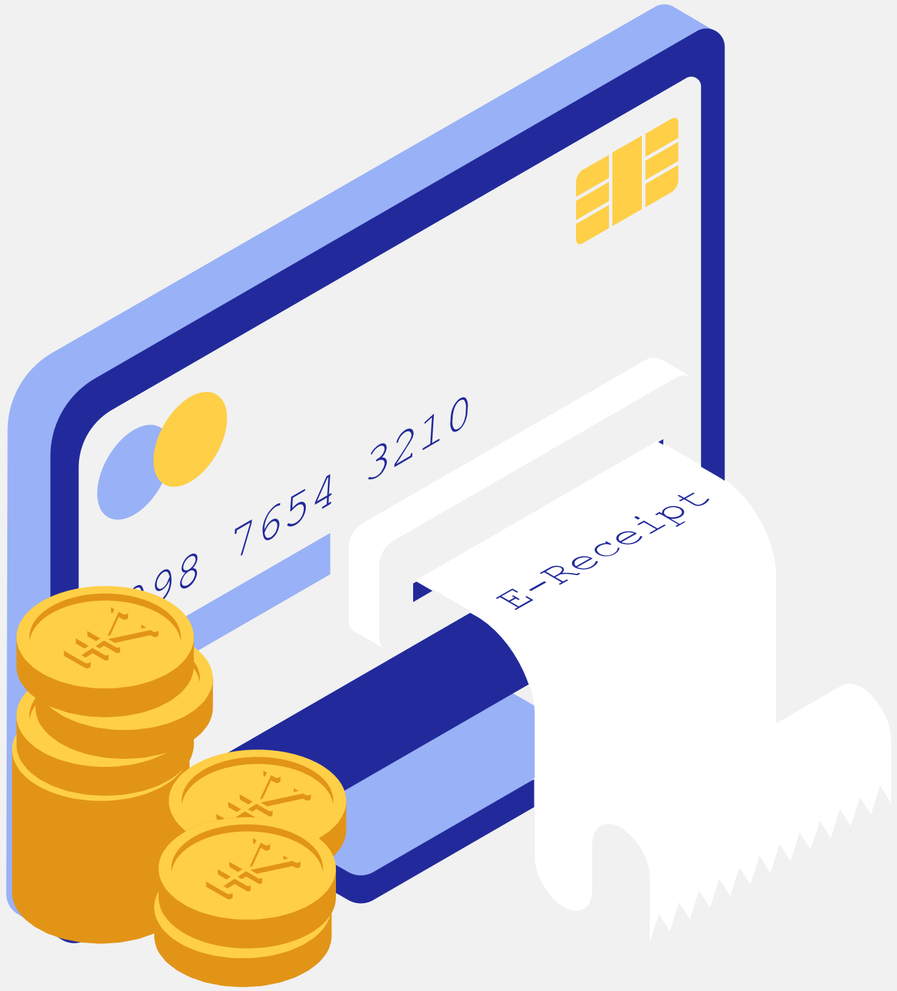


演算法期中作業

區塊鏈相關算法報告

資工三 111110512 沈心怡

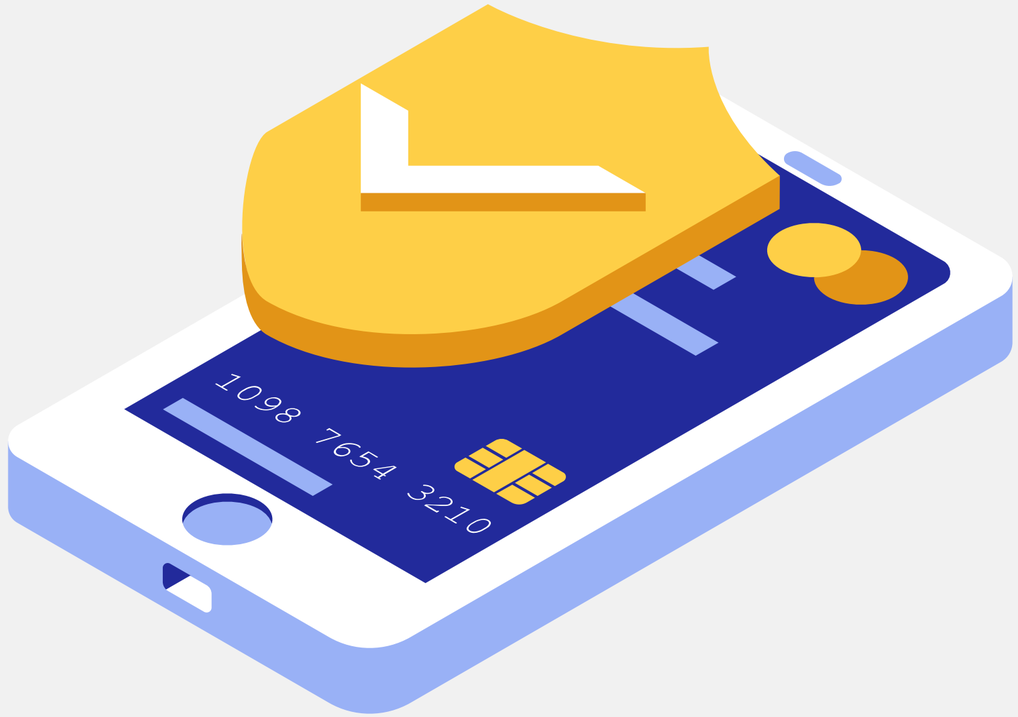
目錄

區塊結構

區塊鏈中的每個區塊都以特定的格式和結構組成，這種結構確保了資料的安全性、完整性和連接性。

區塊鏈算法

指在區塊鏈技術中使用的各種數學和計算方法，這些算法的目的是確保數據的安全性、可靠性和一致性。這些算法幫助區塊鏈系統達成共識、保護數據不被篡改、實現交易的安全驗證，並支持智能合約等功能。



共識算法

這些算法用於確保網絡中所有節點達成一致

工作量證明（PoW）

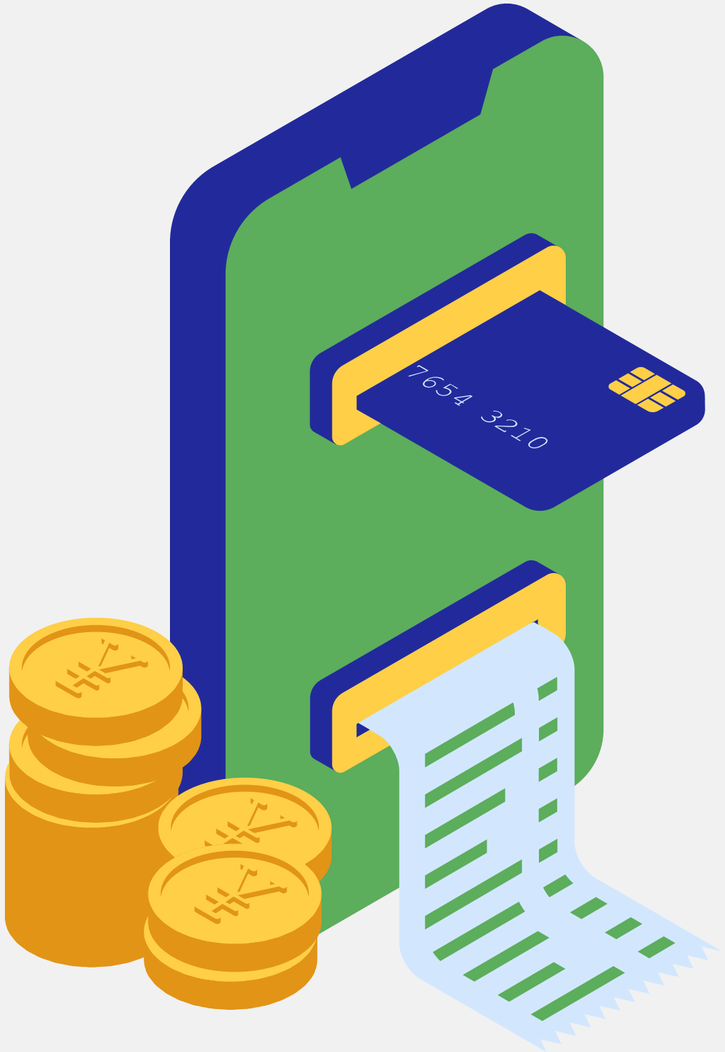
通過計算複雜的數學問題來競爭生成區塊。

權益證明（PoS）

根據持有的代幣數量來確定區塊生成權限。

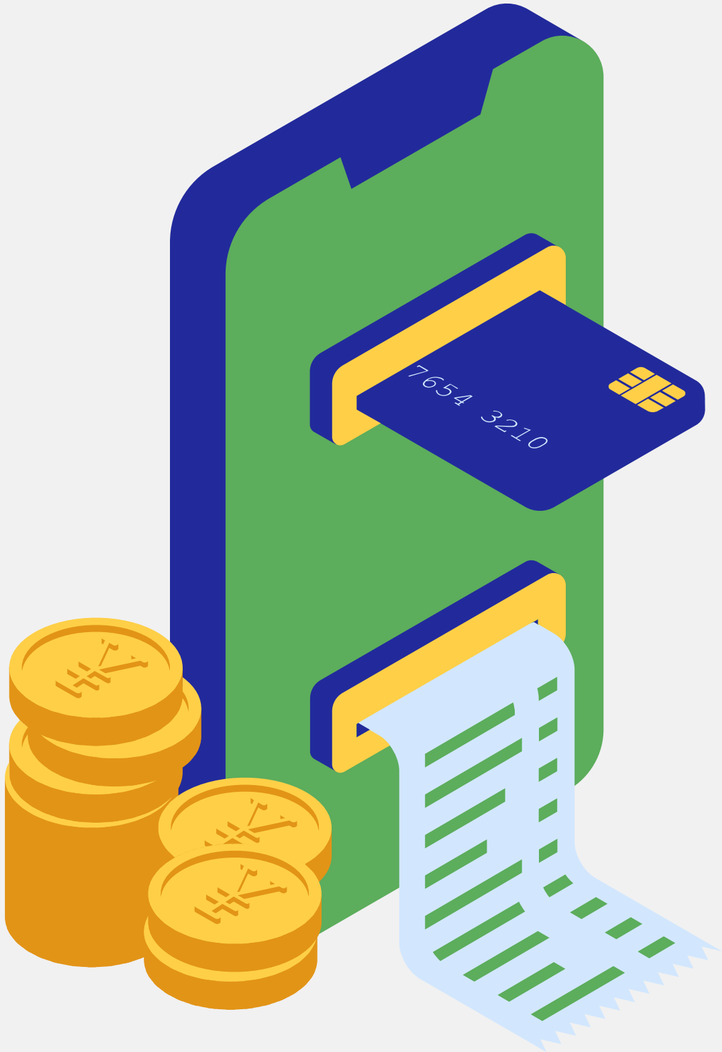
委任權益證明（DPoS）

用戶選擇代表進行區塊生成，提高效率。



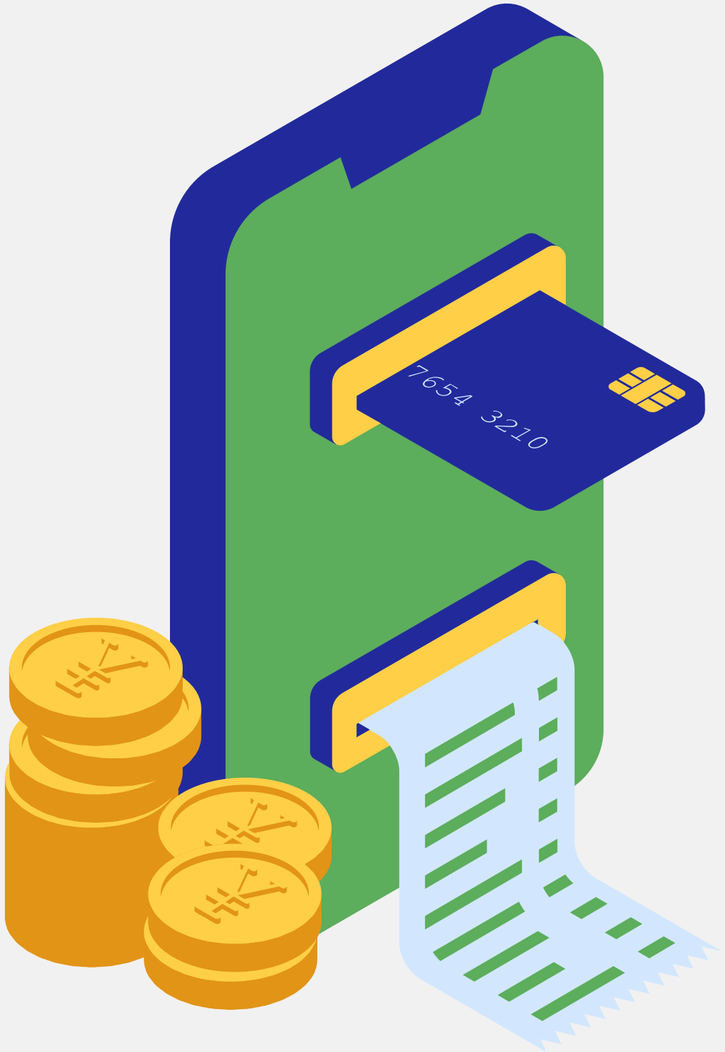
工作量證明（PoW）

- **簡介**：PoW 是最早且最著名的共識算法，主要用於比特幣等加密貨幣中。礦工通過解決複雜的數學問題來競爭生成新區塊。
- **功能**：確保所有節點達成一致，防止雙重支付，增強網絡安全性。
- **應用**：比特幣、以太坊（過渡前）等。



權益證明（PoS）

- **簡介：**PoS 允許擁有代幣的用戶根據其持有的代幣數量參與區塊生成。生成區塊的概率與持幣量成正比。
- **功能：**減少資源消耗，提高交易速度，促進網絡參與。
- **應用：**以太坊2.0、Cardano、Tezos等。



委任權益證明（DPoS）

- **簡介**：用戶選擇一定數量的代表來維護網絡，這些代表負責生成區塊和確認交易。
- **功能**：提高交易處理速度，降低中心化風險。
- **應用**：Steemit、EOS、TRON等。

加密算法

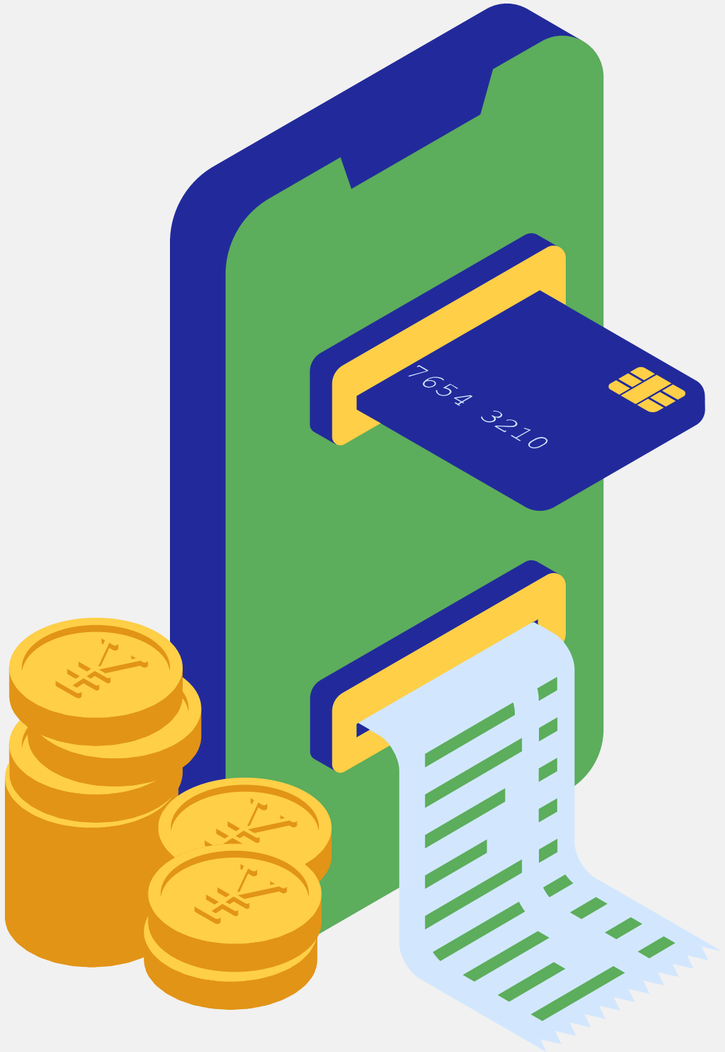
這些算法用於保護數據的安全性

哈希函數（如 SHA-256）

將數據轉換為固定長度的哈希值，確保數據完整性。

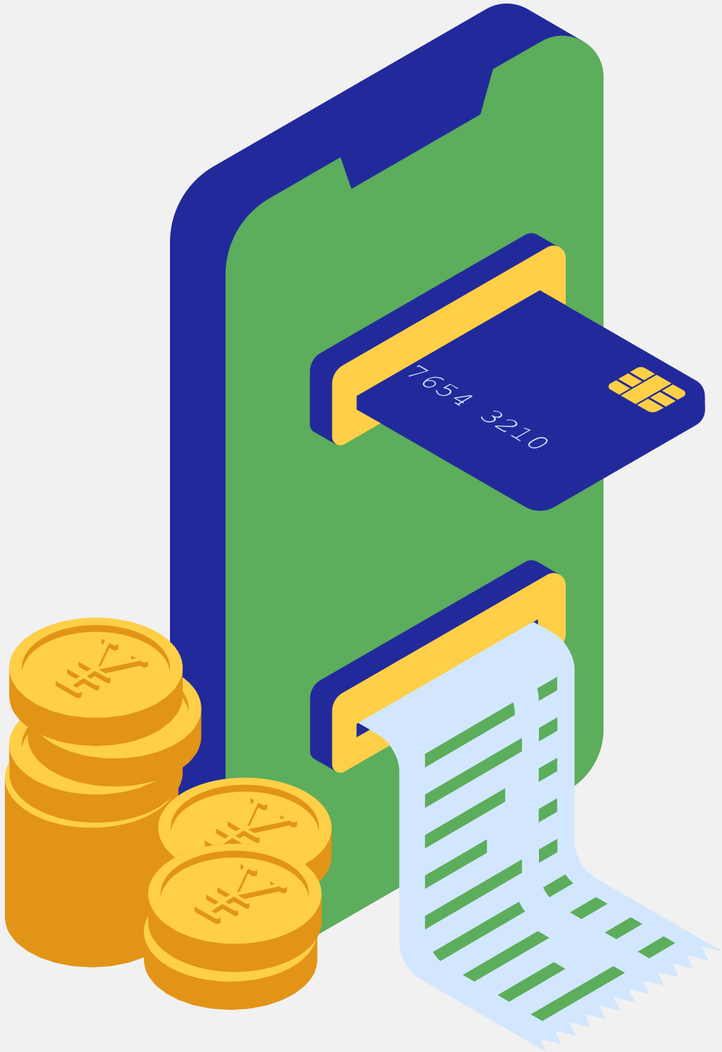
公鑰加密

使用一對密鑰進行安全交易和身份驗證。



哈希函數（如 SHA-256）

- **簡介**：哈希函數將任意長度的數據轉換為固定長度的哈希值，是區塊鏈數據完整性的重要保障。
- **功能**：確保數據的不可篡改性和完整性，快速驗證數據。
- **應用**：比特幣、以太坊等的區塊生成。



公鑰加密

- **簡介**：公鑰加密使用一對密鑰（公鑰和私鑰）進行安全通信和身份驗證。
- **功能**：保障交易的安全性，防止未授權訪問。
- **應用**：幾乎所有加密貨幣和區塊鏈系統。

數據結構

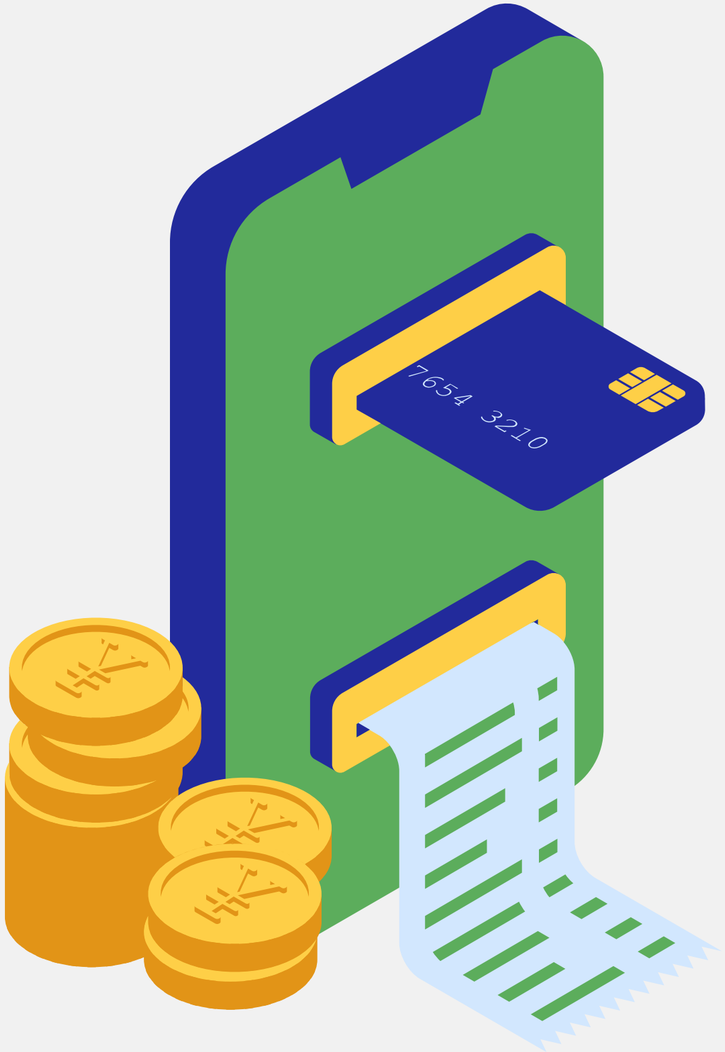
區塊鏈的數據結構影響其性能和安全性

鏈結構

每個區塊包含前一個區塊的哈希，確保數據不可篡改。

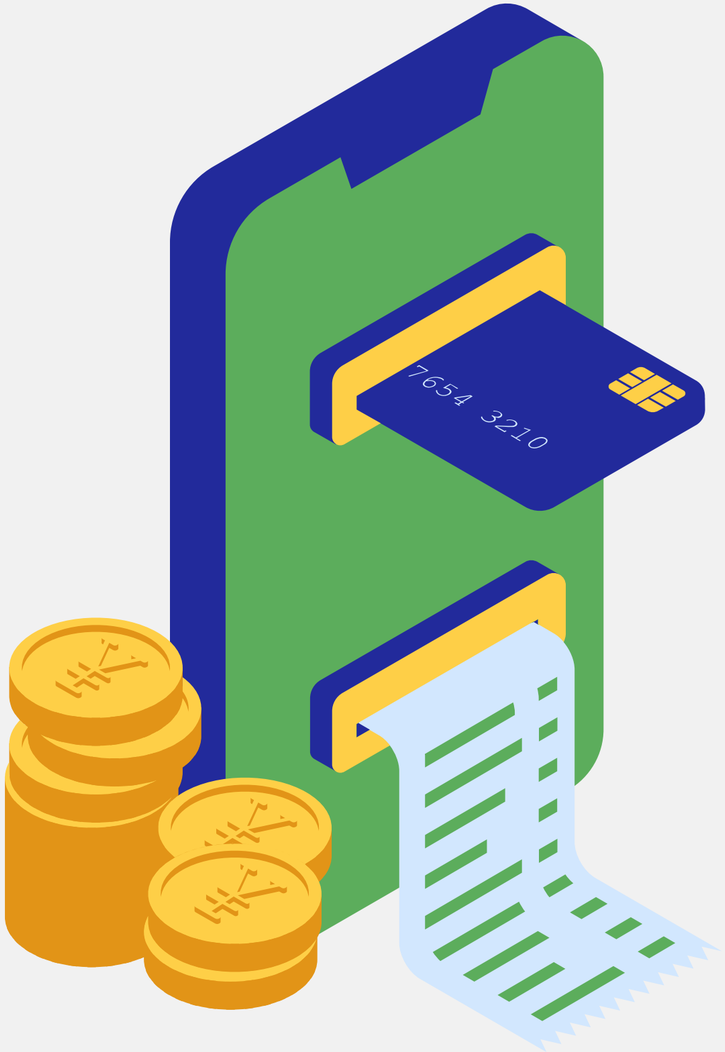
Merkle樹

用於高效驗證大量交易數據的樹形結構。



鏈結構

- **簡介**：區塊鏈的核心數據結構，區塊依序鏈接，每個區塊包含前一個區塊的哈希。
- **功能**：確保數據的順序性和不可篡改性，增強安全性。
- **應用**：所有使用區塊鏈技術的系統。



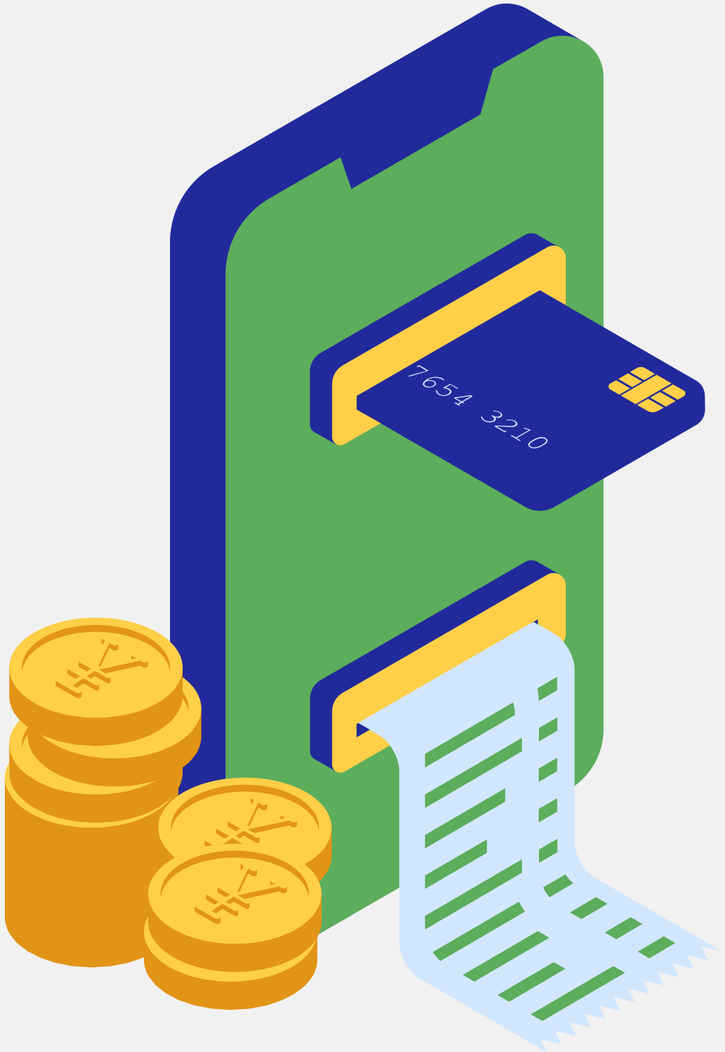
Merkle樹

- **簡介**：一種樹形數據結構，用於高效存儲和驗證大量交易數據。
- **功能**：通過將交易哈希組合成樹狀結構，提高驗證效率和數據完整性。
- **應用**：比特幣和以太坊中的交易驗證。

智能合約

一種自動執行的合約，通常基於以太坊等平台的區塊鏈技術，支持複雜的交易邏輯

Solidity



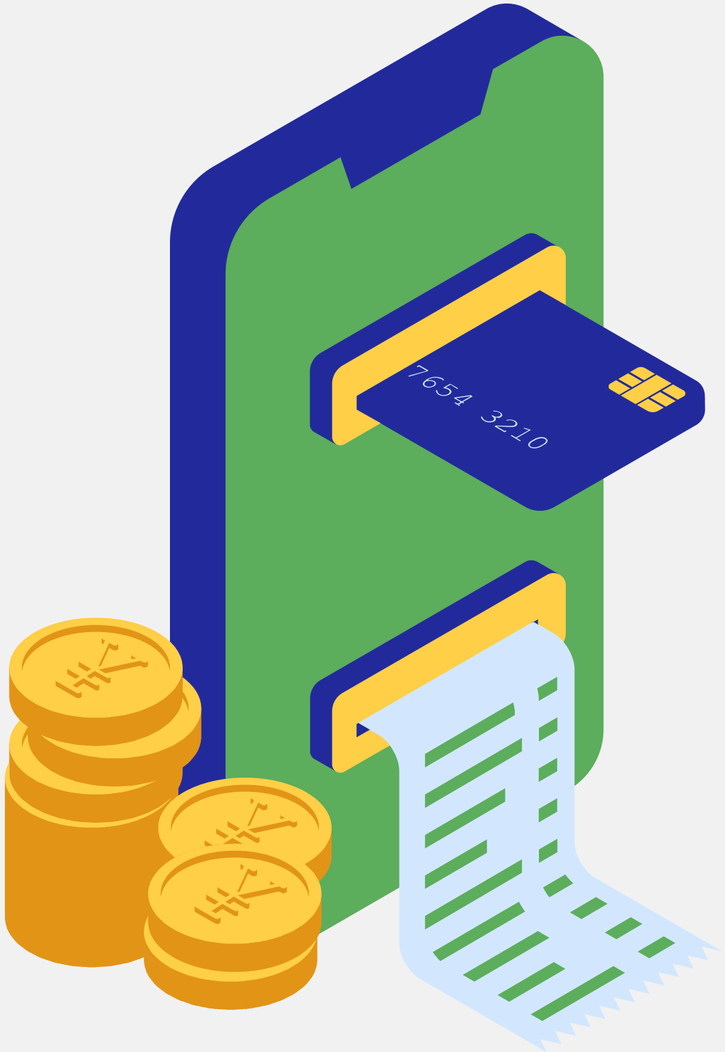
Solidity

- **簡介**：一種專門用於編寫以太坊智能合約的高級編程語言。
- **功能**：支持複雜邏輯的實現，自動執行合約條款。
- **應用**：以太坊平台的各類應用和DeFi項目。

其他算法

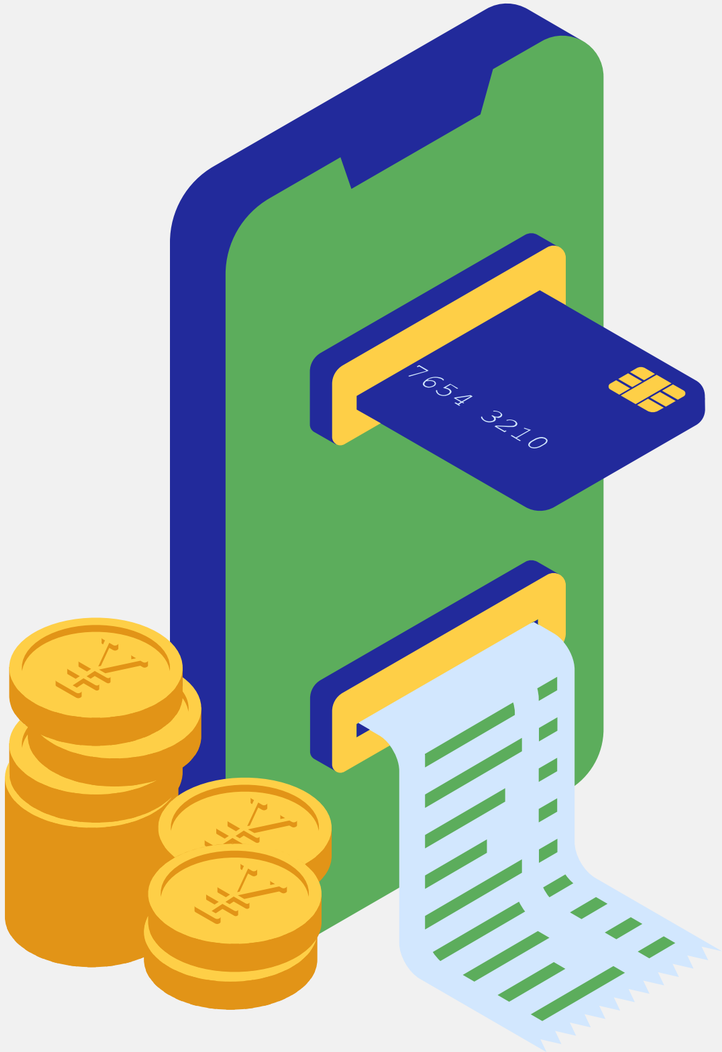
增強交易的隱私性和數據的安全性

拜占庭容錯算法
零知識證明



拜占庭容錯算法

- **簡介**：一種容錯算法，旨在確保在存在故障或惡意節點的情況下系統仍能正常運行。
- **功能**：提高系統的安全性和可靠性。
- **應用**：許多區塊鏈系統，如Hyperledger等。



零知識證明

- **簡介**：一種加密技術，允許一方證明某個聲明是真而無需提供具體信息。
- **功能**：增強隱私性，確保交易和身份信息的安全。
- **應用**：Zcash、以太坊的某些隱私協議等。

參考資料

01 https://chatgpt.com/

02 https://gwarket.com/blockchain-consensus-algorithm/

03 https://www.kaotenforensic.com/blockchain/how-does-blockchain-work/

04 https://www.gaia.net/tc/news_detail/2/241

05 https://www.ithome.com.tw/news/105374

06 https://aws.amazon.com/tw/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc