設計與實作基於多重封包樣態比對之加密貨幣挖礦行為偵測

蔡邦維 [1*]
[1] 國立中央大學資訊管理學系
[1]pwtsai@ncu.edu.tw

摘要

近年來，運用區塊鏈技術所實作的加密貨幣及其相關應用逐漸在資訊金融領域間興起。因為在加密貨幣的交易過程中需要運用密碼學技術來進行雜湊計算，記帳過程中的參與者 (礦工) 會因為提供運算資源 (挖礦) 而獲得獎勵，故吸引了許多人投入。由於挖礦過程中所獲得的加密貨幣獎勵可以透過交易所與法幣進行換匯，因此也容易吸引有心人士透過不正當手段獲取運算資源進行挖礦。常見的手法包括以惡意軟體控制受駭設備進行挖礦，或者在網頁中嵌入腳本讓瀏覽網頁的使用者貢獻設備資源協助挖礦。本研究將以網路封包樣態檢測的角度切入，以常被惡意軟體所選擇挖掘的門羅幣為目標，分析挖礦軟體與礦機之間的溝通行為模式，再根據封包特徵值產出比對規則並進行實驗驗證。本研究中設計的規則可供網路管理人員搭配封包檢測系統使用，並能藉由規則所觸發的事件紀錄進一步追查，評估相關設備是否已淪為惡意軟體所控制的門羅幣礦機。

關鍵詞：加密貨幣、區塊鏈、挖礦惡意軟體、封包檢測

* 通訊作者 (Corresponding author.)

Design and Development of Multi-Pattern Matching Rules for Detecting Cryptocurrency Mining in Packet Inspection

Pang-Wei Tsai[1*]
[1]Department of Information Management, National Central University
[1]pwtsai@ncu.edu.tw

Abstract

In recent years, cryptocurrency built by blockchain technology is getting more and more popular in both information technology and financial industries. Because of providing resources to support hash computing (known as mining) , participants (known as miners) will get cryptocurrency rewards. Therefore, it becomes the reason that attracts many people to join the mining process. Since exchanging cryptocurrency reward to legal money is possible, it interests people with bad intention to use improper means to obtain computing resources for mining, such as using malware to manipulate hacked equipment to install miner software or enabling drive-by download attack to acquire computing resource from web client. This research studies Monero, a cryptocurrency often selected by malwares, trying to investigate its communication progress between miner and mining pool, and extracts packets to get signatures for developing detection rules with corresponding patterns. The experiment results show that applied rules are able to detect suspicious networking activities related to Monero mining. By using implemented rules in this paper, it aims to help network administrators investigate whether the equipment have been infected by Monero mining malware.

Keywords: Cryptocurrency, Blockchain, Mining Malware, Packer Inspection

壹、前言

隨著比特幣[2]和區塊鏈[10]概念的嶄露頭角，近年來運用其相關技術所實作的加密貨幣及其應用逐漸在資訊金融領域興起。雖然世界上大部分金融機構對於加密貨幣多半處於謹慎且觀望的態度[7]，但已經有電子商務支付平台[15]宣布接受使用主流的加密貨幣付款，同時也有信用卡公司允許消費時以加密貨幣為單位進行結算[22]。除此之外，在加密貨幣市場中亦有許多中心化或去中心化的交易所[11, 17]，提供客戶在不同加密貨幣之間換匯或者兌換為法幣。當有企業發新聞稿宣布支援使用加密貨幣付款時，被列入支援清單內的加密貨幣幣價多半會攀升上漲且交易熱絡；倘若政府或金融監管單位發出對加密貨幣非正面的消息時，則幣價很可能應聲跌落。由於漲跌之間會衍生出套利的空間，因此也吸引了投資者將加密貨幣市場視為股市般進行操作，亦有專業人員會設計程式策略去監控不同交易所的幣價，當價差到達門檻時隨即透過自動交易機器人買賣。近幾年比特幣分別在 2013、2017 以及 2021 年與法幣的匯率出現大幅波動，即使法律上對於加密貨幣資產並沒有正式認可，還是吸引了許多人考慮將加密貨幣納入個人資產之中，同時加密貨幣與法幣之間的交易市場份額也持續擴大成長。

對於創建一個新的加密貨幣而言，所需的條件為建立有人維護的節點及區塊鏈網路(也可透過其他既有的鏈作為側鏈運作，此時就不需要維護自己的區塊鏈節點) 。由於創建的過程並不像金融商品需要經由監管機構的審查和取得許可，因此造成了許多新興的加密貨幣如同雨後村筍般地出現。甚至創建新幣成為了一種資訊服務，可以由專業人員協助出資者發行新的加密貨幣和建立其區塊鏈節點維持運作。當一個加密貨幣的區塊鏈節點不再有人願意去維護，也就等同於宣告了這個貨幣的退場。根據調查統計[16]，目前已經有超過 1000 個以上的加密貨幣面臨消失的困境；雖然市場上尚有 3000 多個加密貨幣專案在進行，但其中某些加密貨幣的區塊鏈網路因為節點數量過少，未來的處境也不甚樂觀。即便如此，仍然有許多新的加密貨幣專案持續展開，主流的加密貨幣專案也不斷地在精進其設計以支援更多元的商務應用、更彈性的交易方式、或者是提升對於節點和網路的安全保護以維護其區塊鏈運作。

由於加密貨幣的交易是運用密碼學技術來進行雜湊運算，對於目前以工作量證明(Proof-of-Work, POW[4]) 方式運作的加密貨幣而言，再將交易打包產生新區塊這個過程中，若能夠有越多的分散式運算單元參與競爭 (俗稱挖礦) ，可更加的去中心化並提升交易記帳過程中的安全性。而在這個過程中維護挖礦設備的角色 (也就是俗稱的礦工) ，在新區塊被承認時即會獲得一筆獎勵，因此吸引了許多人投入挖礦的行列。例如將自己個人電腦安裝挖礦軟體 (Mining Software/Miner) ，使用電腦中的 CPU 運算資源挖礦；或者是在主機中配置多張高階顯示卡，運用 GPU 進行挖礦。甚至有礦工會使用 FPGA 或者訂製的 ASIC 來組建針對特定幣種的礦機，並租賃機房場地建立專業礦場集中算力(Hash Rate) 。為確保獲得穩定的獎勵份額，有的礦工會透過礦池 (Mining Pool) 聯合進行挖礦，再根據於礦池中的貢獻度獲得穩定的分潤。獲得獎勵的礦工可以再透過交易所

將加密貨幣換成法幣，也可以和其他加密貨幣進行換匯，又或者把手上的加密貨幣借出收取利息，以獲得更多的利益。

隨著利多的新聞消息持續散佈，挖礦所獲得的回報在幣價上漲時累積起來時非常可觀，因此也吸引了有心人士使用非正規的方式來獲取運算資源進行挖礦。例如讓使用者不經意安裝含有惡意程式的軟體、在網頁伺服器中植入掛馬、或者是藉由資安漏洞感染電腦使其成為殭屍網路 (Botnet) 的一部分，再透過 C&C 伺服器操控電腦進行挖礦。為了防堵這些惡意攻擊的手法，可以透過安裝防毒軟體、設置防火牆、或者是建立應用程式白名單機制去偵測異常挖礦行為。但持續進化的挖礦惡意軟體有時是難以被察覺到的，例如會自主調整其消耗的運算資源總量，讓電腦不會有操作遲緩的感覺，令人防不勝防。特別是在一些較難嚴格控管的設備 (例如學校電腦教室主機、嵌入式系統、物聯網裝置等) ，有較大機會因為系統軟體上的漏洞而成為挖礦惡意軟體的目標。此時除了在裝置上要建立保護措施之外，也應該要在網路層搭配偵測防護的機制，根據監測到的資訊對疑似受害的設備進行處理，例如透過防火牆或路由規則阻斷相關 IP 的網路連線，避免因惡意軟體的挖礦行為佔據資源影響運作。

在本研究中，將以網路封包態樣檢測的角度切入，探討在不牽涉安裝軟體或改變電腦主機配置的前提下，透過封包檢測設備來偵測挖礦軟體所產生的流量，提供網路管理人員可信的資訊判斷是否要進行處理。在研究方法部分會先針對所選定的挖礦軟體之通訊模式進行封包樣態分析，接著萃取出能夠作為判斷依據的特徵值，再轉換為可被封包檢測系統運用的規則，最後實際驗證是否可以達到預期效果。由於門羅幣 (Monero, [18]) 所標榜的 1-CPU-1-vote 策略及其演算法特性，讓具備 CPU 的裝置皆有機會提供算力；相較於其他幣種所使用的雜湊演算法，門羅幣的挖礦門檻低，故較容易受到挖礦惡意軟體的青睞。基於上述原因，本研究將以門羅幣作為研究標的，觀察並分析門羅幣挖礦軟體之運作行為，設計出對應其挖礦行為的偵測規則，再將規則佈署到封包檢測系統中進行實驗，以驗證和評估其偵測效果。

本篇論文第二章為相關文獻之回顧，首先會介紹門羅幣及其挖礦演算法的演進，接著列舉數種常見的惡意挖礦手法，並針對這些手法的特色進行討論。第三章會說明檢測方式的設計、封包的樣態分析、以及如何產出挖礦行為比對之規則。在第四章會實際將能辨識挖礦行為的規則應用到封包檢測系統上，實際驗證所產出的規則是否能被觸發，並評估其辨識結果。最後在第五章會對本研究作出總結。

貳、文獻探討

2.1 門羅幣

門羅幣是在 2014 年時以強化交易隱私為方向發展的加密貨幣[3]，縮寫代號為 XMR，

初始時是基於 CryptoNote 這個開源協議來強化交易的混淆性，藉此讓交易的發起對象和發送對象難以被追蹤，以達到保護加密貨幣交易者隱私的目的，其相關的隱私功能設計如下所述。

環狀簽名 (Ring Signatures) —基於 CryptoNote 發展，在 2017 年實作的 Ring Confidential Transactions (RingCT[6]) 交易方式，其特色是使用環形的方式對交易進行簽章背書。RingCT 裡面包含了兩個實作項目：Multilayered Linkable Spontaneous Anonymous Group (MLSAG) 以及 Confidential Transactions (CTs) 。前者是負責將原始交易模糊化，讓真正的發起人身分混淆，同時也避免交易地址之間的關聯性被得知；後者則是實現交易金額的隱藏，讓原始交易的金額能夠不被追蹤。

隱身地址 (Stealth Addresses) —在門羅幣交易時所使用的錢包地址部分，能夠產生一次性的收款地址來保護接收者。其使用之背景技術是以 Elliptic Curve Diffie-Hellman (ECDH [20]) 為基礎來產生金鑰。

防彈協議 (Bulletproofs)—在 2018 年實作的非交互式零知識證明 (Zero-Knowledge Proof [1]) ，取代了原本在交易中的簽名方式，在不影響交易隱私性的前提下，精簡交易模糊化的過程並同時提升其轉帳效率，藉此讓交易過程的手續費可以降低。在門羅幣導入防彈協議後除了降低轉帳所需的手續費以外，也增加了更多使用者以門羅幣進行小額支付的意願。

蒲公英改進協議 (Dandelion++[18])—在 2020 年針對交易隱私進行強化的設計，改變交易在網路中廣播的方式，讓交易過程難以和區塊鏈節點的 IP 位址產生關連性，藉由混淆廣播交易的來源，以降低門羅幣使用者被追蹤交易身份的風險。

2.2 門羅幣挖礦演算法演進

因為門羅幣匿名的特性，對於非法交易難以追蹤其轉帳資訊，故受到使用加密貨幣進行交易的暗網市場歡迎；再加上運作挖礦軟體的硬體的需求門檻低 (具備 CPU 即可進行) ，也使其成為 Botnet 控制者經常選擇挖礦的幣種[5]。由於常見 POW 幣種的演算法可以透過挖礦軟體以 GPU 的大量核心進行運算，這種情況會讓使用 GPU 進行挖礦的礦工比起使用 CPU 的礦工具備更多的算力輸出。但由於門羅幣社群幣不樂見 GPU 及 ASIC 礦機參與挖礦造成算力和獎勵發放過於集中，故持續的進行挖礦演算法的調整。門羅幣迄今更替的挖礦演算法如表一所示，目前所使用的 RandomX [19]演算法是 2019 年所提出的，當區塊鏈每增加固定區塊數量之後會對驗證用的關鍵區塊雜湊值進行調整，並搭配隨機模式和針對快取容量的要求來降低使用 GPU 及 ASIC 進行挖礦的效率。特別是 ASIC 礦機因為晶片快取記憶體通常空間較小 (使用外部記憶體會因為存取延遲造成運算效率降低) 而受到影響。在切換到 RandomX 演算法後，可讓快取空間不足的 ASIC 礦機在改版中被淘汰，無法繼續進行挖礦。除此之外，由於嵌入式物聯網裝置的 CPU 快取通常容量較小，沒辦法讓挖礦軟體有效運作，因此在這些 low-end 硬體上只能轉挖其

他使用舊演算法的幣種。

表一：門羅幣演算法的演進

演算法名稱	時間	說明
CryptoNight	創建時	CryptoNight 是一開始所使用的演算法，挖礦過程中需要進行大量的 AES 運算以及存取快取記憶體。以 GPU、FPGA 或者訂製的 ASIC 礦機進行挖礦時，會比單純使用 CPU 的礦機更有效率。
CNv1 (CrypotoNight v7)	2018 年 4 月	門羅幣社群開始認為有支援 CryptoNight 演算法的 FPGA 和 ASIC 礦機大量投入，會因為算力壟斷在特定地方不夠去中心化，進而對交易隱私造成衝擊，因此決定進行硬分岔以調整 POW 演算法。
CNv2 (CrypotoNight v8)	2018 年 10 月	社群認為先前的 CNv1 演算法調整未能有效的防堵 FPGA 以及 ASIC 礦機挖礦，因此再次的進行硬分岔以調整 POW 演算法，並開始投入新的 RandomX 演算法開發工作。
CN-R (CrypotoNight R)	2019 年 3 月	即使改成 CNv2 演算法，依然未能有效的防堵 FPGA 以及 ASIC 礦機挖礦，因此門羅幣又再次的進行硬分岔調整成 CN-R 演算法，並加速新的 RandomX 演算法開發工作。
RandomX	2019 年 11 月	由於 RandomX 演算法的特性，使用 CPU 挖礦再度擁有優勢，特別是具備較大 L3 快取的 CPU 表現更佳。儘管 FGPA 礦機調整設計後能夠繼續挖礦，但單張卡的表現不若以往 (增加快取容量會需要用到較多的邏輯閘，但板卡資源有限) 。

2.3 常見之門羅幣挖礦惡意軟體手法

網頁挖礦—透過電腦、手機、或平板瀏覽網頁，是許多人日常生活中不可或缺的一環。若能在網頁植入掛馬，可在使用者不知情的情況下安裝挖礦軟體；又或者是經由網路廣告投放的插件，在瀏覽到廣告頁面時進行網頁挖礦。雖然網頁挖礦能產生的算力有限，但許多台設備累積起來的算力會非常可觀。Coinhive[12]即為其中一個有名的網頁挖礦軟體，是使用 JavaScript 所撰寫的。當使用者瀏覽被植入掛馬的網頁後，會自動下載 Coinhive 挖礦程式進行挖礦。另外根據設定，也可以選擇要啟用多少個執行緒調整算力，避免使用者因網頁瀏覽不順暢、發熱、或者 CPU 使用率過高而察覺異常。CoinIMP [13]

則是另外一個網頁挖礦的專案，同樣也是使用 JavaScript 所撰寫。但在門羅幣更換為 RandomX 演算法之後，由於手機和平板的 CPU 快取通常容量較小，同時網頁挖礦軟體也難以支援其浮點運算需求，故透過網頁進行門羅幣挖礦的惡意軟體已大幅減少，多半已改挖其他對快取大小要求較低的幣種。

藉由網路攻擊手法植入挖礦軟體—在這類型的方式中，可以將開放原始碼的軟體嵌入 bot 程式後偽裝成正常的軟體放在網際網路上，供不知情的使用者下載安裝，另外也可以透過系統軟體漏洞、蠕蟲攻擊、或引誘使用者點擊惡意連結安裝木馬程式等方式植入。例如某知名的網路儲存伺服器製造商的產品，就曾經因為部分使用者未能及時安裝修補軟體，導致伺服器被植入 Coin miner 進行挖礦[14]。此外殭屍網路也一直是惡意挖礦的一個溫床，當受感染裝置被 C&C 伺服器控制時，往往會淪為礦機，為幕後的操控者持續挖礦以賺取加密貨幣。要避免成為受害者，除了提升使用者的資安素養，例如對釣魚信件或可疑的連結能有所警覺之外，同時電腦主機也應該要安裝防毒軟體，持續更新套件和修補程式，避免因漏洞讓設備被植入惡意軟體進行挖礦；同時也可以在網路部分搭配入侵偵測系統或封包檢測設備，監控是否有疑似挖礦軟體的行為，再透過防火牆攔截或於路由器下 blackhole 規則以阻斷相關 IP 的網路連線。

參、研究方法

本章節將說明觀測和蒐集挖礦軟體進行門羅幣挖礦時的細節、挖礦過程中有哪些連線行為封包適合萃取出特徵值作為判斷規則、以及如何去結合網路封包檢測設備運用這些規則，並試作出適用於門羅幣挖礦行為偵測的封包辨識規則組合。

3.1 挖礦行為模式分析

為了解挖礦軟體運作的過程，本研究中先建立了觀察用的實驗環境，安裝蒐集到的軟體模擬礦機的運作，再透過網管型交換器以 port-mirroring 方式導出鏡像流量到分析主機並錄製成 pcap 檔案，接著以腳本針對蒐集到的封包檔進行初步處理，再將收集到的封包 header 及 payload 內容進行解析，最後以人工方式進行資料的彙整。

3.2 態樣分析與特徵值萃取

經由所觀測到的挖礦軟體行為模式，可初步歸納出適合作為判斷規則的動作包含了礦池域名查詢、特定的網路連接埠、礦機與礦池 (或代理伺服器) 與 Stratum Protocol[8] 相關之 JSON-RPC 溝通行為、以及礦機與礦池 (或代理伺服器) 之間的挖礦互動等四種，以下將對這些行為分別進行說明。

礦池域名查詢—首先在礦池域名查詢部分，經由觀察目前主流的大礦池所使用的域名可以發現”mine”、”mining”、”pool”等關鍵字出現的比率極高；另外為凸顯挖掘的幣種是門羅幣，礦池多半會使用帶有”monero”或者是”xmr”作為關鍵字的域名字串，而支援多種幣種挖礦的礦池也會根據不同的幣種名稱再去進一步配置三級域名。因此透過 UDP/53 進行域名查詢的封包且帶有上述關鍵字的話，即可判斷有很高的機率是安裝了挖礦軟體的設備送出 DNS Query，以查找礦池或者是挖礦代理伺服器域名所對應的 IP 位址。雖然目前使用 DNS over HTTPS 方式進行域名查詢的方式尚未普及，但由於加密後的查詢流量會造成比對上的困難，故未來勢必需要針對這部分擬定因應措施。

特定的網路連接埠—經由觀察礦池所提供之挖礦服務連接埠部分，同樣可發現目前主流大礦池所提供的服務埠口會選擇使用 1111、3333、或 5555 這類型的數字。故檢查是否有符合相關目的/來源埠口的封包，即能輔助判斷是否有可疑的連線行為。但由於部分礦池有提供 TLS 的加密連線，會使用 TCP/443 作為挖礦服務的連接埠，這種情況下就較難用此方式進行判斷。頂多在一開始 TLS 交握的過程中，有機會透過檢查憑證中的 Common Name 是否有礦池域名的關鍵字來辨識。因此這部分建議作為輔助參考，需要搭配其他的特徵值進行判斷。

礦機與礦池 (或代理伺服器) 間的 JSON-RPC 溝通行為—在礦池中因為會有許多不同的礦工參加挖礦，因此礦機在進行挖礦動作前會需要先和礦池進行交握，並藉由 JSON-RPC 溝通提供能辨識自己的資訊，例如錢包地址、帳號、或其他登入資訊等 (這樣礦池才能統計礦工所有礦機的貢獻度進行分潤) 。剛開始進行交握的封包內容通常會有”method”的關鍵字，再搭配其他如”login”、”submitLogin”、”authorize”等的關鍵字，將身份辨識資料告知礦池。因此萃取出相關封包特徵值後即可作為檢測的依據，判斷內部網路是否有被礦機所使用的 IP 與外部網路的礦池 (或代理伺服器) 連線。

礦機與礦池 (或代理伺服器) 間的挖礦互動—在挖礦流程中，當礦機完成身份驗證的動作之後，會開始向礦池要求工作 (job) 並 pull 資料回自己本機端進行運算，完成後會回報給礦池；相對的礦池在收到運算結果也會判斷是否為有效的份額 (share) 並回傳結果給礦機。在互動的過程中，封包內容會出現例如”getWork”和”submit”等的關鍵字。由於挖礦過程中會一直持續重複出現 job submit 的動作，故萃取出相關封包特徵值後亦可作為檢測的依據，判斷內部網路是否有礦機和礦池在進行挖礦工作上的互動。

肆、實驗驗證

根據適合作為挖礦判斷的封包特徵值，本研究中總共試作了約 500 條的挖礦檢測規則，並將其調整成符合 snort [9]通用規則的格式。以下將對應到四種行為的規則分別列舉出範例說明，如表二所示。為確認試作的規則是否能有效判別，本研究將試作的挖礦規則檔匯入一台安裝了 suricata[21] 4.0.5 版本的 HP ProLiant DL380 G7 伺服器 (具備兩

顆 Intel E5620 處理器、16G 記憶體及 Ubuntu18.04 作業系統) ，並在 sniffer 模式下灌入測試資料流量進行實驗。將灌入封包之時間戳記對照事件紀錄 (以月為單位劃分，共三個月) 進行統計後，分別產出了約 39 萬筆、43 萬筆、37 萬筆的紀錄。測試的結果符合預期，證明了試作的門羅幣挖礦規則能夠成功被觸發。若進一步交叉比對，過濾掉具有相同 IP 來源的紀錄進行檢視，可發現有 20 多個 IP 疑似出現門羅幣挖礦的流量，大概占全部測試資料中 IP 數量之 0.5%。若實際應用於真實網路環境時，這些資訊可供網路管理人員進一步追查使用相關 IP 的設備，或追蹤連線的對外路由後與資安單位合作進行防堵。

表二：試作的挖礦規則範例

進行礦池域名查詢	alert dns $HOME_NET any -> any any (msg:"Suspicious DNS query for cryptocurrency mining pool (mine.moneropool.com) "; dns_query; content:"mine.moneropool.com"; isdataat:!1,relative; nocase; classtype:string-detect; sid:1000001; rev:1;)
特定連接埠連線	alert tcp $HOME_NET any -> any [1111,2222,3333,4444,5555] (msg:"Suspicious cryptocurrency mining pool connection"; sid:1000002; rev:1;)
JSON-RPC 行為	alert tcp $HOME_NET any -> any any (msg:"Suspicious Stratum cryptocurrency miner login to pool"; flow:to_server,established; content:"method"; depth:6; offset:2; content:"login"; distance:4; within:5; content:"params"; distance:4; fast_pattern; within:6; content:"login"; distance:5; within:5; classtype:string-detect; sid:1000003; rev:1;)
挖礦互動 (登入動作)	alert tcp $HOME_NET any -> any any (msg:" Suspicious general mining protocol miner login to pool"; flow:to_server,established; content:"mining."; pcre:"/mining. (subscribe|authorize) /im"; classtype:string-detect; sid:1000004; rev:1;)
挖礦互動 (上傳動作)	alert tcp $HOME_NET any -> any any (msg:" Suspicious general mining protocol miner submit share to pool"; flow:to_server,established; content:"mining."; pcre:"/mining.submit/im"; classtype:string-detect; sid: 1000005; rev:1;)

伍、結論

本論文介紹了加密貨幣的背景、礦工與礦機之間的關係、以及說明惡意軟體如何取得資源進行挖礦的方式。論文研究中選擇透過 CPU 即可進行挖礦的門羅幣作為探討的

標的。先藉由觀察門羅幣挖礦軟體與礦池之間的互動了解其溝通模式，接著萃取出能作為判斷依據的封包特徵值，再試作可用於封包檢測系統辨識用的規則進行驗證。實驗結果確認了試作的規則可以成功被觸發，相關紀錄亦可供網路管理人員進一步與其他資安紀錄比對，評估使用相關 IP 之設備是否已淪為由惡意軟體所控制的礦機。

[誌謝]

本研究承蒙科技部專題研究計畫 (MOST-109-2221-E-006-167 和 MOST-109-2222-E-008-005-MY3) 補助，以及國立成功大學資通安全研究與教學中心、國家高速網路與計算中心 TWAREN 網路研發團隊協助，特此感謝。

參考文獻

[1] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," *in proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pp.103-112, 1988.

[2] P. Franco, *Understanding bitcoin*, Wiley, 2014.

[3] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security & Privacy*, vol.16, no.4, pp.38-45, 2018.

[4] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols," *Secure Information Networks*, pp.258-272, 1999.

[5] E. Le Jamtel, "Swimming in the Monero pools," *in proceeding of the International conference on IT security incident management & IT forensics*, pp.110-114, 2018.

[6] S. Noether, and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol.1, pp.1-18, 2016.

[7] G. Pieters, and S. Vivanco, "Financial regulations and price inconsistencies across Bitcoin markets," *Information Economics and Policy*, vol.39, pp.1-14, 2017.

[8] R. Recabarren and B. Carbunar, "Hardening stratum, the bitcoin pool mining protocol," *Privacy Enhancing Technologies*, vol.3, pp.57-74, 2017.

[9] M. Roesch, "Snort: Lightweight intrusion detection for networks," *LISA*, vol.99, no.1, pp.229-238, 1999.

[10] Z. Zheng, et al., "Blockchain challenges and opportunities: A survey." *International Journal of Web and Grid Services*, vol.14, no.4, pp.352-375, 2018.

[11] "Binance," [Online], Available: https://www.binance.com (2021/03/05)

[12] "Coinhive," [Online], Available: https://blog.avast.com/coinhive-shuts-down (2021/03/05)
[13] "CoinIMP, [Online], Available: "https://www.coinimp.com (2021/03/05)
[14] "Cryptomining malware on NAS servers," [Online], Available: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/Cryptomining-malware-on-NAS-servers.pdf (2021/03/05)
[15] "Cryptocurrency on PayPal," [Online], Available: https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398 (2021/03/05)
[16] "List of Dead Coins and Failed ICOs," [Online], Available: https://www.coinopsy.com/dead-coins/ (2021/03/05)
[17] "MDEX," [Online], Available: https://mdex.com (2021/03/05)
[18] "Monero: the secure, private, untraceable cryptocurrency," [Online], Available: https://github.com/monero-project/monero (2021/03/05)
[19] "RandomX," [Online], Available: https://github.com/tevador/RandomX (2021/03/05)
[20] "Standards for Efficient Cryptography - SEC 1: Elliptic Curve Cryptography," [Online], Available: https://www.secg.org/sec1-v2.pdf (2021/03/05)
[21] "Suricata," [Online], Available: https://suricata-ids.org (2021/03/05)
[22] "Visa Rewards Card for Crypto," [Online], Available: https://blockfi.com/credit-card-waitlist/ (2021/03/05)