

# 電子商務 Electronic Commerce

## 04 E-commerce Security and Payment Systems

長庚大學 資訊管理學系  
林維昭 Wei-Chao (Vic) Lin  
[viclin@gap.cgu.edu.tw](mailto:viclin@gap.cgu.edu.tw)



## 4.1 電子付款系統的概念

- 電子付款 (Electronic Payment) 是指在網路、電腦的環境下，經由數位資料的交換與第三方的認證來完成付款的過程，藉此取代傳統貨幣的交易模式
- 要建構起電子付款系統，需要加入不同的角色，主要可分為買方、賣方、發行人銀行、收單銀行、公正第三者與認證中心等角色

# 電子付款系統的概念 (續)

 表 4-1 電子付款系統的特性

| 特性   | 說明   | 範例                                 |
|------|--|------------------------------------|
| 貨幣價值 | 當使用者儲值後，電子付款系統就可以當作是普通貨幣進行消費與購買商品。                             | 悠遊卡、iCash                          |
| 相通性  | 電子付款系統可與其他企業的系統、應用程式串連，並且在標準的電腦平台上進行付款流程。                      | 超商、公車、火車等均可用台北捷運悠遊卡                |
| 可轉換性 | 透過不同的存、提款設備，可將電子現金儲存在不同的設備中。                                   | 悠遊卡可以在夜市使用                         |
| 安全性  | 電子付款系統多半會提供多種的安全機制，像是個人資料的認證，來避免使用過程中產生資料外洩的問題。                | HTTPS、WBA2 等加密機制                   |
| 個人化  | 有別於現金交易無法登錄個人資料的問題，透過電子付款系統可以讓企業了解每位消費者購買的產品類別，藉此提供更為個人化的行銷模式。 | 學校可透過學校悠遊聯名卡蒐集學生的使用資料 <sup>3</sup> |
| 可使用性 | 目前電子付款系統的使用方式很簡單，當使用者輸入信用卡資料時，電腦系統就會主動進行加密，而不影響使用者的輸入過程。       | SSL 加密機制                           |



# 電子付款系統的概念 (續)

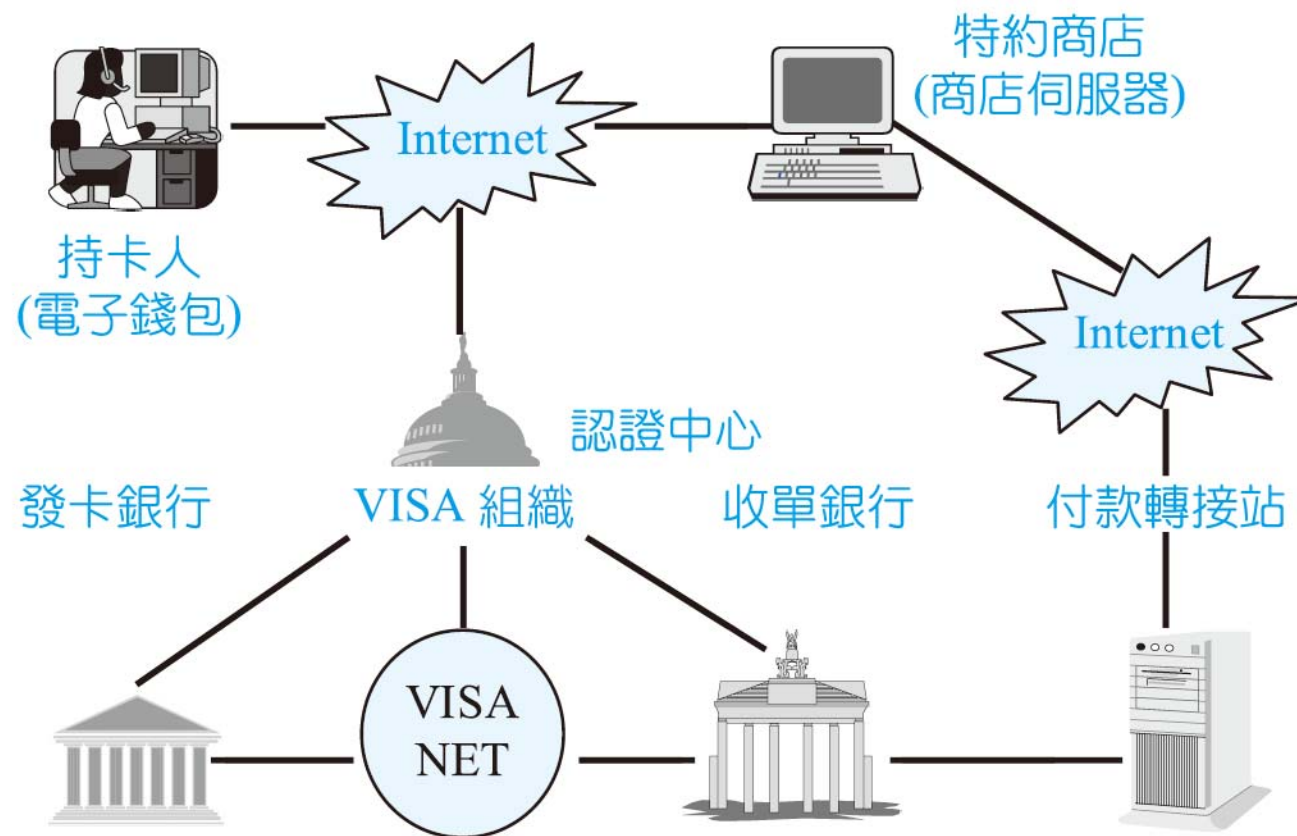


圖 4-3 電子交易付款過程



# 電子付款系統的概念 (續)

---

## ■ 建構電子付款系統，需要加入不同的角色

1. 買方 (Buyer)
2. 賣方 (Seller)
3. 發卡銀行 (Issuer)
4. 收單銀行 (Acquirer)
5. 公正第三者 (Trusted Third Party)
6. 認證中心 (Certificate Authorities)



# 第三方支付

- 第三方支付是由具有金流處理實力與信譽保障的獨立機構，先與各大銀行簽約取得支付結算系統介面的授權，來提供買方、賣方交易時的支付結算平台

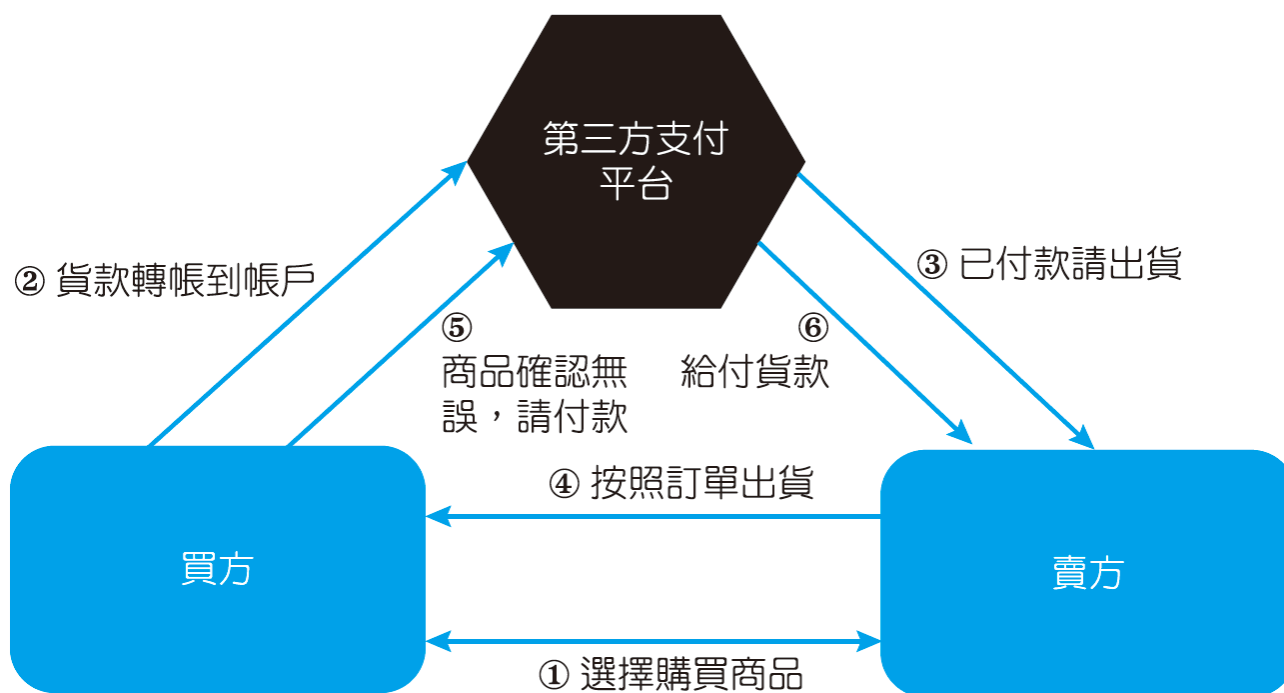



圖 4-4 第三方支付的流程

# 第三方支付 (續)

 表 4-2 第三方支付的流程說明

| 流程           | 說明                                  |
|--------------|-------------------------------------|
| ① 選擇購買商品     | 買方在賣方的商店互動，並且選擇要購買的商品，決定後進行付款。      |
| ② 貨款轉帳到帳戶    | 買方確認商品後就會將所需支付的貨款轉帳到第三方支付的帳號中。      |
| ③ 已付款請出貨     | 當第三方支付收到商品貨款，會通知賣方出貨。               |
| ④ 按照訂單出貨     | 賣方收到第三方支付平台的通知，按照買方需求將商品出貨到指定的地方。   |
| ⑤ 商品確認無誤，請付款 | 買方收到商品後，經由檢查、確認無誤後，通知第三方平台商品無誤，請付款。 |
| ⑥ 給付貨款       | 第三方平台收到買方確認商品無誤，將貨款轉給賣方完成交易活動。      |



# 第三方支付 (續)

---

## ■ 第三方支付平台的好處

1. 付款方式多樣
2. 交易流程約束
3. 交易保障管道



## 4.2 電子付款系統的模式

- 根據電子付款系統的工具，可將電子付款系統分為兩大類：
  1. 代幣式付款系統 (包括電子現金、電子支票、智慧卡與儲值卡)
  2. 信用卡式付款系統 (SSL 電子安全交易)

# 代幣式付款系統

■ 代幣式付款系統模擬傳統的付款方式，將貨幣轉為數位形式，使其適合電子交易的環境，主要分為

1. 電子現金 (e-Cash)
2. 電子支票 (e-Check)
3. 智慧卡 (Smart Card)
4. 儲值卡 (Stored-value Card)

悠遊卡小額消費 (被嗶篇)

<https://www.youtube.com/watch?v=ngPbxW1ZeZ8>



# 代幣式付款系統 (續)

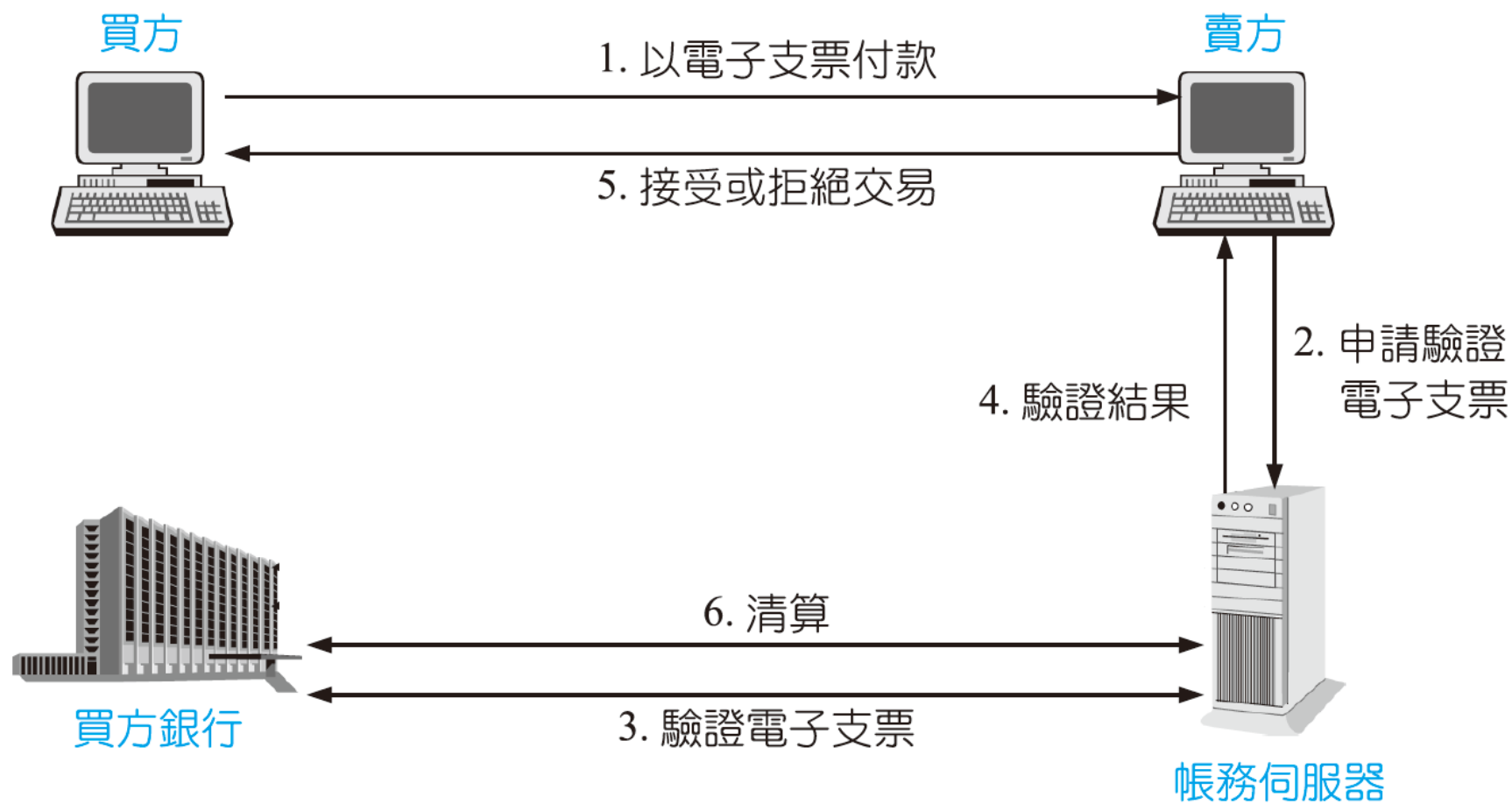


圖 4-7 電子支票流程



# 信用卡式付款系統

---

- 信用卡是一種非現金的交易方式，由銀行或信用卡公司依照申請者的財力核發刷卡的額度
- 網際網路盛行後，在網路上透過 SSL 的加密機制可以讓使用者直接在網路上刷卡





# 信用卡式付款系統的應用

---

1. 機械式複印信用卡交易
2. 磁條式信用卡
3. 晶片式信用卡
4. 網路信用卡交易

# 信用卡式付款系統的應用 (續)

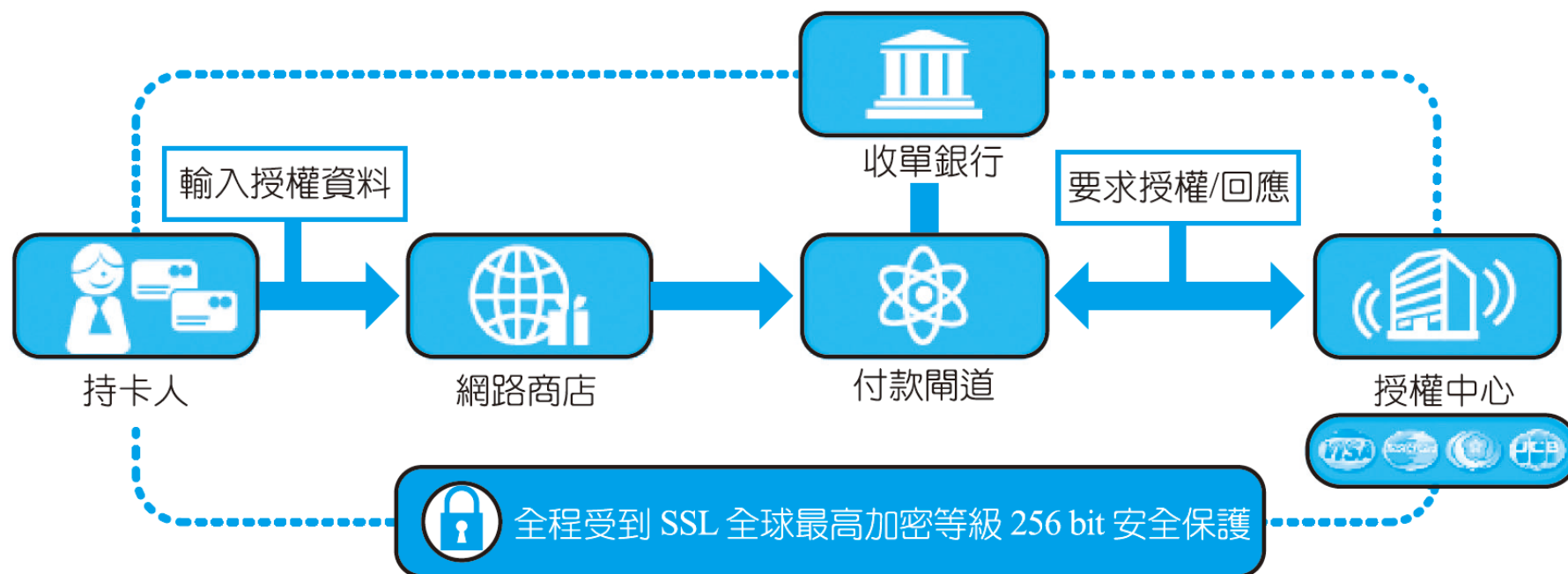


圖 4-13 • SSL 驗證過程



# 信用卡式付款系統的應用 (續)

## 5. 行動支付

- ▣ 行動支付主要利用的技術是近距離無線通訊 (Near Field Communication, NFC)。NFC 是一種短距離的高頻無線通訊技術，建構在非接觸式射頻辨識 (RFID) 技術上，讓電子裝置之間進行非接觸式點對點資料傳輸，在 10 公分的距離之內進行資料的交換

## 6. Apple Pay 的 Tokenization

- ▣ 主要利用序號 (Token) 來取代傳統的信用卡號碼，讓使用者藉由序號來交易，故此模式又稱為 Tokenization

台灣Pay 請你跟我這樣Pay

<https://www.youtube.com/watch?v=7WUHNu7FItI>

# 信用卡式付款系統的應用 (續)

 **表 4-3** 行動支付的特點

| 流程  | 說明   |
|-----|--|
| 移動性 | 行動裝置具有移動、隨身的優點，讓使用者可以透過行動裝置來進行支付行為，改變傳統需要在定點才能支付的模式，只要攜帶行動裝置與感應器就可以完成。                         |
| 便利性 | 由於行動支付利用行動裝置與感應器來取代傳統人工操作，讓行動支付不受營業時間、地點，甚至是銀行的限制，再加上行動支付透過數位進行交易，所以具有不需找零、速度快、隨時隨地都能提供服務的便利性。 |
| 即時性 | 行動支付利用數位來進行交易，使用者支付後可以立刻查詢交易是否完成，免除傳統支付模式需要等待交易完成的時間，讓使用者可以即時完成交易。                             |



# 信用卡式付款系統的應用 (續)

 表 4-4● 行動支付的問題

| 流程         | 說明  |
|------------|---|
| 行動裝置的數量與串連 | 需增加支援行動支付服務的裝置數，包括行動裝置、感應器等，特別是裝設行動感應的店家，需要有夠多的店家來支持。且，目前行動裝置都只支援自家的品牌，不管是 Apple Pay、Google Wallet 或 Samsung Pay 等，無法跨平台來支援其他手機裝置使用，讓使用者的儲值無法在不同行動裝置下進行轉移，增加使用者的困擾。 |
| 行動支付的附加價值  | 行動支付對於使用者的價值不能只有支付的功能，必須具備額外的價值，舉例來說，支付寶在節日促銷時，都會有實體的交易折扣，網路交易時可以獲得折扣，讓使用者願意安裝 app 進行網路交易來獲得實體的優惠。  |
| 行動支付的信任度   | 行動支付的安全性則是另一個問題。大部分的網路使用者對於行動裝置的安全性存疑，目前也只有 PayPal、Amazon 或銀行推出的軟體具有較高的安全性。且，使用者對於支付技術的信任度也不高，目前，只有 Apple Pay 利用序號的模式讓交易過程資料外洩的風險降到最低，對使用者來說，就具有較高的信任度。             |



## 4.3 網路安全

---

- 隨著中毒事件和駭客入侵的案例增多，網路安全逐漸成為大家重視的議題，筆者將由網路使用的概念切入，進而說明網路安全機制和區塊鏈之概念





# 網路使用的觀念

---

## 1. 資料

- ▣ 資料是在網路上最容易被駭客覬覦的東西，許多駭客入侵電腦的目的也是為了要取得電腦中的資料，其可以分為機密性與完整性兩類

## 2. 資源

## 3. 身分

# 網路使用的觀念 (續)

 表 4-5 ● 網路須遵守的觀念

| 概念               | 說明  | 實例        |
|------------------|---|-----------|
| 隱私 <sup>15</sup> | 避免受到其他人干擾的權利，可擁有自己的使用空間。                  | 帳號、密碼遭盜用  |
| 正確性              | 泛指網路上須有正確的使用行為，不能侵犯他人的權利，同時，也須了解受害時求償的管道。 | 165 防詐騙專線 |
| 所有權              | 資料的所有權，通常在作者身上。                           | 盜版 MP3    |
| 存取性              | 資料進行存取、連結等權力，通常此權力的擁有者為作者。                | 複製網路資料    |





# 提高網路安全性

---

## (一) 防火牆

- ▣ Internet 上的防火牆功能類似古代城堡的護城河，用來防止由外部無法信任的網路 (Internet) 使用者進入信任的網路 (Intranet)，以保護內部網路的安全

## (二) 防毒軟體

- ▣ 所謂防毒軟體就是防止電腦病毒入侵的一種軟體程式

# 提高網路安全性 (續)

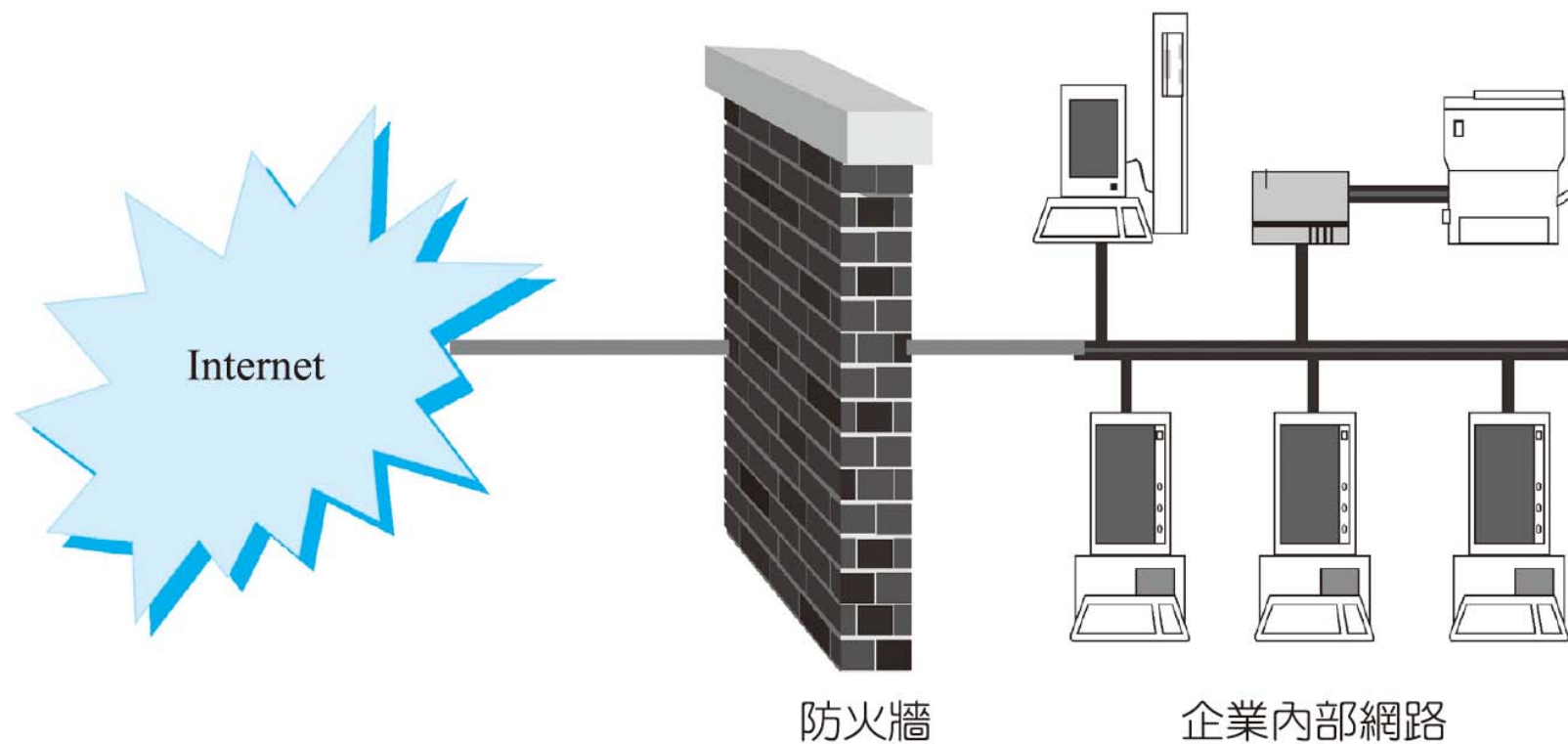


圖 4-19 防火牆的架構



# 提高網路安全性 (續)

 表 4-6● 防火牆的功用

| 功用   | 說明  |
|------|---|
| 集中管理 | 防火牆就像是一個鎖喉之處，所有的安全問題都由此處來解決。當有人欲自外界突破時必須由此進入，因此所有檢查動作都只需在此處執行，而不需將安全措施分散到每一部電腦。 |
| 網路把關 | Internet 所提供的服務本身就具有很多問題，當內部使用者使用這些服務時就可能遭遇這些安全問題，而威脅到內部網路的安全。                  |
| 監視活動 | 因為所有和 Internet 有關的行為都必須經過防火牆，所以防火牆可以記錄所有 Internet 的活動事件。                        |
| 隔離問題 | 防火牆亦可設立在內部網路之中，此時的防火牆就如同船艦中的防水隔離艙門，不讓問題與破壞蔓延而影響到整體組織。                           |

# 提高網路安全性 (續)



圖 4-20 ● 防火牆的設定步驟



# 提高網路安全性 (續)

## (三) 加密保護

□ 加密保護的方式包括私有金鑰及公開金鑰

### 1. 私有金鑰 (Secret Key)

私有金鑰加密法又稱為對稱式加密法或傳統加密法，其特色是加密或解密時必須使用同一把金鑰，明文經此演算法與一組金鑰加密後產生密文，其長度約略與明文的相近，且須使用同一把金鑰才能將密文轉換成明文

### 2. 公開金鑰 (Public Key)

又稱非對稱式加密法，其特色是加密和解密時使用兩組不同的金鑰，這兩組金鑰是成對的，一組是公開金鑰，另一組是私有金鑰

# 提高網路安全性 (續)

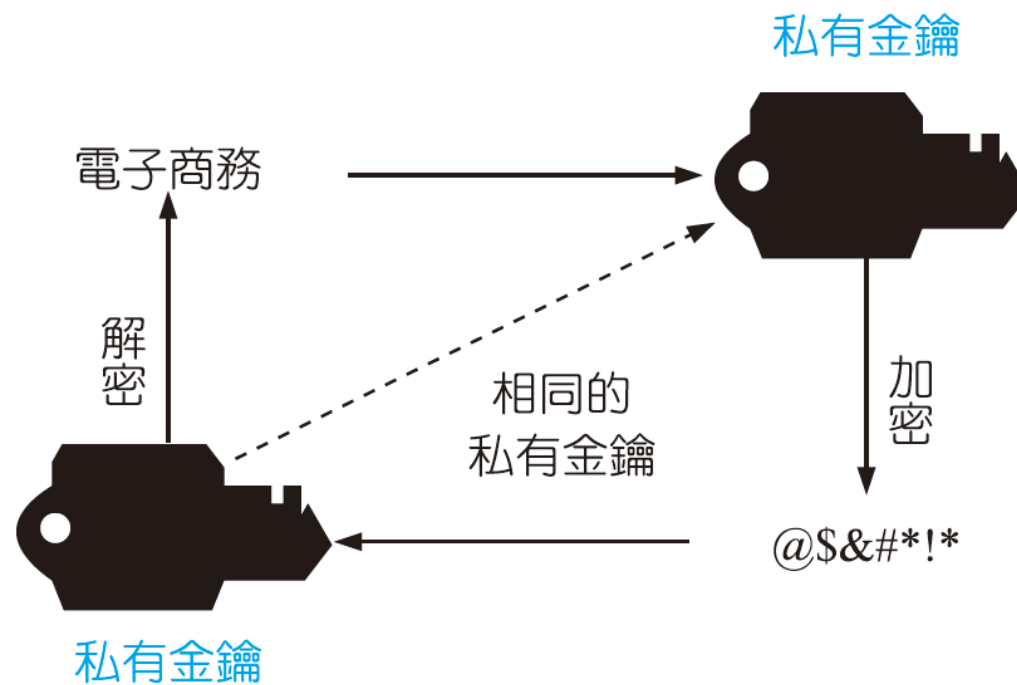


圖 4-24 私有金鑰加密法



# 提高網路安全性 (續)

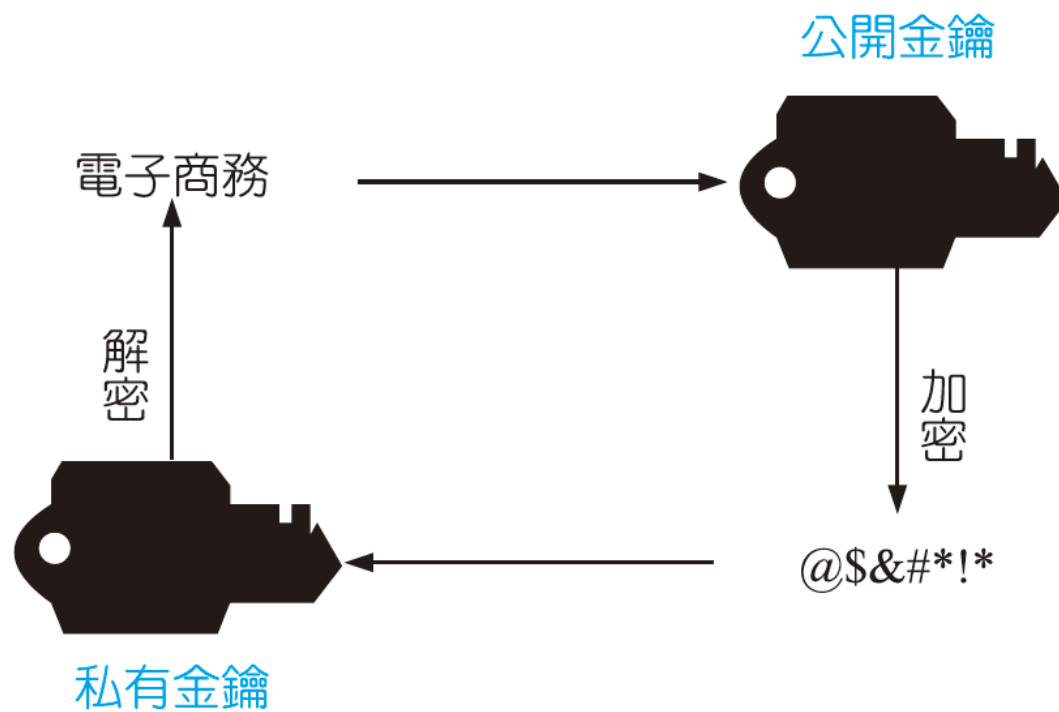



圖 4-25

公開金鑰加密法



# 提高網路安全性 (續)

---

## (三) 加密保護

### ■ 加解密系統的四大功能：

1. 確實性 (Authentication)
2. 機密性 (Confidentiality)
3. 完整性 (Integrity)
4. 不可否認性 (Non-repudiation)



# 區塊鏈的概念

- 區塊鏈 (Block Chain) 是由密碼學、數學、演算法與經濟模型組成，採用分散式共識演算法、點對點的網路關係 (P2P)，來解決傳統分散式資料庫的同步問題

秒懂「區塊鏈」的入門課！

<https://www.youtube.com/watch?v=uKr-rKEALiE>

『發現芬特克！比特幣 & 區塊鏈原理大解析』芬特克 FinTech EP1

<https://www.youtube.com/watch?v=5r8kJCE1S1s>



# 區塊鏈的概念 (續)

---

## (一) 區塊鏈的特性

1. 交易辨識
2. 無法篡改
3. 資料同步





# 區塊鏈的概念 (續)

---

## (二) 區塊鏈的階段

### 1. Blockchain 1.0

- ▣ 數位貨幣 (**Currency**) 的應用，將傳統的實體貨幣轉移到網路或數位上

### 2. Blockchain 2.0

- ▣ 智慧資產 (**Smart Assets**)、智慧契約(Smart Contracts)、股票等新的應用與服務



# 區塊鏈的概念 (續)

---

## 3. Blockchain 2.5

- 人工智慧 (**Artificial Intelligent**)

## 4. Blockchain 3.0

- 應用在金融產業之外，像是政府、醫療、科學、文化與藝術等產業



# 區塊鏈的概念 (續)

 **表 4-7** 區塊鏈發展過程與相關技術

| 年份     | 技術                                   | 說明   |
|--------|--------------------------------------|--|
| 1982 年 | 拜占庭將軍問題 (Byzantine Generals Problem) | 軍隊分散在各地，且隊伍中可能有敵方人員，要取得共識與同時出兵的過程。   |
|        | 密碼學支付系統                              | 注重安全性的密碼學網路支付系統，具備不可追蹤的特性，為比特幣安全機制的雛形。   |
| 1985 年 | 橢圓曲線密碼學                              | 首次將橢圓曲線應用在密碼學，建立公開金鑰加密的演算法。  |
| 1990 年 | eCash                                | 以密碼學網路支付系統為基礎，非去中心化的系統。  |
| 1991 年 | 時間戳                                  | 利用時間戳確保數位文件的安全，此概念也用在比特幣的應用中。  |
| 1992 年 | 橢圓曲線數位簽章演算法                          | 建立在橢圓曲線密碼學的基礎，發展出數位簽章演算法。  |
| 1997 年 | 雜湊現金 (Hashcash)                      | 是一種工作量證明演算法 (Proof of Work, POW)，依靠成本函數的不可逆特性，提高驗證的便利性，又能維持難以破解的特性。初期主要在阻擋垃圾郵件，2002 年正式被發展成論文。 |

# 區塊鏈的概念 (續)

表 4-7 區塊鏈發展過程與相關技術

| 年份     | 技術                   | 說明   |
|--------|----------------------|--|
| 1998 年 | 分散式電子現金系統 (B-money)  | 引入工作量證明機制，建立起點對點交易與不可篡改的特性。                                    |
| 2005 年 | 可重複使用的工作量證明機制 (RPOW) | 結合 B-money 與 Hashcash，在密碼學的基礎上所創造出來的貨幣。                        |
| 2008 年 | 比特幣                  | 中本聰 (Satoshi Nakamoto) 發表一個點對點的電子現金系統，在不具信任的基礎上，建立一套去中心化的交易體系。 |
| 2012 年 | Blockchain 2.0       | 貨幣外的應用，像是股票、債券等。   |
| 2014 年 | Blockchain 2.5       | 強調代幣的應用、分散式帳本、資料層區塊鏈等金融產業的應用。                                  |
| 2015 年 | Blockchain 3.0       | 金融產業外的應用，將區塊鏈的概念延伸到政府、醫療、藝術等領域。                                |
|        | Ujo                  | 第一套運用區塊鏈的音樂平台，讓用戶花 0.6 美元就能下載歌曲，且公開款項的分配過程。                    |





# 區塊鏈的概念 (續)

---

## (三) 區塊鏈的問題

1. 運算速度慢
2. 匿名交易
3. 交易難以變更
4. 交易責任難以釐清



## 習題

---

1. 請列出五種信用卡式付款系統的應用
2. 請說明公開金鑰與私有金鑰的差異