基於公開資料的加密貨幣交易風險識別研究
Research on Risk Identification in Cryptocurrency Transactions Using Public Data

邱黃明蓉
臺北市政府警察局刑事警察大隊科技犯罪偵查隊

董正談
中央警察大學資訊管理學系

*高信雄
中央警察大學資訊管理學系
kao@mail.cpu.edu.tw

摘要

隨著區塊鏈技術蓬勃發展，加密貨幣交易量亦日趨增長。然而，區塊鏈加密及匿名的特性，促使加密貨幣成為不法份子，進行非法交易及洗錢的最佳工具。因此，維護交易的安全及合法性，有效識別加密貨幣交易風險，已成為一大重要課題。本研究嘗試利用區塊鏈交易公開透明的特性，建立深度學習模型，用以識別不同交易型態，藉此預判交易風險，有效解決加密貨幣交易安全性的問題。

本研究為貼近實務上執法人員可取得的資料型態，故從Etherscan平台擷取「高風險」、「混幣器」和「合法」智慧合約的交易資料，總計26,560筆。採用一維卷積神經網路（1D-CNN）、時序卷積網路（TCN）、長短期記憶網路（LSTM）及門控遞迴單元網路（GRU）等4種深度學習模型，並選取交易時間差、油費（Gas fee）及交易次數做為特徵，來進行模型識別工作。實驗結果發現，TCN在準確度(Accuracy)、精確度 (Precision)、召回率(Recall)及F1分數(F1 Score)等4項模型評估指標中，表現最佳，均可達83%以上。鑒於召回率（Recall）著重於所有實際陽性樣本被正確識別的比例，在本研究中，我們致力於提升召回率，以確保高風險交易得到充分識別。透過混淆矩陣分析，發現TCN的召回率達到了87.03%，LSTM則達到了94.34%。結果顯示，這些深度學習模型在捕捉非法金流上，具有良好的效能。最後，本研究提出基於規則的整合模型架構。基於模型在不同類別下的表現能力，結合LSTM及TCN模型來作出最佳的決策結果。此種整合模型架構，能確保模型的穩定性，更能強化識別高風險交易的能力，為加密貨幣的風險監管提供創新視角，顯著提升風險識別成效。

關鍵詞: 加密貨幣、混幣器、深度學習、風險識別

Abstract

With the rapid development of blockchain technology, the transaction of cryptocurrencies is also increasing However, the encryption and anonymity of blockchain technology have made cryptocurrencies a preferred tool for criminals to engage in illegal transactions and money laundering. Therefore, ensuring the security and legality of transactions and effectively identifying risks in cryptocurrency trading have become critical challenges. This study uses blockchain transaction transparency to develop deep learning models that identify transaction types, predicts risks, and address cryptocurrency trading security issues.

This study extracted 26,560 transaction records of "high-risk," "mixer," and "legal" smart contracts from the Etherscan, aligning with the data accessible to law enforcement. This study employs four deep learning models: 1D Convolutional Neural Network (1D-CNN), Temporal Convolutional Network (TCN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU). The features for model identification are transaction time difference, gas fee, and transaction count. Experimental results show that the TCN model excels in accuracy, precision, recall, and F1 score, each over 83%. Since recall measures the proportion of correctly identified positive samples, this study aims to improve it for thorough detection of high-risk transactions. Confusion matrix analysis showed that the TCN model achieved 87.03% recall, while the LSTM model reached 94.34%. The results indicate that these deep learning models perform well in detecting illicit financial flows. Finally, this study proposes a rule-based integration model that selectively uses the LSTM or TCN model based on category performance to achieve optimal results. This model ensures stability, improves high-risk transaction identification, and offers a new perspective for cryptocurrency risk management, significantly enhancing risk detection.

Keywords: Cryptocurrency, Mixer, Deep Learning, Risk Identification

一、緒論

區塊鏈技術緣起 2008 年，由中本聰(Satoshi Nakamoto)於《比特幣白皮書》中提出區塊鏈概念[1]，並於 2009 年創立了比特幣網路，開發出第一個「創世區塊」。區塊鏈係採分散式帳本技術(Distributed Ledger Technology, DLT)，具有去中心性(Decentralization)、不可竄改性(Immutability)、可追溯性(Traceability)、透明性(Transparency)、匿名隱私(Privacy)性及加密性(Encryption)等特性。這些特性使得使用者在缺乏中央監管機構的情況下，能夠確保資料的一致性、透明性及安全性。隨著區塊鏈技術的日益成熟，其在金融、醫療、司法等領域的應用也日益廣泛。

然而，區塊鏈的可追蹤性及透明性，讓每筆交易均被清楚記錄在公開帳本中，也無形暴露了使用者的交易細節。因此，為了強化使用者的交易隱私，混幣器服務如 Tornado.cash 應運而生。這種混幣服務成為加密貨幣在交易隱私加強層面的專用工具，透過混幣器可以將來自多個用戶的資產進行混合，從而模糊資金的原始來源和最終目的，為使用者提供多一層的隱私安全保護。本研究選用在乙太坊中最受歡迎的混幣工具 Tornado.cash，其智能合約已超過 37 億元的乙太幣存入[2]，可見在加密貨幣市場中的重要性。Tornado.cash 即是一種基於乙太坊平台的混幣器[3]，當用戶將乙太幣存入 Tornado.cash 後，其會利用零知識證明（zk-SNARKs）[4]來運行混幣機制，使用戶無法得知實際出幣者身分，達成用戶之間的交易隱私保護。

儘管混幣器的出現大大提升了用戶的匿名性，有效保障合法用戶間的交易隱私，但也成為不法分子作為詐騙、洗錢等犯罪行為的庇護所，藉由贓款轉換為加密貨幣型態，再透過混幣器的混幣機制，來製作犯罪斷點，大幅增加警方偵查上的困難[5]。

本研究利用區塊鏈交易透明的特性，嘗試針對高風險、混幣器和合法智慧合約的入金錢包，進行金流分析識別。透過深度學習模型（如:1D-CNN、TCN、LSTM 及 GRU）來識別不同的交易類型。為更接近實際執法需求，從 Etherscan 平台擷取了 26,560 筆交易資料，並以交易時間差、油費（Gas Price）和交易次數為特徵，來進行模型訓練及分析。在經過模型的綜合評估後，發現 TCN 模型在準確度、精確度、召回率及 F1 分數等性能指標中表現最佳，均超過了 83%，顯示其在辨別不同風險類型的交易上具有顯著優勢。

鑒於本研究目的在於，有效識別高風險交易、混幣器活動及合法交易模式，減少對於實際高風險交易的誤判，因此召回率成為一項關鍵指標。召回率是用來衡量模型識別實際陽性樣本的能力，意即模型的召回率越高，其誤判實際陽性樣本的機率越低。在本研究中，各模型在識別高風險金流方面均表現出較高的召回率，其中 LSTM 達 94.34%，TCN 亦達 87.03%。最後，本研究提出了基於規則的整合模型架構，基於不同模型，在不同類別下的表現情形，選擇性採用 LSTM 或 TCN 模型，作出最終決策結果。透過模型的指標分析及整合化架構運用，來強化模型的泛化能力，有助於警方達到精準打擊的效果。

二、背景知識

在本章節中，我們將重點介紹本研究採用的混幣器 Tornado.cash，以及所使用的各種深度學習方法，包含 1D-CNN、TCN、LSTM 及 GRU。此外，更深入說明各項模型的運

作過程及適用場景。最後介紹如何透過 Softmax 函數將各類別的輸出轉換為機率，作為模型進行最終判斷的依據。

1. 混幣器(Mixer)

本研究係以混幣器Tornado.cash作為實驗標的之一，Tornado.cash於2019年發起其第一版本，並於2021年底啟動beta更新版，其係利用零知識簡潔互動性知識驗證機制（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, 簡稱zk-SNARKs），來達成交易隱私保護，意即在不洩漏任何秘密訊息的情況下，來驗證資料的真實性[6]。

zk-SNARKs是一種加密機制，主要用以增強用戶的隱私保護，該機制在初始化階段，會產生一組公（私）有參數，作為驗證過程的基礎，後續藉由參數與用戶的資料或交易進行運作，並產生一個簡短的加密證明，透過這個加密證明，使第三方可以快速地進行驗證，讓用戶可以在不透漏身分的情形下，確保該資料或交易的真實性，有效保障區塊鏈和加密貨幣交易的隱私安全[7]。

Tornado.cash是個完全去中心化的非託管協議，使用戶得以在鏈上交易的情形下，打破來源地址和目標地址之間的鏈上關聯性，Tornado.cash利用智慧合約接受用戶的加密貨幣存款，並允許用戶從不同的錢包位址提款，Tornado.cash主要提供4種不同的資產池，區分為1ETH、0.1 ETH、10ETH、100ETH，分別對應4個不同智慧合約，提供用戶得以以 1ETH、0.1 ETH、10ETH、100ETH 為提款單位來提取款項，而0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf則為Tornado.cash創始之初的預設智能錢包，相關對應如表1。

表 1:Tornado.cash 智能合約對照表

Tornado.cash	智能合約地址	創立時間
預設EVM版本	0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf	2019-08-04
1ETH	0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936	2019-12-16
0.1 ETH	0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc	2019-12-16
10ETH	0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF	2019-12-16
100ETH	0xA160cdAB225685dA1d56aa342Ad8841c3b53f291	2019-12-16

2. 深度學習方法

深度學習是機器學習領域的一部分，主要透過多層神經網路模仿人類大腦處理訊息的方式。這種技術使模型能夠從資料中自動提取出複雜特徵，進行學習並做出預測。深度學習的關鍵在於其多層結構，能夠進行深入的模型識別，廣泛應用於圖像鑑別、語音識別、自然語言處理等多項領域，更是推動人工智慧發展的重要推手。針對本文所採用的 4 種深度學習模型 1D-CNN、LSTM、GRU 及 TCN 加以說明。

(1) 一維卷積神經網路（1D convolutional neural networks, 1D-CNN）

一維卷積神經網路（1D-CNN）是專門處理序列資料的深度學習模型，適用於時間序列分析、語音識別或自然語言處理等領域。相對於傳統全連接神經網路，1D-CNN 能夠透過卷積層捕捉資料中的時間依賴性，使其分析具有時間延展性的資料集更具效益。

在 1D-CNN 的模型中，會先將分析資料規格化成 $n \times d$ 矩陣，其中n是序列長度，d是特徵維度，並使用核心的卷積層，利用多次學習所得的過濾器（又稱 filter）在整個序列

上滑動，來進而取得一系列的特徵圖。在整個過程中，允許模型自動學習資料集的局部特徵，藉由多層卷積推疊來取得更抽象化的特徵[8]。

1D-CNN 主要包含卷積層（Convolutional Layer）、啟動層（Activation Layer）和池化層（Pooling Layer），各別負責不同的工作，來使模型能捕捉局部特徵及瞭解時間依賴情形，有效處理長時間和高維度的序列資料，其相關運作程式及公式如下[9]。

(一)卷積層（Convolutional Layer）: 一維卷積核沿著輸入序列進行滑動，計算核與輸入序列資料間的點積，生成一系列的卷積特徵。

$$c(t) = \sum_{s=0}^{k-1} w(s) \cdot x(t+s) \tag{1}$$

其中$c(t)$是在時刻t的卷積輸出，k是卷積核的大小，s代表不同的時間偏移量，$w(s)$是卷積核的權重，$x(t+s)$則是輸入的序列資料。

(二)啟動層（Activation Layer）: 通常位於卷積層之後，導入非線性函數，來提升模型的非線性關係。本文係採用常見的 ReLU 啟動函數。

(三)池化層（Pooling Layer）:利用池化層來降低特徵維度，避免模型發生過擬合的問題。此外，更能捕捉出對模型決策的關鍵特徵，來增強模型的泛化能力。

(2) 時序卷積網路（Temporal Convolutional Network, TCN）

時間卷積網路（Temporal Convolutional Network, TCN）是一種專門處理序列資料集的神經網路。TCN 採用卷積處理序列資料，來避免遞迴結構(RNN)帶來的梯度消失和梯度爆炸問題，有效捕捉時間序列中的局部狀況。TCN 使用因果卷積(Causal Convolution)和擴張卷積(Dilated Convolution)，提升處理複雜時間序列上的效能[10]。

因果卷積可以確保 TCN 在進行資料處理時，僅依賴先前的資料來做出判斷，而不會使用到未來的資料，來模擬實際處理序列資料的方式。擴張卷積則是導入擴張率的概念，使模型可以在不變更卷積核大小情形下，利用擴張因子，來提升可以捕捉到的資料特徵範圍，提高處理時間序列或音頻訊號資料集的效率。

TCN 的卷積層結構描述如下[11]。

(一)因果卷積: 用以確保模型在進行預測時，只使用當前及之前的時間資料，而不會使用未來的時間資料。這是為了維持時間序列的因果性，即當前的輸出，只仰賴於過去和當前的輸入，符合時間序列的自然邏輯順序。

(二)擴張卷積: 擴張卷積核涵蓋的時間範圍，並導入擴張因子的概念。擴張因子決定卷積核覆蓋的時間範圍。當擴張因子為 1 時，則擴張卷積等同於標準卷積，意即無擴張。隨著擴張因子的增加，可以使模型在不增加卷積核大小的情形下，覆蓋到更大的輸入範圍。因此，擴張卷積使 TCN 能更有效地處理長時間序列的資料。

假設 TCN 總共有L層卷積，並導入非線性函數*Activation* (如: ReLU 啟動函數)，則每層l在時間t的輸出可表示為$y_t^{(l)}$，當l=L即為最終輸出結果：

$$y_t^{(l)} = Activation\left(\sum_{i=0}^{k-1} w_i^{(l)} \cdot y_{t-d^{(l)}\times i}^{(l-1)} + b^{(l)}\right) \tag{2}$$

k是卷積核的大小，$w_i^{(l)}$是第l層的卷積核中第i個權重、$b^{(l)}$為第l層偏移項，

$y_{t-d^{(l)}\times i}^{(l-1)}$表示為第$l-1$層在時間點$\mathrm{t}-\mathrm{d}^{(\mathrm{l})}\times\mathrm{i}$的輸出，其中$d^{(l)}$為第$l$層的擴張因子。

(3) 長短期記憶網路（Long Short-Term Memory networks, LSTM）

長短期記憶網路（Long Short-Term Memory, LSTM）是一種遞迴神經網路(RNN)架構，於 1997 年由 Hochreiter 和 Schmidhuber 提出[12]，解決 RNN 在處理長序列資料時容易出現的梯度消失問題。LSTM 導入輸入門（Input gate）、遺忘門（Forget gate）和輸出門（Output gate），來靈活控制資料在時間序列的流動，使模型在必要時取捨資料，來達到學習上的穩定及準確性。

在 LSTM 的運作過程中，Sigmoid 函數和 Tanh 函數都扮演著關鍵的角色。Sigmoid 函數是一種常見的啟動函數，特別適用於二元分類問題。其輸出範圍介於 0 到 1 之間，可用以解釋事件發生的機率。Tanh 函數亦是啟動函數的一種，其輸出範圍介於-1 到 1，適用於資料正規化。在兩函數的作用之下，使模型可以處理並記憶長時間序列的資料。其運作方式可描述如下[13]。

(一)輸入門（Input Gate）: 主要控制記憶單元對新訊息的接收程度。首先，透過 Sigmoid 函數評估訊息的重要性，接著使用 Tanh 函數將輸入訊息轉換成適合儲存的格式。藉由兩函數的結合作用，來確定將哪些訊息更新至記憶單元，讓模型能夠有效學習。

(二)遺忘門（Forget Gate）: 控制記憶單元遺忘不重要訊息的能力。透過 Sigmoid 函數產生的值，來決定保留舊記憶的比例，有助於模型處理長期性的訊息

(三)更新記憶單元: 透過遺忘門和輸入門的輸出，產生新的記憶單元。

(四)輸出門（Output Gate）: 控制當前記憶單元決定輸出哪些訊息到下一個隱藏狀態的機制。透過 Sigmoid 函數評估每個記憶單元中訊息被輸出的程度，並利用 Tanh 函數將欲輸出訊息正規化。這種方式確保只有重要且經處理的訊息被傳遞，有效控制訊息的流動，提高模型處理序列資料的能力。

LSTM 藉由導入門匣控制訊息流方式，有效解決傳統 RNN，在遇到長序列資料處理上的梯度問題。

(4) 門控遞迴單元網路（Gated Recurrent Units networks, GRU）

門控遞迴單元（Gated Recurrent Unit, GRU）網路亦是 RNN 的一種。與 LSTM 相同，都是為瞭解決傳統 RNN 的梯度消失問題，然而，在架構上兩者卻有明顯不同。GRU 僅仰賴 2 個門的控制，簡化了 LSTM 的架構，在特定的應用需求下，可以利用較少的參數，達到與 LSTM 類似的成效，提升模型學習的效率。GRU 採用更新門（Update gate）和重置門（Reset gate）的概念，來控制每一次訓練資料的取捨，捕捉序列中的長（短）期依賴關係[14]。

GRU 的運作方式，可描述如下[15]。

(一)更新門（Update Gate）:類似 LSTM 中的輸入門及遺忘門的組合。更新門決定模型之前學習記憶及新輸入資料的保留程度。

(二)重置門（Reset Gate）:用於決定模型更新當前輸入資料隱藏的程度，其取決於過去資料隱藏的狀態。透過重置門適當調節過去狀態對於模型的影響，允許 GRU 在必要時，隱藏不再相關的資料，有助於模型對於新狀態出現的適應。

GRU 藉由較少的門匣控制機制，在特定的情況下，能夠以較高效率進行分類識別的工作。

此外，本文係針對高風險、混幣器和合法金流進行分類問題，故在模型最後加入「全連接層(Fully Connected Layer)」，整合卷積層和池化層處理後的局部抽象特徵，讓模型透過整體的特徵映射，產出各類別的機率分佈，進而做出最終決策結果。藉由全連接層的加入，可以增強模型的學習能力，也是作為特徵學習到結果產出的重要橋梁。本文是採用適用於多項分類工作的 Softmax 啟動函數，作為全連接層。假設模型輸出層有K個神經元，對應於K個類別，Softmax 將這些類別輸出轉換為機率p_i，計算公式如下[16]。

$$p_i = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \tag{3}$$

其中，e是自然指數（約等於 2.71828），z_i是第i個輸出神經元的輸出值，分母是所有輸出值的指數和，以確保p_i範圍在 0 到 1 之間，來判定最終分類。

三、研究方法

本研究首先利用 Etherscan[17]中 Labal Word Cloud 所標記高風險、混幣器及合法的智慧合約，針對入金智慧合約的第一層錢包交易時間差、油費及交易次數，以不同深度學習模型(1D-CNN、TCN 、LSTM 及 GRU)，研究其針對各類別金流的辨識準確度，找出最適合模型。最後，提出基於規則的整合模型架構，利用 LSTM 及 TCN 的模型整合，來應對多樣的金流型態。

本實驗採用 Python 3.11.3 及 Keras 2.15，配置 Intel Core i5-1240P, 1.70 GHz。針對入金高風險、混幣器及合法智慧合約的第一層錢包，先進行資料清洗及預處理，使之生成適用於模型的資料集。接著再將資料集隨機依 8:2 的比例，分為訓練集及驗證集，來提供模型使用。最後再針對實驗結果進行評估及特徵貢獻度分析，實驗架構圖如下圖 1。

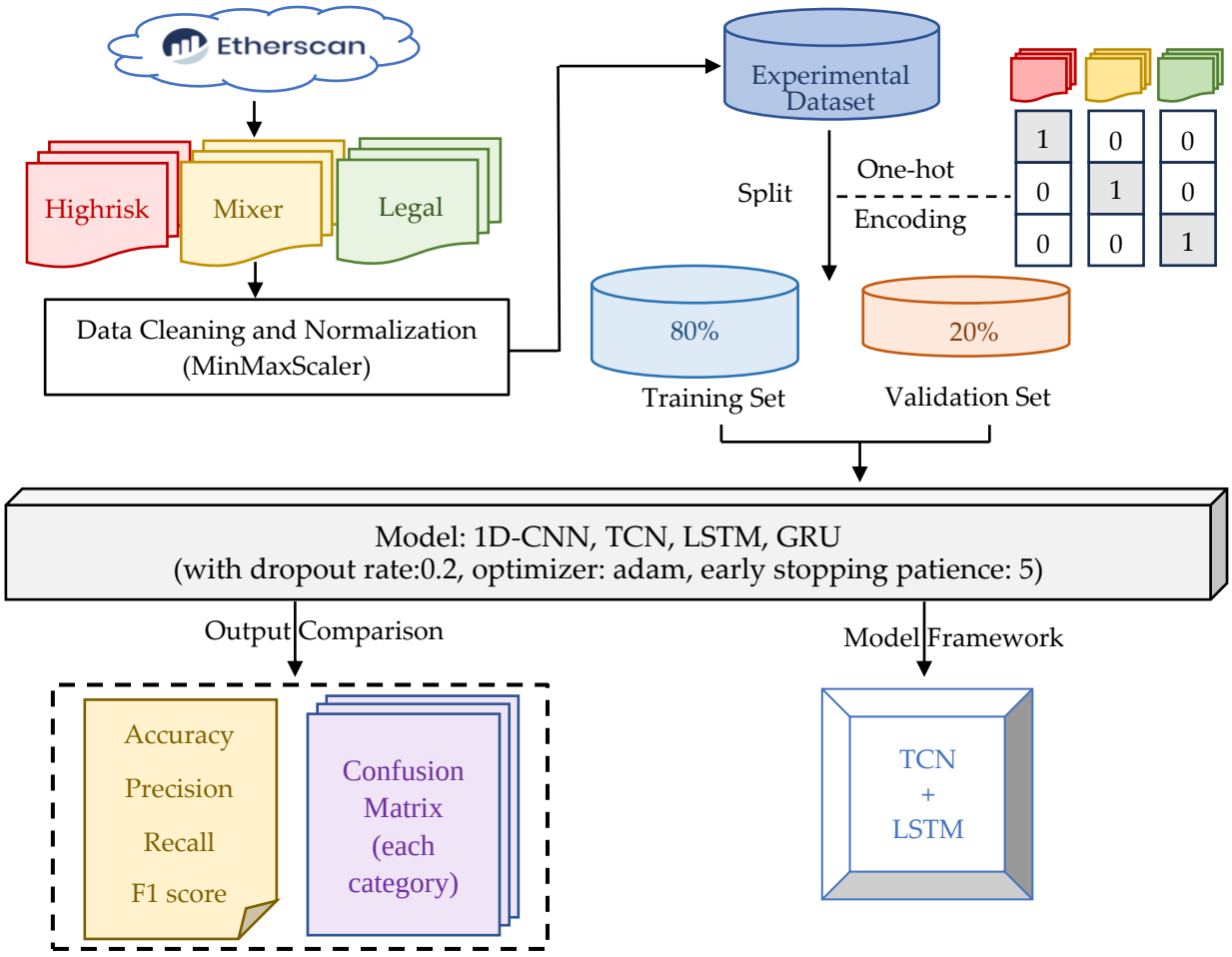


圖 1、實驗架構圖

1. 資料蒐集及處理

本次資料蒐集係利用 Python 程式，並向 Etherscan 申請取得 API Key。針對 Etherscan 中標記高風險、混幣器 Tornado.cash 及合法的智慧合約，分別爬取最近 10,000 筆入金交易，針對擷取出的資料集，進行資料預處理步驟:

(1) 資料清洗:受限於「交易時間差」特徵需有 2 次交易以上，故去除僅 1 次交易的入金錢包作為本次實驗資料集。另外針對首次交易行為，列入「交易次數」計算，但不列入交易時間差計算，以避免空值(N/A)出現。

(2) 資料正規化:

(一) 計算資料集內各個交易時間差(以「分」為單位元元)，交易油費(以「Gwei」為單位)，Gwei 為「Giga-wei」的縮寫，其中「wei」是乙太坊中最小的貨幣單位。1 ether(乙太幣)為 10^{18} wei，1Gwei 為 10^{9} wei，交易油費常見以 Gwei 表示最為適合。

(二) 採用「MinMaxScaler」進行特徵標準化，因考量採用的特徵性質明顯不同，且為保持原始資料分佈型態，故使用 MinMaxScaler 進行特徵縮放，使之限縮在 0 到 1 之範圍內。其標準化計算方式如下，其中X是原始值、$X_{\min}$該特徵最小值、$X_{\max}$是該特徵最大值，及X_{scaled}則是縮放後的值[18]。

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (4)$$

表 1、資料集中交易金流數據範例

From	Gas Price (Gwei)	Time Difference (Min)	Tag
0x00000000000124d994209fbb955e0217b5c2eca1	21.29030388	365472	Legal
0x00000000000124d994209fbb955e0217b5c2eca1	24.98605824	1329960	Legal
0x0000098a312e1244f313f83cac319603a97f4582	15.45545851	131940	Legal
0x0008864763accf8c9a82bafe0c7ffee9e452ce81	35	151435	High-risk
0x0008864763accf8c9a82bafe0c7ffee9e452ce81	64	25453	High-risk
0x0008864763accf8c9a82bafe0c7ffee9e452ce81	64	186	High-risk
0x0008864763accf8c9a82bafe0c7ffee9e452ce81	71.09588991	83905	High-risk
0x0014971dba5b1481296e6abdd7234b0d8474bb8c	22.5	15128490	Mixer

經蒐集篩選後的資料集數量如下表 2。

表 2、初步資料集數據表

Etherscan 標籤	智能合約地址	入金錢包個數	交易次數
高風險 High-risk	0x0ffEf1bF3a19DD96310194E73B38c069d1D1c31F	1,645	6,681
混幣器Mixer (Tornado.cash)	0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936 (1ETH) 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF (10 ETH)	1,303	9,221
合法 Legal	0xD13cfD3133239a3c73a9E535A5c4DadEE36b395c 0xdfdDF7a69716124Bc346bA556d4b9f9E74C4A8Bc 0xA2085073878152aC3090eA13D1e41bD69e60Dc99 0x85Ffb35957203dfD12061eAeCD708dB623Bd567C	1,517	10,658

最後，採用最常見的資料集劃分方式，將整個資料集依 8:2 的比例，分為訓練集(80%)及驗證集(20%)。訓練集用於模型的學習訓練及調整權重，驗證集則是用於評估模型性能，調整超參數(如學習率、層數等)，以防止過擬合(Overfitting)情形發生。

2. 模型建置(Model Construction)

在本次研究中，選擇使用 1D-CNN、LSTM、GRU、TCN 共 4 種常見的深度學習模型，來識別高風險、混幣器及合法 3 種不同智慧合約類別的金流特性，而非使用更複雜的 Transformer 模型(如 BERT、GPT 等)[19]，是因為儘管 Transformer 模型的複雜結構，可使識別金流上有顯著的效能，但其所需耗費參數量大、訓練及運算成本均高，不利於執法人員作立即性判斷，更不符現行執法部門所擁有的資源配置情形。故採用較為簡單、訓練及運算成本相對較低的模型，作為本次研究探討之對象。

在「模型建置」階段，採用 8:2 的比例，將資料集劃分為訓練集及驗證集。因本次研究是要進行高風險、混幣器及合法的三分類工作，故導入 One-Hot Encoding 熱鍵編碼[20]，來進行變量型態的轉換。One-Hot Encoding 是一種處理類別變量的編碼方法，可以將類別型變量轉換成模型可辨識的數值型變量。每個類別在熱鍵中，都會被轉換成二進制的向量，來表示不同類別。在本文中資料集中(參考表 2)，經熱鍵編碼轉換成模型可辨的表 3。

表 3、One-Hot Encoding 轉換

高風險 (High-risk)	混幣器 (Mixer)	合法 (Legal)	入金錢包個數	交易次數
1	0	0	1,645	6,681
0	1	0	1,303	9,221
0	0	1	1,517	10,658

本研究加入 Early Stopping[21]及 Dropout[22]機制，來防止模型過度擬合，提升模型泛化能力。在早停機制下，將耐心值(Patience)設定為 5，意即當模型在訓練過程中，經過 3 個訓練週期結束後，發現驗證集上的損失值(Loss)不再明顯減少，表示不再有顯著改善，隨即停止訓練。另外在丟棄機制下，將 Dropout 設為 0.2，意即在訓練過程中，模型會隨機讓 20%的神經元暫時不參與權重的更新和計算。

針對本研究模型的超參數設定，如表 4。

表 4、深度學習模型參數設定

參數	1D-CNN	TCN	LSTM	GRU
Units(LSTM、GRU)	N/A		64	
Filters(1D-CNN、TCN)	64		N/A	
Kernel Size(1D-CNN、TCN)	2		N/A	
Convolutional Dense Units(Activation Function)	128(Relu)		N/A (Relu)	
Fully Connected Layer Dense Units(Activation Function)	3(Softmax)			
Dropout Rate	0.2			
Batch Size	32			
Optimizer	Adam (with Learning Rate 0.001)			
Loss Function	Categorical_Crossentropy(with onehot encoding)			
Epochs	200(with early stopping patience: 5)			

本研究將這 4 個深度學習模型應用於高風險、混幣器和合法金流辨識工作，來找出最適合用於辨識金流工作的模型，以提供實務上辨識加密貨幣金流的理論基礎及參考指標。

3. 模型訓練(Model Training)

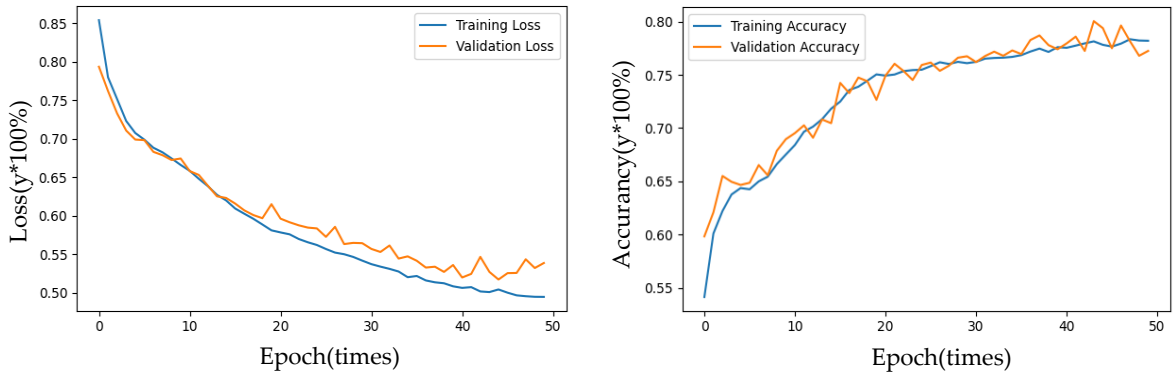
針對建置完的 4 個模型，就其訓練過程分別繪製損失學習曲線(Loss Learning Curve)及準確度學習曲線(Accuracy Learning Curve)。藉由圖形化觀察曲線的變化，來評估模型的學習及泛化能力，避免模型過擬合，並調整優化模型架構[23]。

損失學習曲線(Loss Learning Curve)，透過記錄模型在訓練過程中的訓練損失（Training Loss）及驗證損失（Validation Loss）變化，觀察模型學習狀況。「訓練損失」意即模型

在每個訓練週期(Epoch)結束後，訓練資料的損失程度；「驗證損失」意即模型在每個訓練週期(Epoch)結束後，未參與訓練的驗證資料損失程度。當訓練損失持續下降，但驗證損失開始上升時，表示模型發生過擬合的情形，模型泛化能力下降。然而，當訓練損失及訓練損失持續維持高損失或未有下降趨勢，表示模型沒有充分學習訓練，發生欠擬合的情形。

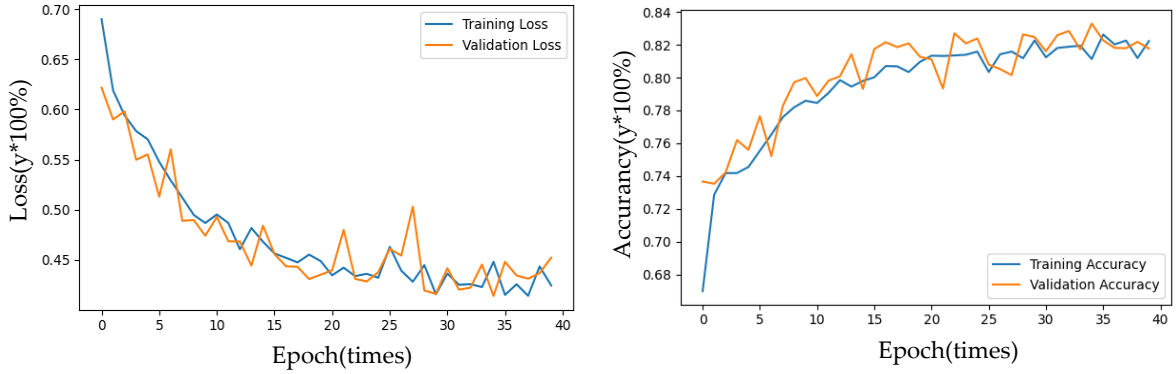
準確度學習曲線(Accuracy Learning Curve)則是直接針對模型的訓練準確度（Training Accuracy）及驗證準確度（Validation Accuracy）繪製曲線。當訓練準確度持續上升到某個程度，驗證準確度卻開始下降時，表示模型發生過擬合情形；而當訓練及驗證準確度持續維持低準確度或未有改善，表示模型發生欠擬合情形。

本研究就 4 個模型繪製學習曲線如圖 2-5



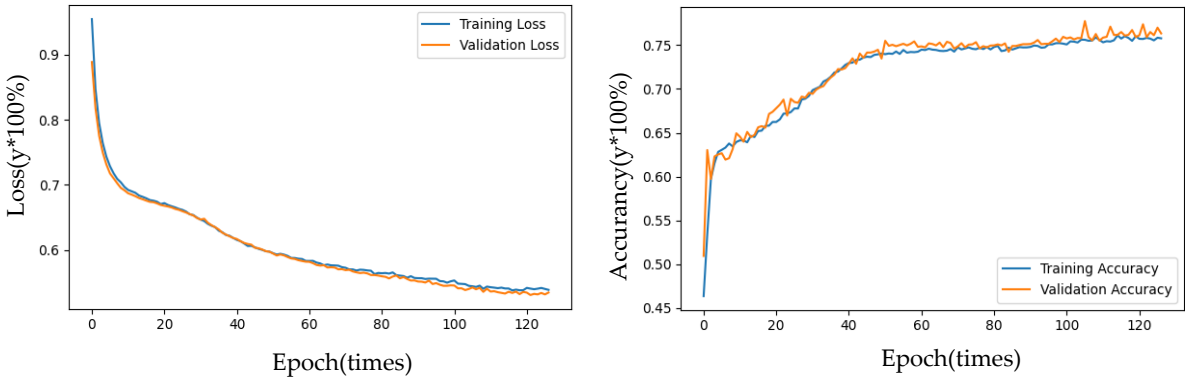
(a) Loss Learning Curve　　(b) Accuracy Learning Curve

圖 2、1D-CNN 模型學習曲線(epoch 50/200 達 early stopping)



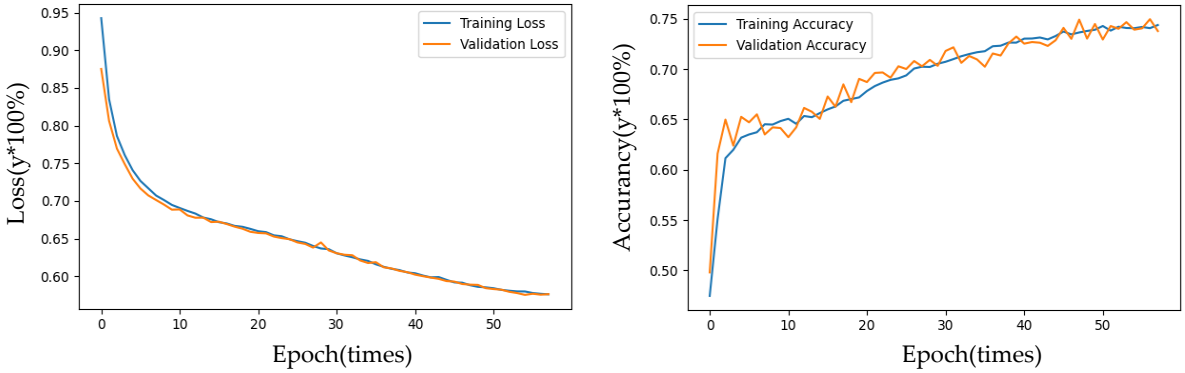
(a) Loss Learning Curve　　(b) Accuracy Learning Curve

圖 3、TCN 模型學習曲線(epoch 40/200 達 early stopping)



(a) Loss Learning Curve　　(b) Accuracy Learning Curve

圖 4、LSTM 模型學習曲線(epoch 127/200 達 early stopping)



(a) Loss Learning Curve　　(b) Accuracy Learning Curve

圖 5、GRU 模型學習曲線(epoch 58/200 達 early stopping)

由上圖 2-5 可知，1D-CNN 及 TCN 模型的學習曲線，較 LSTM 及 GRU 模型學習曲線來的波動性較高，其中 TCN 的波動又較 1D-CNN 高。然而，針對損失學習曲線部分，雖有部分模型波動性較高，但 4 個模型整體而言均是呈現下降趨勢。再者，針對準確度學習曲線部分，4 個模型的訓練及驗證準確度均呈現上升趨勢，且趨於平緩，並無顯著差異。由此可知，4 個模型並無發生明顯的過擬合之情形。

LSTM 及 GRU 是 RNN 的延伸模型，擅長處理時間序列資料。它們能穩定學習資料集中的時間依賴性，從而減少學習曲線的波動。相較之下，TCN 是擴展的 CNN 架構，透過導入擴張因子增加捕捉特徵的範圍，來提升學習效率。因此，TCN 僅在 40 個訓練週期內即達到早停。然而，卻也使 TCN 在初期訓練階段，隨著卷積層數和擴張因子的增加，模型對資料變動的敏感性可能提高，導致學習曲線出現明顯波動，但仍屬可接受的範圍。

四、實驗結果與分析

本章節針對研究實驗結果加以分析，並提出基於規則的整合模型架構，來提升模型的穩定性及泛化能力。本研究採用準確率 (Accuracy)、精確度 (Precision)、召回率(Recall)及 F1 分數(F1 Score)等 4 大性能指標，來評估 4 種不同深度學習模型(1D-CNN、TCN、

LSTM 及 GRU)，在識別高風險、混幣器及合法智慧合約的交易金流表現。再提出基於規則的整合模型架構，來改善單一模型存在的缺陷，進而探討其在實務應用的潛力。

1. 模型識別結果:

將模型結果計算出 4 大性能指標，來評估模型的性能。其中 TP 是真陽性的數量，TN 是真陰性的數量，FP 是偽陽性的數量，FN 是偽陰性的數量，計算公式如下[24]。

(1) 準確度(Accuracy):即正確預測的樣本數(真陽性和真陰性)與總樣本數的比例。

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

(2) 精確度(Precision):即所有被預測為陽性的樣本中，實際上為陽性的比例。

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

(3) 召回率(Recall):即所有實際為陽性的樣本中，被正確預測為陽性的比例。在本研究中，特別重視召回率指標。因高召回率能確保最大限度地識別出，所有潛在的風險交易。故可作為執法人員進行必要介入及阻止不法行為的參考依據

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

(4) F1 分數(F1 Score):即精確度和召回率的調和平均數，為綜合考量精確度和召回率的指標。

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{8}$$

模型結果計算出 4 大性能指標，如表 5。

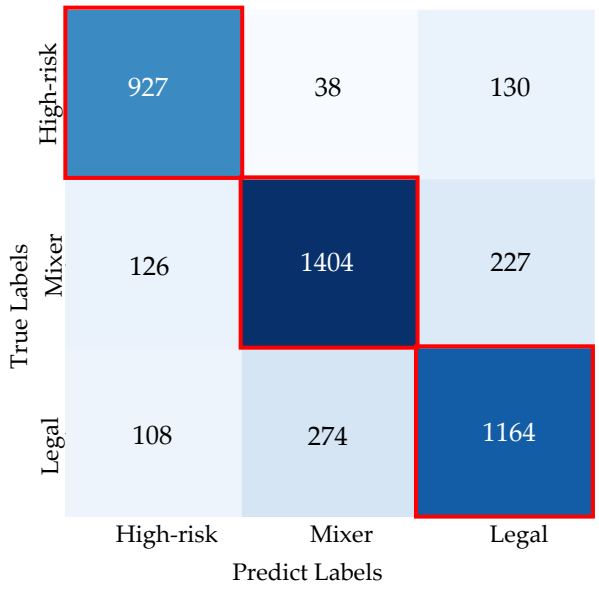
表 5、模型整體評估指標

模型	Accuracy	Precision	Recall	F1 Score
1D-CNN	79.47%	79.40%	79.95%	79.65%
TCN	**83.29%**	**83.07%**	**83.76%**	**83.28%**
LSTM	76.33%	76.44%	78.21%	76.28%
GRU	73.78%	73.57%	75.10%	73.64%

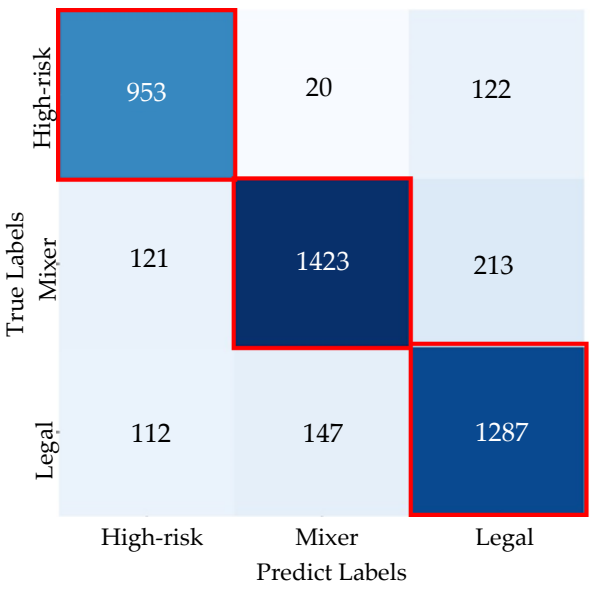
由結果可知，TCN 在 4 種模型中表現最佳，各項評估指標均可達 83%以上，召回率更可達 83.76%，可見其在正確識別實際陽性樣本的能力較其它模型高，誤判率相對較低。在表 5 中呈現模型的整體表現評估。對於各類別的細部表現，將於下一小節進行詳細介紹。

2. 分類識別結果

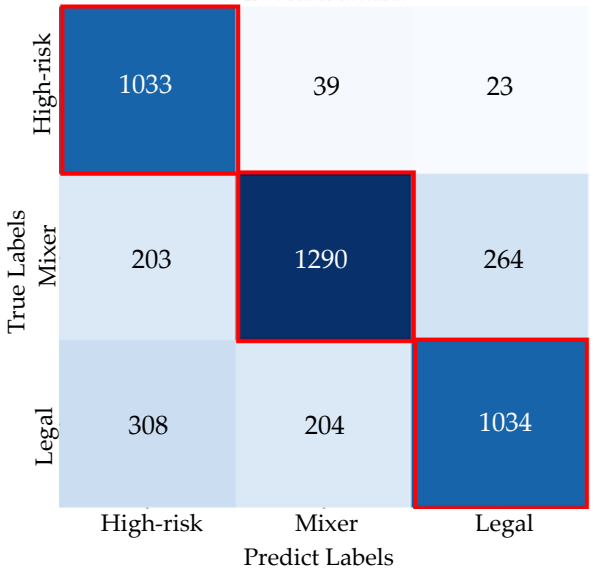
為深入瞭解模型對於各項類別的識別準確度，利用混淆矩陣(Confusion Matrix)[25]，來探討各項類別的識別情形。混淆矩陣是一種常用於評估深度學習分類模型性能的工具，藉由混淆矩陣的呈現，可以理解模型在每個類別的預測表現，有助於優化模型，改善對特定類別的識別能力。針對各項模型繪製混淆矩陣如圖 6。



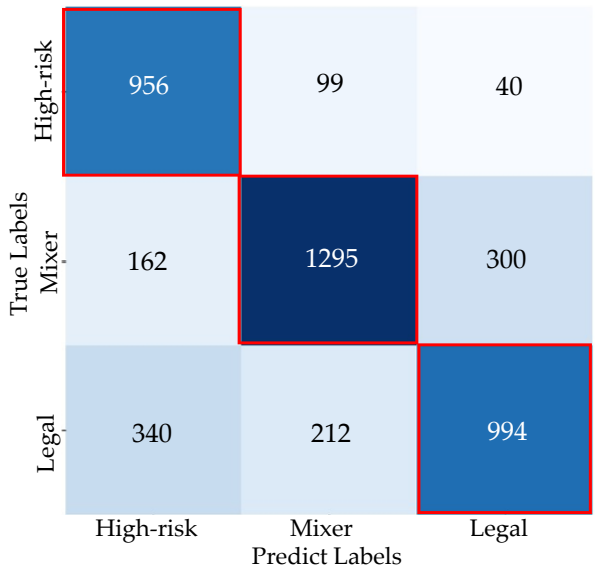
(a) 1D-CNN 模型



(b) TCN 模型混淆矩陣



(c) LSTM 模型混淆矩陣



(d) GRU 模型混淆矩陣

圖 6、4 項模型之混淆矩陣

由上圖 5-8 可知，紅框處為真陽性(True Positive, TP)，其餘部分則為非正確之預測。考量本研究目的在於識別高風險、混幣器及合法交易模式，以便即時遏止犯罪行為，故召回率成為一項關鍵指標。因召回率著重在所有實際為陽性的樣本中，被正確識別為陽性的比例。鑒於偽陰性(False Negative, FN)，即為將高風險金流錯判為混幣器或合法金流等情形，會導致執法人員錯失阻止犯罪的良機，因此本研究尤為重視減少偽陰性的發生。

針對各模型各類別的召回率比較，如下表 6。

表 6、各模型/類別召回率比較

模型	類別	Recall
1D-CNN	Highrisk	84.66%
	Mixer	79.91%
	Legal	75.29%
TCN	Highrisk	87.03%
	Mixer	81.00%
	Legal	83.25%
LSTM	**Highrisk**	**94.34%**
	Mixer	73.42%
	Legal	66.88%
GRU	Highrisk	87.31%
	Mixer	73.71%
	Legal	64.29%

如表 6 所示，4 個模型在識別 Highrisk 類別的召回率均有 80%以上，其中又以 LSTM 在識別 Highrisk 類別的表現最佳，可達 94.34%。然而，LSTM 在識別 Mixer 及 Legal 類別的召回率相對較低，分別為 73.42%和 66.88%。相較之下，TCN 在 3 個類別上的表現較為均衡，召回率均超過 80%，其中識別 Highrisk 類別高達 87.03%。故整體表現而言，TCN 的性能較其他模型更為出色。

3. 實驗結果分析

透過對各模型的混淆矩陣分析，發現 LSTM 在識別高風險金流的召回率高達 94.34%，但在混幣器與合法金流的判斷上，召回率分別只有 73.42%與 66.88%。這一結果顯示 LSTM 在不同類別的表現存在顯著差異，難以被視為最佳模型。相比之下，TCN 模型在高風險金流、混幣器及合法金流的分類上表現最為突出，其準確度達到 83.29%，召回率也有 83.76%。在模型穩定性和評估指標的衡量上，TCN 展現最佳的成效。

因此，為提升模型的穩定性及召回率，本研究提出一種基於規則的整合模型架構(Rule-Based Integration Model)，結合 TCN 及 LSTM，在不同類別下採行最適當的模型，來產

出最佳決策結果，如下圖 7。

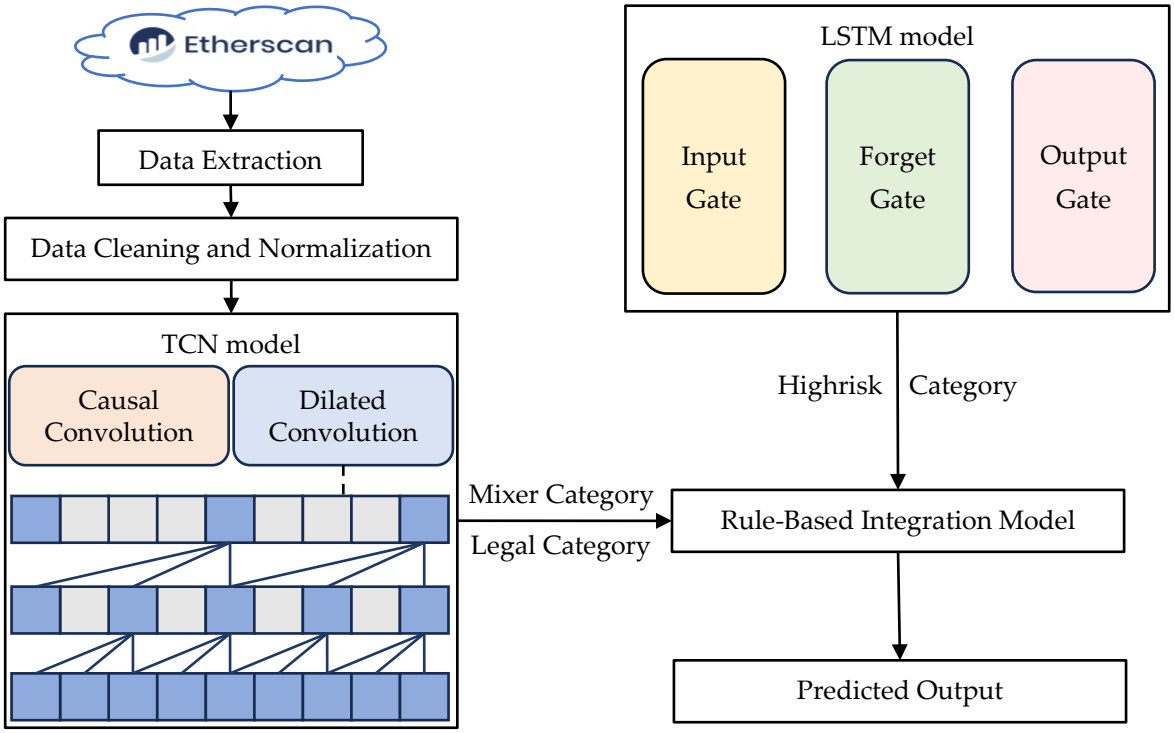


圖 7、基於規則的整合模型架構

在圖 7 中，我們整合 LSTM 及 TCN 模型的優點，以提升對不同交易類別的識別穩定性和準確性。在整合模型架構中，我們先依據預先定義的規則，來選擇不同模型的輸出，作為最終決策的依據。這些規則是建立在各模型在不同類別的表現基礎上。對於高風險金流類別，採用 LSTM 模型的輸出，因其在該類別上具有最高的召回率；而混幣器和合法金流類別，則選擇 TCN 模型的輸出，因其在這些類別的表現上更為穩定且出色。這樣的整合模型架構，使我們能充分利用每個模型的優勢，進而提高整體預測的準確性，確保在關鍵類別上達到最佳的識別效果。

五、結論與未來展望

本研究利用區塊鏈交易的公開透明特性，對 Etherscan 平台上標記為高風險、混幣器及合法的智慧合約，其第一層入金錢包的交易資料進行分析。透過四種深度學習模型，對於不同的交易模式進行分類，發現 TCN 在整體模型決策表現上最為優異，召回率達 83.76%。針對高風險類別交易識別，則以 LSTM 表現較佳，可達到 94.34%的召回率。因此，我們提出基於規則的整合模型架構，結合 LSTM 及 TCN 模型，在不同類別上的表現優勢，更能強化加密貨幣交易的風險評估。

本研究突破加密貨幣匿名性帶來的偵查阻礙，提供另一個新的分析視角。利用區塊鏈公開帳本特性，來獲取交易資料，結合深度學習技術，成功分析不同類型的交易模式，有效提高風險識別的效果。未來將進一步增強模型的泛化能力能，為加密貨幣的交易安全，提供更縝密的監管技術，也為執法人員達到精準打擊的效果。

謝誌：本研究感謝國家科學及技術委員會 (NSTC) 經費支持，計畫編號：NSTC 112-2222-E-015-001、NSTC 113-2221-E-015-001。

參考文獻

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Tornado.Cash Available online: https://dune.com/poma/tornado-cash_1 (accessed on 8 June 2024).
3. Tang, Y.; Xu, C.; Zhang, C.; Wu, Y.; Zhu, L. Analysis of Address Linkability in Tornado Cash on Ethereum. In *Cyber Security*; Lu, W., Zhang, Y., Wen, W., Yan, H., Li, C., Eds.; Communications in Computer and Information Science; Springer Nature Singapore: Singapore, 2022; Vol. 1506, pp. 39–50 ISBN 9789811692284.
4. Santoso, I.; Christyono, Y. Zk-SNARKs As A Cryptographic Solution For Data Privacy And Security In The Digital Era. *International Journal of Mechanical Computational and Manufacturing Research* **2023**, *12*, 53–58, doi:10.35335/computational.v12i2.122.
5. Hu, S.; Zhang, Z.; Luo, B.; Lu, S.; He, B.; Liu, L. BERT4ETH: A Pre-Trained Transformer for Ethereum Fraud Detection. In Proceedings of the Proceedings of the ACM Web Conference 2023; Association for Computing Machinery: New York, NY, USA, April 30 2023; pp. 2189–2197.
6. Wu, M.; McTighe, W.; Wang, K.; Seres, I.A.; Bax, N.; Puebla, M.; Mendez, M.; Carrone, F.; De Mattey, T.; Demaestri, H.O.; et al. Tutela: An Open-Source Tool for Assessing User-Privacy on Ethereum and Tornado Cash 2022.
7. Petkus, M. Why and How Zk-SNARK Works 2019.
8. Dumoulin, V.; Visin, F. A Guide to Convolution Arithmetic for Deep Learning 2018.
9. Kiranyaz, S.; Avci, O.; Abdeljaber, O.; Ince, T.; Gabbouj, M.; Inman, D.J. 1D Convolutional Neural Networks and Applications: A Survey. *Mechanical Systems and Signal Processing* **2021**, *151*, 107398, doi:10.1016/j.ymssp.2020.107398.
10. Bai, S.; Kolter, J.Z.; Koltun, V. An Empirical Evaluation of Generic Convolutional and Recurrent Networks for Sequence Modeling 2018.
11. Lea, C.; Flynn, M.D.; Vidal, R.; Reiter, A.; Hager, G.D. Temporal Convolutional Networks for Action Segmentation and Detection 2016.
12. Hochreiter, S.; Schmidhuber, J. Long Short-Term Memory. *Neural computation* **1997**, *9*, 1735–1780, doi:10.1162/neco.1997.9.8.1735.
13. Van Houdt, G.; Mosquera, C.; Nápoles, G. A Review on the Long Short-Term Memory Model. *Artificial Intelligence Review* **2020**, *53*, doi:10.1007/s10462-020-09838-1.
14. Henry, A.; Gautam, S.; Khanna, S.; Rabie, K.; Shongwe, T.; Bhattacharya, P.; Sharma, B.; Chowdhury, S. Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System. *Sensors* **2023**, *23*, 1–22, doi:10.3390/s23020890.
15. Chung, J.; Gulcehre, C.; Cho, K.; Bengio, Y. Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling 2014.
16. Cardarilli, G.C.; Di Nunzio, L.; Fazzolari, R.; Giardino, D.; Nannarelli, A.; Re, M.; Spanò, S. A Pseudo-Softmax Function for Hardware-Based High Speed Image Classification. *Sci Rep* **2021**, *11*, 15307, doi:10.1038/s41598-021-94691-7.

17. etherscan.io Ethereum (ETH) Blockchain Explorer Available online: https://etherscan.io/ (accessed on 2 June 2024).
18. Maharana, K.; Mondal, S.; Nemade, B. A Review: Data Pre-Processing and Data Augmentation Techniques. *Global Transitions Proceedings* **2022**, *3*, 91–99, doi:10.1016/j.gltp.2022.04.020.
19. Lin, T.; Wang, Y.; Liu, X.; Qiu, X. A Survey of Transformers. *AI Open* **2022**, *3*, 111–132, doi:10.1016/j.aiopen.2022.10.001.
20. Samuels, J. *One-Hot Encoding and Two-Hot Encoding: An Introduction*; 2024;
21. Bai, Y.; Yang, E.; Han, B.; Yang, Y.; Li, J.; Mao, Y.; Niu, G.; Liu, T. Understanding and Improving Early Stopping for Learning with Noisy Labels 2021.
22. Srivastava, N.; Hinton, G.; Krizhevsky, A.; Sutskever, I.; Salakhutdinov, R. Dropout: A Simple Way to Prevent Neural Networks from Overfitting.
23. Viering, T.; Loog, M. The Shape of Learning Curves: A Review. *IEEE Trans. Pattern Anal. Mach. Intell.* **2023**, *45*, 7799–7819, doi:10.1109/TPAMI.2022.3220744.
24. Fawcett, T. Introduction to ROC Analysis. *Pattern Recognition Letters* **2006**, *27*, 861–874, doi:10.1016/j.patrec.2005.10.010.
25. Kulkarni, A.; Chong, D.; Batarseh, F.A. 5 - Foundations of Data Imbalance and Solutions for a Data Democracy. In *Data Democracy*; Batarseh, F.A., Yang, R., Eds.; Academic Press, 2020; pp. 83–106 ISBN 978-0-12-818366-3.