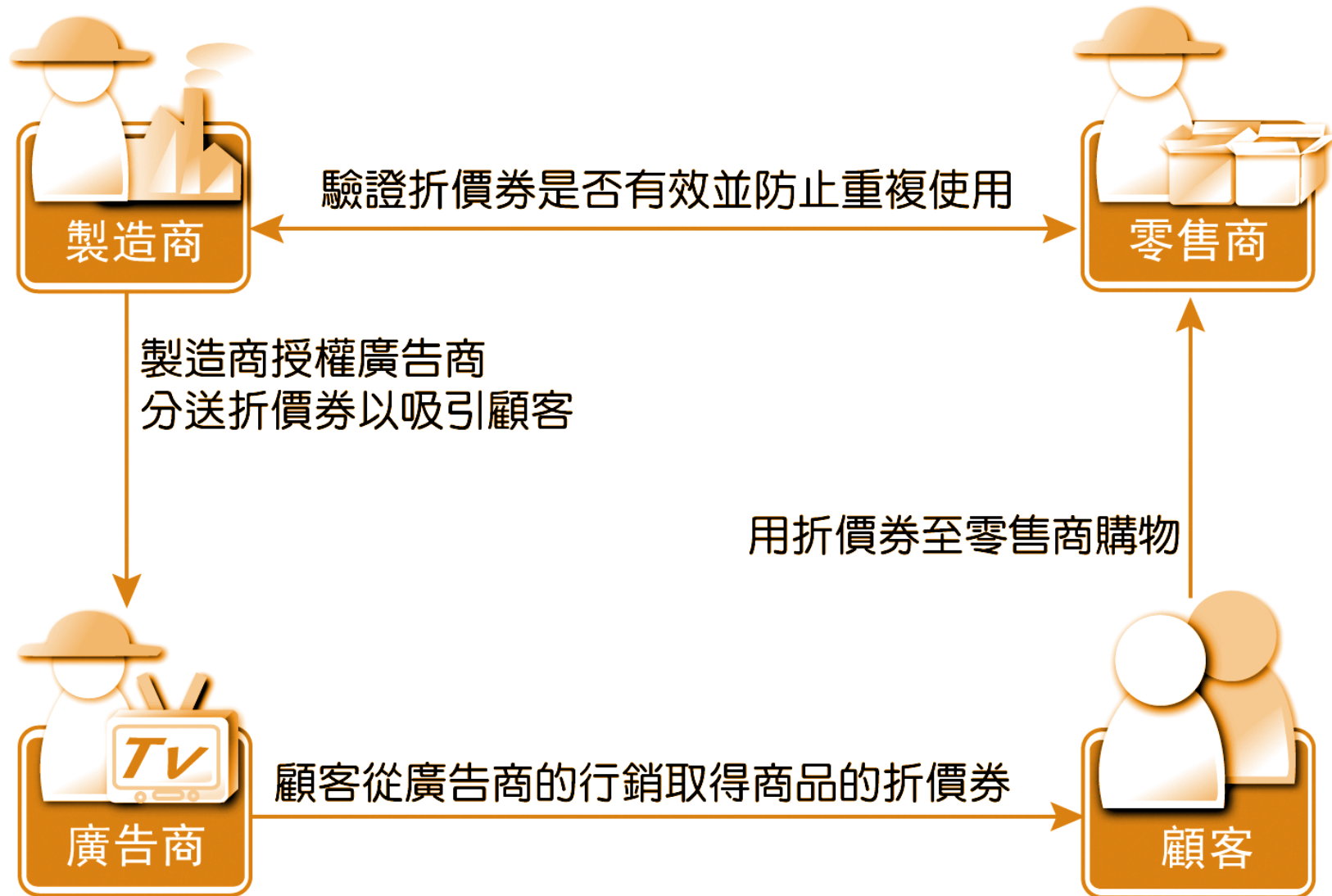
電子折價券機制的系統模式

- 標準模式(BasicModel)
- 延伸模式(Extended Model)

標準模式的電子折價券機制



延伸模式的電子折價券機制



電子折價券機制

在使用上需滿足下列幾項需求：

- 效率(Efficiency)
- 容易使用(Easy to Use)
- 顧客的匿名性(Anonymity)

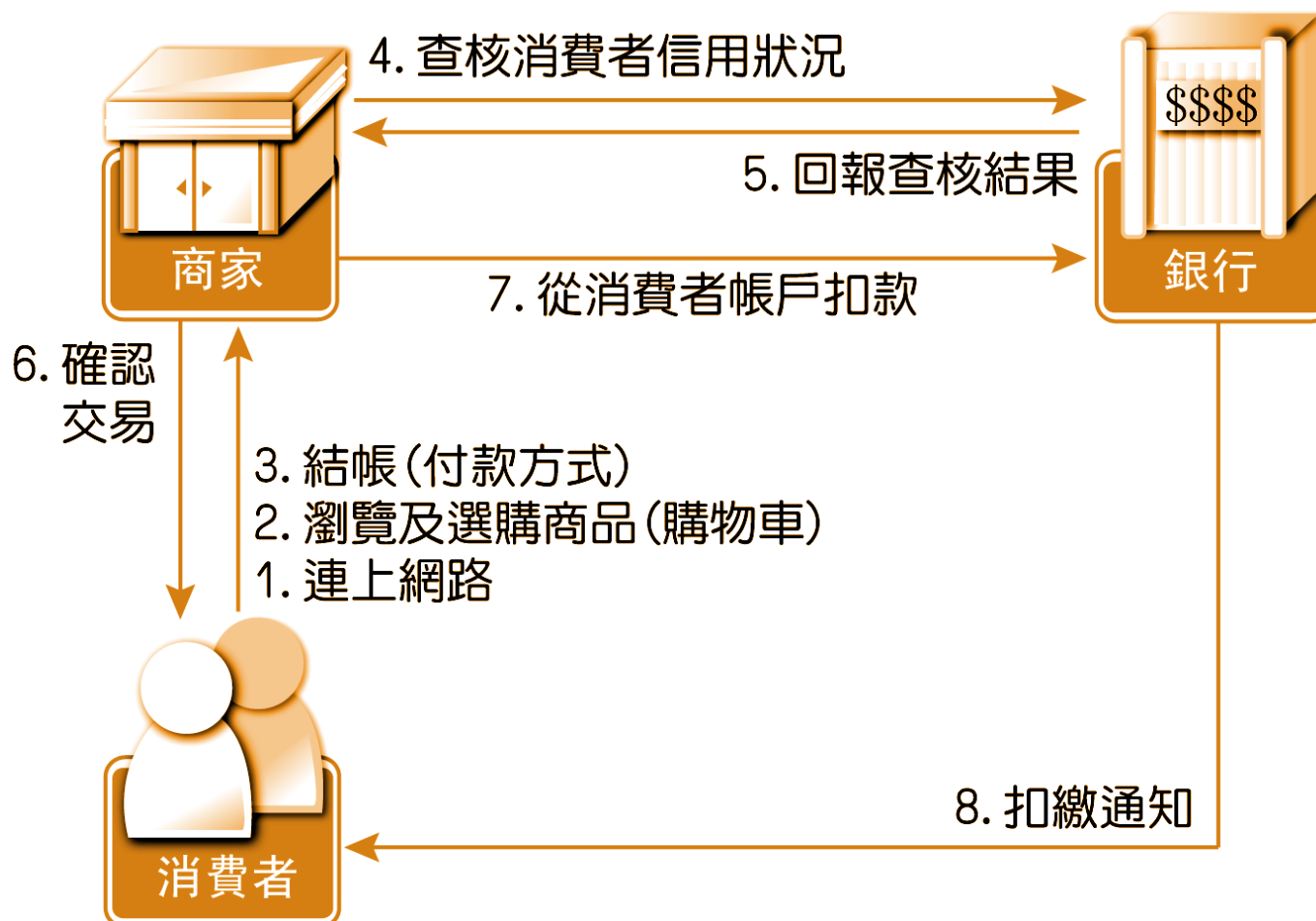
電子折價券機制

需滿足的一些基本安全需求如下：

- 防止未經授權的商店或個體偽造及發行電子折價券
- 防止電子折價券被竄改
- 防止電子折價券被重複使用

16.4 網路交易的安全機制

網路交易流程



O2O (Online to Offline)

- O2O電子商務模式適合必須到實體商店取得商品或服務的交易。
- 通常需透過一個中間的媒介平台，讓消費者可以先在線上先預訂所要的服務或是進行商品團購。
- 例如經營團購的Groupon或是線上餐廳訂位的易訂網(EZTABLE)都是O2O模式的成功案例。

網路交易

網路交易要能蓬勃發展，下列幾個因素是必要的：

- 交易的便利性

- 以網際網路瀏覽軟體(如Navigator或IE)配合其他軟體
- 提供多功能且簡易的產品簡介、訂單處理、及送貨服務
- 提供即時連線(On Line)的信用卡授權服務

- 交易的安全性

- 確認交易對象的身分資訊（買方、商場）
- 保護交易資料在網路上的傳輸保密性及完整
- 連線信用授權，達到信用交易的安全性及迅速性

- 簡單的付款工具

- 以信用卡、電子現金或其他方式作為交易的付款工具

線上購物系統常見的功能

- 會員資料管理功能
- 使用者瀏覽功能
- 網路購物車功能
- 線上討論功能
- 暢銷商品排行榜功能

安全機制

- DES資料加密(Data Encryption)
- 數位信封(Digital Envelop)
- RSA數位簽章(Digital Signature)
- 雙重簽章(Dual Signature)
- SHA-1雜湊函數(Hash Function)
- 數位憑證(X.509 Version 3 Format)

16.5 電子付款機制

電子付款機制可分為以下三種型態

- 電子現金(Electronic Cash)
- 電子支票(Electronic Check)
- 信用卡(Credit Card)

電子付款中常見的威脅

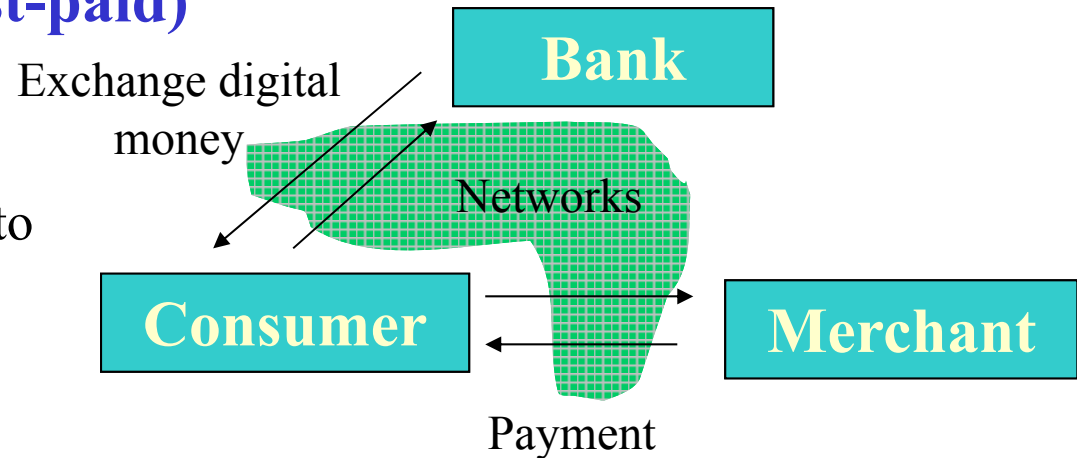
- 網路環境是不安全的
 - 偽造 (Fabrication)
 - 竄改 (Modification)
 - 中斷 (Interruption)
 - 攔截 (Interception)
- 顧客可能不誠實
 - 重複消費 (Double Spending)
- 商家可能不誠實
 - 重送(Replay)

電子付款的特徵

1. 先付(Pre-paid)或後付(Post-paid)

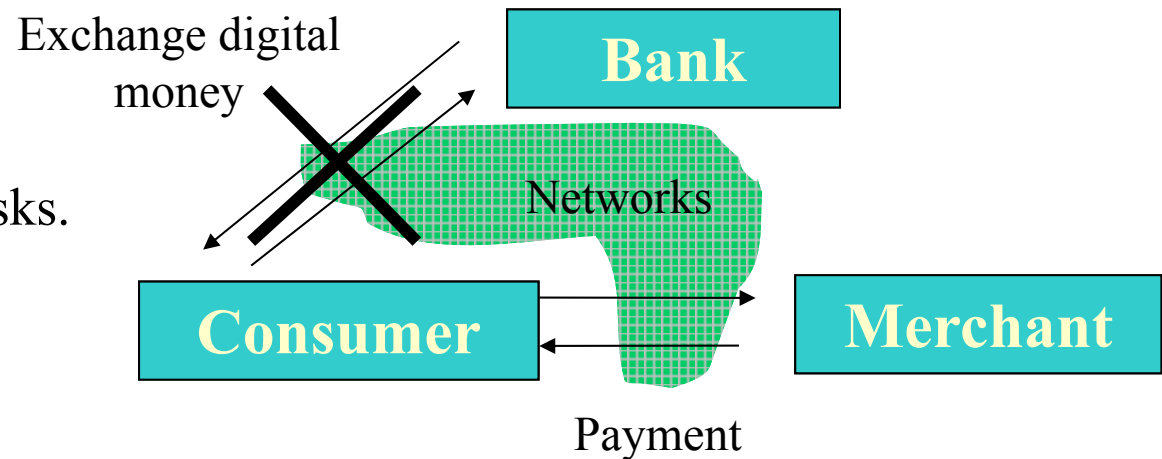
先付:

- good for merchant but is not fair to the consumer.
- preventing double spending.



後付:

- good for consumer but the merchant and bank take some risks.
- preventing replay attack.



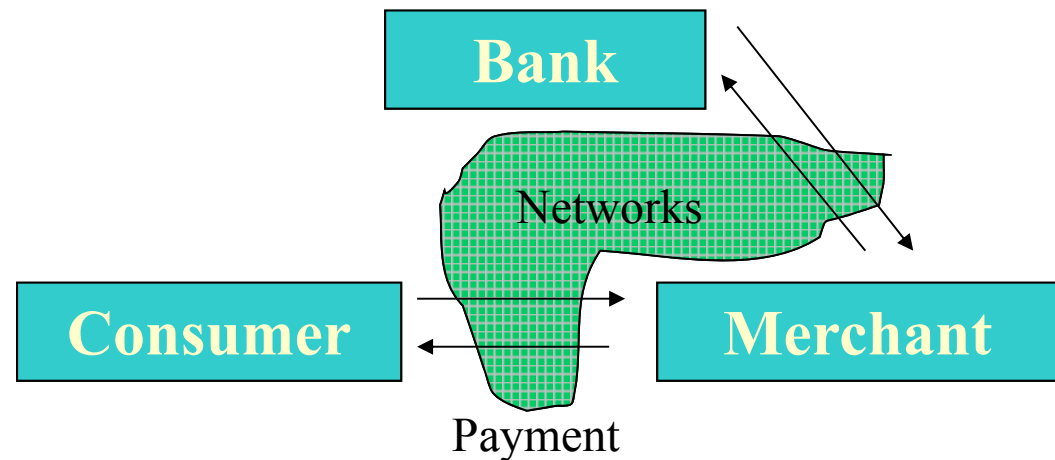
電子付款的特徵

2. 透過銀行線上(On-line)認證與否

透過銀行：較多的訊息傳遞

On-line: involving the bank

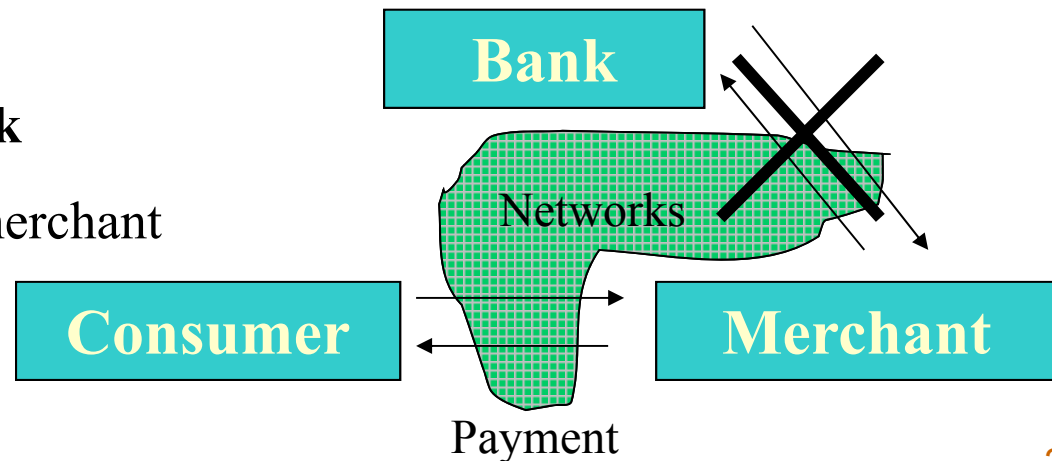
- detecting double spending
- checking the customer's credit
- **more communications**



未透過銀行：較少的訊息傳遞

Off-line: not involving the bank

- verifying the payment by the merchant
- **less communications**



摘要

電子現金	電子支票	信用卡
Pre-pay	Pay-later	Pay-later
On-line verifying	On-line verifying	On-line verifying
Untraceability	Traceability	Traceability
Anonymous	Partial anonymous	Partial anonymous
Database records the used cash to prevent double spending	Database records the account information	Database records the credit card information

盲簽章

- 盲簽章技術最早是在1982年由著名的密碼學家David Chaum所提出的，盲簽章的目的是讓驗證者只能驗證某一份文件的數位簽章是否正確，但卻無法找出此文件與簽署時的文件有任何關聯，這個特性稱之為「不可追蹤性」(Untraceability)。

盲簽章機制

春嬌

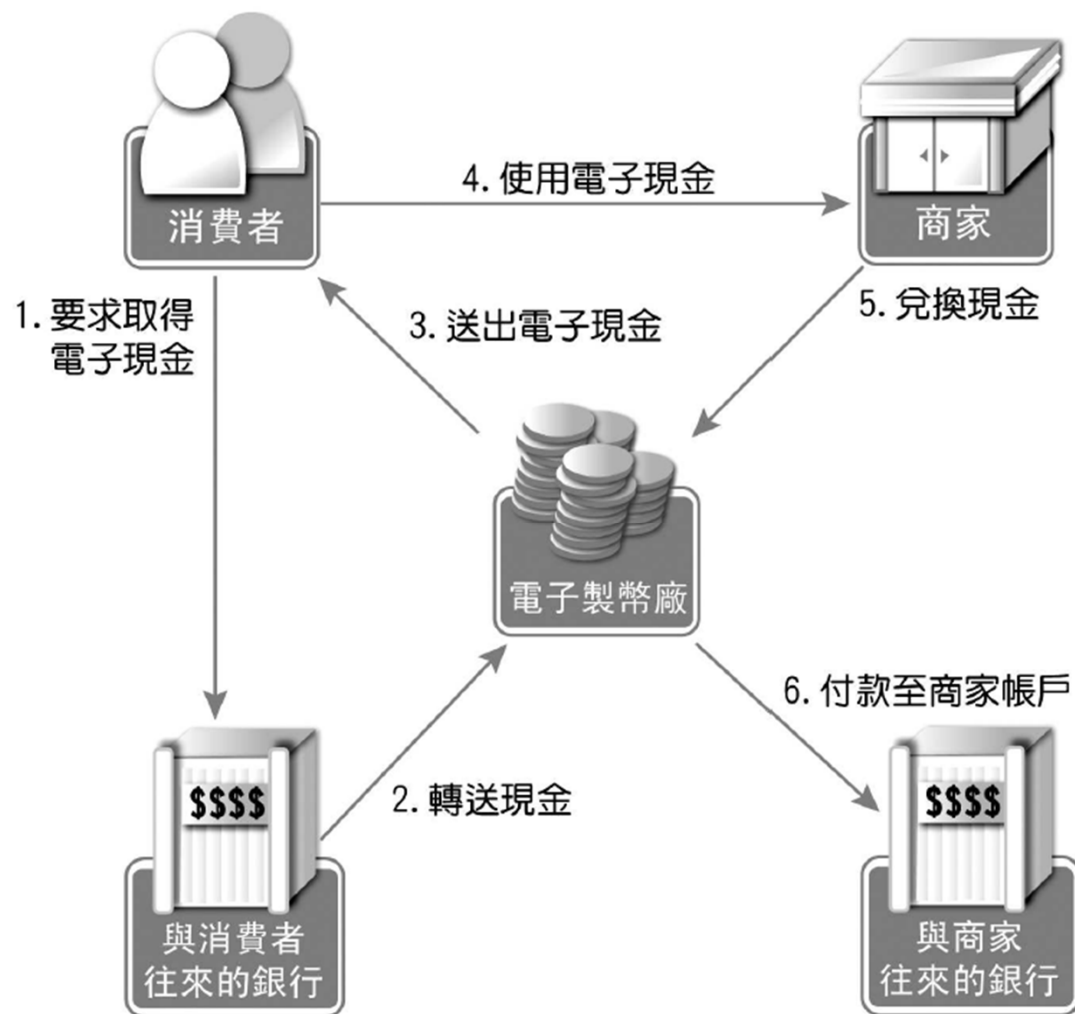
志明

1. 選擇一亂數 r
2. 計算並傳送 $M = m \times r^e \bmod n$ \longrightarrow
3. 計算並傳送 $S_M = M^d \bmod n$ \longleftarrow
4. 計算 $S_m = S_M \times r^{-1} \bmod n$

16.6 電子現金

- 電子現金(Electronic Cash)是將原本的現金改以電子的方式儲存，為了要安全的保存這些電子現金，通常會使用軟體或IC卡來當作儲存電子現金的電子錢包。
- 電子現金是預先付款的機制(Pre-pay)，也就是消費者在消費時就要預先換好電子錢，因此較不被消費者所接受。
- 電子現金也不具傳輸性，每筆電子現金僅能使用一次。
- 盲簽章(Blind Signature)技術在實現電子現金系統中扮演了非常重要的角色。

電子現金系統



電子現金機制

- 1). 消費者首先跟其往來銀行申請電子現金，並支付所要兌換電子現金之金額，每一筆電子現金都會有唯一的識別序號 m ，此序號類似實際鈔票上的序號，消費者選擇一機密的亂數 r ，並計算 $M = m \times r^e \bmod n$ ，其中 (e, n) 為電子製幣廠 (E-Mint) 的公開金鑰，然後消費者將 M 傳送給銀行。
- 2). 銀行將訊息 M 及所要兌換的現金傳送給電子製幣廠。
- 3). 電子製幣廠使用其私密金鑰 d 對訊息 M 進行簽章：

$$S_M = M^d \bmod n$$

接著電子製幣廠將 S_M 送給消費者。

- 4). 消費者收到 S_M 之後，因為只有他本人知道所選擇的亂數 r ，所以可以輕易地將 S_M 裡面的亂數 r 移除，然後得到

$$S_m = (S_M \times r^{-1}) \bmod n$$

電子現金機制

所得到的 S_m 即為電子製幣廠對電子現金序號 m 所做的簽章，將 m 及 S_m 組合起來， (m, S_m) 就成了電子現金。有了此簽章便可以證明此電子現金的確為電子製幣廠所發行，然後消費者便可用此電子現金進行消費。

- 5). 商家收到電子現金 (m, S_m) ，會先利用電子製幣廠的公開金鑰 (e, n) 來做驗證，若驗證成功，商家就確信此電子現金的確是由電子製幣廠所發行，而非他人偽造。

但僅驗證電子現金的簽章是不夠的，因為電子化的文件很容易遭到複製，因此電子現金很容易複製成許多份，消費者可能重複使用同一筆電子現金，這個問題稱為「重複消費」(Double Spending)。要解決重複消費的問題，必須有一套機制去查核消費者所使用的電子現金是否已經被使用過。一個防止重複消費的作法是電子製幣廠必須維護一個資料庫來記錄所有被使用過的電子現金序號，

電子現金機制

商家收到消費者的電子現金時必須至電子製幣廠的資料庫查看此電子現金是否已被使用過，若尚未使用過，則商家就接受此電子現金，完成付款動作。日後商家再向電子製幣廠兌換累積的電子現金。

- 6). 電子製幣廠會先驗證商家所要兌換的電子現金是否正確。若正確，電子製幣廠將所要兌換的金額支付給予商家往來的銀行。

電子現金存在的問題

- 電子現金是**預先付款**的機制 (Pre-pay)，較不被消費者所接受。
- 電子現金也不具**傳輸性**，每筆電子現金使用過一次後就無法再繼續使用。
- 為**線上交易** (On-line Transaction) 模式，需連線到銀行，由銀行代為查驗是否重複消費 (Double Spending)。
- 現行的電子現金**不能找零錢**。
- 電子現金若遺失或毀損將**無法復原**。