國立臺北大學
National Taipei University

加密貨幣交易紀錄分析與粉塵攻擊辨識之研究—以比特幣為例

Research on Cryptocurrency Transaction Record Analysis and Dust Attack Detection: Based on Bitcoin

關鍵字：區塊鏈、比特幣、加密貨幣異常交易、攻擊、辨識、大數據、粉塵交易

溫演福
國立臺北大學
資訊管理研究所 教授

張凱倫
國立臺北大學
資訊管理研究所 碩士生

摘 要

比特幣兼具匿名性與去中心化優勢，卻衍生粉塵攻擊等濫用行為。粉塵攻擊透過大量低價值、低費率交易（遠低於手續費）製造零碎UTXO，造成內存池壅塞、延長正常交易確認時間，並推高手續費率。本研究從系統面與使用者面探討粉塵攻擊對網絡穩定與交易效率的影響，並開發即時辨識演算法，鎖定粉塵交易與攻擊者行為。分析重點包括：粉塵UTXO在不同地址類型與腳本複雜度下對受害者手續費成本的累積效應；攻擊者利用低費率與多重簽名、時間鎖等腳本放大解鎖成本；以及透過SegWit與Legacy地址轉換優化攻擊成本與效率。

研究問題與方法分析

- **粉塵攻擊危害面向**
  1. **系統層(比特幣內存池)**：觀察內存池受到粉塵攻擊的壅塞狀況、交易手續費率變化、以及粉塵攻擊的交易特徵。
  2. **使用者層(比特幣地址)**：針對受害者地址，分析在持有粉塵UTXO時的解鎖成本。
- **資料蒐集與建立**
  1. **系統層粉塵攻擊危害資料集**：蒐集2024/6/16–12/19內存池Pending交易 59,359,347筆。
  2. **使用者層粉塵 UTXO 危害資料集**：蒐集2024全年度區塊內接收到粉塵UTXO的受害交易7,807,178筆。
- **粉塵攻擊辨識評估機制**
  1. **粉塵攻擊辨識評估機制**：評估不同型態的粉塵攻擊交易對內存池造成的危害，並分析受到粉塵的攻擊效應與額外付出成本。
  2. **粉塵UTXO字節數危害評估演算法**：評估粉塵UTXO的字節數，以及分析粉塵UTXO是否故意使用多簽腳本增加字節負擔。
  3. **粉塵UTXO攻擊效應危害評估機制**：評估並觀察粉塵交易是否以低費率發送UTXO，迫使受害交易因字節數增加額外成本。
  4. **粉塵UTXO轉址攻擊危害評估機制**：評估並觀察粉塵交易是否透過轉地址的方式，以低費率由SegWit發送粉塵UTXO至Legacy，從而放大攻擊效應，迫使受害花費更高額外成本。

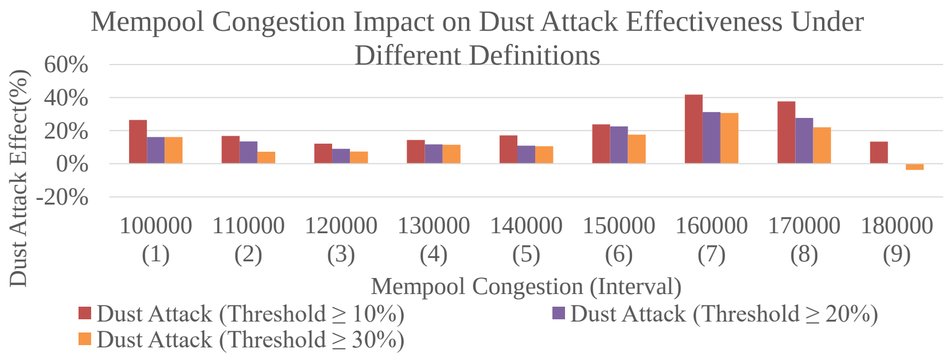
研究結論

實驗結果顯示：實驗一中，Mempool 高壅塞時粉塵攻擊效應顯著提升，且粉塵閾值較低(≥10%)時ROI最大，高達40%。實驗二發現，多簽與複雜腳本地址在解鎖粉塵UTXO時的成本遠高於單簽型，最高可超過600bytes。實驗三顯示，腳本型地址在攻擊下的ROI可達數十倍至上萬倍，尤其受Runes帶動的Ordinals與BRC-20類交易影響最為明顯。實驗四證實，轉址攻擊中P2TR(Key Path)→Legacy或P2SH的ROI中位數超過 400%，而 SegWit→Legacy 策略能顯著放大攻擊效應。

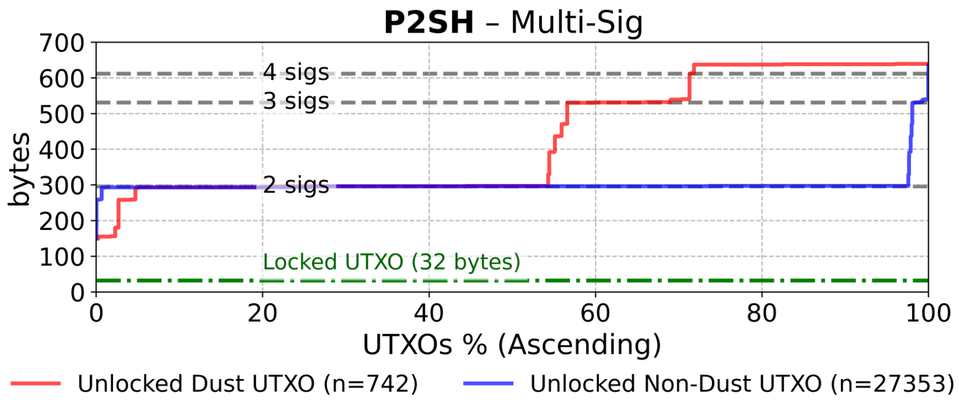
總結而言，本研究從系統層（Mempool 壅塞、費率變化）與使用者層（UTXO解鎖成本、地址轉換策略）全面分析粉塵攻擊的影響，提出整合辨識、字節數負擔、攻擊效應與轉址策略的評估機制。結果證明，在高壅塞與特定轉址策略下，粉塵攻擊對比特幣網路穩定性及使用者經濟負擔構成重大威脅，顯示需優先發展即時防禦措施與BIP協議優化以降低其危害。

實驗評估與分析

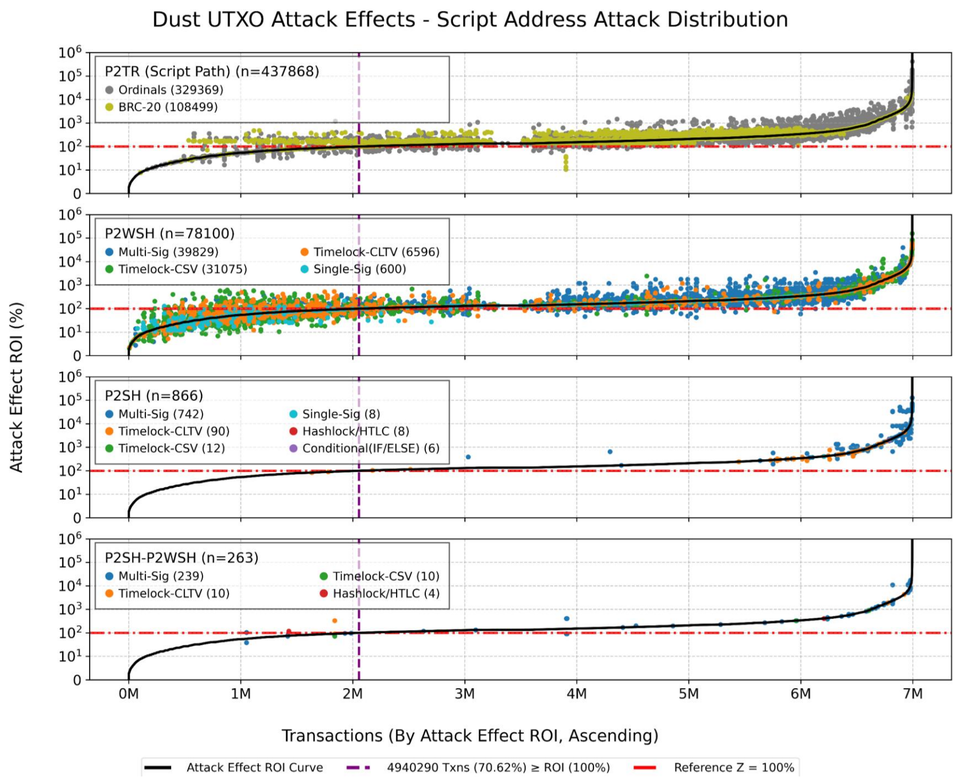
- **實驗1 評估不同粉塵攻擊定義對比特幣系統影響**



- **實驗2 評估粉塵UTXO字節數負擔影響**



- **實驗3 評估粉塵UTXO攻擊效應與地址影響**



- **實驗4 評估粉塵UTXO轉地址攻擊效應**