

2022 年第 25 屆資訊管理學術暨
警政資訊實務研討會
——「元宇宙的創新應用與偵查」

論文集

目 錄

1	以機器學習方法驗證短網址之安全性 (邱靖宸、張明桑、林曾祥).....	01
2	智能合約在刑案數位證據區塊鏈之應用—以警示帳戶解除為例 (李崎維、高信雄、董正談、鄧少華).....	09
3	數種具元宇宙元素平台應用程式之數位鑑識初探(鄧思源).....	20
4	涉加密貨幣刑事案件錢包追蹤自動化之研究 (張哲維、高信雄、董正談、鄧少華).....	26
5	Applying Routine Activity Theory to Columbaria Investment Scam (楊基成、陳怡如、高大宇).....	35
6	基於量化值迭代計算的單位圖彩色區塊截短編碼技術 (王梓熏、洪維恩).....	42

**2022 年第 25 屆資訊管理學術暨
警政資訊實務研討會
——「元宇宙的創新應用與偵查」
大會組織**

大會主席：

陳校長擇文

大會副主席：

蘇副校長志強

籌備及議程委員會主席：

林主任建隆

林主任曾祥

籌備委員：

林主任建隆、林主任曾祥、王教授朝煌

吳教授國清、鄧教授少華、王教授旭正

顏副教授志平、董助理教授正談

執行秘書：

簡助教羚茜

序 言

本校與內政部警政署為促進資訊管理學術與警政資訊實務之交流，結合資訊管理學術與警察資訊實務工作，期經由警察資訊應用技術的開發來提昇警察工作效能，進而促使警察能夠採取更經濟有效的方法來服務社會。為具體落實此項目標，本校定期舉辦資訊管理學術暨警政資訊實務研討會，期能藉由舉辦研討會交流學術研究成果與實務經驗智慧，共同研討尋求解決方案。此外有鑒於資訊科技不斷地創新應用與發展，資訊科技不但已經成為現代化社會、生活與工作的必備利器，更讓我們能夠突破時空的侷限來進行過去無法完成的事項；而社會環境不斷地變遷，對於警察角色的定位也有所轉變，已經從法律與治安的維護者，擴大為社會與民眾的服務者，因此如何整合並運用資通訊科技來維護治安與打擊犯罪，並以創新的思維來面對警察工作的挑戰已成為迫切的課題。本次研討會主題為「元宇宙的創新應用與偵查」，相信在各位作者的熱情參與下，對於警察資訊人員如何以創新的思維跟上時代的脈動並順利完成各項警察工作，將會有更宏觀的認識與啟發。

論文發表部份，本屆研討會因疫情關係，改為線上發表方式，總計刊登 6 篇文章，分別探討「以機器學習方法驗證短網址之安全性」、「智能合約在刑案數位證據區塊鏈之應用—以警示帳戶解除為例」、「數種具元宇宙元素平台應用程式之數位鑑識初探」、「涉加密貨幣刑事案件錢包追蹤自動化之研究」、「Applying Routine Activity Theory to Columbaria Investment Scam」、「基於量化值迭代計算的單位圖彩色區塊截短編碼技術」，涵蓋學術與實務領域，契合本研討會之宗旨。

本屆研討會得以順利舉辦，首先要感謝陳校長、蘇副校長、霍主任秘書、王教務長、警察科技學院王院長以及各級長官的鼎力支持與協助，為資訊管理學系添購各項軟硬體設備，並充實教學與研究環境，其次感謝本系所有教師以及學校各單位同仁通力合作共襄盛舉，並感謝本系簡羚茜助教以及所有在幕後任勞任怨付出與幫忙的所有審查委員們，最後感謝各位先進、前輩、校友以及警界同仁的熱情參與，希望藉由大家的參與交流集思廣益，能夠進一步提昇國內資訊管理學術與警政資訊實務的發展與研究水準。

中央警察大學資訊管理學系主任**林曾祥**敬序

中華民國 111 年 6 月

以機器學習方法驗證短網址之安全性

邱靖宸

中央警察大學資訊管理研究所研究生

im1093064@mail.cpu.edu.tw

張明桑

中央警察大學資訊管理研究所教授

mschang@mail.cpu.edu.tw

林曾祥*

中央警察大學資訊管理研究所教授，通訊作者

jslin168@mail.cpu.edu.tw

摘要

網頁位址是網際網路上標準的資源位址，就是網路上的門牌。長的網址難以紀錄和傳送，若網址中含有特殊符號時，容易被視為惡意的網址而不讓使用者連結，因此縮短網址服務成為使用者的喜愛，它可以將網址縮成一定的長度，方便閱讀及傳送。然而縮短網址服務近年來被用來包裝釣魚網站，透過短網址重新導向的功能，避開防毒軟體的偵測，造成使用者難以辨別，導致使用者的身分資訊遭竊取或所使用的裝置遭惡意程式攻擊，致使財物損失。本論文提出一個模型，將短網址還原成原始網址，再透過線上釣魚網站資料庫比對後，提取原始網址的特徵值，利用機器學習的方式進行預測，讓使用者能安心判別該短網址是否安全。

關鍵字: 短網址、網路釣魚、機器學習、Weka。

Abstract

The web address as like the house number is the standard resource address on the Internet. Long URLs are difficult to record and transmit. If the URL contains special symbols, it is used to be regarded as a malicious URL and will not allow users to link. Therefore, the URL shortening service has become the favorite of users. It not only can shorten the URL to a certain length but can easily be read and transmit. However, in recent years, URL shortening service has been used to package phishing websites. Through the redirection function of URL shortening, it avoids detection by anti-virus software, making it easy for users to be difficult to identify, resulting in malicious programs attacking their devices and users' identity information being compromised. This study proposes a model that first restores the short URL to the original URL, and then compares it with the online phishing website database, extracts the feature values of the original URL, and uses machine learning to make predictions, so that users can identify the short URL with confidence.

Keywords: short URL、Phishing、Machine Learning、Weka。

一、前言

縮短網址的服務於2000年註冊專利[8]，迄今已成為網路使用者喜好的工具，透過短網址服務，使用者可以將欲分享出去的網址縮短，縮短成一段固定長度的網址。如此可以使所傳送的訊息版面簡潔，也可以有效因應社交媒體所限制撰寫貼文的文字數目，如Twitter限制每篇推文僅能140個字符。

儲存在雲端服務的檔案網址是非常長的一串文字，使用縮短網址服務可以有效的縮短該網址，方便使用者接收訊息，但因短網址是有固定的長度，透過暴力破解的方式容易排列組合找到有效的短網址，可以去竄改

雲端空間內的文件內容、遷入惡意程式甚至竊取使用者的身分資訊[6]。

根據趨勢科技全球技術支援與研發中心的報告，短網址在2010年被發現用來傳送垃圾訊息、於2012年發現一隻Skype蠕蟲病毒利用短網址快速傳播，該短網址會指向一個惡意檔案，讓點選連結的使用者成為殭屍網路（Botnet）的傀儡。在2014年出現ACH的詐騙電子郵件，點擊時會導向含有一個惡意程式的.zip檔案，讓使用者的裝置中毒[11]。而現今短網址則常被用來包裝釣魚網站，釣魚網站利用短網址重新導向的特性，容易規避防毒軟體的偵測。

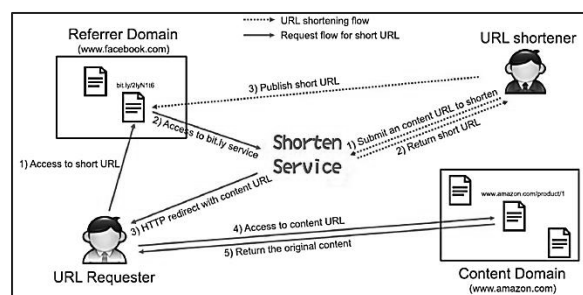
水能載舟亦能覆舟，短網址雖然帶來便利的服務，同時被惡意使用也帶給使用者負面的影響，因此，本文章提出一種驗證短網址安全性的模型，先將短網址還原成原始網址，透過 PhishTank、OpenPhish、及 PhishRepo 等三個線上蒐錄釣魚網站的資料庫平台比對後，再將原始網址擷取多個特徵值後，利用 UCI Machine Learning Repository 所收錄釣魚網站資料集[3]，透過 Weka 軟體生成 3 種不同機器學習預測模型進行比對，來預測該網址是否為釣魚網站，供使用者判斷網址的安全性。

本文接下來將於第二節文獻探討，第三節說明本研究模型的實驗方法，第四節則展現實驗結果及分析，最後於第五節進行結論與未來展望。

二、文獻探討

縮短網址是一種將原始網址映射到一個短網址的技術，透過短網址可以重新導向回原始網址。最初設計短網址的概念是為了防止使用者在複製網址字符的過程中破壞原始複雜網址的完整性及當時並沒有可以讓長網址換行的符號[9]。

現今網路上有許多縮短網址的服務，該服務會將使用者所輸入的原始網址生成一段固定長度的短網址，而該網址係由三部分組成，如：「https://tinyurl.com/mu6penmj」(此網址係由中央警察大學的原始網址 https://www.cpu.edu.tw/ 經由 TINYURL 縮短服務所產出的網址)係由 https、tinyurl.com、mu6penmj 三部分所組成：https 代表通訊協定、tinyurl.com 是該服務的網域名稱、mu6penmj 則是一段固定長度的雜湊碼。短網址的產生可以簡潔的訊息、讓使用者容易閱讀其他說明文字，不因原始網址的冗長而佔用太多訊息版面。



圖一：縮短網址服務的運作流程

縮短網址的運作可以分為將網址縮短端的使用者(URL shortener)、點選短網址端的使用者(URL Requester)、提供短網址服務的稱為 Referrer Domain 還有原始網址的 Content Domain 四部分，如圖一所示[5]。

URL shortener 先將欲縮短的網址，傳送到縮短網址服務平台，縮短網址服務平台就會回傳一個短網址給使用者，使用者就可以將該短網址加以分享、傳送；當另一 URL Requester 接收到短網址時，短網址就向他所屬的服務平台檢索該原始網址，然後幫使用者重新導向到原始網址，使用者就可以向原始網站內容要求連線存取資料，該原始網站就會提供後續服務。

過去有許多學者對短網址進行研究：

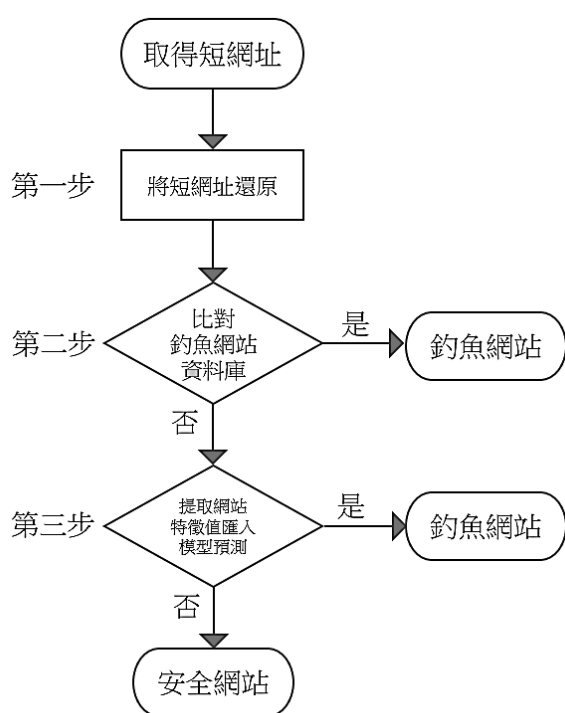
1. Demetris 於2011年分析Twitter社交媒體平台短網址的使用情形，包含每日統計數據、被轉貼(推)的次數、被點擊的次數。
2. Klien 與 Strhmaier 於2012年研究短網址被惡意濫用的情形，由於短網址可以隱藏原始網址的內容，該學者研究短網址被濫用發送垃圾郵件的情形。
3. Chhabra 於2011年研究釣魚網站如何透過 Bit.ly 縮短網址服務進行分享及 PhishTank (釣魚網站資料庫) 所蒐集的數據集進行比對，同時在 Twitter 平台上短網址被運用的情形是最多的。
4. Wang 於2013年提出一個基於Twitter 社交平台檢測郵件中是否還有短網址的垃圾郵件。
5. Maggi 於2013年蒐集了兩年內被使用的短網址，發現短網址被惡意使用的情形，發現所帶來的威脅所造成的損害，其實並不如長網址所帶來的威脅。
6. Nikiforakis 於2014年提出一個報告稱，基於廣告性質的短網址，容易被惡意軟體濫用進而感染使用者取得機敏的資料。
7. Daejin Choi 等學者於2018年針對Bit.ly縮短網址平台，收集了8千萬筆的短網址，分析42億次點擊的資訊，發現大多生成的短網址的原始網址內容是無效的。

綜上的文獻資料可知，目前學者的研究並沒有提出一個有效辨識短網址是否安全的機制。所以本文提出將短網址先比對公開資料庫的釣魚網址，在提取該網址的特徵值，透

過經機器學習訓練好的模型，去預測短網址是否為惡意釣魚網址的安全性機制。

三、實驗方法

本研究所提出的模型分為三步驟(如圖二所示)，第一步先將短網址還原成原始網址、第二步將原始網址透過蒐集釣魚網站的線上公開網站 PhishTank、OpenPhish、及 PhishRepo 去比對是否已被通報為釣魚網址、第三步則提取該網址的 30 個特徵，透過 Weka(3.8.5 版本)預先以 Naive Bayes、J48、Random forest 等三種機器學習方法建立的釣魚網站預測模型，再透過本文蒐集的網址進行預測，比對三種機器學習法預測準確率。



圖二：本實驗流程

1. 釣魚網站的特徵值

根據 APWG (Anti-Phishing Working Group) 的定義釣魚網站是一種利用社交工程 (Social Engineering) 的技術來竊取消費者個人身份數據和金融帳戶憑證的非法網站。而社交工程指的是透過設計或欺騙粗心的受害者，讓使用者相信他們正在連結可信賴的網站，例如使用假冒的電子郵件和欺騙性的訊息，引導消費者連結到偽造網站，藉此誘騙收件人洩露自己的財務資訊，如使用者用戶名稱和密碼[4]。

我們採用 UCI Machine Learning Repository(國外著名公開資料庫)中，於2015

年所蒐錄的網站資料，內含有11,055 筆的有效網站的資料集，其中 6,157 筆為Phishing(釣魚網站)；4,898 筆網站則顯示為Legitimate(合法網站即非釣魚網站)，從中提取網站的30個特徵值，用來判斷是否為合法網站或是釣魚網站的依據，如表一所列[10]。

欄位	欄位說明
A	Using the IP Address.
B	Long URL to Hide the Suspicious Part.
C	Using URL Shortening Service "TinyURL"
D	URL's having "@" Symbol.
E	Redirecting using "//".
F	Adding Prefix or Suffix Separated by (-) to the Domain.
G	Sub Domain and Multi Sub Domains
H	HTTPS
I	Domain Registration Length.
J	Favicon
K	Using Non-Standard Port
L	The existence of "HTTPS" Token in the Domain Part of the URL.
M	Request URL.
N	URL of Anchor
O	Links in <Meta>, <Script> and <Link> tags.
P	Server Form Handler (SFH).
Q	Submitting Information to Email.
R	Abnormal URL.
S	Website Forwarding
T	Status Bar Customization
U	Disabling Right Click.
V	Using Pop-up Window
W	Iframe Redirection.
X	Age of Domain
Y	DNS Record
Z	Website Traffic
AA	PageRank
AB	Google Index
AC	Number of Links Pointing to Page
AD	Statistical-Reports Based Feature

表一、釣魚網站的30個特徵值

三十種網站的特徵值以判斷的性質區分，可以分為四種類別「以網址為主」、「以網域為主」、「以網域語法」、「異常」之特徵，以下分述如下：

1)以網址為主之特徵：

- A.使用IP位址
- B.網址冗長，用以隱藏可疑的部分
- C.使用TinyURL的縮短網址服務的網址
- D.網址內含有@的符號
- E.網址內含有「//」重新導向的符號
- F.網址內含有「-」的符號
- G.網址含有多個子網域
- H.是否使用HTTPS的通訊協定
- I.使用網域所註冊的時間
- J.是否含有網站縮圖
- K.使用非標準的通訊協定
- L.在網址內遷入HTTPS的字詞

2)以網域為主之特徵：

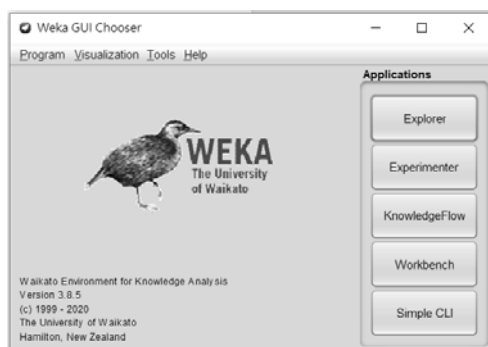
- M.網頁的內容是由另一個網域所加載的
- N.網站內容出現<a>的語法超過比例
- O.原始碼大量的<Meta>、<Script>、<Link>
- P. 伺服器的表單處理程序包含空白的字串
- Q.表單中允許使用者提交個人的訊息
- R.用Whois查詢該網域是否有申登資料

3)以網域語法之特徵：

- S.網站重新導向另一個網域的次數
- T.網站是否遭嵌入虛假的Javascript
- U.網站是否禁用滑鼠點擊
- V.網站是否有出現彈跳視窗
- W.網站中的Iframe是否被隱藏
- X.網域存在的壽命
- Y.網域是否在Whois被查找到的

4)異常特徵：

- Z.該網站的流量是否被Alexa數據庫識別
- AA.網頁的排名
- AB.網頁在網路上的重要性
- AC.網站是否在Google被搜尋的到
- AD.網域跟IP是否已被通報可疑網站

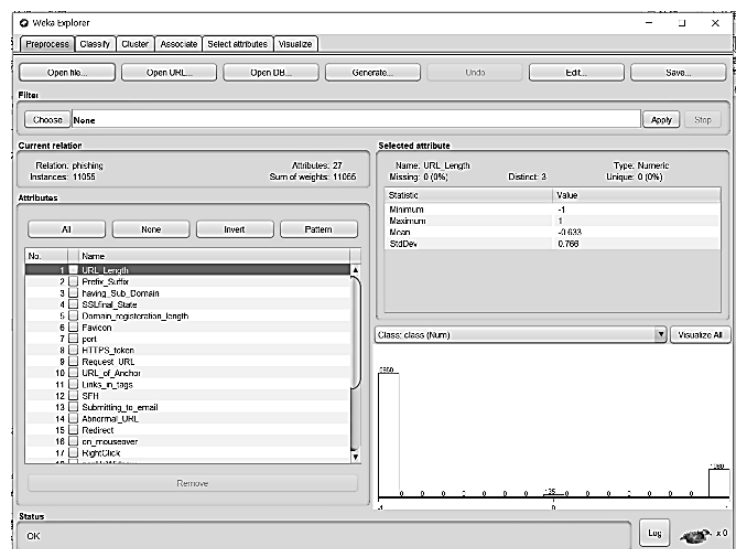


圖三: Weka開啟畫面

2. Weka

Weka是由紐西蘭的懷卡托大學所研發，是由 Waikato Environment for Knowledge Analysis 片語的字首所組成。Weka 是一套提供資料探勘 (data mining) 以及機器學習 (machine learning) 工具的一套軟體，包括資料前置處理工具、分類工具、回歸分析等，而且能將資料以視覺化的方式呈現。這套軟體以 Java 程式語言編撰 [7]。

軟體介面包含了資料探勘的方法：預處理、分類、分群、關聯性規則、資料屬性的選擇(如圖四所示)，資料使用「.arff」檔案格式。Weka可以將數據集進行資料分析，找出資料間的關聯性、可以使用機器學習模型來對新的資料進行預測、也可以透過不同的機器學習方法比較適合的模型來進行預測。



圖四：Weka操作介面

本文就前述每個網站所提取的30個特徵值，先加以進行正規化：以「1」、「0」與「-1」值來表示，分別代表『Phishing釣魚網站』、『Suspicious疑似為釣魚網站』、『Legitimate合法網站』。接著再透過Weka將釣魚網站資料集以3種機器學習的演算法建立預測模型，分述如下：

1) Naïve Bayes：

朴素貝葉斯分類演算法，是以貝氏定理 (Bayesian theorem) 為基礎的分類方法，貝氏定理是由條件機率所推導出來的。而條件機率指的是「在A條件下發生B事件的機率」等於A、B同時發

生的機率除以 A 發生的機率，如式(1) 圖六

$$P(B|A) = P(A \cap B) / P(A) \quad (1)$$

以Naïve Bayes 將釣魚網站資料集建立模型，其準確率為 94.0554% 如圖五所示。

```
=== Summary ===
Correctly Classified Instances      2310      94.0554 %
Incorrectly Classified Instances    146      5.9446 %
Kappa statistic                    0.8797
Mean absolute error                0.0766
Root mean squared error            0.2137
Relative absolute error            13.5145 %
Root relative squared error        42.9911 %
Total Number of Instances          2456

=== Detailed Accuracy By Class ===

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	FRC Area	Class
	0.932	0.053	0.934	0.932	0.933	0.880	0.987	0.984	1
	0.947	0.068	0.946	0.947	0.946	0.880	0.987	0.989	-1
Weighted Avg.	0.941	0.061	0.941	0.941	0.941	0.880	0.987	0.987	

```

=== Confusion Matrix ===
      a   b  <-- classified as
1020  74 |  a = 1
 72 1290 |  b = -1

```

圖五：以NaiveBayes演算法對釣魚網站資料庫之特徵值建模

2) J48：

J48 是一種決策樹類型的演算法，也稱為 C4.5 演算法，是一種基於從上到下的遞迴的分治策略，選擇某個屬性放置在根節點，為每個可能的屬性值產生一個分支，將實例分成多個子集，每個子集對應一個根節點的分支，然後在每個分支上遞迴地重複這個過程，當所有實例有相同的分類時才停止。

J48核心演算法繼承了 ID3 演算法的優點，同時增進了以下面向：

- I. 運用資訊增益率(Information gain rate)來選擇屬性，克服了用資訊增益(Information gain)選擇屬性時會偏向取值多的屬性。
- II. 在樹狀構造過程中能進行剪枝。
- III. 能夠對連續屬性的離散化處理。
- IV. 能夠對不完整的資料進行處理。

```
=== Summary ===
Correctly Classified Instances      2333      94.9919 %
Incorrectly Classified Instances    123      5.0081 %
Kappa statistic                    0.8989
Mean absolute error                0.0643
Root mean squared error            0.1988
Relative absolute error            13.0069 %
Root relative squared error        39.9902 %
Total Number of Instances          2456

=== Detailed Accuracy By Class ===

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	FRC Area	Class
	0.956	0.055	0.933	0.956	0.944	0.899	0.986	0.983	1
	0.945	0.044	0.964	0.945	0.954	0.899	0.986	0.985	-1
Weighted Avg.	0.950	0.049	0.950	0.950	0.950	0.899	0.986	0.984	

```

=== Confusion Matrix ===
      a   b  <-- classified as
1046  48 |  a = 1
 75 1287 |  b = -1

```

圖六：以J48演算法對釣魚網站資料庫之特徵值建模 5

3) Random Forest：

Random Forest稱為隨機森林，基本原理是結合多顆CART樹（Classification and Regression Tree），並加入隨機分配的訓練資料，以大幅增進最終的運算結果。

隨機森林演算法的理論是根據大數法則，由k顆決策樹組成一個森林，同時也產生k個隨機向量 Θ_k ，而隨機向量都是獨立且均分的，利用訓練集以及隨機向量生成決策樹，會產生分類器 $h(x, \Theta_k)$ ，其中x為一個輸入向量。在多顆決策樹生成後，選出最多的分類，簡單來說就是輸出的類別是由個別樹輸出的類別的眾數而定[1]。

隨機森林的除了準確高之外，能處理很高維度的資料（多特徵的資料），不用進行特徵選擇，在訓練完時速度快，過程中之後，隨機森林能給出哪些特徵比較重要，能夠檢測到feature之間的影響。對於不平衡資料集來說，隨機森林可以平衡誤差。若有很部分的特徵遺失，仍然可以維持準確度，所以最受大家的喜愛，將釣魚網站特徵用隨機森林演算法建模情形高達97.7606%，如圖七所示。

```
=== Summary ===
Correctly Classified Instances      2401      97.7606 %
Incorrectly Classified Instances    55      2.2394 %
Kappa statistic                    0.9547
Mean absolute error                0.0616
Root mean squared error            0.1423
Relative absolute error            12.4622 %
Root relative squared error        28.6364 %
Total Number of Instances          2456

=== Detailed Accuracy By Class ===

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	FRC Area	Class
	0.974	0.020	0.975	0.974	0.975	0.955	0.997	0.996	1
	0.980	0.026	0.979	0.980	0.980	0.955	0.997	0.997	-1
Weighted Avg.	0.978	0.023	0.978	0.978	0.978	0.955	0.997	0.997	

```

=== Confusion Matrix ===
      a   b  <-- classified as
1066  28 |  a = 1
 27 1335 |  b = -1

```

圖七：以隨機森林將網站資料集進行建模

3.實驗設計

本文透過著名釣魚網站公開資料平台PhishTank、OpenPhish、及PhishRepo的網站，分別蒐錄111年2月至3月被確認為釣魚網站的短網址總數100組(因惡意的短網址，經研究平均生存時間僅50天，故僅以本年取2個月的資料進行實驗)以及100組合法網站透過縮短網址服務平台，將其縮短為短網址，透過本文實驗的機制，將所

蒐集的200組短網址進行實驗，比對利用3種不同的機器學習演算法，成功判別合法網站及惡意釣魚網站的成功率，透過混淆矩陣呈現實驗結果。

混淆矩陣(confusion matrix)是可視化工具，常用於機器學習中的監督學習。矩陣的每一列代表一個類的實例預測，而每一行表示一個實際的類的實例，通過這個矩陣可以方便地看出機器是否將兩個不同的類混淆，所以稱為混淆矩陣，而混淆矩陣中由四個元素組成：TP、TN、FP、FN：

- 1) TP (True Positive) :
模型預測為真，而且真實情況亦為真的情況下即為True Positive，真陽性。
- 2) TN (True Negative) :
模型預測為非，而且真實情況亦為非的情形下即為True Negative，真陰性。
- 3) FP (False Positive) :
模型預測為真，但是真實情況為非的情形下即為False Positive，偽陽型。
- 4) FN (False Negative) :
模型預測為非，但真實情況為真的情形下即為False Negative，偽陰性。

表二、混淆矩陣：

	模型預測為真 (positive)	模型預測為非 (negative)
「真實情況」 為真	True Positive (TP)	False Negative (FN)
「真實情況」 為非	False Positive (FP)	True Negative (TN)

四、實驗結果與分析

本研究將200組短網址，經過本文的實驗流程第一步及第二步的預處理，發現其中100組惡意的短網址，經過還原成原始網址後，去比對公開釣魚網站平台的資料庫，已經有34筆原始網址被判定為被通報的釣魚網址，可見不法人士為了Phishing成功的效率，簡單而直接地將原始網址包裝成短網址，嘗試去騙取使用者的信任，一來成功規避防毒軟體對於惡意網站的檢測，二來不需要再透過建置新的釣魚網站，申請相關網域空間，直接透過短網址服務重新導向的特性，節省成本。而其餘的66筆網址，則進行下一步的特徵

存取；相對另100組合法網址，自然不是被通報惡意網站的網址。

根據前述3種機器學習的演算法，我們將實驗結果以混淆矩陣方式呈現如下：

表三、以Naive Bayes模型預測之結果：

	被判斷為 釣魚網站	被判斷為 合法網站
實際上是 釣魚網站	TP : 76	FN : 24
實際上是 合法網站	FP : 9	TN : 91

以Naive Bayes模型評估指標：

- 1、準確率： $(76+91)/200 = 83.5\%$
- 2、精確率： $76/(76+9) = 89.4\%$
- 3、召回率： $76/(76+24) = 76\%$

表四、以J48模型預測之結果：

	被判斷為 釣魚網站	被判斷為 合法網站
實際上是 釣魚網站	TP : 79	FN : 21
實際上是 合法網站	FP : 7	TN : 93

以J48模型評估指標：

- 1、準確率： $(79+93)/200 = 86\%$
- 2、精確率： $79/(79+7) = 95.18\%$
- 3、召回率： $79/(79+21) = 79\%$

表五、以Random forest模型預測之結果：

	被判斷為 釣魚網站	被判斷為 合法網站
實際上是 釣魚網站	TP : 86	FN : 14
實際上是 合法網站	FP : 6	TN : 94

以Random forest模型評估指標：

- 1、準確率： $(86+94)/200 = 90\%$
- 2、精確率： $86/(86+6) = 93.47\%$
- 3、召回率： $86/(86+14) = 86\%$

由上述實驗數據可得知，使用機器學習的方法對於資料的預測，準確率是相當高的，其中又以Random forest 演算法的預測結果是最好的，主因為其透過不同的決策樹所組成，各個決策樹彼此獨立不互相影響；而Naïve Bayes 相較之下，就顯得低一些，可歸因於此演算法是根據機率所得的演算法，透過在某個條件下可能發生的機率來預測，所以沒有那麼的細緻，但相對的簡單，較為減省時間；介於兩者之間的J48演算法，則較為折衷，不像Naïve Bayes演算法太簡單，而可以自己修剪決策樹的枝葉，針對未知的特徵值(屬性資料)進行處理，較為靈活運用。

五、結論與未來研究方向

縮短網址服務已成為網路使用者不可或缺的工具，透過它可以將冗長的網址縮短成一段固定長度的網址，方便使用者閱讀、分享，所帶來的便利卻也被惡意使用，包裝成釣魚網址，在使用者在即使有防毒軟體的保護下，無法辨識短網址的安全性，可能導致使用者遭釣魚網站受騙，自身的個人身分資料及銀行帳號密碼在無形中遭騙取，導致財務損失，甚至在不知情況下，手機或電腦就成為殭屍網路的一員，而藉由本文所提出的機制，利用機器學習的方式來驗證短網址的安全性，分析3種演算法的效果，提供讀者一個安全的驗證短網址安全機制。

因釣魚網站本身存活的時間有限，且會針對系統的漏洞或使用者安全意識降低不斷推陳出新，而本研究使用的釣魚網站資料庫為2015年所建置的，部分提取的特徵值已不符合現今的環境，未來我們將優化釣魚網站的特徵值，期能更有效的辨識釣魚網站，同時也呼籲提供縮短網址的服務平台，可以負起社會責任，先對使用者預先提供的原始網址進行安全驗證機制，若屬於惡意釣魚網站者，就不要提供轉址的服務，有效降低使用者受騙的風險。

六、參考文獻

1. 李孟潔，「以隨機森林演算法及極限梯度提升法分析台灣五十之交易策略」，國立高雄科技大學金融資訊系碩士論文，2020年，第14頁。
2. 林曾祥、張明桑、邱靖宸，「短網址安全性之研究」，第26屆國際資訊管理暨實務研討會，2021，第56頁。
3. 洪慕藍，「以機器學習演算法探討網路釣魚網站之特徵值」，南臺科技大學資訊管理研究所碩士論文，2019，第32~35頁。
4. APWG, "Phishing Activity Trends Report 4th Quarter 2021", 2021, pp: 4.
5. Daejin Choi, Jinyoung Han, Selin Chun, Efstratios Rappos, Stephan Robert, Ted Taekyoung Kwon, "Bit.ly/practice: Uncovering content publishing and sharing through URL shortening services", Telematics and Informatics 35, 2018, pp: 1312.
6. FARADAYSEC, "Urlhunter - A Recon Tool That Allows Searching On URLs That Are Exposed Via Shortener Services", Jan. 03, 2021.
7. Ian H. Witten, Eibe Frank, Mark A. Hall, "Data Mining: Practical Machine Learning Tools and Techniques", Third Edition, pp403-406.
8. Martin Georgiev and Vitaly Shmatikov, "Gone in Six Characters: Short URLs Considered Harmful for Cloud Services", 2016, pp: 2.
9. Neha Gupta, Ponnurangam Kumaraguru, Anupama Aggarwal, "bit.ly/malicious: Deep Dive into Short URL based e-Crime Detection", June 2014.
10. Rami M. Mohammad., Fadi Thabtah, and Lee McCluskey, "Phishing Websites Features", 2015.

11. Trend Micro, “Are shortened URLs safe?”, March 4, 2016. (https://news.trendmicro.com/2016/03/04/are-shortened-urls-safe/?_ga=2.62317164.1944866259.1650848527-1531672071.1618020367)

智能合約在刑案數位證據區塊鏈之應用—以警示帳戶解除為例

李崎維

中央警察大學資訊管理所研究生

im1103044@mail.cpu.edu.tw

高信雄

刑事警察局電信偵查大隊偵查正兼任助理教授

k601516@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授

tung@mail.cpu.edu.tw

鄧少華

中央警察大學資訊管理所教授，通訊作者

pdeng@mail.cpu.edu.tw

摘要

近來，詐欺案件層出不窮，詐騙集團廣泛利用網際網路、電話及各項通訊設備實行詐騙行為，利用金融機構的轉帳、匯款功能及提款機取得詐騙款項，詐騙手法更是推陳出新，使得民眾無法有效防範。人頭帳戶氾濫情形日益增加，金融帳戶成為詐騙集團主要犯案工具，詐騙款項在多個人頭帳戶間流通，使被害情形無限擴大，導致警方查緝不易、被害款項不易追回。警示帳戶的設立管制成為喝止金融詐欺犯罪的一大利器，有效阻止犯罪。警示帳戶設定後便無法正常使用交易功能，待案件結束且滿足解除條件後才得以解除警示，帳戶的解除須本人親赴警察機關辦理，徒增困擾及不便利。故延續先前之研究引入雲端運算及區塊鏈技術佈建跨機關間資料傳遞交換系統，建置雲端運算環境，提供法院、檢警調及金融機關間的運算、儲存資源及安全管理機制。以區塊鏈去中心化、安全性等特點，確保各項資料符合證據監管鏈規定，使各機關間有效運用資料，並透過智能合約設定自動解除警示帳戶，提供民眾可信、便利的資訊系統。

關鍵字:雲端運算、區塊鏈、數位證據、智能合約、警示帳戶

一、前言

近年資訊科技發達，詐騙集團利用購物詐欺、投資借貸詐欺、冒用身分詐欺等詐騙行為，並利用各項轉帳、匯款功能，透過提款機取得詐騙贓款。犯罪手法的推陳出新，使民眾防不勝防，且詐欺犯罪施行地點不因區域而限制，跨海操控的方式更是層出不窮，輕易躲避警方查緝。低成本、低風險、高報酬的犯罪行為，可獲得高額不法利益，因此吸引許多觀念偏差的人加入詐騙集團的行列。詐欺行為近年來成為臺灣最普遍發生的犯罪行為之一，大多數的民眾都曾接到過詐騙電話、訊息等。根據警政署統計室統計通報資料顯示，民國 105 年至 110 年間，每年的詐欺案件數為 20 餘萬件且有逐年上升趨勢，其中 110 年 1-6 月詐欺案件發生數計 11,447 件，較 109 年 1-6 月增加 446 件(+4.05%)，對民眾的影響不容小覷，嚴重影響金融秩序[19]。人頭帳戶氾濫情形日益

增加，金融帳戶儼然成為詐騙集團犯罪的工具。本於便利民眾的各項金融措施，如網路轉帳、語音轉帳、自動存款機、無卡提款、約定帳戶等，被詐騙集團作為不法使用，輕鬆的將詐騙贓款流通於多個人頭帳戶之間，無形中被害情形日益擴大，使得警方在查緝上越來越不容易。被害的款項也不容易追回。因此行政院為了解決詐欺氾濫的問題多次召開跨部會議研擬各項對策，如要求金融機構加強執行「認識客戶」程序（Know Your Customer）、涉及帳戶匯款詐欺案件之設定警示帳戶及啟動金融機構聯防機制、人頭資料庫供金融機構查詢等措施。建立「警示通報機制」以及「人頭資料庫」，給予人民財產的保障更多了一層保護[17]。「警示帳戶通報機制」制定之目的在於有效喝止犯罪、斷絕資金竄流、協助被害者取回被害款項，但有時卻因為各種原因導致誤設警示帳戶或帳戶申請人解除不易、不知如何解除以及

求助無門的窘境，衍生出許多無辜的被害人，因此該項制度設計顯然有所缺失，實有檢討改進之必要。

自區塊鏈（Blockchain）技術誕生至今，便成為近年來最具革命性的技術之一而廣為應用，顛覆了傳統的交易模式。區塊鏈具有匿名、可追溯、不可篡改、去中心化等特性，區塊鏈是一個分散式帳本，透過分散式節點進行資料傳輸、儲存、驗證，使用相同技術標準的任何人皆可視為節點(Node)並延伸其區塊鏈，維護區塊鏈的運作。

雲端運算中最主要的應用之一是「雲端儲存」，其可以隨時隨地存取檔案和文件[7]。雲端運算的功能是將各機關所上傳的數位證據存放在雲端數位資料庫內進行保存，建置雲端運算基礎環境，提供各機關所需龐大運算與儲存資源及安全管理機制。故數位證據透過區塊鏈加密上鏈後，最重要的就是在法院、檢察署、警察及金融機關間傳遞、利用，並依據各偵查機關服務需求量的變化進行調整與擴充，確保數位證據在雲端系統上之穩定度與效能。

警示帳戶的解除須民眾親赴警察機關申請且須配合警察機關之正式公文函發金融機關(圖1)，申請解除警示帳戶約3~5天後才會收到解除警示公文，帳戶所屬銀行在1~2個星期後才會收到解除警示公文，公文往返時間冗長及造成民眾不便。為有效警示帳戶的通報、管理以及解除機制，針對各機關間數位證據資料提供保全、保存及傳遞的架構及方法，使資料在不同機關間轉移利用時能依循數位證據監管鏈基本原則。本研究藉由區塊鏈智能合約機制導入法院、檢警調與金融機構，共同維護建置以太坊區塊鏈網路，以雲端資料庫系統作為儲存各類數位證據資料。透過智能合約條件觸發後自動解除警示帳戶的管制，減少民眾、法院、檢警調及金融機關因程序往返而耗費的時間，期望有效整合及提升行政效率。

二、文獻探討與基礎知識

1. 「警示帳戶」的基本概念

詐欺案件在國內日益盛行，為了有效杜絕犯罪嫌疑人利用金融人頭帳戶轉帳詐騙，財政部函請銀行商業公會於客戶開戶契約書中增訂「警示帳戶」條款，一旦被警察機關認定為進行犯罪的人頭帳戶，銀行將有權逕行終止客戶使用所有轉帳及提款卡服務，且提款卡將一併收回作廢。所謂的警示帳戶，指法院、檢察

署或司法警察機關因偵辦刑事案件(多為詐欺案件)需要進行通報，金融機構透過金融聯合徵信中心(以下簡稱聯徵中心)的警示帳戶網路，通報全國金融機構，金融機構會暫停「警示帳戶」全部交易功能，匯入「警示帳戶」的款項，也會遭到退回匯款銀行[2]。一旦被通報為警示帳戶，帳戶便會失去所有金融功能，不只是通報的銀行帳戶會被凍結，其名下所有的帳戶都無法使用。

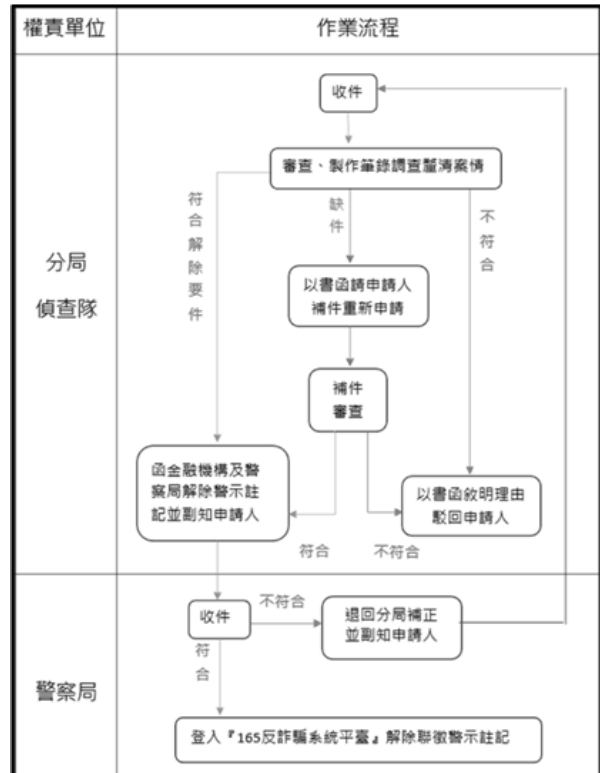


圖1: 警察機關受理詐欺案件通報(解除)警示帳戶流程圖

(1)何謂「衍生管制帳戶」

係指警示帳戶的所有人，開立的其他存款帳戶，包括警示帳戶銀行開立的其他帳戶以及在其他銀行所開立的存款帳戶。存款帳戶若屬「衍生管制帳戶」者，金融機構便會暫停帳戶語音轉帳、提款卡、網路轉帳以及其他電子支付功能的使用。衍生管制帳戶的設立是為了杜絕犯罪嫌疑人利用同一人在不同金融機構的其他帳戶繼續詐騙行為。鑒於金融機構對存款帳戶應善盡管理的責任，金融機構針對可能有問題的其他存款帳戶暫時停止款項的進出，匯入的款項也會退回匯款行。

(2)警示帳戶通報處理機制

民國94年4月警政署成立了「165反詐騙諮詢專線」提供民眾若接獲可疑電話時的諮詢、查證服務，成立之初常發生民眾撥打「165反詐騙諮詢專線」佔線之狀況。經內政部透過多

次跨部會反詐騙聯防會議，並邀請專家學者、電信業者、金融機關合力建置「165反詐騙聯防平台」將原本單純的諮詢專線與電信公司、金融機關等資訊結合，整合以往的人頭資料庫系統，並於民國97年4月正式成立啟用「金融機構警帳戶資訊交換平台」，各警察機關、派出所擁有了系統權限，就近提供民眾正確諮詢服務，員警於受理案件時即時將相關資料登載於該系統，可疑電話門號輸入後即由165平台專責人員進行驗證，一經查證明確屬詐欺電話最快30分鐘即可斷除通話，以避免更多民眾受害。金融帳戶部分，警察機關以電話、傳真或其他通訊方式，將「受理詐騙帳戶通報警示簡便格式表」通知金融機關將該存款戶列為警示帳戶，可疑帳戶的資料輸入平台查證後，由刑事警察局「165反詐騙諮詢專線」作為金融機構聯繫窗口供各警察機關調閱各項資料。165專責人員負責電信、帳戶資料，確保資料庫的完整性[18]。

(3) 警示帳戶聯防機制

依據「異常帳戶管理辦法」第七條第一、二項規定「存款帳戶經法院、檢察署或司法警察機關通報為警示帳戶者，銀行應即查詢帳戶相關交易，如發現通報之詐騙款項已轉出至其他帳戶，應將該筆款項轉出之資料及原通報機關名稱，通知該筆款項之受款行，並通知原通報機關。」、「警示帳戶之原通報機關依前項資料進行查證後，如認為該等受款帳戶亦須列為警示帳戶者，由該原通報機關再進一步通報相關銀行列為警示。」同條第四項將相關通知方式、通知範圍及所需文件等作業程序，授權由中華民國銀行商業同業公會全國聯合會訂定，經金融監督管理委員會（簡稱金管會）核備後執行，「金融辦理警示帳戶聯防機制作業程序」，業於95年11月起實施，透過該聯防機制維護民眾權益，即時有效阻斷民眾受詐騙款項的流出，以減少民眾損失。

(4) 金融機構辦理警示帳戶聯防機制作業程序

A、存款帳戶經通報為警示帳戶衍生之聯防機制：

(A) 警示帳戶所屬金融機構之通報窗口接獲法院、檢察署或司法警察機關（以下簡稱檢警調單位）開具之「受理詐騙帳戶通報警示簡便格式表」或相關通報公文等傳真文件通報警示帳戶時，除確認通報來源並依前述文件設定警示帳戶外，亦須查閱該警示帳戶內被通報之詐騙款項是否已轉出至

其他金融機構；如款項已轉出，應立即填寫「金融機構聯防機制通報單」傳真通知下一受款行之通報窗口。如款項已轉出至多家受款行，則須分別填寫「通報單」傳真通知各受款行。

(B) 受款之金融機構通報窗口在接獲前一受款行傳真之「通報單」，應立即查詢受款帳戶之交易，如款項已遭轉出，則接續填寫前一受款行傳真之「通報單」，將轉出資料傳真通報下一受款行及之通報窗口。如款項已轉出至多家受款行，則須影印前一受款行傳真之「通報單」並分別接續填寫，再傳真通知各受款行之通報窗口。如款項已遭提領，則須將通報單傳真回報檢警調單位。

(C) 受款之金融機構通報窗口在接獲前一受款行傳真之「通報單」，並應依「管理辦法」第七條第三項規定對該帳戶交易進行審慎查證，如查證受款帳戶確有犯罪事實者，則就被通報之受款金額做圈存或止扣；如帳戶餘額小於被通報之受款金額，則圈存帳戶目前餘額。

(D) 於圈存或止扣後，如接獲「檢警調單位回報受款行設定警示帳戶通報聯」通知該受款帳戶須列為警示帳戶，則改設定為警示帳戶。

B、存款帳戶經民眾通知，疑為犯罪行為人使用衍生之聯防機制：

(A) 受詐騙民眾於金融機構營業時間中，親自至任何一家金融機構櫃檯告知遭受詐騙時：

① 金融機構櫃檯人員於確認民眾身分、匯款或轉帳單據及瞭解民眾被詐騙事由後，請民眾填寫「切結書」並撥打165報案電話。

② 金融機構憑切結書及匯款轉帳相關單據填寫「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」，再將此通報單及切結書傳真至受款行之通報窗口。

③ 警察機關須於2小時內派員到金融機構受理民眾報案完畢並傳真「簡便格式表」至受款行之通報窗口。

(B) 受款行之通報窗口

① 憑金融機構傳真之「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」及「切結書」，確認通報來源。

② 立即查詢受款帳戶之交易，如款項已遭轉出則將款項轉出資料填寫於「金融機構聯防

機制通報單」，傳真通報下一受款行之通報窗口。如款項已轉出至多家受款行，則須分別填寫「通報單」傳真通知各受款行之通報窗口。

- ③如款項已遭全數提領，則立即填寫「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」下聯之受款行通報窗口之處理情形並傳真回報給受理報案之警察機關。
- ④受款行於接獲金融機構傳真之「金融機構協助受詐騙民眾通知疑似警示帳戶通報單」及「切結書」時，並應依「管理辦法」第五條第三款規定，對該受款帳戶交易進行審慎查證，如經查證確有不法情事者，則就被通報之受款金額做圈存或止扣；如帳戶餘額已小於被通報之受款金額，則圈存帳戶目前餘額。
- ⑤俟接獲警察機關傳真之「簡便格式表」或「檢警調單位回報受款行設定警示帳戶通報聯」通知須列為警示帳戶，始改設定為警示帳戶。

(C)後續受款行之通報窗口

- ①憑前一受款行傳真之「通報單」，確認通報來源。
- ②立即查詢受款帳戶之交易，如款項已遭轉出，則接續填寫前一受款行傳真之「通報單」，將款項轉出資料傳真通報下一受款行之通報窗口。如款項已轉出至多家受款行，則須影印前一受款行傳真之「通報單」並分別接續填寫，再傳真通知各受款行之通報窗口。
- ③如款項已遭全數提領(即最後一家受款行)，則將處理情形填寫於原「通報單」並傳真回報給受理報案之警察機關。
- ④受款行於接獲前一受款行傳真之「通報單」，並應依「管理辦法」第五條第三款規定對該受款帳戶交易進行審慎查證，如經查證確有不法情事者，則就被通報之受款金額做圈存或止扣；如帳戶餘額已小於被通報之受款金額，則圈存帳戶目前餘額。
- ⑤俟接獲警察機關回傳之「檢警調單位回報受款行設定警示帳戶通報聯」通知須列為警示帳戶，始改設定為警示帳戶。

2.證據監管鏈(chain of custody)

證據監管鏈的定義為用於維護和記錄證據時間歷史的過程，依據政府機關(構)資安事件數位證據保全標準作業程序，各機關基於資安事件之調查，需進行電腦系統之數位證據識

別、蒐集、擷取、封緘與運送作業時，適用本作業程序。故證據監管鏈原則係指需要確保數位證據的完整性、一致性，避免數位證據遭受竄改等不當行為發生[5]。

(1)數位證據特性

數位證據具有容易複製與修改、不易證實其來源完整性、無法直接被人類所感知及理解的內容、不易蒐集取得、容易偽造、變造、不易保存等特性。取得證據之程序更須小心謹慎，避免脆弱的數位證據因人為不當取證，而喪失證據能力及減弱證明力的成效[1]。

3.雲端運算(Cloud Computing)

近來因網際網路及寬頻無線網路的盛行，致使催生「雲端運算」服務的來臨。「雲端運算」緣起於1983年昇陽電腦所提出「網路是電腦」(The Network is the computer)的概念，將軟/硬體均視為資源，經由網際網路以服務的形式提供給使用者[7]。使用者可以不必負擔管理問題並依其需求從雲端中取得服務，與傳統自行建立的IT(Information Technique)模式不同。雲端運算是一個模式，透過網際網路存取設定好的共享運算資源池(如伺服器、儲存裝置、應用程式以及各類服務)。可以用最少的管理工作或服務供應商互動，進行快速配置和發佈。依據2012年5月NIST,美國國家技術標準局)所發布SP800-146建議書，指出雲端運算定義為無所不在使用、方便、隨需求應變的網路以及共享無限的運算資源等，如網際網路、伺服器、儲存、應用程式及服務，快速提供各項服務。

(1)雲端運算五大特性

(A)隨需自助服務(On-demand Self-service)

使用者可以依需求隨時取用雲端服務，如雲端資源或是雲端服務伺服器，不需再與雲端供應商進行互動聯繫。

(B)網路無所不在(Broad Network Access)

服務供應商可不受地域及時間限制在網路取用，且無論使用者平臺架構為何，皆可以透過網路存取標準服務機制進行。

(C)資源彙整(Resource Pooling)

供應商透過多重租賃模式(Multi-tenancy)服務，依據消費者需求，來提供實體及虛擬資源，在獨立所在地的概念下，消費者幾乎無法得知資源確切位置，大多只能知道國家、州或資料中心等範圍較大的地點。其中資源包括儲存、處理、記憶、頻寬和

虛擬機等。

(D)高度彈性(Rapid Elasticity)

彈性是指能依據消費者需求快速且彈性調整資源大小，對於消費者來說，所提供的資源規模幾乎是無限制的，隨時依據需求增加或減少資源額度。

(E)服務可計算(Measured Service)

控制最佳化、自動化與測量各類服務運算資源，如儲存、運算能力、頻寬與帳戶數等，服務提供商及消費者皆能監視與控制資源運用狀況。

4.區塊鏈演進、運作原理及應用

「區塊鏈」最早是由中本聰在2009年「比特幣：一種點對點的電子現金系統」文中所提出的其中一種技術，依據點對點網路、密碼學技術、時間戳技術、區塊鏈技術等理論構築。其是一個依據時序(Timestamp)的公開的交易紀錄，它可用檢驗交易是否出現「雙重支付」的情況。區塊鏈本身是一個信任機制，透過各種模型出現，如密碼學、數學、演算法等。區塊鏈技術為整合跨領域的應用機制，交易無需再透過第三方機構的認證，即使在交易雙方彼此互不信任狀態下，也能透過區塊鏈就能完成交易驗證[8]。

(1)區塊鏈演進

區塊鏈的演進分為三階段，其說明如下：

(A)區塊鏈1.0為中本聰所提出分散式帳本(去中心化)的概念，利用於支付系統與虛擬貨幣，並透過密碼學Hash值演算法取代了受信任第三方角色，難以被竄改的特性，資料的安全性與完整性得以保存在區塊上，節點在每一分散式帳本中維持一致性[15]。

(B)區塊鏈2.0為以太坊，它的基本技術與比特幣的區塊鏈技術相同，但其具有能自動執行的智能合約，被當作提前設定好的程式，當交易進行和事件發生的同時，只有符合事先設定好的事件及邏輯條件才可以繼續進行。

(C)區塊鏈3.0為超級帳本，它將區塊鏈應用技術與智能合約的功能進一步延伸，透過權限控制和安全保障，使運作更加精細，區塊鏈技術實現分散式帳冊整合跨行業開放標準平台，不只運用在經濟領域，也開發出許多新的設計與應用，如分散式身分驗證、電子票卷、醫療服務等。

(2)區塊鏈運作原理

區塊鏈技術的誕生，不僅打破以往傳統的交易模式，更利用在不同的產業及領域，不論如何運用其運作原理都與中本聰所提出所提的區塊鏈比特幣設計原理無太大差異[11]。

(A)點對點架構

區塊鏈為一個分散式資料庫，網際網路上的電腦或伺服器各個節點的參與者可以透過點對點相互連結通訊的網路來交易數位資產及儲存記錄[4]。點對點間存在著對等關係使多個不特定節點間得以建立通訊。

(B)時間戳記

區塊鏈是以交易驗證及時間戳記的方式儲存紀錄資料，交易紀錄是以「區塊」的方式儲存，每一區塊內含有不同雜湊函數、交易紀錄以及時間戳記等，其中每一區的塊雜湊函數是以隨機重新排列的方式產出，新的區塊鏈藉由交易證認紀錄方式疊加到舊有區塊鏈上，形成一塊具有許多區塊的長鏈。

(C)共識機制

共識機制具有規則性及安全性，雙方交易時需透過公私鑰進行加解密以及利用數位簽章達到安全性，每節點都須經過雙方驗證，共識演算法確認交易並決定由有那些人負責驗證這筆交易，透過這種方式使區塊保持了整條鏈最新共享狀態[9]。

(D)分散式帳本

交易中的區塊會被儲存在各個節點的分散式帳本中，即便區塊內其中一個節點故障損壞，亦可從其他節點的帳本來確認交易情形新的區塊會保存舊的區塊交易資訊(雜湊函數)，使區塊如同鏈狀方式互相連結組成區塊鏈。

區塊鏈中，所有的交易節點都儲存在一個分散式帳本中，即便其中一個交易節點受到破壞，其他的節點也可以證明交易紀錄，不會影響整條鏈的運作。點對點架構有助於紀錄區塊鏈交易訊息的不變性及完整性。分散式協議雖可以確認交易完整性，但也不是完全都不會被改變，有心人士可能會從中修改交易紀錄(如假造區塊、時間差等)致使區塊鏈產生不同結果。因此選擇較長的鏈，其擁有更多的資訊且更能被信任[16]。

(3)區塊鏈的應用

根據Casino進行區塊鏈應用的相關文獻研究發現[10]，自2017年開始，對於區塊鏈的研究大量出現，在工商業最為明顯。Casino將區塊鏈應用分為工商業、隱私與安全性、教

育、醫療、物聯網、政務、驗證、金融業、資料管理與雜項申請等10種。

(4)區塊鏈基礎技術

(A)工作量證明(Proof of Work, POW):

工作量證明被用於阻止拒絕服務攻擊(DDOS)、反垃圾信件等一些服務濫用的對策。第一個工作量證明運用於1996年Adam Bac所開發的“Hashcash”，垃圾信件的過濾使用工作量證明共識機制。工作量證明共識機制演算法採用SHA-256計算HASH值，其特點為難以計算，但卻相當容易驗證[3]。

區塊鏈上的節點可以透過工作量證明，快速驗證彼此是否擁有記帳權。採用了SHA-256運算Hash值，若改變Hash值的原始數據中的任何一部份，所輸出的Hash值也會隨之變化。

(B)雜湊運算

透過輸入任意長度的數值進行一定的計算，輸出端產生出一固定長度字串(圖2)。常見的演算法：MD4、MD5、SHA-1等，SHA-256為經常使用的雜湊函數，輸出端的輸出值長度為256bit（32byte）。主要的功能在於驗證及確保傳送資訊的正確性，避免訊息在傳送的過程中遭到破壞或竄改，以符合安全機制內的鑑定性需求[6]。

雜湊運算之三大特性如下

- ①單向雜湊函數，具有不可反逆性，無法在雜湊值中以最終輸出值反推輸入值。
- ②任意輸入值，固定長度輸出值。
- ③雜湊值碰撞率低。

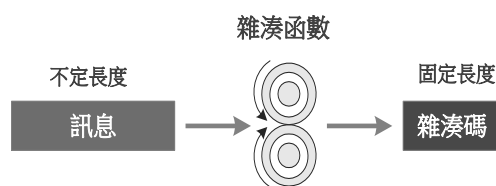


圖2:雜湊值運算

(C)數位簽章(Digital Signature)

為公開金鑰系統中重要的應用之一。它具有確定傳送訊息內容的「完整性」與傳送端的「不可否認性」功能，數位簽章是一種電子加密驗證圖章，用於電子郵件、巨集或電子文件等數位資訊。簽章可以確認資訊來自簽章者，且未遭到竄改。數位簽章運用於電子文件時，用以確認電子文件的簽章者的身分與電子文件內容是否相符，類似簽名的概念。數位簽章使用非對稱式密碼系統，以公開金鑰系統並具有確認性、完整性及不可否認性。傳送方及接

收方各具有一對金鑰，一把為公開金鑰，另一把為私密金鑰。

(D)共識演算法

共識機制為區塊鏈領域重要的議題之一，自比特幣的工作量證明開始，便不斷的改進現有的共識機制，其目的是為了讓區塊鏈效能更加優化，且在速度、安全性以及去中心化三者之間達成平衡。區塊鏈中的節點參與數據記錄，防止惡意節點阻擋訊息或傳送不正確資料，且為確保記錄同一份的正確數據，故須採用共識演算法。

(E)智能合約(Smart Contracts)

智能合約是區塊鏈中所使用的特殊協議，一種自動執行的合約，將雙方的協議條款寫入代碼中。常見的智能合約是應用在加密換幣合約中，建構一個智能合約快速運行於以太坊上的新加密代幣。另一用途智能合約也可用作各式自動服務機構。透過分散在各地節點上運作的智能合約，運作與決策都是公開、公正透明的，降低了交易的不確定性，以太坊(Ethereum)上的智能合約使用Solidity語言來撰寫。撰寫好Solidity程式碼(.sol)後，將程式碼編譯成EVM（Ethereum Virtual Machine）能讀懂的二進位Contract ByteCode後才部署到以太坊的區塊鏈上執行(圖3)。區塊鏈上的智能合約包含事件處理、資料儲存以及狀態機制，必須在鏈上進行保存。一旦條件觸發，智能合約便能採取相對應措施，保存鏈上資料的完整性[12]。

Solidity 語言中的 payable 屬性限制 function，虛擬貨幣才可以使用。透過對使用者權限的記錄方法為Solidity的mapping型別，將使用者身份與其各自權限做對應，權限管理合約的目的為記錄使用者建立的權限管



理資訊與應用，並對其進行管理的操作。

圖3:區塊鏈上的智能合約運作模式

(F)區塊結構

區塊鏈(Blockchain)是由複數個區塊(Block)所組成(圖4)，其基本結構是以區塊為單位，包含了元資料(Metadata)的區塊頭(Block Header)和交易資料的區塊體(Block Body)所構成。區塊體中儲存許多資訊，包含交易資料及前一區塊的連結[14]。

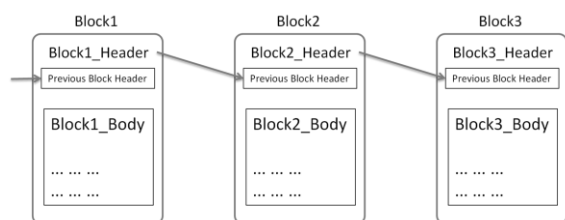


圖4:區塊鏈結構

(G) 區塊鏈分類

根據區塊鏈性質、傳送範圍、功能設計及結構區分，區塊鏈歸納為為公有鏈、私有鏈及聯盟鏈等三種[9][13]。

① 公有鏈

公有鏈採取公開透明方法任何人皆可參與區塊鏈內運作，如區塊鏈內容讀取、傳送等，資料內容公開透明，高度去中心化無須透過中央機構，運作方式皆在公開的網路環境下運行，形成高度可信任的網路系統。比特幣、以太幣等加密貨幣皆使用公有鏈機制進行。

② 私有鏈

指須授權才可進入不對外開放，僅可在組織內部使用，需進行身分驗證具備完善管理系統，用於獨立單位、單一機構內部使用，提升機關間內部交流的效率，具有相當中心化的系統。因此，交易速度較公有鏈快、內部具有隱私性、交易成本低等，私有鏈的設計使得資料內容數據較難以竄改，縱使遭到修改也可追蹤到修改方。

③ 聯盟鏈

為私鏈的一種，但不同之處在於一般私鏈類似於單一服務的公司，而聯盟鏈則是聚焦於多家組織公司與產業之間的服務。身分認證及許可權管理較為嚴格，一定時間內的節點數量是確定的，適用於組織間需達成共識的業務。

三、 解決方案—自動化警示帳戶之解除

1. 司法程序終結文書及其處理流程

(1) 解除警示帳戶具備文書

警示帳戶之解除，須填具解除警示帳戶申請書外，應檢附相關司法文書及執行完畢之證明，檢附資料如下說明

(A) 不起訴處分：須檢附不起訴處分書。

(B) 無罪判決：須檢附無罪判決書。

(C) 罰金：

① 單純裁判罰金處分。

② 單純裁判罰金處分未能完納，遭強制執行或易服勞役執行完畢者，須檢附判決書強制執行或易服勞役執行完畢證明。

(D) 判刑執行完畢：

① 徒刑執行完畢須檢附判決書及出監證明書。

② 科處罰金並繳納完畢者，須檢附判決書及罰金繳款收據。

③ 受拘役或罰金之宣告，易以訓誡者，須檢附判決書及易以訓誡執行完畢證明。

④ 經法務部准許假釋者，須檢附相關證明文件。

(E) 緩起訴：須檢附緩起訴處分書及緩起訴附負擔或指令執行完畢證明。

(F) 緩刑：

① 單純宣告緩刑者，須檢附判決書。

② 宣告緩刑並附帶緩刑負擔或指令者，須檢附判決書及緩刑負擔或指令執行完畢證明。

(G) 保護處分：按少年事件處理法第42條第1項有關保護處分之規定。

① 訓誡，並得予以假日生活輔導。

② 交付保護管束並得命為勞動服務。

③ 交付安置於適當之福利或教養機構輔導。

④ 令入感化教育處所施以感化教育。

(2) 警示帳戶解除流程

警政署為迅速協助民眾解除之申請，業於100年3月11日警署刑偵字第1000001185號函檢送修正「民眾解除警示帳戶申請書」供各警察機關配合辦理。民眾遭冒名申辦開戶之解除警示，申請人應攜帶證明身分證件資料及聯徵中心之信用報告書親赴管轄警察機關，請求協助調查及解除相關事宜。民眾因一般商業交易糾紛、存款帳戶遭盜用或遭誤設警示案件，應檢附有關證明文件親赴戶籍地之警察分局偵查隊主動接受調查，以釐清誤設原委。司法程序終結案件之解除警示，應檢附身分證件資料、刑事判決書、執行完畢證明或罰金繳納收據影本，親送或郵寄至各地警察分局偵查隊辦理(圖5)。

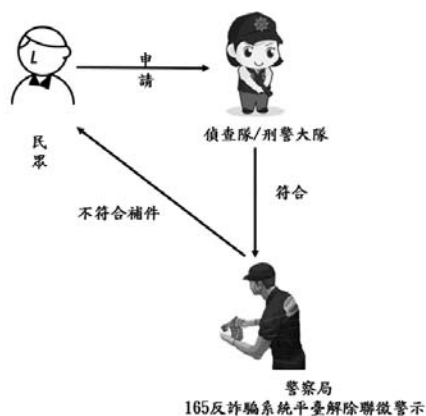


圖5：警示帳戶解除流程

2. 區塊鏈及雲端運算結合智能合約用於金融警示帳戶

法院、檢警調及金融機關將相關資料(司法文書、警示帳戶解除申請書、金融機關通報單等)數位化並利用區塊鏈演算法取得Hash值後導入區塊鏈中,藉由區塊鏈技術分散式帳本技術,使數位證據資料在各節點上都可以進行讀取,縱使其中一節點端故障或是被修改,都能於其他節點讀取或是認證,以確保原始證物狀態。利用智能合約來實現交易合約中的條款與條件設定及條件驅動,使警示帳戶在符合相關條件後自動解除。使用者在鏈上的所有活動皆會被紀錄,數位證據資料在辨別、保存、傳遞及檢驗利用的過程更加方便,花費的時間成本也將大幅下降,進而保障民眾的權益。

隨著警示帳戶案件的增加使得案件資料量增多,將數位證據資料儲存在區塊鏈上後,並上傳至雲端金融警示帳戶資料庫中進行儲存,其資料儲存空間相當大,且區塊鏈之分散式帳本可讓數位證據資料具有備援效果,使數位證據資料能妥善保存、利用。

(1) 數位證據資料上傳雲端金融警示帳戶資料庫

警示帳戶相關數位證據資料,經由法院、檢警調及金融機關蒐集彙整後,需透過完善的監管機制使證據文書具有法效性,用以證明是否得以解除警示帳戶之條件。透過區塊鏈技術將取得之數位證據資料上鏈,並以證明所取得之據證資料未遭到竄改及破壞。

為使各機關間在調閱相關事證及文書上能有效地傳遞利用,各機關須將完整蒐集且上鏈之數位證據資料傳送至雲端金融警示帳戶資料庫保存(圖6)。透過身分驗證機制,使有權限之機關才得以調閱、下載雲端金融警示帳戶資料庫內證據,輔以各單位在偵查期間調閱

證物之方便性以及建立各單位間對於案件資訊傳遞有良好平台。

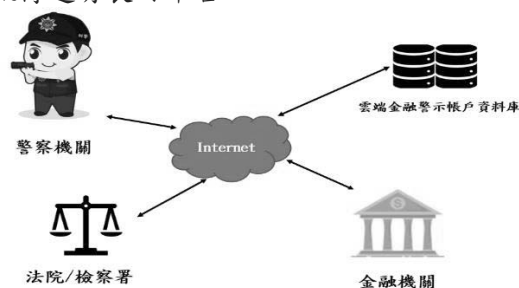
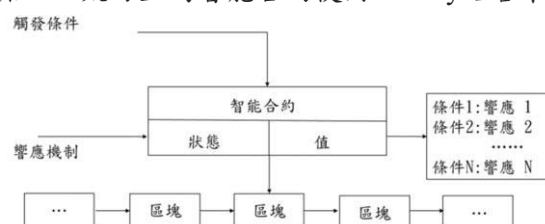


圖6：雲端金融警示帳戶資料庫

(2) 智能合約

分散在各地節點上的智能合約,其運作與決策都是公開、公正透明的,降低交易的不確定性。以太坊上的智能合約使用solidity語言來



撰寫。撰寫好solidity程式碼(.sol)後可部屬到區塊鏈上執行。智能合約可以自動執行電腦程式(圖7),區塊鏈上的智能合約必須在鏈上進行保存。一旦條件觸發,智能合約便能採取相對應措施,保存鏈上資料的完整性。

圖7：智能合約運作流程

(3) 聯盟鏈

介於公有鏈及私有鏈之間,使用者須是被授權的人或是機關才得以參與共識機制,具備完善管理系統,效率高、成本低及保障性好、交易速度快、內部具有隱私性等。只有獲得對方的授權金鑰才可以看到其他參與者的數據資料,有效解決安全性及隱私性問題實現去中心化。聯盟鏈的設計使得資料數據傳輸具安全性較難以竄改,若是遭到修改也可追蹤到修改方。因此提供保障證據資料的安全性、一致性,故採用聯盟鏈模式,驗證身分及授權各項權限。

(4) 雲端運算

最主要的應用之一是「雲端儲存」,可以隨時隨地存取檔案和文件,虛擬化技術將資源分割利用,規劃出不同層級的虛擬化資源,建置雲端運算基礎環境使數位證據透過區塊鏈加密上鏈後上傳至雲端金融警示帳戶,確保數位證據在雲端系統上之穩定度與效能。

(5) 數位簽章

其加密技術為非對稱式加密法，發送端及接收端，皆有一組公鑰及私鑰，簽名時使用私鑰，驗證時使用公鑰，將數位簽章用於交易程序中，佐以證明交易者身分。法院、檢警調及金融機關發送交易（警示帳戶相關資料）時，交易內容以本身私鑰簽屬，並將簽屬內容加到在交易中。其他節點收到訊息後，將數位簽章進行驗證，驗證完畢及確認發送者身分，交易才會繼續進行。

3.系統實作

使用Go語言開發go-ethereum（簡稱為geth）作為警示帳戶數位證據資料區塊鏈節點應用程式，智能合約以Solidity程式語言實作，使用者介面透過Java應用程式搭載web3j套件。web3j為一個高度模組化且安全性高，Java類庫提供豐富API，運用於處理以太坊智能合約及以太坊的客戶端（節點）整合。透過編碼將警示帳戶案件相關數位證據資料的雜湊值存於區塊結構中，新區塊記錄舊區塊上的位置並且串連起來成刑案數位證據區塊鏈，並保有同副本資料，以確保資料的一致性與完整性。

建立警示帳戶數位證據資料區塊鏈平台架構分為：開發構建新節點、數位證據資料建檔、數位證據資料傳送與接收，說明如下。

(1)開發構建新節點

使用者先至Go Ethereum網站（<https://geth.ethereum.org>）取得節點應用程式，下載並安裝（圖8）。

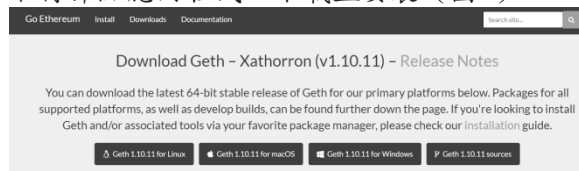


圖8：節點程式檔案下載

使用者為法院、檢警調、金融機關等，使用者的電腦藉由網路相互連接，形成以太坊網路共同維護、保存數位證據資料（圖9）。利用Geth架設警示帳戶數位證據資料區塊鏈Node，架設四步驟為：1.建立創世區塊鏈文件、2.建立Chain帳號、3.連結其他Node並取得資訊、4.建立一個完整的共識系統。Geth建立完成之後，使用者可以得知參與節點數量及狀態。區塊鏈在系統管理權限上也較為完備與公有鏈不同的是，其節點數量像相對較少。因此，系統具有更好的效能及隱私安全；且管理系統能得知參與者數量及節點狀態，節點數遠小於公有鏈，因此具備更高的效能與更好的隱

私安全。在區塊鏈內，資料無法隨意變更修改，即便資料被竄改或刪除，也能追查到修改方，並追究其法律上之責任。

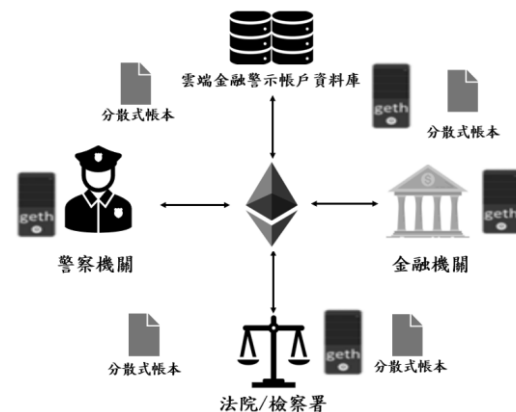


圖9：以太坊網路圖

(2)雜湊值建檔

將警示帳戶數位證據資料以SHA-256雜湊函數取其雜湊值，不起訴處分、無罪判決、刑執行完畢須檢附判決書、金融機關警示帳戶資料、民眾解除警示帳戶申請書等資料，將其各自取得雜湊值，使資料為具有雜湊值的集合並存在鏈上。

(3)雜湊值傳送

傳送方使用本身之私密金鑰加密警示帳戶數位證據相關資料後上傳至警示帳戶數位證據區塊鏈平台，傳送方各自具有以太坊網路節點、證據資料庫及應用系統，傳送者會以公開金鑰確認資料傳送者的身分。

(4)雜湊值接收

接收方經由區塊鏈功能驗證資料傳送方身分資訊，正確無誤後將雜湊值紀錄於智能合約，透過智能合約設定進行讀取、修改及製作警示帳戶數位證據相關資料。

四、模擬案例探討

1.模擬案例說明

民眾甲於社群媒體臉書與民眾乙進行商品之交易，因近期疫情肆虐導致商品運送遲誤無法在預定期間內交貨，民眾乙認為自己上當受騙，因此至警察機關報案（詐欺案），進而導致民眾甲的金融帳戶遭警方通報設立為「警示帳戶」，以致甲名下帳戶失去所有金融交易功能且無法正常使用。

俟案件審判終結後，因民眾甲對於解除警示帳戶流程不甚瞭解以致名下的帳戶遲遲無法正常使用而影響其權益甚鉅。故本研究透過

區塊鏈智能合約應用，警示帳戶案件審判終結或達成解除條件後自動解除帳戶警示。

2.系統應用

(1)利用區塊鏈及雲端技術保全(存)警示帳戶數位證據相關資料

法院、檢警調及金融機關，將詐欺案件相關資料(如案件偵辦書、不起訴書、解除帳戶通報單等)傳輸至數位證據區塊鏈及雲端金融警示帳戶資料庫。

(A)法院、檢警調及金融機關將所蒐集的數位證據(案件偵辦書、不起訴書、解除帳戶通報單等)傳送至數位證據區塊鏈平台並利用SHA-256演算法，對所蒐集的數位資料進行雜湊運算，取得雜湊演算法產生的專屬雜湊值。

(B)法院、檢警調及金融機關利用本身的私密金鑰對所要傳送的數位資料雜湊值進行加密後上傳至區塊鏈，區塊鏈上產生多個集合的雜湊值，完成上鏈及加密後的數位證據傳送至雲端金融警示帳戶資料庫進行保存。

(C)其他機關如分局偵查隊或金融機關接收到廣播消息後，利用法院、檢警調及金融機關之公開金鑰進行確認，完成確認並驗證傳送者身分，該交易才會觸發後續證據製作流程。

(2)智能合約系統設定達到警示帳戶解除

(A)智能合約系統設定應用程式的邏輯，來實現交易合約中的條款與條件，由法院、檢警調負責製作數位證據監管鏈表，藉由各機關人員所上傳之案件相關證據(如案件偵辦書、不起訴書、解除帳戶通報單等)對數位證據進行案情研判、分析案件歸屬。

(B)如資料需修改，由法院、檢警調將資料修改編輯後再上傳一次，以便各單位進行資料確認及驗證。

(C)數位證據監管表製作完成後，利用SHA-256演算法取得其雜湊值，將數位證據監管表雜湊值以本身私密金鑰加密上鏈，並廣播至各節點供驗證其正確性。

(D)當各節點驗證數位證據監管表內登載之內容正確無誤，便完成數位證據傳遞間安全性之保障。

(E)當偵查機關對各項證據資料驗證完畢並達成智能合約所設定的觸發條件後，由金融

機關自動解除帳戶的警示，使帳戶恢復各項金融交易功能。

五、結論及後續研究工作

詐欺案件相關數位證據資料於傳輸時導入區塊鏈技術，透過加密方式後上傳資料並以分散式儲存，保障資料的一致性、完整性、不可竄改性，使數位證據資料具有證明力，提升資料驗證的能力及縮短工作時間。數位證據區塊鏈及雲端金融警示帳戶資料庫之應用，促使各偵查單位間在傳輸、製作及儲存數位證據能力更為提升並確保資料完整性及傳遞運用方便性。

後續研究期望將區塊鏈及雲端技術結合智能合約用於金融警示帳戶導入各偵查機關及金融機關中，使各機關間在資料傳輸、證據保全及運用能力更加提升。透過智能合約條件觸發後自動解除警示帳戶的管制，減少民眾、法院、檢警調及金融機關因程序往返而耗費的時間，有效整合及提升行政效率。

六、參考文獻

- 1.王逸嵐，區塊鏈在交通事故數位證據保全上的應用，中央警察大學第二十四屆資訊管理學術暨警政資訊實務研討會論文，2021年，第2-8頁。
- 2.王怡婷，警示帳戶通報處理機制之研究，中央警察大學刑事警察研究所碩士論文，2009年，第7-24頁。
- 3.田箴照博，「區塊鏈的整體概念」，區塊鏈智慧合約開發與安全防護實作，旗標科技股份有限公司，台北市，2018年，第1-2~1-8頁。
- 4.李柏諭，利用區塊鏈技術防止媒體散播假新聞，國立高雄科技大學資訊工程系(所)碩士論文，2020年，第4頁。
- 5.李崎維，區塊鏈及雲端技術在刑案數位證據保全之應用，雲林科技大學第二十六屆國際資訊管理暨實務研討會論文，2021年，第15-16頁。
- 6.吳順裕、粘添壽，資訊與網路安全技術，旗標，臺北市，2004年，第11-26頁。
- 7.吳翊銘，M-POLICE警用行動電腦整合雲端應用與資訊安全問題探討，中央警察大學

- 數位鑑識與科技偵查研討會論文，2014年，第3-4頁。
8. 華為區塊鏈技術開發團隊，區塊鏈技術原理，區塊鏈技術與應用，五南圖書出版股份有限公司，台北市，2020年，第36-38頁。
 9. 華為區塊鏈技術開發團隊，區塊鏈技術原理，區塊鏈技術與應用，五南圖書出版股份有限公司，台北市，2020年，第73-81頁。
 10. 翁嘉好，基於區塊鏈之數位鑑識證據監管鏈，國立政治大學資訊科學系碩士論文，2019年，第20-21頁。
 11. 賴寒彰，區塊鏈探討與應用，國立高雄第一科技大學資訊管理系企業電子化碩士班碩士論文，2017年，第11-16頁。
 12. Buterin, V., "A Next-Generation Smart Contract and Decentralized Application Platform", white paper, 2014.
 13. Casino, F., Dasaklis, T. K. and Patsakis, C., "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues", Telematics and Informatics, Vol. 36, 2019, pp: 55-81.
 14. Nofer, M., Gomber, P., O. Hinz, and Schiereck, D., Blockchain, Business & Information Systems Engineering, Vol. 59, No. 3, 2017, pp: 183-187.
 15. Pilkington, M., Blockchain Technology: Principles and Applications", Research handbook on digital transformations, Vol. 225, 2016.
 16. Swan, M., Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.
 17. 行政院金融監督管理委員會，網址：http://www.fscey.gov.tw/news_detail2.aspx?icuid=34362，存取時間：2022.03.18。
 18. 臺北市政府警察局，申請解除警示帳戶作業流程。<https://police.gov.taipei/>，存取時間：2022.04.24
 19. 警政統計年報，警察機關受(處)理刑事案件統計。<https://www.npa.gov.tw/ch/app/data/list?module=wg056&id=18128>

數種具元宇宙元素平台應用程式之數位鑑識初探

鄧思源

法務部調查局臺北市調查處 組長

mjib.teng@gmail.com

摘要

元宇宙為由虛擬空間組成的 3D 數位世界，主要聚焦於社交連結，人們可以在虛擬世界中透過代表建立的虛擬替身進行活動，並與現實世界同步。元宇宙係以使用者為中心，使用者可以自行開發或製作內容與物件，並且進行販售與獲得收益。元宇宙概念較新，因此其大部分功能仍在開發中。Facebook(Meta)、Microsoft 和 Nvidia 等公司也開始建立其元宇宙版本。目前 Decentraland、The Sandbox、Axie Infinity及Roblox等電玩和虛擬資產平台已在其生態系統中實作某些區塊鏈及加密貨幣等元宇宙元素。由於元宇宙概念平台的迅速發展，使更多用戶開始投入大量資金到元宇宙平台上，以致駭客增加對流行之元宇宙平台進行網路釣魚攻擊的頻率，非同質化代幣(NFT)是元宇宙經濟的核心，目前 NFT 騙局無處不在，最常見的 NFT 騙局之一是 Discord 駭客攻擊，透過虛假的 Discord 鏈接要求受害者提供助記詞以便從加密錢包中騙取貨幣，在元宇宙平台亦有可能遭到被駭或被深偽(DeepFake) 技術操縱看起來或聽起來像某些我們所熟悉之數位人物詐騙。因此本研究嘗試對目前市面上較流行的元宇宙概念平台應用程式進行基本數位鑑識與分析，以解析當犯罪者透過這些平台進行網路犯罪活動時，鑑識人員如何從涉案之個人電腦或行動裝置識別、蒐集、分析與檢視相關之數位跡證。研究範圍以 4 種元宇宙概念平台應用程式作為研究標的，並選定以微軟視窗桌面作業系統及Android行動裝置作業系統作為實驗平台，整理及歸納出相關數位痕跡與特徵，結果顯示鑑識人員可由檔案系統、記憶體、瀏覽器、應用程式資料庫及網路封包等資料中採集到相關特徵資料，以作為犯罪事證之數位證據。

關鍵字: 元宇宙平台鑑識、數位證據、加密貨幣調查、數位鑑識、數位跡證。

一、前言

隨著Facebook (Meta)、Microsoft 和 Nvidia 等公司宣佈建立其元宇宙版本，為了提供身臨其境的元宇宙虛擬體驗，許多科技公司整合區塊鏈、擴增實境(AR)和虛擬實境(VR)、3D 重建、人工智慧(AI) 和物聯網(IoT)等尖端技術來推動 3D 世界的發展，使得具宇宙元素之各類平台商品發展多樣化，也讓更多用戶開始投入更多資金到不同的具元宇宙元素之平台，使得元宇宙元素商品市場成為最受歡迎的新興投資市場，也成為駭客覬覦的目標。各類駭侵活動時有所聞，例如由 Axie Infinity 元宇宙遊戲平台開發商 Sky Mavis 所建立一個能與以太坊相容的區塊鏈網路，也是該遊戲使用的側鏈錢包 Ronin 網路，於 2022 年 3 月 23 日，遭駭客使用外洩的私有密鑰偽造提款，共偷竊 173,600 個以太幣(ETH)及 2,550 萬美元穩定幣(USDC)，價值總計約 6.25 億美元[1]。著名的元宇宙遊戲和遊戲創作平台 Roblox，亦發生駭客透過 Discord 與 Roblox 用戶共享，發動網路釣魚

攻擊，讓受害者的電信營運商被誘騙向駭客控制的 SIM 卡發送簡訊及電話，使駭客能繞過 2 階段驗證保護，並更改用戶的密碼，入侵後使用偽造的 Paypal 螢幕截圖來控制目標帳戶，使 Roblox 公司誤認駭客就是帳戶所有者，這些被駭客盜竊之貴重物品，就會在許多未經授權的 Roblox 黑市上出售[2]。NFT 是元宇宙經濟的核心，許多元宇宙平台及市場使用 NFT 作為遊戲內代幣和收藏品，與比特幣和以太幣等加密貨幣不同，NFT 不能相互交易，因為每一種都視為一種獨特的實物資產。正如犯罪分子利用非加密遊戲貨幣一樣，基於區塊鏈的資產也越來越多地被用於洗錢，NFT 市場越來越成為犯罪分子通過複雜的網路釣魚攻擊和詐騙來誘騙受害者的熱門目標[3]。駭客對這些品牌元宇宙平台進行網路釣魚的攻擊頻率，最常見的 NFT 騙局之一是 Discord 駭客攻擊，透過虛假的 Discord 鏈接要求受害者提供助記詞以便從加密錢包中騙取貨幣，在元宇宙平台亦有可能遭到被

駭或被深偽(DeepFake) 技術操縱看起來或聽起來像某些我們所熟悉之數位人物詐騙[4]。

因此不法犯罪者對這些流行的具元宇宙元素平台進行網路犯罪活動時，並嘗試隱匿及規避犯罪調查時，鑑識人員如何從涉案之個人電腦或行動裝置識別、蒐集、分析與檢視相關之數位跡證。研究範圍以

「Decentraland」、「The Sandbox」、「Axie Infinity」及「Roblox」等 4 種具元宇宙元素平台應用程式作為研究標的，並選定以微軟視窗桌面作業系統及Android行動裝置作業系統作為實驗平台，整理及歸納出相關數位痕跡與特徵，結果顯示鑑識人員可由檔案系統、記憶體、瀏覽器、應用程式資料庫及網路封包等資料中採集到相關特徵資料，以作為犯罪事證之數位證據。

二、相關文獻與背景知識

目前對元宇宙與網路犯罪有關之研究可概分為三大部分，其一為對具元宇宙元素之虛擬網路空間，可能所導致之犯罪類型與防制之探討，其二為與元宇宙安全性及隱私權之探討，三為如何應用元宇宙技術來協助犯罪調查與鑑識的研究，Mackenzie(2022) 對元宇宙帶來的新興加密貨幣市場與灰色加密經濟之另類金融系統，幾乎完全沒有犯罪控制且充滿騙局，提出犯罪學的探討與研究[5]。Song等人(2022)對元宇宙虛擬世界之Roblox或Zeppetto等遊戲平台中發生的犯罪類型進行分類，並制定犯罪預防策略及提出相對其法規和法律修訂等各種制度性補充機制[6]。d'Argenlieu(2022)認為隨著元宇宙或Web 3.0的出現，恐怖分子將會利用這個新興 3D數位世界，出現招募和攻擊計劃的可能性，執法單位需要一套新的法律、法規和能力，以確保用戶安全並防止將元宇宙平台用於恐怖目的[7]。Osivand(2021)對元宇宙構建元素，例如虛擬場景和角色、聽覺、文本元素等計算藝術所涉及之加密貨幣進行全面調查[8]。Wang等人(2022)認為元宇宙繼承的底層技術或在新生的數位生態中存在嚴重的隱私權侵犯和安全漏洞問題，加上虛擬世界的內在特徵，使得安全配置上可能出現一連串的挑战，進而阻礙其廣泛部署。因此，需要對未來元宇宙系統及平台構建制定對策[9]。Zhao等人(2022)從元宇宙中的用戶訊息、通信、場景、商品等 4 個角度分析可能存在的安全和隱私問題，並提出需要從哲學的角度全面解決安全和隱私問題[10]。Priestley(2021)認

為可以使用元宇宙的虛擬世界來模擬犯罪現場，為法律系統和陪審團創造一個身臨其境的环境，從多個角度瞭解犯罪行為[11]。

上述研究並未針對主流使用之元宇宙平台應用程式以數位鑑識之角度，探討該等平台如涉及網路犯罪時，如何識別及蒐集應用程式所留存之數位跡證，亦欠缺系統性的整理。因此本研究針對目前較流行 4 種具元宇宙元素平台之應用程式進行相關實驗，並嘗試提出一系統性的鑑識框架與鑑識特徵，以供調查或鑑識人員在從事該等數位證據取證作業時參考。

2.1 Decentraland 元宇宙平台簡介

虛擬房地產平台Decentraland於 2016 年在阿根廷創立，是一個由以太坊區塊鏈推動的去中心化虛擬實境平台，為目前最古老的元宇宙平台之一。在平台內，用戶可以創建、體驗他們的內容和從應用程式中獲利。在平台中稱 90,601 個不同的 3D 虛擬空間為地塊(LAND)，一種由以太坊智能合約維護之不可替換的數位資產，每個地塊都以不可替代的代幣 (NFT)表示，並以笛卡爾坐標標識。以太坊區塊鏈用於維護土地所有權，這些地塊由社區成員永久擁有，並可以Decentraland 原生加密貨幣 MANA 購買，用戶必須將其 MANA 代幣保存在以太坊錢包中，土地交易就是 NFT 交易。用戶可以使用構建器在自己的土地上創建自己的 3D場景到更具交互性的應用程式或遊戲。一些地塊進一步組織成主題社區或地區。通過將地塊組織成區域，社區可以創建具有共同興趣和用途的共享空間，而所有權和交易在以太坊區塊鏈上進行驗證[12]。

2.2 The Sandbox 元宇宙平台簡介

Pixowl 遊戲工作室在 2011 年推出 Sandbox行動遊戲平台以對抗玩家眾多的Minecraft遊戲，其後，在 2020 年推出用戶原創內容的平台專案，玩家可以在網站上使用VoxEdit 和 Game Maker等應用程式，建構並創造他們專屬包括頭像、虛擬商品，甚至是整個遊戲的非同質化代幣 (NFT)，讓用戶不僅能夠使用虛擬商品與其他玩家互動，還可以在 Sandbox 市場上交易這些 NFT 來賺取收益，成為一款邊賺邊玩的區塊鏈遊戲，不同於其他受歡迎的邊賺邊玩遊戲，Sandbox 沒有預先打造遊戲世界，而是讓玩家免費使用

便利的工具來自訂一切。Sandbox 市場是 NFT 市場，可讓用戶使用 Sandbox 供給量 30 億枚 SAND 的 ERC-20 代幣來交易遊戲內資產 (ASSETS)。取得 ASSETS 後，用戶即可運用 Game Maker 在 LAND(以太坊區塊鏈上獨特的 ERC-721 代幣) 將數位房地產加以合併，進而創造出獨一無二的遊戲。這些 NFT 可以是實體、建築物、穿戴式裝置等更多項目，而且都可以在 Sandbox 平台中使用 [13]。

2.3 Roblox 元宇宙平台簡介

Roblox 平台成立於 2004 年，目前在全球擁有 4700 萬用戶和 950 萬開發者，用戶大部分是青少年和兒童，Roblox 在 2020 年推出大型多人線上遊戲開發元宇宙共享平台，提供工具和平台供開發者自由創作沈浸式的 3D 遊戲，及由玩家使用自己的頭像創建獨特數位身份來進行社交，允許設計自己的遊戲、道具和服裝，並可遊玩自己和其他開發者所建立的各種遊戲。遊戲中可以使用該平台所發行的 Robux 代幣購買、出售和交易平台內的遊戲和道具等商品，也可以兌換成實體世界中的貨幣，以上這些要素都非常接近元宇宙 [14]。

2.4 Axie Infinity 元宇宙平台簡介

2018 年 3 月越南工作室 Sky Mavis 發行一款建立在以太坊區塊鏈上的寵物對戰遊戲平台 Axie Infinity，在遊戲中玩家可以培育和繁殖以 NFT 形式發行，名為 Axie 的數位寵物，並透過交易和戰鬥獲取寵物。藉著區塊鏈技術的協助，開發一套基於以太坊的 Ronin 側鏈錢包，協助玩家創建遊戲帳戶、購買 Axies、轉移遊戲獎勵代幣 SLP 和遊戲治理代幣 AXS 代幣。Axie 營運著一種全新的玩遊戲賺錢 (Play-to-Earn) 模式，玩家只要在遊戲投入精力和時間就能從遊戲機制和生態體系中獲得獎勵。要加入遊戲，玩家必須先把實體世界的貨幣兌換成以太幣並購買 3 隻 Axies，跟其他遊戲購買虛擬角色或是道具不同，玩家能獲得 Axie 的所有權，在遊戲中玩家可以自由決定是否要持續戰鬥破任務賺取 AXS 及 SLP，或是將 Axies 和代幣兌換成實體貨幣變現後離開，Axie Infinity 虛擬世界中的土地也是可交易的，在 Lunacia 大陸上會生成怪獸和遊戲代幣。每一塊土地都是一個 NFT 並開放拍賣 [15]。

三、具元宇宙元素平台應用程式之鑑識價值

隨著具元宇宙元素平台之玩家人數與日俱增，因此也衍生出與之有關之網路犯罪問題，在案件發生後，如何在應用程式安裝之用戶端裝置中找尋有關之數位跡證以供調查，即為本研究之目的。本研究以簡易鑑識步驟及程序，並以提出之鑑識工作框架，用於識別、擷取與蒐集、檢驗與分析用戶端使用此類應用程式後可能留存之數位跡證，用以認定相關犯罪事實。

四、具元宇宙元素平台應用程式之鑑識方法與框架

4.1 鑑識方法

本研究實驗之桌面平台為於 VMware Work-station V16.2.3 軟體上分別安裝 Microsoft Windows 11 之虛擬機，在 Android 行動裝置方面則以 Asus ZenFone 3 (Android 8) 及 LDplayer V4.0 1150 模擬器作為實驗平台，實驗之應用程式版本及支援平臺如表 1，實驗之鑑識工具與版本如表 2。本研究實驗設計重點可分為：(1) 在桌面系統、行動裝置及網頁瀏覽器中安裝及使用實驗之元宇宙平台應用程式，並觀察檔案系統中存有那些具有鑑識價值之資料；(2) 觀察桌面系統、行動裝置及網頁瀏覽器在連網使用時之網路封包，分析連線 IP 與網站等資訊；(3) 個別觀察應用程式特有的功能，並進行鑑識分析，找出具鑑識價值之數位跡證。

表 1、實驗之作業系統與元宇宙遊戲平台版本

作業系統\軟體名稱與版本	Decentraland	The Sandbox(maker)	Roblox	Axie Infinity
Windows 11	V0.1.37.0	V0.6.24(1053)	V2.423.63880.0.	V1.2.3
Android 8	No	V1.99981	V2.526.426	V1.1.3
LD Player Emulator v4.15(Android 7.1)	No	V1.99981	V2.526.426	V1.1.3

表 2、鑑識分析工具與版本

作業系統版本	檔案系統、網路封包鑑識 安裝之應用程式與瀏覽器鑑識	記憶體(含程序記憶體)鑑識	應用程式資料庫鑑識
Windows 11 Enterprise Evaluation	X-Ways Forensics v19.9, SysTracer v2.1.0, FolderchangeView v2.32	Wireshark v3.6.5, Http Analyzer Standalone v7.5.2	Volatility v2.6, Process Hacker v2.39.124
			X-Ways Forensics v19.9, DB Browser for SQLite

Android 7.1.8	Cellebrite UFED v7.33, Android Studio SDK Platform Tools v29.0.0	PacketCapture v2.0.1	Frida v12.6, Fridump	v3.11.2, SQLite Forensics Explorer 2.0
---------------	--	----------------------	----------------------	--

4.2 鑑識框架

本研究提出之鑑識框架如圖 1 所示，係以「證據識別」、「蒐集與擷取」、「檢驗與分析」及「報告與展示」等不同階段且符合數位證據鑑識標準程序對「Decentraland」、「The Sandbox」、「Axie Infinity」及「Roblox」等 4 種應用程式進行鑑識分析。

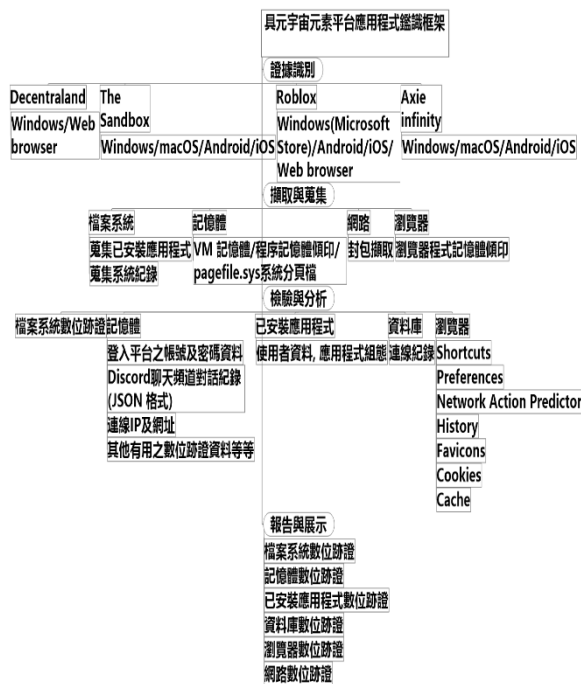


圖 1 跨平台遊戲語音聊天應用程式鑑識框架

在「證據識別」階段，為如何在微軟視窗桌面系統及Android行動裝置系統中識別是否有安裝此類應用程式。在「蒐集與擷取」階段可分為(1)檔案系統蒐集安裝之應用程式及系統紀錄等資料，(2)記憶體則擷取虛擬主記憶體檔、應用程式記憶體及系統分頁檔(Pagefile.sys)等資料，(3)蒐集平台應用程式使用時之網路封包資料，(4)擷取與蒐集瀏覽器檔案與程序記憶體資料。在「檢驗與分析」階段，則對檔案系統檢驗那些系統檔案會留存使用應用程式時所產生之鑑識特徵資料；在記憶體則分析有無使用元宇宙平台Discord聊天頻道之對話紀錄、使用之加密貨幣錢包地址、加密貨幣公鑰、使用者登入帳號與密碼、連線IP與URL網址或其他有用的鑑識特徵等等；在應用程式則檢驗安裝路

徑、使用者及程式設定或組態等具有鑑識特徵之資料；在資料庫方面，則分析由系統及應用程式在使用時所產生之資料庫檔案內容，並找出存放關鍵資訊之資料表；在網頁瀏覽器方面，則從Preference、Network Action Predictor、History、Favicons、Cookies及Cache等資料項目進行分析，找尋加密貨幣錢包服務的登錄記錄等相關之數位跡證。在「報告與展示」階段，則是將上述從檔案系統、記憶體、已安裝應用程式、資料庫、網頁瀏覽器及網路封包等 6 方面所檢驗與分析出之鑑識特徵資料進行歸納與整理，並提出以供調查與鑑識實務工作者參考利用。

五、結果討論

由實驗結果發現「Decentraland」、「Axie Infinity」及「Roblox」皆使用與Google Chrome相同之LevelDB本地化儲存Key-value資料庫技術，因此可以相同的鑑識方法找尋相關特徵；另分析應用程式之程序記憶體及主記憶體檔案資料，可以發現在應用程式程序未結束狀態下，仍可擷取到Discord格式(JSON)之頻道對話內容、使用之加密貨幣錢包地址、加密貨幣公鑰、使用者登入帳號或其他重要資料。由應用程式或檔案系統所產生之特定資料庫檔中仍可取得相關重要資料，本研究實驗之應用程式在桌面及行動裝置系統所產生之重要鑑識特徵，分為檔案系統、已安裝應用程式、資料庫、網路封包、網頁瀏覽器及記憶體等 6 類，整理如表 3：

表 3 本研究採集之數位跡證與證據特徵

平台名稱	作業系統	數位跡證型態	證據特徵
Decentraland	Windows	檔案系統，已安裝應用程式及資料庫	[Program Files\Decentraland, \Users\{account}\AppData\Local\explorer-desktop-launcher-updater, \Users\{account}\AppData\LocalLow\Decentraland\Decentraland, \Users\{account}\AppData\Roaming\explorer-desktop-launcher\]as like google chrome structure]
Decentraland	Android	檔案系統	[app\com.discord-1, \data\com.discord][google app measurement local.db, com.google.android.datatransport.events,

		統，已安裝應用程式及資料庫	androidx.work.workdb]
The Sandbox	Windows	檔案系統，已安裝應用程式及資料庫	[\\Program Files (x86)\\The Sandbox\\Maker\\Users\\{account}\\AppData\\LocalLow\\TSBGAMING\\The Sandbox Maker]
The Sandbox	Android	檔案系統，已安裝應用程式及資料庫	[\\app\\com.pixowl.thesandbox.android-1, \\data\\com.pixowl.thesandbox.android]
Axie Infinity	Windows	檔案系統，已安裝應用程式及資料庫	[\\Program Files\\Axie Infinity, \\Program Files\\Axie Infinity – Origin, \\Users\\{account}\\AppData\\LocalPrograms\\@axielauncher\\, \\Users\\{account}\\AppData\\LocalLow\\Sky Mavis\\Axie Infinity, \\Users\\{account}\\AppData\\Roaming\\ Mavis Hub \\]
Axie Infinity	Android	檔案系統，已安裝應用程式及資料庫	[\\app\\com.skymavis.genesis-1, \\app\\com.axieinfinity.origin-1, \\data\\com.skymavis.genesis]
Roblox	Windows	檔案系統，已安裝	[\\Program Files\\WindowsApps\\ROBLOXCORPORATION.ROBLOX_2.423.63880.0_x86__55nm5eh3cm0pr, \\Users\\{account}\\AppData\\Local\\Packages\\ROBLOXCORPORATION.ROBLOX_55nm5eh3cm0pr][as like google chrome structure]

		應用程式及資料庫	
Roblox	Android	檔案系統，已安裝應用程式及資料庫	[\\app\\com.roblox.client-1, \\data\\com.roblox.client]
Decentraland	[Windows, Android,]	網路封包	104.19.217.110 [api.decentraland.org] [play.decentraland.org] [feature-flags.decentraland.org] [config.decentraland.org] [peer.decentraland.org] [sni.cloudflaresl.com] [peer-ap1.decentraland.org] [peer-ec1.decentraland.org] [peer-eu1.decentraland.org] [peer-wc1.decentraland.org] [peer-ec2.decentraland.org]
The Sandbox	[Android]	網路封包	20.189.173.6 [onedscolorprdwus05.westus.cloudapp.azure.com] [teams-events-data.trafficmanager.net] [teams.events.data.microsoft.com]
Axie Infinity	[Windows, Android]	網路封包	104.154.26.183 [game-api-origin.skymavis.com] (Other) 172.67.23.198 [tracking.skymavis.com] [athena.skymavis.com]
Roblox	[Windows, Android]	網路封包	52.113.196.254 [teams-ring.msedge.net]
[Decentraland, The Sandbox, Axie Infinity, Roblox]	Windows	網頁瀏覽器 (Google Chrome)	\\Users\\{account}\\AppData\\Local\\Google\\Chrome\\User Data\\Default\\Top Sites, Shortcuts, Preferences, Network Action Predictor, Cache, History, Favicons, Cookies]
[The Sandbox, Axie Infinity, Roblox]	Android	網頁瀏覽器 (Google Chrome)	\\data\\com.android.chrome\\cache\\
[Decentraland, The Sandbox, Axie Infinity, Roblox]	Windows	記憶體	[Decentraland.exe], [The Sandbox Maker.exe], [axie_game.exe, AxieInfinity-Origin.exe], [Win10Universal.exe]
[The Sandbox, Axie Infinity, Roblox]	Android	記憶體	[com.pixowl.thesandbox.android-1, com.axieinfinity.origin-1, com.skymavis.genesis-1], com.roblox.client-1]
[Decentraland, The Sandbox, Axie Infinity,	[Windows, Android]	Discord頻道對	[https://discord.com/channels/417796904760639509/433376431603580970, https://discord.com/channels/497312527093334036/497312527550775297, https://discord.com/channels/410537146672349205/916398226813370419 globe,

Roblox]		話	https://discord.com/channels/869302105586933912/869422596721111070 philippines, https://discord.com/channels/870667037498830878/870675370209316865 spanish, https://discord.com/channels/887448599607251004/88744859926026271 portuguese], https://discord.com/channels/150074202727251969/406999049619898378]
---------	--	---	---

六、結論與未來研究方向

本研究所列之 4 種元宇宙遊戲平台及其應用程式之實驗結果顯示使用者在使用此 4 種應用程式仍會在系統中留下相關數位跡證或鑑識特徵，本研究提出之鑑識方法與框架亦將有助於此類跨平台應用程式之相關研究，有關該等平台之加密貨幣與 NFT 公鑰和私鑰之調查與加密貨幣及 NFT 密鑰恢復之鑑識值得做為後續深入的研究方向。

七、參考文獻格式

- 1.Decrypt, 2022, Axie Infinity Delays Ethereum NFT Game Upgrade After \$622M Hack, online <https://decrypt.co/96541/axie-infinity-delays-ethereum-nft-game-overhaul-after-hack>.
- 2.PC Gamer, 2022, A new report on Roblox reveals how hackers and scammers are continuing to rip off kids, online <https://www.pcgamer.com/a-new-report-on-roblox-reveals-how-hackers-and-scammers-are-continuing-to-rip-off-kids/>.
- 3.The New Republic, Will the Metaverse Unlock a New Virtual Universe of Cybercrime, online <https://newrepublic.com/article/164497/facebook-metaverse-cybercrime-marc-zuckerberg>.
- 4.Analytics India Magazine, 2020, Fighting cybercrime in metaverse, online <https://analyticsindiamag.com/fighting-cybercrime-in-metaverse/>
- 5.MACKENZIE, S., Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. The British Journal of Criminology, 2022.
- 6.SONG, H.J., NAM, W., A Study on the Types of Crime and Scalability in Metaverse. Journal of the Society of Disaster Information, 2022, 18.1: 218-227.
- 7.D'ARGENLIEU, E., Terrorist use of the Metaverse: new opportunities and new challenges. Technology, 2022.
- 8.OSIVAND, S., Investigation of Metaverse in cryptocurrency. GSC Advanced Research and Reviews, 2021, 9.3: 125-128.
- 9.WANG, Y., et al., A survey on metaverse: Fundamentals, security, and privacy. arXiv preprint arXiv:2203.02662, 2022.
- 10.ZHAO, R., et al., Metaverse: Security and Privacy Concerns. arXiv preprint arXiv:2203.03854, 2022.
- 11.Metapunk, 2021, Using the Metaverse to Simulate Crime Scenes, online <https://www.metapunk.co.uk/metablog/7-2021-using-the-metaverse-to-simulate-crime-scenes>
- 12.Decentraland, 2022, Decentraland Documentation, online <https://docs.decentraland.org/>
- 13.The Sandbox, 2022, About The Sandbox Team , online <https://www.sandbox.game/en/about/>
- 14.Roblox Blog, 2022, All the latest news direct from Roblox employees, online <https://blog.roblox.com/>
15. Axie Infinity, 2022, FAQ _ Axie Infinity, online <https://axieinfinity.com/faq/>

涉加密貨幣刑事案件錢包追蹤自動化之研究

張哲維

中央警察大學資訊管理所研究生

im1103045@mail.cpu.edu.tw

高信雄

刑事警察局電信偵查大隊偵查正兼任助理教授

k601516@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授，通訊作者

tung@mail.cpu.edu.tw

鄧少華

中央警察大學資訊管理所教授

pdeng@mail.cpu.edu.tw

摘要

傳統貨幣交易到現今各類電子支付，皆是金融中心化，而加密貨幣係透過區塊鏈加密技術所建立之虛擬貨幣，具有去中心化、匿名性、透明公開、不可竄改及加密等特性，無須透過政府或金融機構監管，現在除投資標的外，也可用於區塊鏈上的交易，然而亦成為不法分子之洗錢手段。加密貨幣造成的影響逐漸受到政府重視，我國於2021年7月1日將加密貨幣正式納入洗錢防制法中，有鑑於此，現階段實務查緝線上博弈網站、洗錢轉帳及詐騙等犯罪機房的電腦硬體設備數量龐大，為有效快速確認犯罪嫌疑人關係，本研究建構一套自動化系統，透過正規表達式於犯嫌電腦設備中搜尋比特幣地址字串，再透過比特幣瀏覽器確認是否為錢包地址以及目標交易地址，輸入警政署刑事局區塊鏈及虛擬貨幣分析平台連結比對我國合作虛擬貨幣交易所，操作結果將告訴使用者此錢包地址使用人及其他交易者真實身分，以利後續偵查作為。

關鍵字：比特幣、正規表達式、錢包地址。

一、前言

2008年9月美國投資銀行雷曼兄弟控股公司（Lehman Brothers）倒閉，刺激出加密貨幣的蓬勃發展現象。法國比特幣交易所的諾瓦札（Pierre Noizat）於2011年創辦時表示，一小群銀行菁英建立了金融規定強制大家遵守，但雷曼兄弟倒閉導致菁英建立的傳統體系遭到質疑，因此主打去中心化，以點對點的加密貨幣逐漸受到投資客的喜愛，然而新科技的好壞都是由使用者的使用方式界定，近期勒索病毒猖獗，透過綁架受害者電腦檔案，要求使用比特幣來交易贖金或者藉由主打採礦或共同投資比特幣的名義，實行不法吸金、高投資收益詐欺[10]與洗錢，直接或間接造成被害人負債輕生或無辜者涉嫌違法，不僅使社會大眾誤解加密貨幣的本質，更遭有心人士的利用。

1. 研究動機

2015年，身價上千億元的香港東方明珠石油主席黃某，涉案獲交保後來台隱居，九月間遭人擄走。綁匪寄勒贖影片，勒贖七千萬

港幣，畫面中黃某遭凌虐；警方連月追查，最終逮捕嫌犯蔡嫌等十四人，並在中部地區一間廢棄空屋救出雙腳被銬的黃某，被綁長達三十八天。綁匪一開始就要求以「比特幣」付贖金，家屬與警方一聽無法理解，因為無人懂得比特幣操作方式；警方一方面協助家屬與歹徒周旋，一方面加緊補充比特幣相關知識。比特幣在我國並不被視為有效貨幣，且具有高度私密性，當時警方毫無這方面專業，贖金只要付出，根本無法追蹤。考量加密貨幣為現已成為犯罪集團新的交易媒介(比特幣為大宗)，所牽扯之犯罪類型廣泛，雖然目前我國加密貨幣常見相關案件以吸金詐騙為主，但其他國家也曾發生洗錢情事，而原因不外乎是毒品交易、貪汙、甚至資助恐怖攻擊等犯罪，且因虛擬貨幣並非法定貨幣，導致各國有不同的方式管理，我國警方極需發展新的偵查技術加以因應[2]。

2. 研究目的

國際貨幣基金組織 IMF(International Monetary Fund)於2016年的虛擬貨幣研究報告指出，虛擬貨幣及區塊鏈技術可提供更有效率及低成本的金融服務，有助於發展中國家擴大金融服務普及性，但虛擬貨幣交易價格波動劇烈，使其無法具備法償貨幣的功能。發展虛擬貨幣仍須克服的挑戰則是非法使用，包括：洗錢、資助恐怖主義、避稅及詐欺等用途，且虛擬貨幣的匿名性，也是監管面必須克服的挑戰[6]。

我國司法及金融機構，在2019年金管會才開始針對加密貨幣加強監管作為。故針對加密貨幣，目前多數偵辦案件僅著重於偵辦詐騙吸金相關類案件，考量加密貨幣會對國家安全帶來的衝擊並非僅此，詐騙僅僅是表層之類案，查緝深度嚴重不足，故加強加密貨幣錢包地址為本研究主要的目的。

本研究期望提供警方於詐騙或洗錢機房查扣的犯罪電腦硬體中，建構一套自動化程式，運用正規表達式搜尋可能錢包地址字串，接著於比特幣瀏覽器確認是否存在和其曾有過的交易地址，表示犯罪不法所得金錢流向，輸出所有交易地址，並匯入警政署刑事局區塊鏈及虛擬貨幣分析平台，連結比對我國合作虛擬貨幣交易所，將該錢包地址使用人以及交易對象資料一一陳列，以此方式快速確認犯罪嫌疑人是否使用加密貨幣做為不法所得及確認洗錢可能性，並且有效比對犯罪嫌疑人及關係人之個人資料，以提高警方偵查加密貨幣案件之效率。

二、基礎知識背景與文獻探討

1. 虛擬貨幣

虛擬貨幣又稱數位貨幣，由非國家政府之開發者發行、管控。根據2012年歐洲央行的定義為：「一種無法律約束，由開發者發行與管控，在特定虛擬社群成員中接受和使用的數位貨幣」。美國財政部金融犯罪執法網

絡 (FinCEN) 於2013年定義其為：「虛擬貨幣為在某些環境下像實體貨幣一樣運作的交換媒介，惟不具備實體貨幣的所有屬性。」也不具有法定貨幣的地位。2014年，歐洲銀行業管理局定義其為：「並非由央行或政府部門發行的，也不必要與法定貨幣相關聯的一種數碼形式的價值，但是它作為一種支付途徑被自然人和法人所接受，並可以電子地轉帳，儲存和交易」。其中，又可把虛擬貨幣區分為可轉換虛擬貨幣（開放虛擬貨幣）和不可轉換之虛擬貨幣（非開放式虛擬貨幣），可轉換虛擬貨幣（如遊戲點數卡）和實質貨幣等值而且可以來回兌換成實質貨幣，如：比特幣、以太幣等加密貨幣。而不可轉換虛擬貨幣有獨自主要用途及自己封閉的交易市場，如：天堂天幣、RO仙境的RO幣等線上遊戲遊戲幣。

2. 加密貨幣

中本聰(Satoshi Nakamoto)於2008年[14]發布了首個比特幣，是一種加密貨幣和全新型態的支付系統，比特幣透過區塊鏈達到完全去中心化，其總量為2100萬顆比特幣。自推出以來，比特幣的市場價值迅速增長，儘管加密貨幣問世僅十餘年，但快速成長、價格急速上漲及背後的區塊鏈技術，吸引不少學術界的眼光。加密貨幣是一條鏈形成的產物，本身有自己獨立的區塊鏈及協議內容，所有交易都在鏈上進行，用以確保其運轉機制，如同貨幣般可以進行轉移或交易。加密貨幣運用區塊鏈之分散式帳本結構，其系統中的密碼學用來產生和分配貨幣單位，過程要求在去中心化的情況下對交易進行核對，包括付款人擁有貨幣與否、確認交易金額，同時確保貨幣單位不會產生雙重支付問題，此驗證過程稱為「挖礦」。因有此驗證過程使用戶可以對每筆交易不會產生疑慮。

表一：熱錢包與冷錢包比較

	熱錢包	冷錢包
優點	<ul style="list-style-type: none"> ● 交易比較快速、方便 ● 私鑰生成和保存在線上伺服器裡 	<ul style="list-style-type: none"> ● 有較高的安全性 ● 私鑰生成和保存都是離線進行
缺點	<ul style="list-style-type: none"> ● 需要上網使用 ● 有駭客入侵的可能 	<ul style="list-style-type: none"> ● 永遠不會接觸網路 ● 需要購買硬體設備 ● 交易繁瑣、耗時

加密貨幣錢包有冷熱之分（表一），區別在於私鑰的生成、存儲、交易是否離線，而冷錢包由於不連線網路，減少駭客竊取私鑰的機會，其安全性比熱錢包來得高[7]。

3. 比特幣

比特幣作為虛擬貨幣一種，其發行、流通及管理權不屬於任何一個人、組織或國家；它平等地屬於參與其中的每一個人。有一台能連上網路的電腦，軟硬體資源夠強，透過運行一個自由的開放源代碼的軟件，任何人皆能參與比特幣的交易市場。所有參與的人之中不存在所謂的管理員、中心節點或特權人員，其屬於一種平等的點對點之對等網路（P2P）系統，統稱比特幣系統。在比特幣系統中四大特徵：

(1) 點對點傳輸方式及分散式網路節點

集中式網路結構係指有集中式服務單位作為中心服務點來提供網路服務(如銀行)，而點對點的直接傳輸則運用分散式網路節點的概念，分佈於不同地點的電腦系統連成網路結構，每個節點至少有兩條線路與其他任一節點相連[5]。

(2) 去中心化

作為一種虛擬貨幣的發行，包含數據儲存(交易支付及貨幣儲存)、傳輸，都不是由某個特定的單位或人來實施。比特幣設置的區塊(block)概念，以及平等任意的節點、點對點(P2P)概念的設置，均支持一個無控制中心及中介系統的運行機制。為有效解決信用問題，比特幣使用一套密碼學計算法，使得參與比特幣主要區塊鏈構建的所有用戶皆必須付出相當的努力才能證明其信用；同時，比特幣產生的過程受到全體網路使用者的監督，難以有欺騙的行為產生。比特幣成功利用密碼學的手段，使得其發行不需要依賴任何政府或機構，並與網路的去中心化特點高度符合。換言之，比特幣的運行體系中不僅沒有一個貨幣發行中心和管理中心，而且是強制去除此種中心管制思想的。沒有中央銀行或其他銀行的中介服務，去中心化屬於比特幣的核心概念。

(3) 總量確定，公平競爭

比特幣被設計出任何人都能參與比特幣發行工作的功能，每一參與比特幣挖礦的參加者，運用自己的能力參與其中的計算環節，並根據預設的公開規則，藉此獲取比特幣。於此環節中，所有參與其中的計算能力與計

算工作都是平等的。比特幣的發行數量或其增長數量屬既定，它被按照計算總量平均分配予各礦工(參與者)。此一環節的設置，實際是給比特幣提供一種特殊的信用證明機制，換言之，比特幣沒有外在賦予的信用授予，其於發行運行中產生自我證明的信用，此種信用實際基於透明及可追溯的公平性。

(4) 基於密碼學原理的運行設置

比特幣的公鑰是透過橢圓曲線加密演算法對私鑰進行加密後所產生的一組亂數。橢圓曲線密碼學的算法為不可逆。即使公鑰暴露，也不會影響私鑰的安全性，因為沒辦法藉由公鑰推算出私鑰，可說整個加密貨幣密碼學的匿名和安全都是架構於這個基礎之上。私鑰是一段由電腦隨機產生的亂數，包含了大約五十個數字和大小寫字母，沒有固定的邏輯和規則。私鑰與公鑰是成對產生的，世界上只會有一組，不會重複，在加密貨幣的世界裡，公鑰會散布在網路上，但私鑰只能本人持有，因此私鑰就代表資產的所有權，誰擁有私鑰誰就擁有該錢包地址中的使用權。比特幣地址是根據公鑰經過兩次雜湊函數（SHA256）轉換為公鑰哈希，這個過程同樣是不可逆的，之後再將公鑰哈希經過編碼推算得到地址。地址的功能是接收比特幣，某個地址收到比特幣後，只有擁有該地址對應私鑰的人才能使用它。從私鑰這步開始產生了一組私鑰後，經過複雜的演算法推出了公鑰，再由公鑰算出地址，由此可知地址是由私鑰推算出來的，反之不同的私鑰推算出的地址也會不同，透過最後一段我們也可以知道，只有擁有地址對應私鑰的人才能使用這個地址裡面的資產，私鑰也只會產生一組對應的地址，而地址也只會對應一組私鑰。

4. 虛擬貨幣交易所

加密貨幣是由一條原生鏈形成的產物，本身與有自己獨立的區塊鏈及協議內容，所有貨幣交易都在這條鏈上進行，而加密貨幣的價值則取決這個生態系是否有市場需求。既然加密貨幣會因為市場需求而產生價值，又可以像貨幣一樣移轉或交易，那就需要一個機制讓民眾能把當地法幣轉換成加密貨幣，以及把加密貨幣轉換成當地法幣，而這個機制即為加密貨幣交易所。

由coinmarketcap.com資料顯示，截至2021年12月，全球較具規模的加密貨幣交易所超過300間，全球前三大交易所分別為：(1)Crypto.com Exchange，每日加密貨幣成交

金額約37億美金；(2)幣安(Binance)，每日加密貨幣成交金額約120億美金；(3)Coinbase Exchange，每日加密貨幣成交金額約26億美金。加密貨幣交易所的獲利主要來自於用戶買賣加密貨幣及使用各種加密貨幣金融商品的手續費，然而加密貨幣交易所繁多，且推出的功能皆有所差異，常會讓新手不知如何選擇合適的交易所。此外，加密貨幣具有去中心化及匿名化不易追蹤的特性，交易所遭駭客入侵的事件時有所聞，更讓新手使用者需要花更多的時間與精力去選擇加密貨幣交易所[1]

5. 比特幣交易模式

比特幣存在於用戶的比特幣地址之中，當使用者消費比特幣時，是在轉移特定數量比特幣的持有權，將比特幣自身的錢包地址輸入至接收者的錢包地址之中[8]。一筆交易是由許多比特幣網路的元素所促成，以支付者的角度來看，支付比特幣時需要使用的包括[3]：

(1) 密鑰

在交易時會運用到一對建立於數位簽章基礎上的密鑰，分別是公鑰 (Public Key) 以及私鑰 (Private Key)。公鑰主要目的是用來創建地址，並提供辨識，錢包地址如同銀行的帳戶號碼，不論是支付或接收都雙方錢包地址才能夠進行交易；私鑰用以進行驗證，當用戶欲消費比特幣時，系統會對用戶進行驗證，查驗其私鑰與公鑰是否是一對，可想像為銀行帳戶密碼，代表著用戶對其比特幣的存取權，需要好好保存。比特幣每一組密鑰都代表比特幣網路中的一個帳戶，而每一個公鑰必定有其相對應的私鑰，兩者緊密關聯。私鑰的創建是隨機的，在系統創建私鑰之後，會將私鑰執行一項不可逆的單向加密，稱為橢圓曲線數位簽章算法 (Elliptic Curve Digital Signature Algorithm，ECDSA)，目的是確保加密機制是單向的，無法從公鑰回推到私鑰。

(2) 錢包地址

錢包地址應用前開密碼雜湊函式技術，由公鑰加密產出[9]，將公鑰進行一連串數學運算後可以得到如下之比特幣地址：

1fg1sa52asfg42z2a45g78ga4aw5g45aga25ash，加密過程分別使用SHA256雜湊安全演算以及RIPEMD160 雜湊演算法，最後再以Base58Check編碼重新呈現比特幣地址，先對公鑰進行SHA256雜湊安全演算，對於任意長

度的訊息，SHA256都會產生一個256bit長的雜湊值，稱作訊息摘要，這個摘要相當於是個長度為32個位元組的陣列，通常用一個長度為64字元的十六進位制字串來表示。而RIPEMD160雜湊演算法則是產生160位元的字串，1位元組為8位元，故其結果為一20位元組 (40字元) 的字串。比特幣地址呈現最終的樣態之前，會先通過「Base58Check編碼」程序。此方法使用Base58數字系統中的58個字符以及校驗碼來提升比特幣地址之可讀性以及輸出交易之正確性，如此一來便能避免因為視錯覺而導致的技術錯誤[11][12]。

三、解決方案

1. 運用正規表達式搜尋錢包地址

正規表達式 (Regular Expression，又稱regex) 可用來在字串中搜尋「符合特定規則」的子字串，例如使用正規表達式'[0-9]+'，可以從金額66元中搜出數值'66'。其中[0-9]代表一個0~9的字元，而+則表示前一個字元(就是[0-9])可以重複1到多次，因此字串中只要有連續的數字都會被搜出，例如'6'、'23'、'1038'等都符合條件。

常規表達式的常用語法可分為「單一字元、重複次數、頭尾字元、轉義字元」4部分[4]：

(1) 單一字元

主要是用來指定哪些字元可以符合條件 (例如[0-9]表示0~9都可以符合)。(A)一般字元直接比對。(B)代表任意字元，但不包含換行字元(\) (C)在[]中可列舉符合的字元、最前面加^表示不包含、也可用-表示區間範圍。

一個[]就代表一個字元，[s-x]就等同於[stuvwx](由s到x的任一字元都符合)。列舉字元和區間範圍可以合併使用，例如[des-xS-X0-5]表示d、e、s-x、S-X、0-5都符合。若在[]的最前面加^，則表示除了[]中列舉的字元以外都符合，例如[^dx]就是指不為d、x的任意字元。由於在[]中的-、^、]有特殊意義，因此必須用轉義字元\來表示原來的符號，例如用[^\-]]來代表可以是^、-或]的一個字元。但如果這三個符號是被放在不會被誤解的位置，例如^不是放在最前面、]是放在最前面、或-是放在最前面或最後面，則是否用\來轉義都可以，例如[]^-]和[]^\-]是相同的意義(代表可以是]、^、或-字元)。

(2) 重複次數

主要是加在字元後面，表示該字元可以有幾個。(A)+代表前一個字元可以出現1次以上(無上限)。(B)*代表前一個字元可以出現0次以上(無上限)。(C)?代表前一個字元可以出現0或1次。(D){m}代表前一個字元要出現m次。(E){m,n}代表前一個字元出現m-n次都可以符合。

以上{m,n}中的m或n也可省略：{,n}表示0~n次，{m,}則表示m次以上。例如Bd{,2}可搜出BleBdleBddle。前面都是針對單一字元來指定重複次數，如果要指定一連串字元重複次數，則可用小括號括起來例如d(Bd)+可搜出ddBdBdd。所有的重複次數符號在[]中都沒有作用(因為[]代表一個字元，沒有重複的需要)，而會被當成一般的字元。例如[*?+]就代表可以是*、?、或+的一個字元。最後，正規表達式預設會以貪婪模式搜尋，也就是會盡量找出最多字元的子字串，例如用a.+c來搜尋abc-c-cde字串會搜到abc-c-cde，此時我們可以在重複次數(+、*、?、{ })的後面加一個?，表示要使用非貪婪模式來找出最少字元的子字串，例如a.+?c會搜到最少字元的abc-c-cde。

(3) **頭尾字元**可用來指定必須是開頭或結尾的字元。(A)^必須以後面的字元為開頭(B)\$必須以前面的字元為結尾。^必須放在正規表達式的最前面，而\$必須放在最後面。

(4) 轉義字元

轉義字元是計算機專業詞彙。在計算機當中，我們可以寫出123，也可以寫出字母abcd，但有些字元我們無法手動書寫，例如當我們需要對字元進行換行處理，但無法寫出換行符，當然我們也看不見換行符。像這種情況，我們需要在字元中使用特殊字元時，就需要用到轉義字元，在python裡用反斜槓\轉義字元。(A)\後面的符號以一般符號處理(B)\\代表\字元(C)\n換行字元。

2. 比特幣錢包地址格式

比特幣區塊鏈基本上是地址之間的交易記錄。通過查看輸入地址的所有交易，我們可以確定該地址的餘額。這意味著一定數量的比特幣歸比特幣區塊鏈上的一個地址所擁有。以下為三種常見的比特幣地址格式[13](表二)：

表二：比特幣地址樣式種類

地址版本	例子	描述	付款方式
Legacy	15e15hWo6CShMgbAfo8c2Ykj4C6BLq6Not	最舊的比特幣格式。字串開頭為1。	P2PKH
Script hash addresses (BIP-13)	35PBEaofpUeH8VnnNSorM1QZsadrZoQp4N	第二個主要地址格式。字串開頭為3。	P2SH
Native Segwit	bc1q42lja79elem0anu8q8s3h2n687re9jax556pcc	第三個主要地址格式。字串開頭以bc1q開始。	P2WPKH

(3) Native SegWit(Bech32)格式

(1) Legacy(P2PKH)格式

地址以「1」開頭，是比特幣最初沿用至今的地址格式，也是最常見的地址格式；至於P2PKH是「Pay To PubKey Hash」（付款至公鑰哈希值）的縮寫。

(2) Nested SegWit(P2SH)格式

地址以「3」開頭，從這種格式我們無法辨別它們到底是多重簽章(MultiSig)地址還是隔離見證兼容地址；P2SH是「Pay To Script Hash」（付款到腳本哈希值）的縮寫，支援比Legacy格式更複雜的功能，例如指定多個數位簽章來授權事務。

地址以「bc1k」開頭，屬於本地SegWit地址格式，專為SegWit而開發的地址格式，有些交易所可能還未有支援這種格式的地址，目前在這種格式的地址上的比特幣數量在三種格式中是最少的。由於更多交易數據可以儲存在單個區塊，而Bech32格式地址本身與SegWit相容，不需要額外的空間來將SegWit地址放入P2SH地址，因此從這種地址發送比特幣時的平均費用可能會較低。

Bech32在2017年底在BIP173（Bitcoin Improvement Proposal，比特幣改進提案）被定義，該格式的主要特點之一是它不區分大

小寫（地址中只包含0-9，az），因此在輸入時可有效避免混淆且更加易讀。由於地址中需要的字元更少，地址使用Base32編碼而不是傳統的Base58，計算更方便、高效。數據可以更緊密地存儲在二維碼中。Bech32提供更高的安全性，更好地優化校驗和錯誤檢測代碼，能夠將出現無效地址的機會降到最低。

3. 比對比特幣瀏覽器確認是否存在和使用交易

開啟Blockchain比特幣瀏覽器並輸入搜尋到的目標字串，搜尋該字串是否為比特幣的錢包地址，若目標地址確實存在，將會顯示其交易訊息以及目前擁有的比特幣數量及金額，也能確認其是否有與他人交易。

4. 目標交易錢包地址

透過比特幣瀏覽器確認目標地址交易的地址，並彙整紀錄所有交易地址。

5. 警政署刑事局區塊鏈及虛擬貨幣分析平台

警政署刑事局區塊鏈及虛擬貨幣分析平台為警政署刑事局與我國虛擬貨幣交易所合作建立之合作平台，輸入目標錢包地址及所有交易地址確認是否為我國人民註冊，如比對成功即可線上成功調閱個人資料。

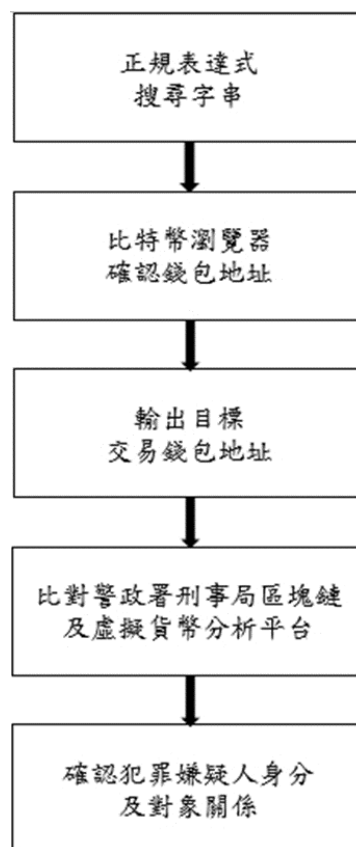
四、案例模擬

1. 模擬案例說明

(1) 2020年5月，以大雄為首的詐騙集團，隨機撥打電話向民眾鼓吹投資未上市股票，利用話術諸如股票即將上市上櫃、獲利數倍、公司營收成長幅度驚人云云，取得被害人信任後互加Line好友繼續施以騙術，將其收購價為每股新台幣20至30元不等之數家未上市股票以每股新台幣120至130元賣予被害人，牟取暴利，總計販售逾3百張股票，經被害人驚覺受騙或察覺有異時，便封鎖被害人斷絕聯繫，經查計有被害人14人，損失金額高達2千餘萬元，警方始據以偵辦並報請地方檢察署檢察官指揮偵辦。歷經數月蒐證完成後，分持地院核發之搜索票及拘票執行搜索並拘

提犯罪嫌疑人大雄主嫌等11人到案，現場查扣犯罪所得新臺幣136萬3千餘元等證物，犯罪現場使用大量電腦主機設備進行線上博弈操作，除保存現場數位證據外，亦應把握時間避免加密貨幣遭到轉移之可能。

2. 解決方案-涉加密貨幣案件錢包追蹤自動化流程(圖一):



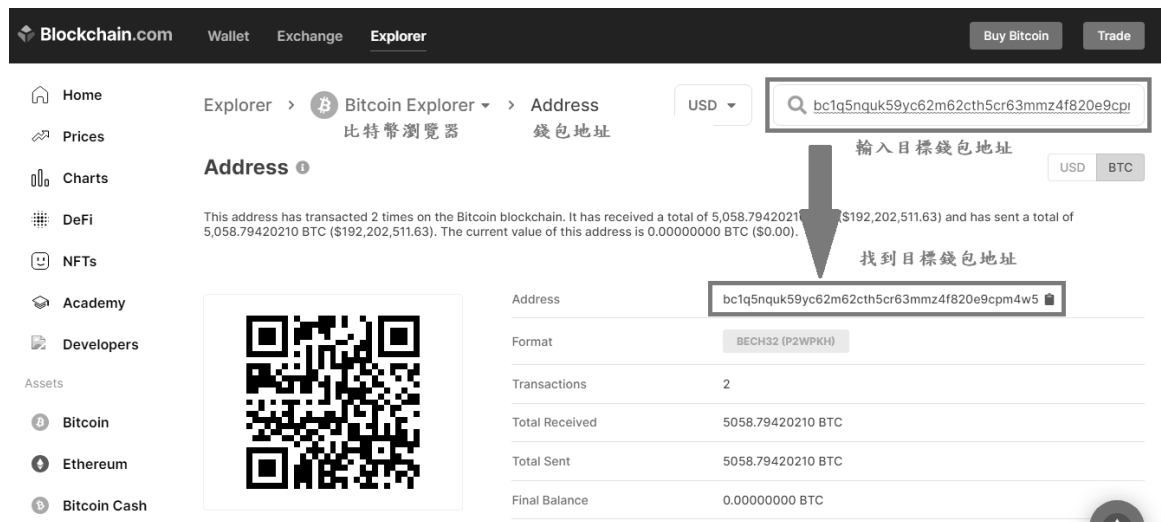
圖一：涉加密貨幣案件錢包追蹤自動化流程

(1) 使用正規表達式搜尋符合錢包地址字串

運用正規表達式：「[1,3,bc1q] [0-9,a-z]* {20,25}」對犯罪現場電腦主機進行搜索字串，找出符合疑似比特幣錢包地址之字串若干。

(2) 比特幣瀏覽器確認字串為錢包地址

將犯罪現場電腦主機搜尋到的字串輸入於比特幣瀏覽器之中，顯示出目標字串確實為存在之比特幣錢包地址（圖二）。



圖二：比特幣瀏覽器搜尋

(3) 輸出目標錢包地址

將目標錢包地址透過比特幣瀏覽器，確認目標錢包地址與其他錢包地址確實有在進行

交易（圖三），並將交易之對象錢包地址彙整輸出（圖四）。



圖三：目標錢包地址交易資訊

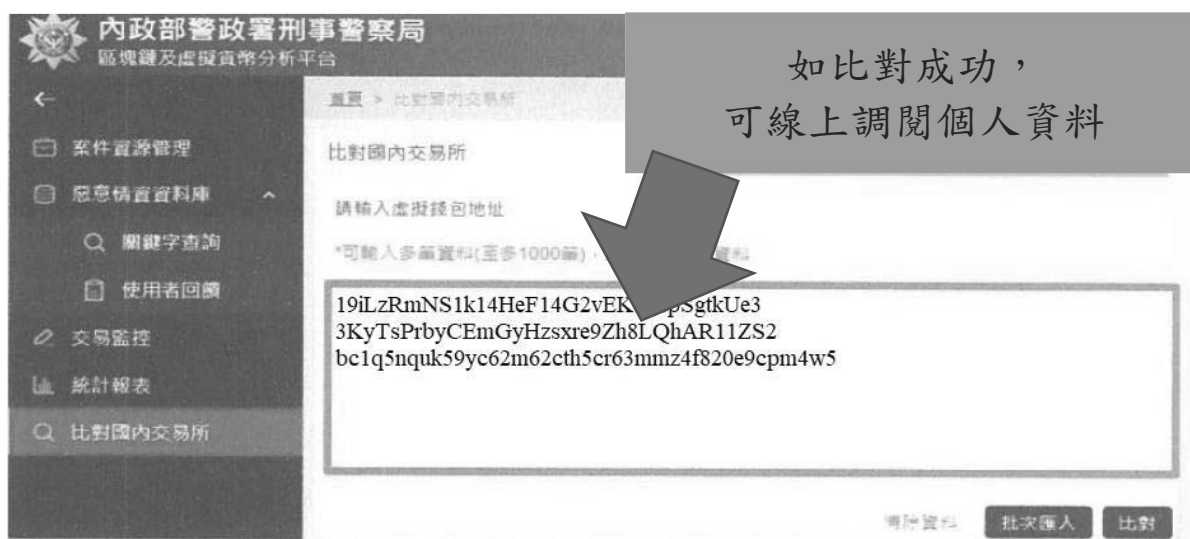


圖四：交易對象錢包地址

(4) 比對警政署刑事局區塊鏈及虛擬貨幣分析平台

將輸出的交易對象錢包地址與警政署刑事局區塊鏈及虛擬貨幣分析平台進行比對（圖

五），若該比特幣錢包地址為我國申請註冊之交易所錢包地址，即可比對出錢包地址持有人之個人資料，供警方做後續偵查作為。



圖五：警政署刑事局區塊鏈及虛擬貨幣分析平台

五、結論

加密貨幣擁有匿名性、去中心化、不可竄改等特性，對於執法機關造成極大的挑戰，本研究結果建構一套自動化系統，透過正規表達式對於犯罪電腦硬體設備快速搜索相關錢包地址字串，接著在比特幣瀏覽器上確認是否為有效使用之比特幣地址，將目標錢包地址交易對象錢包地址輸出，再與「警政署刑事局區塊鏈及虛擬貨幣分析平台」連結比對，獲得犯罪嫌疑人與其他交易對象之個人資料，可馬上與交易所聯繫並要求其凍結目標帳戶或提供該目標私鑰，運用警方專屬冷錢包將不法所得扣押並進入證據監管鏈。此外，也提供警方對於現場電腦犯罪設備有效地篩選涉及比特幣或其他加密貨幣做為不法所得和洗錢的可能性。後續研究方面，本研究期望建立警方專用之熱錢包以保管查扣加密貨幣，避免冷錢包因遺失、故障等原因而流失加密貨幣證據。

參考文獻

1. 尹衍傑，「產品知識對消費者選擇加密貨幣交易所意願之影響：以幣安交易所為例」，開南大學碩士論文，2022，第6頁。
2. 呂余晨，「虛擬貨幣對資助恐怖份子洗錢之因素分析與因應措施」，國立臺北科技大學碩士論文，2020，第2頁。

3. 施志鴻，「加密貨幣犯罪偵查之研究」，2021警務生態系統發展新思維研討會論文集，2021，第42頁。
4. 施威名研究室，Python 技術者們：實踐！帶你一步一腳印由初學到精通，台北：旗標科技股份有限公司，2018，第一篇，第五章。
5. 高俊杰，「網路虛擬貨幣法律問題研究-以比特幣為中心」，東吳大學碩士論文，2016，第62~63頁。
6. 郭秋榮，「我國因應數位貨幣發展之對策與政策建議」，國發會107年研究發展作品評選，2018，第15頁。
7. 張哲維，「加密貨幣刑事案件之偵查技術」，2021IMP第26屆國際資訊管理暨實務研討會論文集，2021，第3頁。
8. 陳明志，「加密貨幣之探討：以比特幣為例」，中華大學碩士論文，2019，第14頁。
9. 蕭余芷，「區塊鏈及數位加密貨幣的應用範例及挑戰」，元智大學碩士論文，2019，第6頁。
10. 潘韋丞，「防制比特幣投資詐欺之研究—以刑事警察局為中心」，國立臺北大學碩士論文，2020，第37頁。
11. 蔡馥璟，「跨境犯罪非法金流之分析—以比特幣為例」，2021警務生態系統發展新思維研討會論文集，2021，第6~7頁。

12. Antonopoulos,A.M., Mastering Bitcoin: unlocking digital cryptocurrencies, O'Reilly Media, Inc, Sebastopol, 2014.
13. Matthew Baas, “Introduction to Bitcoin address formats”,
<https://rf5.github.io/2022/02/14/btc-address-intro.html> , 存取時間：2022-01-07 。
14. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Consulted, Vol. 1, 2008, p. 28.

Applying Routine Activity Theory to Columbaria Investment Scam

Chi-Cheng YANG ¹

¹ Department of Foreign Affairs Police, Central Police University, Taiwan
chichen@mail.cpu.edu.tw

Yi-Ju CHEN ²

² Department of Information Management, Central Police University, Taiwan
miajoa1211@gmail.com

Da-Yu KAO ^{2,*}

² Department of Information Management, Central Police University, Taiwan

*Corresponding author: dayukao@gmail.com

Abstract

Columbarium scam is high-profit investment fraud. Offenders will use the enormous profits of an investment as bait and let targets (victims) suffer financial losses in the end. This paper takes a practical columbaria scam, for example, and analyzes the three elements in Routine Activity Theory (RAT): motivated offenders, suitable targets, and the absence of a capable guardian. The observations indicate that appropriate alertness and self-questioning can reduce susceptibility to columbarium scams. Strategies to battle columbarium scams are further proposed to stay away from motivated offenders, avoid being a suitable target, and let capable guardians be involved.

Keywords: Investment Fraud, Columbarium Scam, Routine Activity Theory. Mobile Forensics

1. Introduction

1.1. Columbarium Scam

Investment fraud of columbarium scam has been rampant these years. Offenders use columbaria to attract investors and set up several dummy companies to target suitable victims who have columbaria in their hands. They claim that many potential buyers want to buy columbaria in large quantities and at high prices. They lobbied the victim to mortgage the property, take out a loan, and invest much

money to profit tens of millions. Offenders often prevaricate no profits for various reasons, such as failed transactions, postponed contact, or disappeared cooperation. It was not until victims had no money that they were shocked to be deceived. Information about recruiting people to invest can be seen everywhere on social media in the wake that people want to make quick profits. That social problem cannot be underestimated. In Fig. 1, the number of fraud cases has increased in the past decade [6].

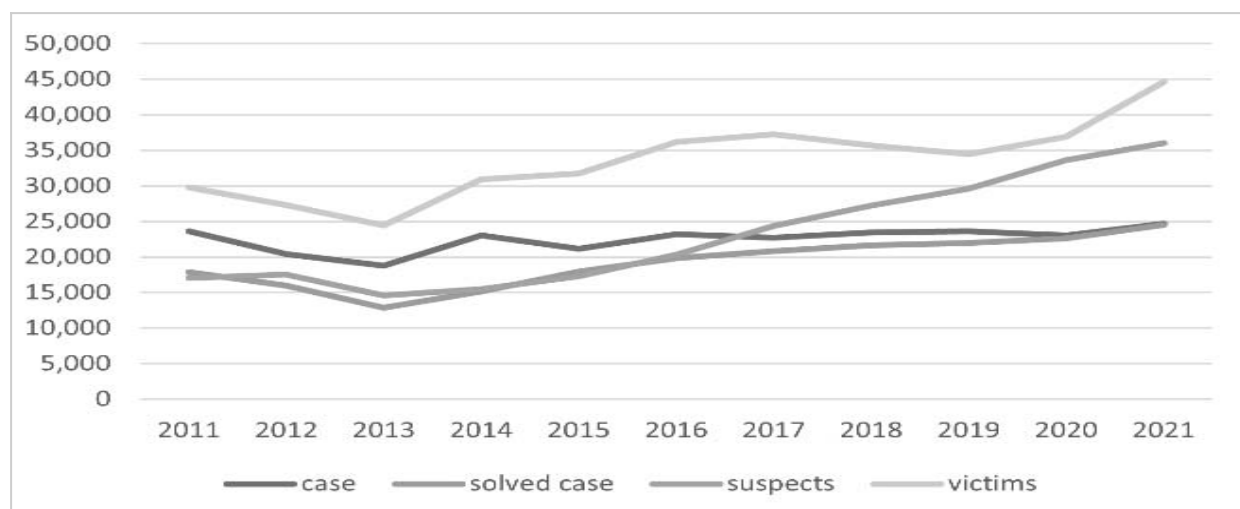


Fig. 1 Taiwan fraud statistics

1.2. RAT Elements

In Routine Activity Theory (RAT), crime often occurs when three essential elements converge in space and time: a motivated offender, a suitable target (victim), and the absence of a capable guardian [1]. All three elements must come together for criminal activity to be realized. Offenders are rational in their decision-making. RAT relies on the same rational choice methodology as situational crime prevention techniques [3]. That theory takes a macro-level view and emphasizes broad-scale shifts in victim and offender behavior patterns. Not only individuals are inclined to commit a crime. The target and the offender also have similar routine activities to let crimes happen. Crime could be committed from the offender's opportunity [2]. Fig. 2 illustrates three factors that create a criminal offense.



Fig. 2 RAT Crime Triangle

This paper is organized as follows. In Section 2, the observations of the columbarium scam are discussed and analyzed from the three elements in Routine Activity Theory (RAT): motivated offenders, suitable targets, and the absence of a capable guardian. The proposed strategies to battle columbarium scams are proposed in Section 3. The conclusions are given in Section 5.

2. Case Study

2.1. Columbarium Scam

Fig. 3 introduces the relevant characteristics of motivated Offenders (O for short), suitable Targets (T for short), and the

absence of a capable Guardian (G for short). Taiwan prosecutors have indicted the owners and staff of this columbarium scam group that sold columbarium niches on fraud charges of a cheated victim/target (T1) out of NT\$20 million. Columbaria are often housed in pagoda-like towers for urns containing cremated remains and for the dead in Chinese traditions. That enables families to conduct ancestral worship rites and memorial services. Six people (O1~O6) were wrapped up in an investigation into an alleged scam run. They were selling columbarium niches and swindling T1 out of her life savings. These offenders contacted T1 about purchasing one or two columbarium niches as final resting places for their elders. Then these offenders' pitches became more vigorous and convinced the victim to buy more columbarium niches as investments, which could be sold later for a high profit. After paying lots of money, the victim realized she had been swindled when she had no buyer. Columbaria sale scams are rife, and numerous cases have occurred over the past decade. The temporal case scenarios in Fig. 3 and Fig. 4 can be organized as follows:

(1) Pretending to Help Sell

On March 31, 2017, O5 made a false claim to help T1 sell 24 columbaria for NT\$ 8 million. Offenders promise victims more money if only T1 sends them an advance fee (NT\$ 260,000). T1 only sold two columbaria.

(2) Demand Has Increased Falsely

In July 2017, O1 made a false claim to help T1 make a NT\$ 30 million profit. She remitted NT\$ 1.2 million to buy 10 Columbaria.

(3) Raise Incentives Again

O1 and O3 signed a contract with T1. If the project cannot be completed on time, O3 is willing to pay NT\$ 1.8 million in compensation. Afterward, O1 and O3 could not be completed due to legal issues.

(4) Transfer House Property

The house ownership belonged to her husband, G1. O1 and O3 persuaded T1 to steal G1's official identification documents. O6 helped T1 to transfer ownership through the couple's gift procedure. Later on, T1 set up a

mortgage loan and withdrew NT\$ 9 million. The house ownership becomes the creditor O4.

(5) Target Finds Out the Fact

The NT\$ 9 million was divided and taken away by O1, O2, and O6. The value of transferred columbaria for T1 was minor than NT\$ 7.2 million. The investment contract has

been overdue, but T1 did not receive liquidated damages. The offenders fabricated many excuses. Then T1 finally realized that she had been defrauded. Table 1 and Fig. 4 show that T1 was created at NT\$ 10.46 million in 2017. The blue arrows describe the changing status of house ownership.

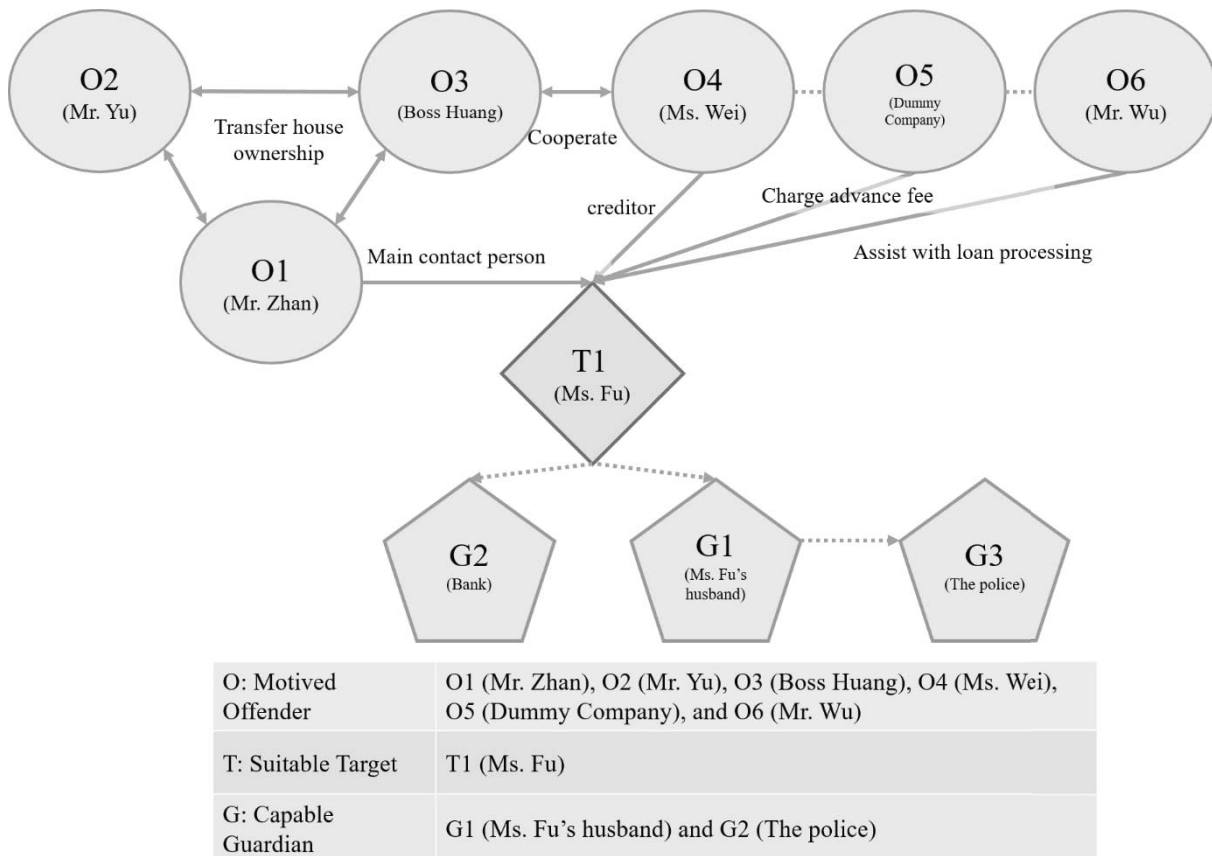


Fig. 3. RAT relational analysis

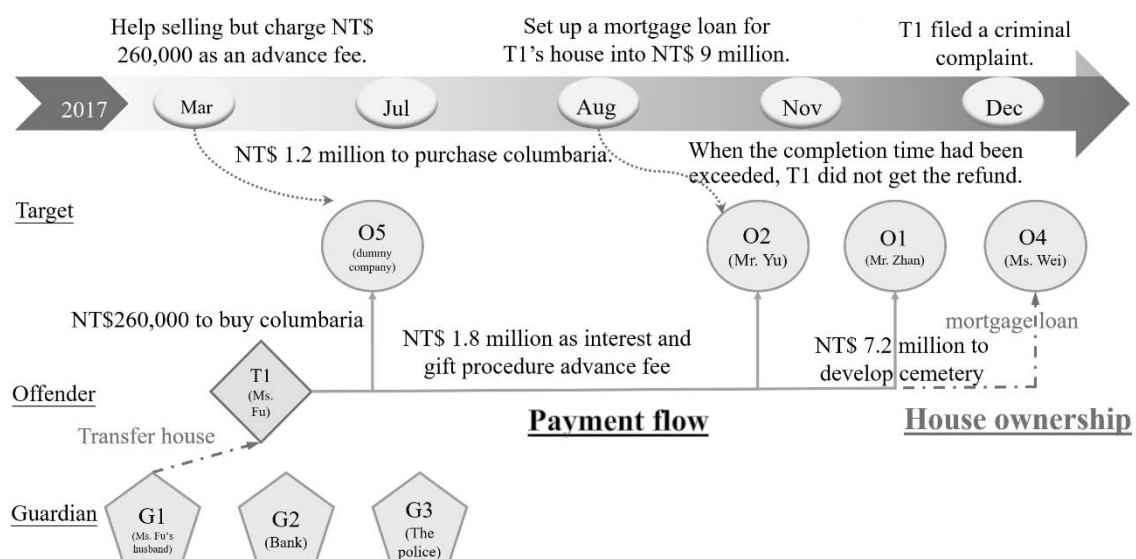


Fig. 4 RAT temporal analysis

Table 1. Temporal analysis in columbarium scam

Time	Participating Offenders	Event
March 31, 2017	O5	Charging NT\$ 260,000 advance fee
July 17, 2017	O1	Asking for NT\$1.2 million to buy columbaria
August 14, 2017	O1 and O3	Ask T1 to set up a mortgage loan for the house
August 17, 2017	O4	Becoming the owner of the house
August 21, 2017	O1, O2, and O6	Divided NT\$ 9 million cash from mortgage

2.2. Scam Observations

The scam is growing fast. Offenders steal money in an untraceable, irreversible columbarium scam. It is an excellent time for motivated offenders to find enormous pools of potential victims from the web, social media, and online services. These vulnerable victims need to take back control of their lives. When someone calls us with that same scam, we hang up the phone. We will never forget her or her story. The scam observations are cross-referenced among criminology theories in Fig. 5.

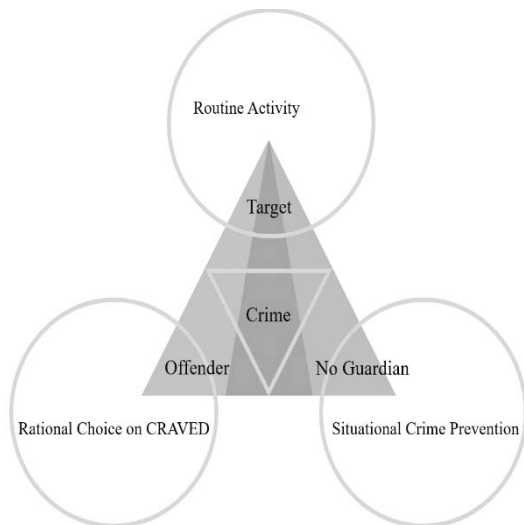


Fig. 5. Cross-reference among criminology theories

2.2.1. Investment Tricks from Motivated Offenders

The choice to commit fraud follows a path that intentionally deceives victims [7]. Offenders often targeted elderly civil servants. They further claimed that a NT\$ 6,000 investment could quickly recover three to ten times within months. High compensation is a

way offenders urge other buyers to take over and reward victims.

2.2.2. High Compensation for Suitable Targets

The offenders' argument for defrauding victims of money varies. For instance, the columbaria can be sold at high market value, and T1 requires dozens of items. Once offenders discover that the target's family members are interfering, they will sign a non-disclosure agreement. However, it is too late to recover the money.

2.2.3. Non-Disclosure Agreement to Avoid Capable Guardian

Offenders would claim that the permanent use of the columbaria is valuable. A civil investment dispute can be a perfect escape and exemption from criminal liability. That investment is even forged in some printed serial numbers. Offenders' words are mixed with true and false. It is too late when the victim finds out.

2.3. RAT Observations

A well-known RAT provides a straightforward explanation of why crimes occur. It argues that three things happen simultaneously when a crime problem occurs: a motivated offender, a suitable target, and the lack of a capable guardian.

2.3.1. Motivated Offenders

Offenders will rationally select targets during appropriate timing according to differential situations.

(1) Fraud Group Management

Fraud group management is typically embedded in the form of defined responsibilities and written ongoing procedures that implement an effective cheating program. After the

grassroots employees come in, they first undergo strict training. Everyone must copy the work words and memorize them until they are familiar. These offenders often have precise, strict management to perform their duties in daily meetings. Their words are retouched or enhanced immediately to touch the victim's mind.

(2) Rational Choice on CRAVED Components

Offenders' opportunity weighs heavily in choices according to Clarke and Cornish's rational choice perspective. A crime involvement decision refers to the offender's choice in actually carrying out an offense [7]. Newman and Clarke proposed the acronym CRAVED to explain e-commerce crime [4]. The authors identified, collected, examined, analyzed, and utilized available mobile forensic data related to the victim during and after the crime. It is possible to explain the selection of particular targets/victims of property offenders based on indicators related to CRAVED but adapted to the columbarium scam. Measuring CRAVED can be appropriate to the form of a specific context scam. These indicators are uniquely conceptualized and carefully reviewed below. The following CRAVED components are relevant to the columbarium scam.

- **Concealable:** Offenders will set up many dummy companies. Fabricated data is not open to the public. The victim has difficulty checking their hidden information or distinguishing the authenticity.

- **Removable:** Offenders can quickly move from one place to another. The fact that dummy companies are quickly established helps explain why the victim can be cheated repeatedly.

- **Available:** The Internet provides a quick way for offenders to find an attractive new victim, exchange their victim information, and discuss the follow-up countermeasures.

- **Valuable:** Judging whether there is a profit or not is a critical condition for offenders to choose a target.

- **Enjoyable:** Offenders in a fraud group have a performance competition system and a

generous bonus, encouraging them to commit crimes effectively.

- **Disposable:** Offenders have many targets to locate the next victim without hesitation. They prefer victims that are easy to cheat.

2.3.2. Suitable Targets

Offenders choose easy targets to constitute reasonable goals. A suitable target can include a person, an object, or a place. There must be a suitable target present at the very beginning. The VIVA acronym can be used to describe the judgment of a suitable target [5]:

- **V (Value):** According to the columbarium scam, T1 was a retired school teacher seeking long-term growth with moderate investment risk. She could have the potential to dispose of G1's valuable real estate. Several dozen withdrawals from her account were made, many going to several offenders' accounts.

- **I (Inertia):** T1 has low sensitivity and a lack of fraud vigilance. T1 fit the characteristics of a suitable target and was eventually targeted by offenders.

- **V (Visibility):** T1 had been engaged in the columbaria investment for a while. She was visible on the watchlist of scammers.

- **A (Access):** T1 enjoyed her investment and was willing to buy columbaria. She lived nearby offenders who could interview her weekly. That made it easy for offenders to approach and increased the persuasiveness possibility.

2.3.3. The Absence of a Capable Guardian

The presence of a capable guardian could discourage a crime from taking place. Guardianship can be effective in deterring offense from occurring. A capable guardian is anything or any person that discourages crime. Examples of capable guardians include alarm systems, spouses, and police officers. A simple control stops crime in space and time [5]. Her husband might be present in due time but may not have sufficient awareness to be an effective deterrent.

- Effortless: G1 was not informed until T1 was bedridden. Then, G1 could not be an effective deterrent in due time.

- Easy inducement: G1, busy at work, could hardly notice that T1 had taken his ID card and seal to transfer G1's house property.

- Low risk: The perception of fraud prevention and detection varies significantly in complexity, inherent risk, and size throughout the columbarium scam. There is no one-size-

fits-all method to address all issues or reduce risks.

3. Strategies to Battle Columbarium Scams

There are three RAT elements for forming the crime. If one of the three elements is missing, the crime can be effectively avoided. The following will explore the RAT prevention possibility. Fig. 6 illustrates the perspectives of criminals, victims, and guardianship from various components.

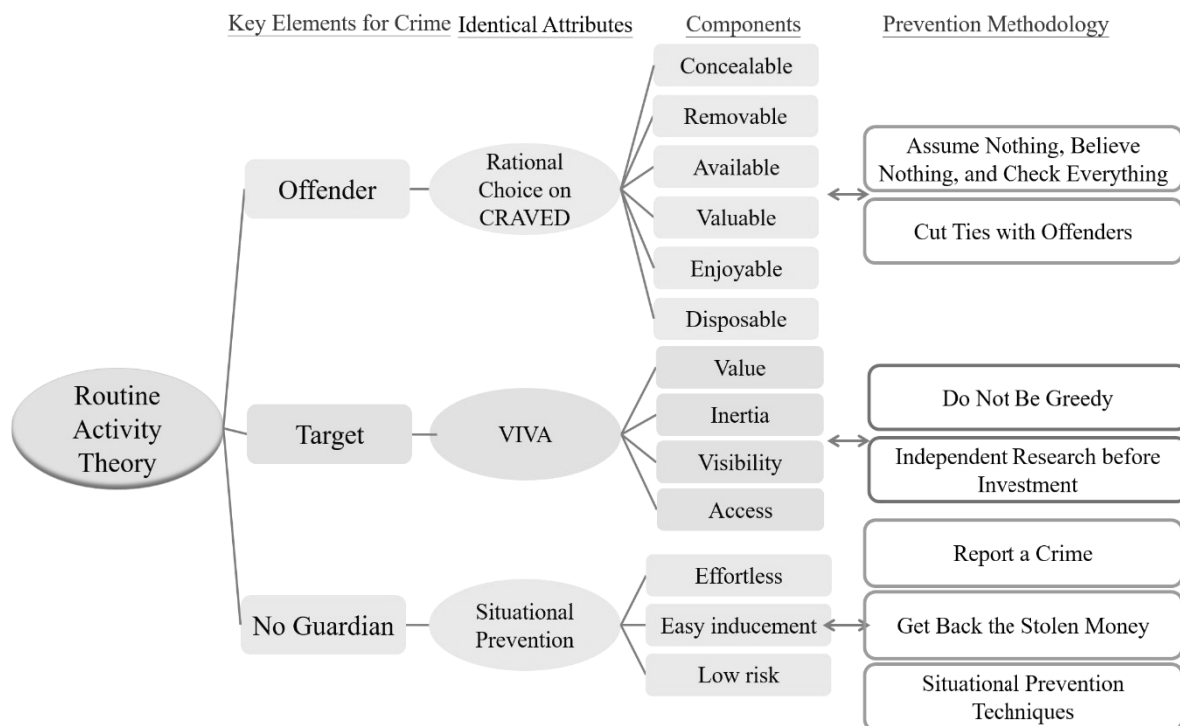


Fig. 6. Functional prevention analysis

3.1. Stay Away from Motivated Offenders

(1) Assume Nothing, Believe Nothing, and Check Everything

People should be vigilant and stay alert if someone talks about money, personal information, and bank accounts. Different columbarium scams may proclaim as friends, relatives, police, or prosecutors. That could be a red flag if a sale presentation focuses on how many persons have bought those products.

(2) Cut Ties with Offenders

Many scams are just listening to the other party's words, following his words, operating the remittance, and transferring money. Stop any phone calls, Internet communications, and

various requests from the other party when something abnormal happens.

3.2. Avoid being a Suitable Target

(1) Do Not Be Greedy

Not being greedy can help people steer clear when it comes to scams. A scam might happen if people are trying to get something for nothing. Offenders hit their targets with various persuasion techniques and know our weaknesses under the surface. Targets are usually tailored to psychological profiles. Under the right conditions, that inner lurking can be exploited.

(2) Independent Research before Investment

Fraud offenders count on people not to investigate before they invest. Fend them off by

digging for more information or references from other information sources. People should take time to do independent research.

3.3. Let Capable Guardian Involved

(1) Report a Crime

Police intervention can help victims get connected to other resources. They were afraid that reporting to the police might result in losing privacy. However, personal safety is the priority, and people's experiences may vary.

(2) Get Back the Stolen Money

If unfortunately deceived, legal means must be taken to have a chance to get it back. After reporting a crime, the victim should inform the bank account number, amount, time, and location. The complete information is critical to announce the fraudulent account as a warning account in the shortest possible time. The police can assist in activating a deposit mechanism to detain bank funds to prevent criminals from withdrawing them. The beneficiary bank will temporarily detain the amount and restrict the beneficiary account from withdrawing or remitting money. That is critical in getting cheated money back.

If people are lucky enough to freeze the fraudulent bank account immediately, offenders might not have time to collect the money. People can bring the criminal case report triple sheet, remittance proof document, ID card, and seal to request a refund. After the remaining funds in the account are returned to the closing statement, the defrauded money can be recovered. However, the return process is subject to repeated verification, taking two to three months. When a disputed case or other victims must be investigated together, it will take a long time to return the case and even wait until all the lawsuits are over.

(3) Situational Prevention Techniques

In 2003, Cornish and Clarke proposed strategies and techniques to prevent and reduce crime [5]. The methods applied in this case are listed below:

- Increasing the effort: Be careful with personal information making it difficult to access targets.

- Increasing the risks: Extend guardianship like bankers' vigilance.

- Reducing the inducement: Identify property and keep an eye on it.

4. Conclusions

There are three RAT causes of crime: a motivated offender, a suitable target, and the absence of a capable guardian. Offenders can randomly gain access to victims. People can protect themselves by not being an appropriate target and by not disclosing personal information on the Internet, questionnaires, or social media. Before engaging in investment, people should inquire about relevant information from trusted channels. People will be less likely to be led away by offenders' words with a deep understanding. If people are unfortunate to be defrauded, immediately reporting to the police can help protect our bank accounts or other property.

References

1. Cohen, L. E. and Felson, M., "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, Vol. 44, No.4, pp. 588-608, 1979.
2. Felson, M. and Cohen, L. E. "Human Ecology and Crime: A Routine Activity Approach," *Human Ecology*, Vol. 8, No. 4, pp. 389-406, 1980.
3. Fennelly, L. J., *Handbook of Loss Prevention and Crime Prevention* (6th ed.), Butterworth-Heinemann Publishing, pp. 1-50, 2020.
4. Newman, G.R and Clarke, R.V., *Superhighway Robbery: Preventing E-commerce Crime*, Willan Publishing, pp. 1-25, 2003.
5. Siegel, L. J., *Criminology: Theories, Patterns, and Typologies* (13th ed.), Cengage Learning Publishing, pp. 99-342, 2018.
6. Statistics-National Police Agency, <https://ba.npa.gov.tw/>
7. Wilcox, P., *International Encyclopedia of the Social & Behavioral Sciences* (2nd ed.), Elsevier Publisher, pp.194-199, 2015.

基於量化值迭代計算的單位圖彩色區塊截短編碼技術

王梓熏¹

國立臺中科技大學資訊工程系

¹sl110732017@nutc.edu.tw

洪維恩^{2,*}

國立臺中科技大學資訊工程系

^{2,*}wienhong@nutc.edu.tw

摘要

單位圖區塊截短編碼 (Single Bit-Map Block Truncation Coding, SBM-BTC) 是降低 AMBTC 用於彩色圖像壓縮的儲存成本為目標的有損圖像壓縮技術。因為 BTC 在計算上簡單，並且壓縮後圖像擁有不錯的品質，適用於雲端運算、物聯網和多媒體驗證等方面。過往的研究已經改進 SBM-BTC 的性能，但是改進後的圖像品質經常受到 SBM-BTC 的限制。本文針對 Hu et al. 提出的基於 SBM-BTC 的彩色圖像編碼方案中第一個方案，提高其壓縮後的圖像品質。此方案採用最佳規則生成公共位圖，並且使用量化值重新計算，來提高 SBM-BTC 的圖像品質。在本文研究中發現此方法產生的彩色圖像，其圖像品質還可以提升在，於是提出一個方法，將重新計算後的量化值用於產生新的公共位圖，再以新的公共位圖重新計算量化值，並控制重複執行次數。根據實驗結果，提出方法的平均圖像品質比 Hu et al. 的第一個方案多了 0.229 dB，證明提出方法確實有提供更好的圖像品質。

關鍵字：Color image coding、Block truncation coding、Single bit map block truncation coding。

一、緒論

隨著現代技術的快速發展，彩色圖像成為了使用廣泛的媒體，彩色圖像可以呈現這麼多種顏色是因為彩色圖像是由 R、G、B 三種顏色組合而成，每個顏色的像素值範圍為 0 到 255，約有 1600 多萬種組合。彩色圖像在儲存上會需要大量的空間，所以需要一種有效的有損圖像壓縮技術來降低圖像的儲存空間和提高傳輸速度。Joint Photographic Experts Group (JPEG) [14, 15] 是一種常見的有損圖像壓縮技術，它可以除去冗餘的圖像數據，並且可以在獲得極高壓縮率的同時擁有不錯的圖像品質。Vector Quantization (VQ) [9, 10] 會隨著資料密度分佈的變化影響權重，其壓縮的失真比例會隨著資料密度成反比。Block Truncation Coding (BTC) [7, 8] 該方法將圖像劃分為不重疊的塊，每個塊的壓縮碼由兩個量化值和一個位圖表示。BTC 所需的計算成本比 JPEG 和 VQ 低，並且提供不錯的圖像品質，因此 BTC 適用於低計算成本的多媒體應用。BTC 的主要缺點是高位元率，為了降低位元率採用了幾種方法，包括位圖省略 [4]、塊分類 [2, 13] 和量化值調整 [6]，這

些方法同時可以保持不錯的圖像品質。

Hu [4] 發現如果兩個量化值的差小於預定義的閾值，則位圖在重建圖像品質中的作用不是很重要。Chen et al. [2] 是根據圖像的複雜性將圖像劃分為不同大小的塊，然後採用 AMBTC 和位圖省略技術對圖像塊進行編碼。Hong [6] 根據位圖被替換後的翻轉率，優化了量化值，從而可以減少位圖更改的影響。

BTC 的提出是為了灰階圖像編碼，但是它也可以用在彩色圖像的壓縮，其做法是將彩色圖像分為三張灰階圖像，然後使用 AMBTC 壓縮灰階圖像，每個彩色圖像塊的壓縮碼由三個位圖和六個量化值組成。為了降低 AMBTC 用於彩色圖像壓縮的儲存成本，Wu 和 Coll [12] 提出 Single Bit-Map Block Truncation Coding (SBM-BTC)，使用一個公共位圖代替三個位圖來進行彩色圖像壓縮。[1, 16] 是基於 SBM-BTC 的改進圖像編碼方案，但這些方法圖像品質會受到 SBM-BTC 的限制。

Hu et al. [5] 提出了一個基於 SBM-BTC 的彩色圖像編碼方案，此方案的第一個方

案在和 SBM-BTC 相同的比特率下，有著比 SBM-BTC 更好的圖像品質。在 Hu et al. 的方法中，公共位圖和重新計算的量化值會影響重建圖像的質量。他們的方法在編碼過程中，產生公共位圖和重新計算的量化值只做一次，如果可以多進行幾次這兩個動作，可以使重建圖像的質量更好。本論文將 Hu et al. 第一個方法計算後的量化值重新生成公共位圖，然後再次重新計算量化值，並使用參數控制要重複執行幾次。與 Hu et al. 的方法相比獲得更好的圖像品質。

二、文獻探討

Block Truncation Coding (BTC) 由 Delp 和 Mitchell [3] 提出，為了使用 BTC 來壓縮灰階圖像，首先將圖像劃分為 N 個大小為 $m \times m$ 且不重疊的塊。對每個被劃分的塊，計算其平均值 v 。對塊中小於 v 和大於等於 v 的像素進行平均，可以得到低量化值 a 和高量化值 b 。使用大小為 $m \times m$ 的位圖 B 來記錄在解碼時應該使用哪些量化值。如果塊中的像素值小於等於 v ，則位圖上和該像素值對應的位元值設為 0；像素值大於 v ，則位圖上和該像素值對應的位元值設為 1。BTC 使用 (a, b, B) 來表示每個塊的壓縮碼，在解碼時需要掃描位圖 B 中記錄的位元值，若位元值為 0，則使用低量化值 a 重建像素，否則使用高量化值 b 重建像素。BTC 的編碼和解碼示例如下。假設 (55 72 73 78; 61 79 82 81; 75 83 81 82; 75 83 81 82) 為要編碼的圖像塊，其中分號為行尾。可以計算出此塊的平均值 $v = 76.4375$ 。將塊中小於 76.4375 的像素值進行加總並平均，最後在四捨五入到最近的整數，可以得到低量化值 $a = 69$ ，類似地可以得到高量化值 $b = 81$ 。再來可產生位圖 $B = (0001; 0111; 0111; 0111)$ 。最後， $(a, b, B) = (69, 81, (0001; 0111; 0111; 0111))$ 。要解碼 (a, b, B) ，將 B 中的 0 和 1 分別用 69 和 81 替換，可以得到解壓縮後的塊 (69 69 69 81; 69 81 81 81; 69 81 81 81; 69 81 81 81)。

Single Bit-Map Block Truncation Coding (SBM-BTC) 方法由 Wu 和 Coll 提出，是用來對彩色圖像做壓縮，其目的是為了降低 BTC 的比特率。此方法只使用一個公共位圖來進行彩色圖像塊的壓縮，而非使用三個位圖。在此方法中提出了三個規則用來產生公共

位圖，分別是多數規則、亮度規則和加權規則。多數規則中，若要壓縮一個 $m \times m$ 大小的彩色圖像塊，需要先將其依 R、G、B 三通道分成三個灰階圖像塊，然後使用 BTC 將每個灰階圖像塊進行壓縮，每個塊的壓縮碼分別為 (aR, bR, bmR) 、 (aG, bG, bmG) 和 (aB, bB, bmB) 。為了產生公共位圖 bmM ，需要比對 bmR 、 bmG 和 bmB 三個位圖，如果有兩個或三個相應的位元值為 1，則公共位圖 bmM 對應的位元值設為 1，否則設為 0。每個彩色圖像塊的壓縮碼為 $(aR, bR, aG, bG, aB, bB, bmM)$ 。亮度規則中，先將 $m \times m$ 大小的彩色圖像塊分成三個灰階圖像塊，然後使用 BTC 進行壓縮獲得壓縮碼 (aR, bR, bmR) 、 (aG, bG, bmG) 和 (aB, bB, bmB) 。在此規則中要生成公共位圖 bmL ，需要將彩色圖像塊的像素，經由公式 (1) 轉換成灰階像素。在公式 (1) 裡， cpR 、 cpG 和 cpB 分別為彩色圖像塊的 R、G、B 三通道的像素值：

$$cpL = 0.299 \times cpR + 0.587 \times cpG + 0.114 \times cpB \quad (1)$$

彩色圖像塊經過公式 (1) 轉換後，可以得到一個 $m \times m$ 大小的灰階圖像塊，接下來計算灰階圖像塊的塊平均，再用塊平均當作閾值，生成公共位圖 bmL 。當灰階圖像塊中的像素值大於塊平均，則 bmL 對應的位元值設為 1，否則設為 0。每個彩色圖像塊的壓縮碼為 $(aR, bR, aG, bG, aB, bB, bmL)$ 。加權規則中，先將 $m \times m$ 大小的彩色圖像塊分成三個灰階圖像塊，然後使用 BTC 進行壓縮獲得壓縮碼 (aR, bR, bmR) 、 (aG, bG, bmG) 和 (aB, bB, bmB) 。在此規則中要生成公共位圖 bmW ，需要將彩色圖像塊的像素，經由公式 (2) 轉換成灰階像素：

$$cpW = wR \times cpR + wG \times cpG + wB \times cpB \quad (2)$$

公式 (2) 裡， cpR 、 cpG 和 cpB 分別為彩色圖像塊的 R、G、B 三通道的像素值， wR 、 wG 和 wB 分別為 R、G 和 B 三通道轉灰階時的權重。此規則中，可以通過改變三通道的權重來生成不同的灰階像素值，作者依據他們的實驗將三通道的權重設為 $1/3$ 。彩色圖像塊經過公式

(2) 轉換後，可以得到一個 $m \times m$ 大小的灰階圖像塊，接下來先計算灰階圖像塊的塊平均，再用塊平均當作閾值，生成公共位圖 bmW ，當灰階圖像塊中的像素值大於塊平均，則 bmL 對應的位元值設為 1，否則設為 0。每個彩色圖像塊的壓縮碼為 (aR , bR , aG , bG , aB , bB , bmW)。

Hu et al. 提出了一個基於 SBM-BTC 的彩色圖像編碼方案，此方案中的第一個方法提出的目的是為了提高 SBM-BTC 的圖像品質 (PSNR)，並且維持相同的位元率。為了要編碼彩色圖像，首先將圖像劃分為大小為 $m \times m$ 且不重疊的彩色圖像塊。每個彩色圖像塊依照 R、G、B 三通道分成三個灰階圖像塊，這裡將三個灰階圖像塊稱為 GBR、GBG 和 GBB。對每個灰階圖像塊，計算其平均值，然後計算高低量化值。這裡將 aR 和 bR 作為 GBR 的高低量化值； aG 和 bG 作為 GBG 高低量化值； aB 和 bB 作為 GBB 的高低量化值。為了生成 $m \times m$ 大小的公共位圖 bmC ，需要計算 d_0 和 d_1 ，記錄將 0 和 1 分配給 bmC 中彩色像素 cp 對應的位元值造成的圖像失真，然後我們可以得到最好的選擇。 d_0 和 d_1 根據公式 (3)、公式 (4) 計算：

$$d_0 = (cp_R - a_R)^2 + (cp_G - a_G)^2 + (cp_B - a_B)^2 \quad (3)$$

$$d_1 = (cp_R - b_R)^2 + (cp_G - b_G)^2 + (cp_B - b_B)^2 \quad (4)$$

這裡 cp_R 、 cp_G 和 cp_B 分別是 GBR、GBG 和 GBB 中的像素。選擇 d_0 和 d_1 中較小的值，從而設置對應的位元值。如果 d_0 小於等於 d_1 ，則 bmC 中的對應位元值為 0； d_0 大於 d_1 ，則 bmC 中的對應位元值為 1。接下來使用量化級別重新計算，將每個灰階圖像塊的高低量化值重新計算。為了重新計算灰階圖像塊 GBR 的低量化值 aR 和高量化值 bR ，將 GBR 中和 bmC 對應位元值為 0 的像素加總並平均，將結果儲存給 aR 。類似地，將 GBR 中和 bmC 對應位元值為 1 的像素加總並平均，將結果儲存給 bR 。GBG 和 GBB 的高低量化值也可通過上述相同規則重新計算。最後，可以生成每個採測圖像塊的壓縮碼 (aR , bR , aG , bG , aB , bB ,

bmC)。為了使用接收到的壓縮碼 (aR 、 bR 、 aG 、 bG 、 aB 、 bB 、 BMC) 重建每個壓縮的彩色圖像塊，掃描公共位圖 bmC 中記錄的位元值，若位元值為 0，則使用低量化值重建像素，否則使用高量化值重建像素。當 $m \times m$ 的灰階圖像塊中的每個像素重建完成，則彩色圖像塊重建。將所有彩色圖像塊的壓縮碼以相同方式依次解碼後，即可得到壓縮後的彩色圖像。

三、提出的方法

在文獻探討中提到了 Hu et al. 的第一個方法，在研究中我們發現此方法產生的彩色圖像，其圖像品質還可以提升。在接下來的內容中，我們將提出改善的方法。在 Hu 等人的第一個方法中，將彩色圖像劃分成彩色圖像塊後，需要再將彩色圖像塊分為三個灰階圖像塊，然後計算三個灰階圖像塊各自的高低量化值，接著產生公共位圖，最後重新計算三個灰階圖像塊各自的高低量化值，得到每個彩色圖像塊的壓縮碼。在上述步驟中，產生公共位圖和重新計算高低量化值的部分，只做了一次，若是將重新計算的高低量化值，再次生成公共位圖，然後再重新計算高低量化值，最後生成壓縮碼，解壓後的彩色圖像比原本 Hu et al. 的圖像品質更好。

3.1 編碼過程

輸入：彩色圖像 I 、塊的大小 $m \times m$ 、要重複執行產生公共位圖和重新計算高低量化值的次數 cnt 。

輸出：每個分解塊的壓縮碼 (aR , bR , aG , bG , aB , bB)。

步驟一：將 I 劃分為大小為 $m \times m$ 且不重疊的彩色圖像塊。

步驟二：將彩色圖像塊依照 R、G、B 三通道分成三個灰階圖像塊。

步驟三：對每個灰階圖像塊，計算其平均值，然後計算高低量化值。

步驟四：使用公式 (3) 和 (4) 計算出 d_0 和 d_1 ，通過比較 d_0 和 d_1 ，產生公共位圖。

步驟五：重新計算每個灰階圖像塊的高低量化值。

步驟六：將步驟五重新計算的高低量化值代回步驟四產生公共位圖，再執行步驟五，依此循環重複執行 cnt 次。

步驟七：重複步驟二到步驟六，直到所有的彩色圖像塊都編碼完成。

3.2 解碼過程

輸入：所有的彩色圖像塊壓縮碼、塊的大小 $m \times m$ 、原始圖像的長和寬。

輸出：解壓縮後的彩色圖像。

步驟一：依次掃描彩色圖像壓縮碼。

步驟二：用壓縮碼中的公共位圖恢復三個灰階圖像塊，再依照 R、G、B 三通道組合成彩色圖像塊。

步驟三：重複步驟二，直到所有壓縮碼恢復成彩色圖像塊，再使用所有彩色圖像塊組成彩色圖像，即可得到解壓縮後的彩色圖像。

四、實驗結果

在本節的實驗中，使用了六張大小為 512×512 的彩色圖像作為測試圖像，包括 Lena、Jet、Tiffany、Pepper、House 和 Splash，如圖一所示。這些圖像可以從 USC-SIPI 圖像資料庫 [11] 中獲得。每個測試圖像被劃分為 4×4 大小的非重疊圖像塊。採用峰值信噪比 (PSNR) 度量來評估圖像品質，PSNR 根據公式(5)計算，其中的 MSE 為原始圖像和壓縮後圖像的均方差：

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ (dB)} \quad (5)$$



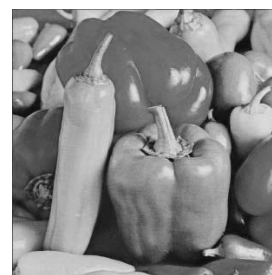
(a) Jet



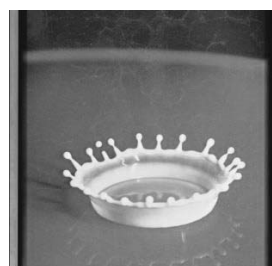
(b) House



(c) Lena



(d) Pepper



(e) Splash



(f) Tiffany

圖一：六張測試圖像

在表一中，展示了提出方法的圖像品質，在這裡參數 cnt 為 1 到 4，從這張表中可以發現隨著 cnt 數值上升圖像品質有逐漸提高。因為 4 之後的圖像品質已經不顯著提升，所以不列舉出來。

表一：提出方法的圖像品質表(單位：dB)

圖像	Cnt=1	Cnt=2	Cnt=3	Cnt=4
Jet	32.586	32.627	32.638	32.641
House	29.883	29.904	29.908	29.909
Lena	32.745	32.767	32.770	32.771
Pepper	32.015	32.053	32.064	32.066
Splash	36.238	36.270	36.273	36.274
Tiffany	34.129	34.157	34.161	34.162
平均	32.933	32.963	32.969	32.971

在表二中，展示了提出的方法和 Hu 等人第一個方法 (First Scheme, FS) 的圖像品質，用於比較的參數 cnt 設為 4，平均圖像品質分別為 32.971 dB 和 32.742 dB，提出方法的平均圖像品質比 FS 多了 0.229 dB，並且提出方法的圖像品質都比 FS 高，其中測試圖像 Splash 提升了 0.548 dB，提升得最多。以上表示提出方法的圖像品質確實比 FS 的更好。

表二：提出方法和 FS 圖像品質表(單位：dB)

圖像	Cnt=4	FS
Jet	32.641	32.464
House	29.909	29.787
Lena	32.771	32.657
Pepper	32.066	31.815
Splash	36.274	35.726
Tiffany	34.162	34.005
平均	32.971	32.742

五、結論

本研究針對 Hu et al. 提出的基於 SBM-BTC 的彩色圖像編碼方案中，第一個方法做出改進，將計算後得到的高低量化值，再次產生公共位圖，然後再重新計高低量化值，並且使用參數控制重複次數。實驗結果表明，提出的方法確實可以比 Hu et al. 的第一個方法提供更好的圖像品質。

六、參考文獻

1. Chang, C.C., Chen, T.S., and Chung, J.C., "A colour image compression scheme based on two layer absolute moment block truncation coding," Imaging Sci. J. 2000, 48(2), 53 - 62.
2. Chen, W.-L., Hu, Y.-C., Liu, K.-Y., Lo, C.-C., and Wen, C.-H., "Variable-Rate Quadtree-segmented Block Truncation Coding for Color Image Compression," Int. J. Signal Process. Image Process. Pattern Recognit. 2014, 7, 65 - 76.
3. Delp, E.J. and Mitchell, O.R., "Image coding using block truncation coding," IEEE Trans. Commun. 1979, 27, 1335 - 1342.
4. Hu, Y.-C. "Low-complexity and low-bit-rate image compression scheme based on absolute moment block truncation coding," Opt. Eng. 2003, 42, 1964 - 1975.
5. Hu, Y. C., Chang, I. C., Liu, K. Y., and Hung, C. L., "Improved Color Image Coding Schemes Based on Single

- Bit Map Block Truncation Coding," Optical Engineering, 2014, vol. 53, no. 9, Art. no. 093104.200
6. Hong, W., "Efficient Data Hiding Based on Block Truncation Coding Using Pixel Pair Matching Technique," Symmetry 2018, 10, 36.
7. Lin, C. C., He, S. L. and Chang, C. C., "Pixel Pair-wise Fragile Image Watermarking based on HC-based Absolute Moment Block Truncation Coding," Electronics, Vol. 10, No. 6, pp. 690, 2021-02. (SCI)
8. Nguyen, T. S., Son, Lin, C. C. and Chang, C. C., "High Capacity Reversible Data Hiding Scheme based on AMBTC for Encrypted Images," Journal of Internet Technology, Vol. 23, No. 2, pp. 255-266, 2022-03. (EI)
9. Qin, C., Chang, C.-C., and Chiu, Y.-P., "A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting," IEEE Trans. Image Process. 2014, 23, 969 - 978.
10. Qin, C., and Hu, Y.-C., "Reversible data hiding in VQ index table with lossless coding and adaptive switching mechanism," Signal Process. 2016, 129, 48 - 55.
11. The USC-SIPI Image Database. Availableonline: <http://sipi.usc.edu/database/>
12. Wu, Y., and Coll, D. C., "Single bit-map block truncation coding of color images," IEEE J. Sel. Areas Commun. 1992, 10(5), 952 - 959.
13. Xiang, Z., Hu, Y.-C., Yao, H., and Qin, C., "Adaptive and dynamic multi-grouping scheme for absolute moment block truncation coding," Multimed. Tools Appl. 2018, 78, 7895 - 7909.
14. Xie, X. Z., Lin, C. C. and Chang, C. C., "A Reversible Data Hiding Scheme for JPEG Images by Doubling Small Quantized AC Coefficients,"

- Multimedia Tools and Applications,
Vol. 78, No. 9, pp. 11443-11462,
2019-05. (SCI)
15. Xie, X., Chang, C. C. and Horng, J. H., "An EMD-based Data Hiding Scheme for JPEG Images," Connection Science, Vol. 33, No. 3, pp. 515-531, 2021-11. (SCI)
 16. Yang, C.K., Lin, J.C., and Tsai, W.H., "Color image compression by moment-preserving and block truncation coding techniques," IEEE Trans. Commun. 1997, 45(12), 1513 - 1516.

國家圖書館出版品預行編目（CIP）資料

資訊管理學術暨警政資訊實務研討會. 2022年第25屆：「元宇宙的創新應用與偵查」論文集/邱靖宸, 張明桑, 林曾祥等著. -- 初版. -- 桃園市：中央警察大學資訊管理學系, 2022.06

面；公分

ISBN 978-626-95418-2-9（平裝）

1.CST:警政 2.CST:警政資訊系統 3.CST:文集

575.807

111009148

2022年第25屆資訊管理學術暨警政資訊實務研討會-「元宇宙的創新應用與偵查」論文集

發行者：陳擇文

編輯者：林曾祥

出版者：中央警察大學資訊管理學系

作者：邱靖宸、張明桑、林曾祥等著

地址：33304 桃園市龜山區大崗里樹人路 56 號

電話：(03)328-5189

印刷者：尚曄文化事業有限公司

地址：22066 新北市板橋區板新路 103 號 4 樓之 1

電話：(02)2958-6010

二〇二二年六月初版集

版權所有，翻印必究