

虛擬資產案件的美麗與哀愁



臺灣臺北地方檢察署檢察官

洪敏超

Jan.06.2024

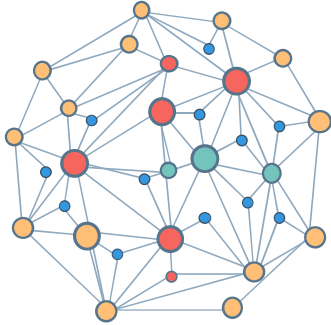
About Me

洪敏超
北檢檢察官
CHFI資安鑑識調查專家
CEH駭客技術專家
CBP區塊鏈專家
法務部財務金融高階證照





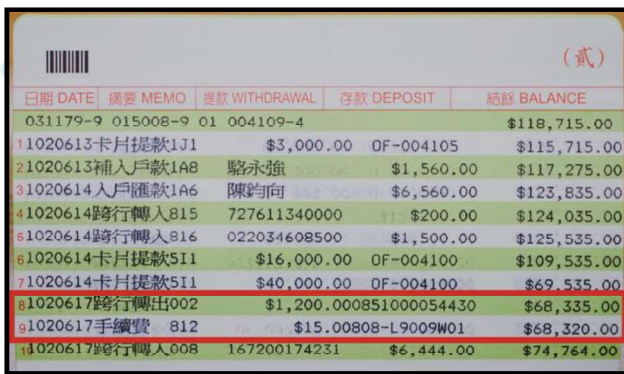
/01 In Money We Trust?



In Money
We Trust ?

102 區塊鏈與虛擬資產

把錢存進銀行，然後呢？



| 日期 DATE | 摘要 MEMO | 提款 WITHDRAWAL | 存款 DEPOSIT | 結餘 BALANCE |
|----------|------------------------------|---------------|-----------------|--------------|
| 031179-9 | 015008-9 01 004109-4 | | | \$118,715.00 |
| 1 | 1020613 卡片提款1J1 | \$3,000.00 | 0F-004105 | \$115,715.00 |
| 2 | 1020613 補入戶款1A8 駱永強 | | \$1,560.00 | \$117,275.00 |
| 3 | 1020614 入戶匯款1A6 陳鈞向 | | \$6,560.00 | \$123,835.00 |
| 4 | 1020614 跨行轉入815 727611340000 | | \$200.00 | \$124,035.00 |
| 5 | 1020614 跨行轉入816 022034608500 | | \$1,500.00 | \$125,535.00 |
| 6 | 1020614 卡片提款5I1 | \$16,000.00 | 0F-004100 | \$109,535.00 |
| 7 | 1020614 卡片提款5I1 | \$40,000.00 | 0F-004100 | \$69,535.00 |
| 8 | 1020617 跨行轉出002 | \$1,200.00 | 000851000054430 | \$68,335.00 |
| 9 | 1020617 手續費 812 | \$15.00 | 00808-L9009W01 | \$68,320.00 |
| 10 | 1020617 跨行轉入008 167200174231 | | \$6,444.00 | \$74,764.00 |

存戶把錢存到金融機構以後，「存款金額」就只是金融機構帳務系統內存戶帳戶內的數字，表彰存戶對金融機構的金錢債權。此外，在轉帳的過程中，並沒有發生實際金錢的移轉，而是在概念上銀行先進行帳務清算，再將異動內容記載於帳務系統內而做成紀錄。

LINE Pay

街口支付
JKOPAY

網路遊戲裡的代幣、裝備及寶物在哪裡？



在網路遊戲中，玩家可以遊戲中的代幣購買遊戲中的裝備、寶物，或以遊戲的裝備、寶物升級或合成為其他裝備、寶物。這些代幣、裝備、寶物性質上都只是電磁紀錄，並沒有實體的物品在現實中發生得、喪、變更，其異動也只是遊戲公司在系統紀錄中進行。

把錢存進銀行，安全嗎？



在存戶領出帳戶內存款之前，帳戶內存款餘額都只是紙上富貴。

1. 資料不公開，除存戶本人外無法確認紀錄內容
2. 紀錄內容可能遭偽造
3. 資料內容雖正確，但帳上所列存款未必實際留在中心化的金融機構內

Yahoo奇摩新聞

SVB風暴蔓延》11天4家歐美銀行倒掉 第5家銀行也岌岌可危

SVB風暴蔓延》11天4家歐美銀行倒掉第5家銀行也岌岌可危·《彭博》3月21日報導，4家歐美銀行自3月9日以來接連倒閉，還有一家搖搖欲墜，這種速度震驚投資人...

虛擬資產是什麼？

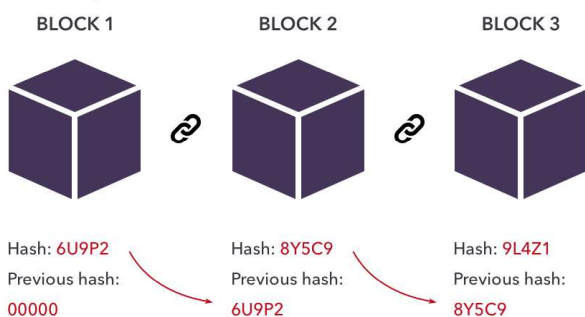


虛擬資產（含俗稱之虛擬貨幣、加密貨幣、NFT）之本質

- 1.屬於數位帳本上的數據資料及紀錄（類似於遊戲點數及虛擬寶物）並存在於網路上
- 2.使用區塊鏈及分散式帳本技術

區塊鏈是什麼？

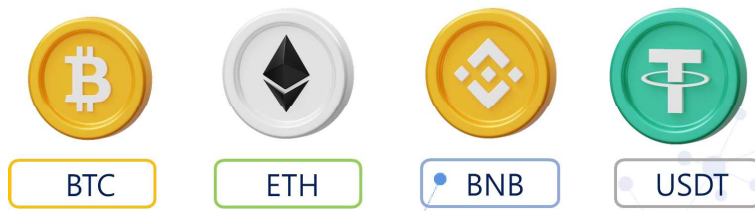
在特定P2P網路中，於一定時間內將一筆或多筆交易紀錄依序打包成一個區塊，並利用雜湊方式彼此鏈結，形成一條由區塊組成的鏈型帳本的技術。（活頁本+騎縫章）



常見虛擬資產介紹

虛擬資產知多少？

<https://coinmarketcap.com>



常見虛擬資產介紹

虛擬資產知多少？

<https://coinmarketcap.com>

<https://www.coingecko.com/zh-tw>



名詞介紹

BTC：比特幣，俗稱大哥，特徵為「1」（34位）、「3」（34位）或「bc1」（42位）開頭，貨幣代碼為XBT。

ETH：以太幣，俗稱二哥，特徵為「0x」開頭(42位)。

穩定幣：stablecoin，宣稱其價格與特定幣種維持1:1之掛勾，以保持代幣價格穩定，常見者為USDT、USDC。

USDT：泰達幣，為Tether公司利用智能合約發行在不同鏈上的代幣，宣稱每枚價格錨定1美元，持有者可隨時向Tether公司贖回，俗稱「U」。



 Metamask：錢包的一種，俗稱「狐狸」。VS「蝸牛」

名詞介紹

幣商：以買賣虛擬資產賺取價差獲利之人。

搬磚：在不同交易所或個人間買賣虛擬資產賺取價差套利的行為。

CEX：中心化交易所，提供虛擬資產買賣等服務之實體事業，如Maicoïn、Binance等。

DEX：去中心化交易所，透過智能合約或協定在區塊鏈上提供數幣種的兌換服務的交易所，如Uniswap、sushiswap等。

ICO：首次代幣發行(Initial Coin Offering)，一種對外發行代幣以募資的作法。



/03 虛擬資產與犯罪



虛擬資產之不法使用態樣



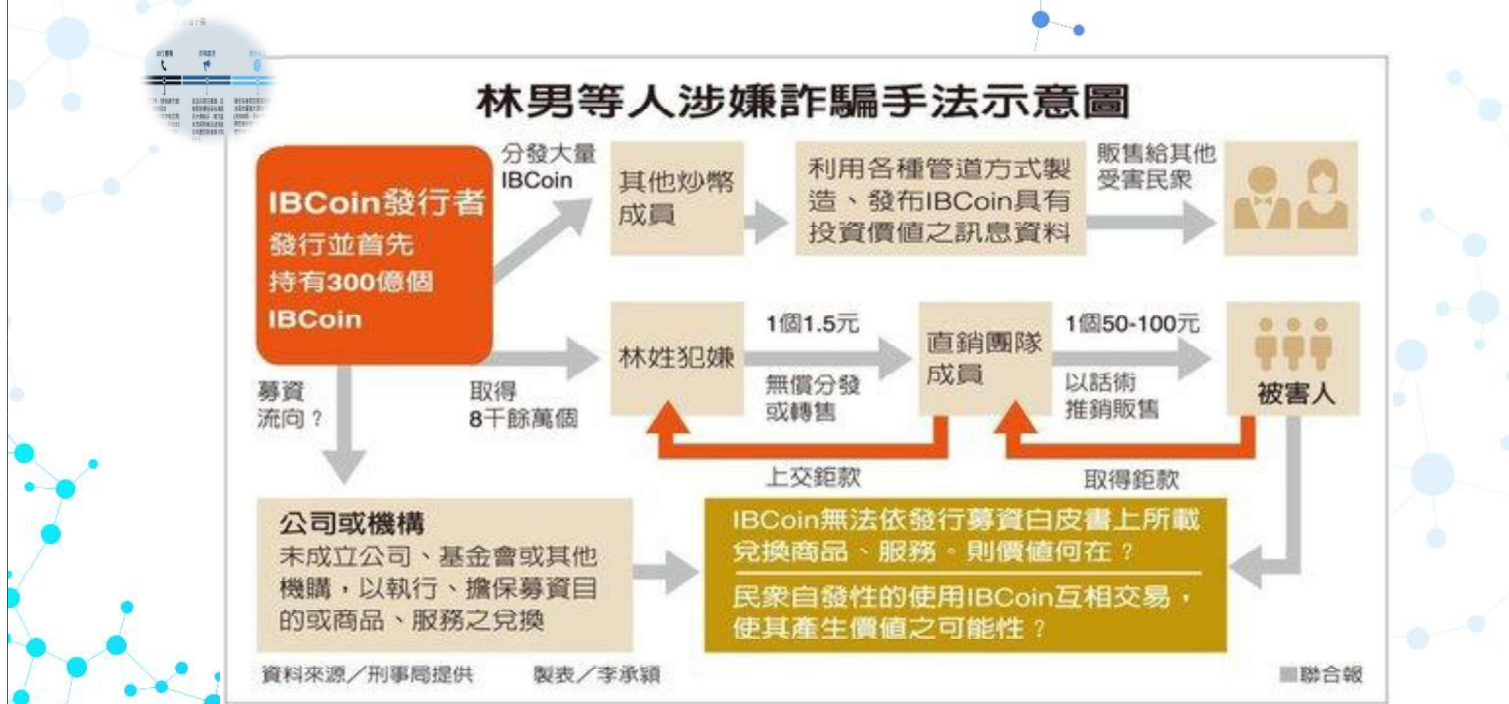
2021年
國家洗錢資恐及資武擴風險評估報告
National ML/TF/PF Risk Assessment Report

我國執法機關近年偵辦案件，可辨識出5大虛擬資產犯罪態樣，包含詐欺、擄人勒贖、恐嚇取財（含電腦勒贖軟體）、強盜及竊電挖礦等，其中又以詐欺最為常見。

虛擬資產之不法使用態樣

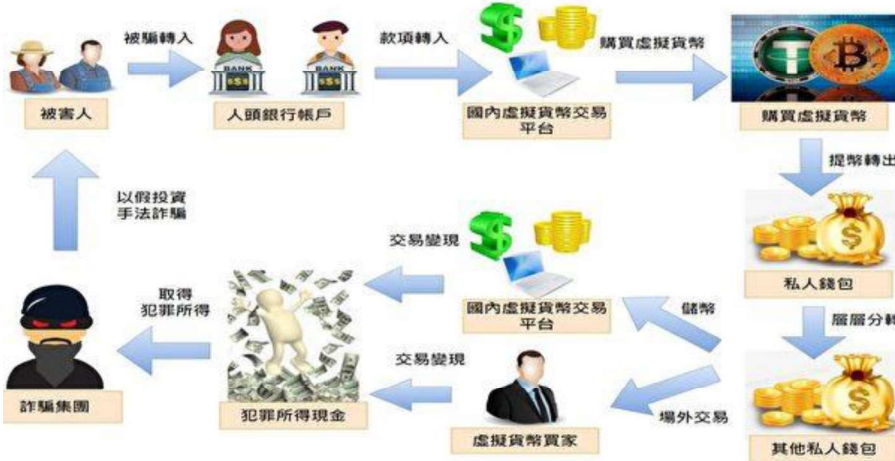


虛擬資產之不法使用態樣：ICO



虛擬資產之不法使用態樣：詐欺

詐欺水房洗錢流程圖



虛擬資產之不法使用態樣：妨害電腦使用





/04 錢包、地址與助記詞



創建自己的錢包（以MetaMask為例）



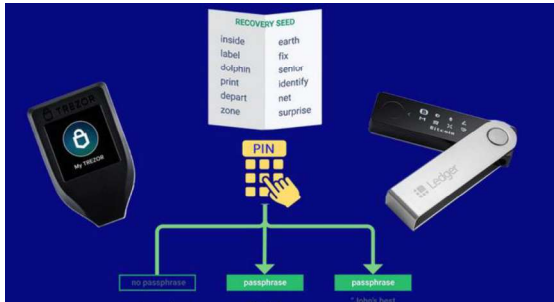
歡迎來到 MetaMask

MetaMask 是以太坊安全身份識別金庫

我們很高興看到你。

開始使用

創建自己的錢包（以MetaMask為例）



METAMASK
←上一頁

Secret Recovery Phrase

助憶詞將可協助您用更簡單的方式備份帳戶資訊。

警告：絕對不要洩漏您的助憶詞。任何人只要得知助憶詞代表他可以竊取您所有的以太幣和代幣。

improve brother

轉後提醒我 下一頁

提示：

您可以使用密碼管理系統例如 1Password 等軟體儲存助憶詞。

將助憶詞寫在紙上，並保存在安全的場所。若想要更安全，將助憶詞分別寫在不同紙張上並存放在不同的地方。

絕對不要忘記您的助憶詞。

下載助憶詞文字檔案，並安全的保存在有加密功能的外接硬碟或其他儲存裝置。

錢包地址、助記詞與私鑰



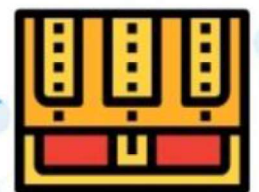
1. 輸入助記詞

= 唸出咒語



2. 取得錢包私鑰

= 施展魔法



3. 創建/復原錢包

= 召喚及開啟魔法錢包

虛擬資產錢包之類型

託管錢包 VS 非託管錢包

區別：私鑰（管理權限）由何人所支配



105 虛擬資產的收、發與移轉

如何取得虛擬資產？



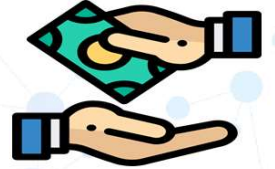
挖礦取得



購買取得



質押放貸




















現實交易



/06 常見虛擬資產交易所介紹 (含KYC資料)

淺介常見中心化虛擬資產交易所

| | | | | |
|---|---|---|--|--|
| 1 |  Binance |  Bybit |  Gate.io |  ACE |
| 2 |  Coinbase Exchange |  OKX |  BingX |  BITGIN |
| 3 |  Kraken |  Crypto.com Exchange |  Pionex | |
| 4 |  KuCoin |  MEXC |  MAX Exchange | |
| 5 |  Bitstamp |  Huobi |  BitoPro | |

<https://coinmarketcap.com/zh-tw/rankings/exchanges/>

淺介常見虛擬資產交易所（海外）



幣安交易所，<https://www.binance.com/zh-TC>

coinbase交易所，<https://www.coinbase.com/>

歐易交易所，<https://www.okx.com/>

CRO交易所，<https://crypto.com/exchange>

火幣交易所，<https://www.huobi.com/>

抹茶交易所，<https://www.mexc.com/zh-TW>

冰棒交易所，<https://bingx.com/zh-hk/>

芝麻開門交易所，<https://www.gate.io/zh-tw>

淺介常見虛擬資產交易所（境內）



現代財富科技有限公司



桑費斯特有限公司



幣託科技股份有限公司



鏈科股份有限公司



王牌數位創新股份有限公司



畢竟科技股份有限公司



幣鍊有限公司



禾亞數位科技股份有限公司

中心化交易所紀錄與KYC

實體法幣帳戶



以人名查詢存戶個人資料

01

虛擬資產錢包

以人名查詢用戶個人資料？



函調帳戶開戶資料、往來明細

02

調交易所開戶資料、往來明細

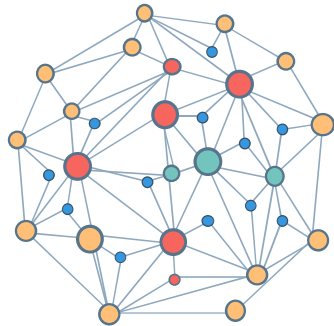
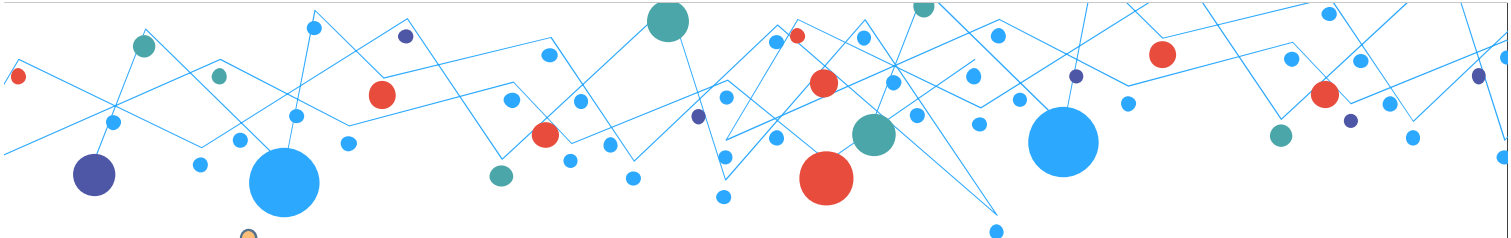


網銀登錄IP、提款影像等

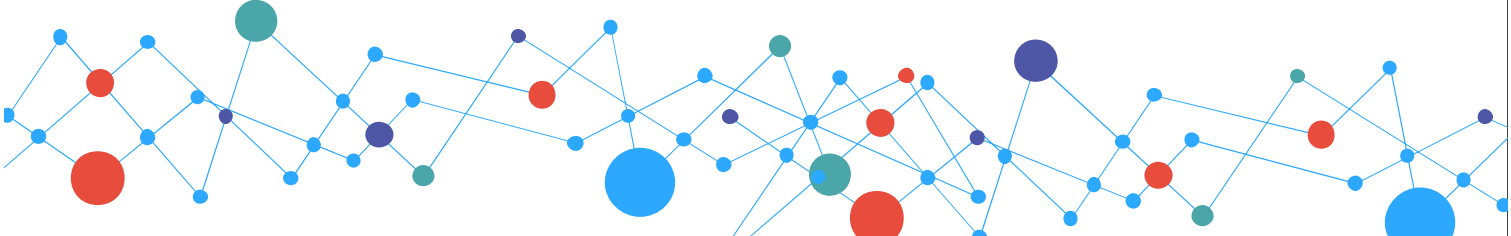
03

交易所、節點登錄IP、提款影像等





101 虛擬資產移轉紀錄 (基礎知識篇)



QUIZ



某判決記載

「被告應返還如附表所示之項目予原告」等文字，
有什麼問題嗎？

| 返還項目 | 備註 |
|--|-------------------------------|
| 電子錢包「0x2c2439cc1f9ff6260054b7111ceff7f05f7c64d8」之管理權限，包含私鑰及助記詞 | 應存放有19億5,242萬7,068顆PIXIU Coin |

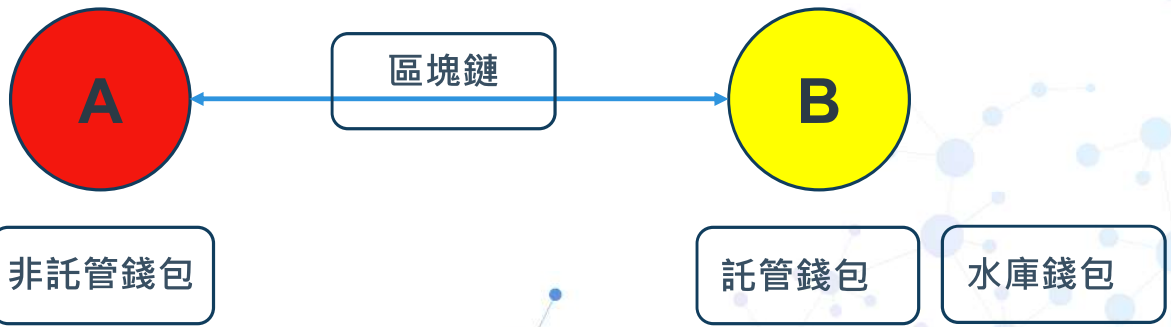
虛擬資產的移轉與區塊鏈紀錄



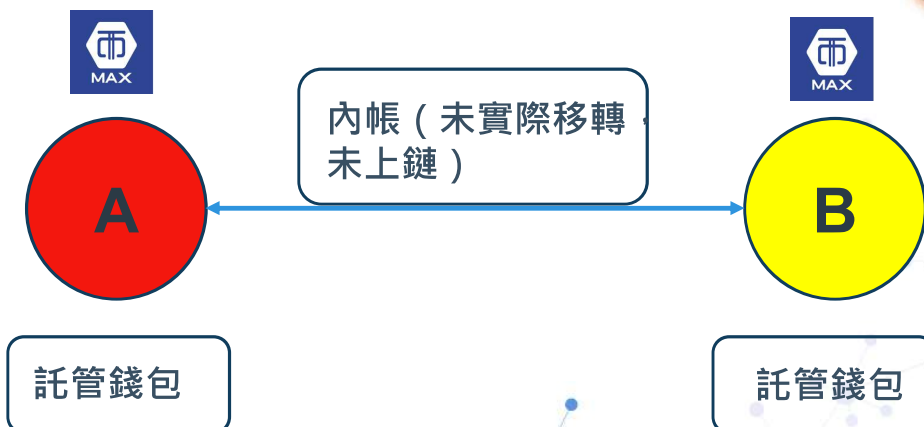
虛擬資產的移轉與區塊鏈紀錄



虛擬資產的移轉與區塊鏈紀錄



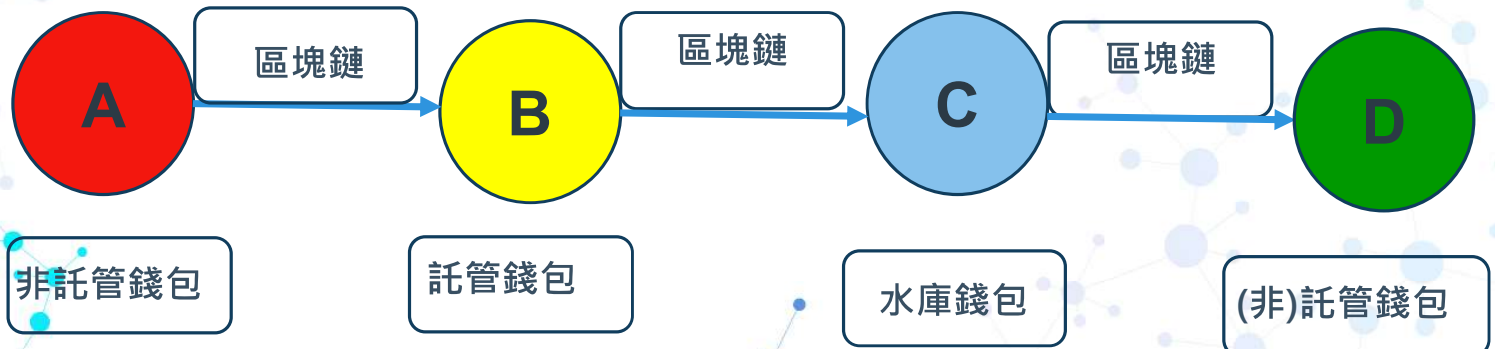
虛擬資產的移轉與區塊鏈紀錄



虛擬資產的移轉與區塊鏈紀錄



虛擬資產的移轉與區塊鏈紀錄 一般中心化交易所出入金紀錄



幣與鏈：平台通路與商品



108 虛擬資產資料判讀 (公開帳本篇)

帳本裡面紀錄了什麼？

護童基金收支明細表

| 日期 | 支出 | 存入 | 餘額 | 說明 |
|----------|--------|---------|---------|----------------|
| | | | 152,610 | 97學年度餘額 |
| 98.10.22 | | 1,000 | 153,610 | 家長捐款 |
| 98.10.23 | | 20,000 | 173,610 | 家長捐款 |
| 98.10.28 | | 5,000 | 178,610 | 家長捐款 |
| 98.10.28 | | 3,000 | 181,610 | 家長捐款 |
| 98.10.28 | | 3,000 | 184,610 | 家長捐款 |
| 98.10.28 | | 3,000 | 187,610 | 家長捐款 |
| 98.10.28 | | 50,000 | 237,610 | 家長捐款 |
| 98.10.30 | | 3,000 | 240,610 | 家長捐款 |
| 98.11.03 | | 235,041 | 475,651 | 家長小額募款 |
| 98.11.13 | | 1,000 | 476,651 | 家長捐款 |
| 98.11.13 | | 5,000 | 481,651 | 家長捐款 |
| 98.11.17 | | 2,000 | 483,651 | 家長捐款 |
| 98.11.18 | 28,000 | | 455,651 | 9.10月廁所清潔費用 |
| 98.11.21 | | 136 | 455,787 | 活息 |
| 99.01.11 | 36,000 | | 419,787 | 11.12.1月廁所清潔費用 |
| 99.01.28 | | 64,000 | 483,787 | 愛苗基金轉入 |
| 99.03.11 | | 9,035 | 492,822 | 家長捐款 |
| 99.03.11 | 13,188 | | 479,636 | 志工保險費 |
| 99.03.12 | | 93 | 479,729 | 利息 |
| 99.05.05 | 64,000 | | 415,729 | 護童基金轉入愛苗基金 |

起訴書犯罪事實欄：
人、事、時、地、物

區塊鏈公開帳本：
時間、內容（敘事）、
Txhash、驗證者

帳本裡面紀錄了什麼？

區塊鏈帳本紀錄著每一筆交易的內容及細節，包含各筆交易的時間（含區塊高度）、發送方、接收方、交易內容、手續費、交易雜湊、以及呼叫智能合約的情形。每筆交易都會花費手續費，以該區塊鏈原生幣種支付。

※在查詢交易紀錄時，Txhash、發送方、接收方及交易數額（幣種）都是識別、確認特定交易的重要條件。在呼叫智能合約的情形時，呼叫類型及智能合約的內容有時也是調查的重點。此種交易的手續費目前仍然是以原生鏈（平台）的幣種來支付。※

常用區塊鏈瀏覽器

- 通用區塊鏈瀏覽器
<https://www.blockchain.com/explorer>
- 以太坊區塊鏈瀏覽器
<https://etherscan.io/>
- 熱門交易所參考
<https://coinmarketcap.com/rankings/exchanges/>
- 通用區塊鏈瀏覽器
<https://blockchair.com/>

常用區塊鏈瀏覽器

- 波場鏈區塊鏈瀏覽器
<https://tronscan.org/#/>
- BSC區塊鏈瀏覽器
<https://bscscan.com/>
- 通用區塊鏈瀏覽器
<https://www.oklink.com/zh-hk>
- 通用區塊鏈瀏覽器
<https://explorer.bitquery.io/zh>

區塊鏈帳本初探(查詢交易基本條件)

區塊鏈帳本紀錄著每一筆交易的內容及細節，包含各筆交易的時間（含區塊高度）、發送方、接收方、交易內容、手續費、交易雜湊、以及呼叫智能合約的情形。每筆交易都會花費手續費，以該區塊鏈原生幣種支付。

| Txn Hash | Method | Block | Date Time (UTC) | From | To | Value | Txn Fee |
|-----------------------|-----------|--|------------------------|---------------------|---------------------|--------|------------|
| 0x0783ec5cda8cdf98... | Transfer | 17568623 | 2023-06-27 5:25:47 | 0x8a5A57...a00e3D58 | 0x26232C...552a6604 | 81 ETH | 0.00029304 |
| Transaction Hash: | 交易雜湊 | 0x0783ec5cda8cdf98b4c4e66d6b565a59b03bf7da710f0d50abb9b5e6355f6f1 | | | | | |
| Status: | | Success | | | | | |
| Block: | 區塊高度 | 17568623 | 17 Block Confirmations | | | | |
| Timestamp: | 交易時間 | 3 mins ago (Jun-27-2023 05:25:47 AM +UTC) Confirmed within 1 sec | | | | | |
| From: | 發送方 | 0x8a5A57bdCB8D926899F6aDb5A8D5f758a00e3D58 | | | | | |
| To: | 接收方 | 0x26232Cd75843D158A1641a8D4E43Aac9552a6604 | | | | | |
| Value: | 交易數額 (幣種) | 81 ETH (\$151,366.32) | | | | | |
| Transaction Fee: | 手續費 | 0.000293047448631 ETH (\$0.55) | | | | | |

在查詢交易紀錄時，Txhash、發送方、接收方及交易數額（幣種）都是識別、確認特定交易的重要條件。

區塊鏈帳本初探(辨識交易中的智能合約)

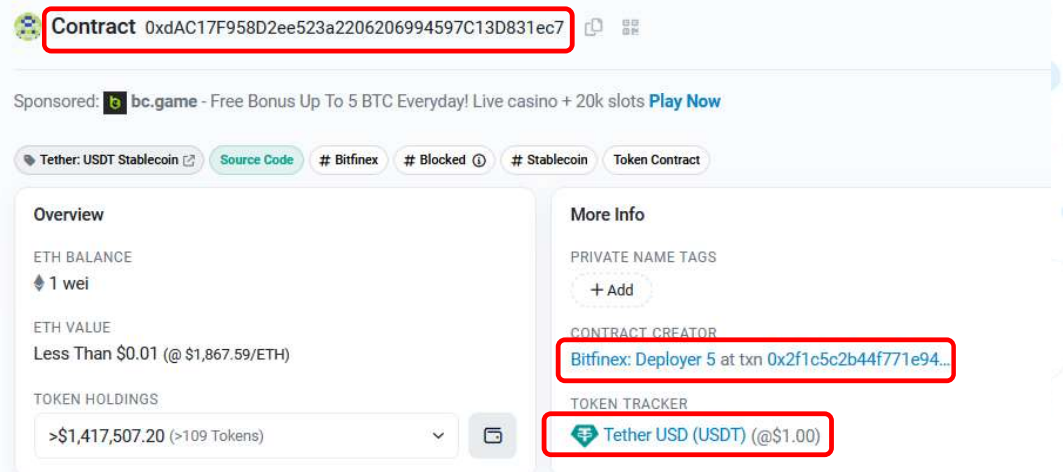
區塊鏈帳本紀錄著每一筆交易的內容及細節，包含各筆交易的時間（含區塊高度）、發送方、接收方、交易內容、手續費、交易雜湊、以及呼叫智能合約的情形。每筆交易都會花費手續費，以該區塊鏈原生幣種支付。

| Txn Hash | Method | Date Time (UTC) | From | To | Value | Token | |
|----------------------------|------------|--|------------------------|-------------------------|---------|-------------------|--|
| 0xaf29df0e2b2b9aca1... | Transfer | 2023-06-27 5:49:23 | 0x7B90eB...0AB16CAD | OUT 0xFbddd4...82ef35D3 | 100,000 | Tether USD (USDT) | |
| Transaction Hash: | | 0xaf29df0e2b2b9aca13746b3fbc4495a8a5f14cd5568f5a08357af717648bc1c5 | | | | | |
| Status: | 交易雜湊 | Success | | | | | |
| Block: | 區塊高度 | 17568741 | 10 Block Confirmations | | | | |
| Timestamp: | 交易時間 | 2 mins ago (Jun-27-2023 05:49:23 AM +UTC) Confirmed within 30 secs | | | | | |
| From: | 發送方 | 0x7B90eBe1A4133A5cD8A98138876Fb6BE0AB16CAD | | | | | |
| Interacted With (To): | 呼叫之智能合約地址 | 0xdAC17F958D2ee523a2206206994597C13D831ec7 (Tether: USDT Stablecoin) | | | | | |
| ERC-20 Tokens Transferred: | 交易去向、數額、幣種 | From 0x7B90eB...0AB16CAD To 0xFbddd4...82ef35D3 For 100,000 (\$100,000.00) Tether USD... (USDT...) | | | | | |
| Value: | | 0 ETH (\$0.00) | | | | | |
| Transaction Fee: | 手續費 | 0.000796672621160654 ETH (\$1.49) | | | | | |

在呼叫智能合約的情形時，呼叫類型及智能合約的內容有時也是調查的重點。此種交易的手續費仍然是以原生鏈（平台）的幣種來支付。

區塊鏈帳本初探(辨識交易中的智能合約)

「合約地址」代表「智能合約」在區塊鏈帳本紀錄裡所在位置，內容包含智能合約的程式碼本身及相關代幣數額，「錢包地址」可以透過與「合約地址」的互動而呼叫、調用及執行智能合約進而發行或移轉代幣。「錢包地址」與「合約地址」互動之內容亦可透過區塊鏈網路瀏覽器加以查詢。



The screenshot displays a blockchain explorer page for a contract. At the top, the contract address `0xdAC17F958D2ee523a2206206994597C13D831ec7` is highlighted with a red box. Below this, there are tabs for 'Tether: USDT Stablecoin', 'Source Code', '# Bitfinex', '# Blocked', '# Stablecoin', and 'Token Contract'. The 'Overview' section shows an 'ETH BALANCE' of `1 wei` and an 'ETH VALUE' of 'Less Than \$0.01 (@ \$1,867.59/ETH)'. The 'TOKEN HOLDINGS' section shows a balance of `>$1,417,507.20 (>109 Tokens)`. The 'More Info' section includes 'PRIVATE NAME TAGS' with an '+ Add' button, 'CONTRACT CREATOR' with the text 'Bitfinex: Deployer 5 at txn 0x2f1c5c2b44f771e94...' (highlighted with a red box), and 'TOKEN TRACKER' with 'Tether USD (USDT) (@\$1.00)' (highlighted with a red box).

區塊鏈帳本初探(查詢交易紀錄步驟)

1. 確認欲調查的紀錄屬於何區塊鏈之紀錄 (BTC、ETH、BSC、SOL...)
2. 選擇該幣種之區塊鏈瀏覽器
3. 以所知的條件進行搜尋 (收發錢包地址、交易時間、交易雜湊、交易數額等)
4. 如有查明相關紀錄的必要，確認目標地址之前後交易紀錄及相關收發錢包地址，釐清彼此關聯性。

視覺化分析工具網站：oklink

<https://www.oklink.com/zh-hk/>




- | | | |
|----------------|--------------------|--------------------|
| Bitcoin > | OKB Chain (Test) > | Tether USD > |
| Ethereum > | OKT Chain > | Solana > |
| Beacon Chain > | OKT Chain (Test) > | Aptos > |
| EthereumPoW > | TRON > | Ethereum Classic > |
| EthereumFair > | Fantom > | Litecoin > |
| BNB Chain > | Arbitrum One > | Bitcoin Cash > |
| Polygon > | Optimism > | DASH > |
| Avalanche-C > | zkSync Era > | |

函詢交易所取得案關資料



如不確定各層錢包地址屬性，可從該錢包地址之餘額、入出金次數及金額判斷是否為交易所之錢包，進而以Txid及錢包地址函詢國內交易所開戶，函調與該交易有關之用戶其餘KYC認證、交易、儲值、法幣出金、登錄IP、登錄設備等資料。



109 虛擬資產案件實務問題研析 (人頭、幣商篇)

告代/辯護人能做的準備



1. 建立相關時序表 (案情時序、實體金流及虛擬資產flow)
2. 請保存及準備正確、清楚、完整的 (受騙) 交易細節相關紀錄等證據資料 (本案、非本案) ，避免闕漏或錯誤，必要時輔以文字說明。
3. 常見Q&A要熟記，避免答非所問
4. 錢包地址、帳戶號碼或網站網址務必正確



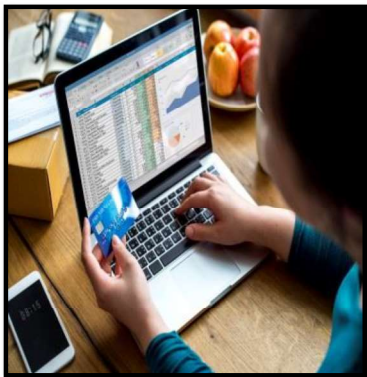
/10 透視虛擬資產案件司法判決

臺灣高雄地方法院

112年度金訴字第377、479號刑事判決

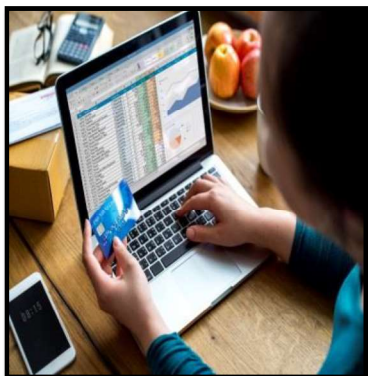


起訴書記載之犯罪事實



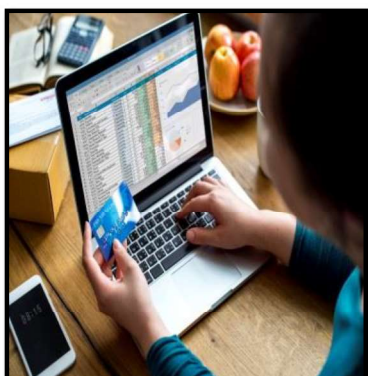
被告王女基於洗錢及詐欺取財之不確定故意，於民國111年3月初某日，將其申設之永豐銀行帳戶作為詐欺集團成員交易虛擬貨幣洗錢使用。其後被害人因遭詐欺而匯款至詐欺集團成員使用之第一層帳戶後，款項復遭轉匯至被告之永豐銀行帳戶內，再由被告以轉匯、提領方式上繳給詐欺集團成員。

判決無罪之理由:被告學經歷等家庭背景



被告王女於案發時年僅23歲，依其智識程度及工作經驗觀之，被告一直以來均是從事餐飲服務業，工作內容單純，並無任何金融相關背景，是否知悉虛擬貨幣特色如何使用加密技術、個人幣商又係如何完成交易，並非無疑；衡以被告收入不豐，尚須扶養2名幼子，亦難認其從事虛擬貨幣兼職工作，有何違反目前社會生活經驗之處。

判決無罪之理由:主要理由



被告王女於111年3月25日起至4月22日止，在買家「酷樂」告知匯入購買USDT款項後，亦有依「酷樂」指定數量向賣家「祥恩」(即「勝中」)購入USDT後，將USDT轉至「酷樂」之虛擬錢包地址，無法排除詐欺集團利用「三角詐欺模式」，輾轉取得詐騙款項。被告非無遭詐欺集團利用，而在不知情之情況下淪為詐欺、洗錢工具之可能。

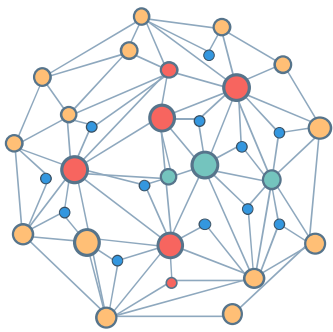
Q:



本案判決所憑事實及理由您怎麼看？



/11 未談到的其他



未談到的其他



- NFT
- ICO
- 銀行法
- Market Maker
- Oracle
- KOL代言
- Inside Trade.....

Thank you
For
Listening

bfp339@gmail.com

