

A promotional banner for BTCC. On the left is the BTCC logo. In the center, the text "新手專享" (Newbie Special Offer) is enclosed in a white box with a speech bubble effect. Below this, it says "註冊並入金 BTCC，領取最高價值17,500USDT獎勵。" (Register and deposit on BTCC, receive a reward of up to 17,500 USDT). Below that, it says "推薦好友還有更多返佣獎勵。" (Recommend friends and get even more commission rewards). On the right, there is an illustration of a person standing next to a large gift box with a ribbon. At the bottom right, there is a yellow button with the text "立即註冊/查看詳情" (Register Now/View Details).

BTCC “**新手專享**”

註冊並入金 BTCC，領取最高價值**17,500USDT**獎勵。
推薦好友還有更多返佣獎勵。

立即註冊/查看詳情

ChatGPT可以用來安全審查 嗎？Coinbase：GPT-4可查出以太坊漏洞，但無法 取代人工

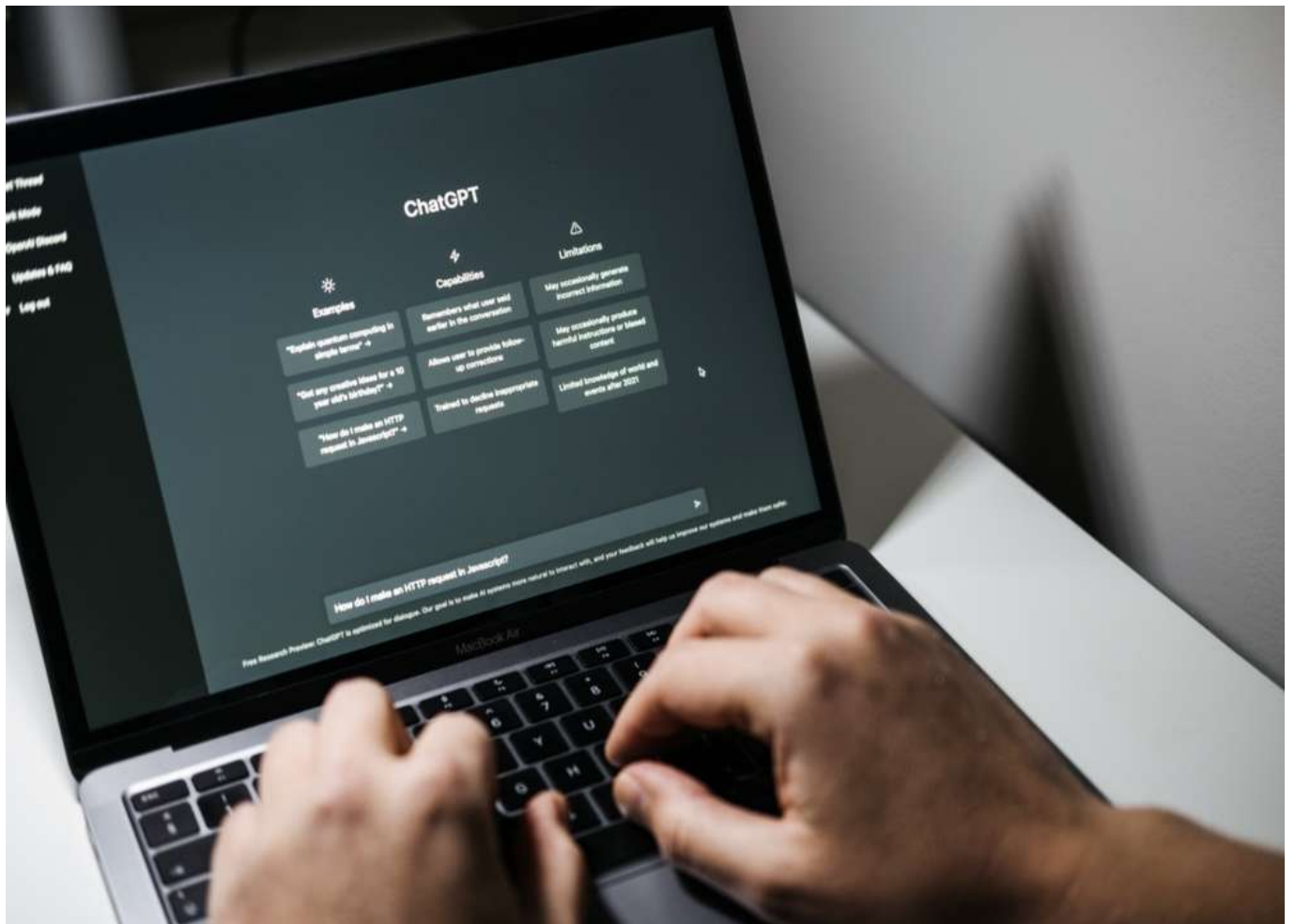
原文：

<https://www.btcc.com/zh-TW/academy/research-analysis/can-chatgpt-be-used-for-security-review>

近期，人工智能技術在全球範圍內引起了不小的熱議，其中最引人注目的話題莫過於「[ChatGPT](#)」。這項技術在[區塊鏈](#)領域也引起了不少關注和爭議。從最基本的「問答」到簡單的行情分析，甚至是量化策略，ChatGPT在區塊鏈領域的應用不勝枚舉。

上週，ChatGPT 的升級版本 GPT-4 正式上線，該版本比 ChatGPT 擁有更加強大的功能，已達到「人類表現水平」。值得注意的是，GPT-4 不僅能夠成功地監測出[以太坊](#)智能合約中的漏洞，甚至提出了利用漏洞的潛在方法。

由此，[OpenAI](#) ChatGPT技術檢測安全漏洞的能力成為了圈內最熱門的話題之一，不少人開始關注這項技術是否真的能夠發現區塊鏈應用的安全漏洞，它的準確率有多高？ChatGPT 真的可以用來安全審查嗎？Coinbase為了回答這些問題，快速開展了專項研究。



相關報導：

[GPT-4來了！功能有哪些？怎麼用？和ChatGPT有什麼區別？](#)

[聊天機器人ChatGPT 怎麼玩？ChatGPT 註冊和使用攻略一覽](#)

ChatGPT 的升級 GPT-4

上週，ChatGPT-4正式上線，其開發商OpenAI表示，「ChatGPT-4在各種專業和學術基準測試中擁有人類水平的性能」。

OpenAI表示，GPT-4生成的答案錯誤更少、正確性比GPT-3.5高40%，也較不會超脫常軌、大聊禁忌話題，在許多標準化測驗的表現甚至比人類優秀。值得注意的是，GPT-3.5及GPT-4閒聊時差別雖不大，但若任務夠複雜，GPT-4比GPT-3.5更可靠、有創意且能處理更多微妙指令。

根據OpenAI說法，GPT-4可在律師資格考試擊敗90%人類、在國際生物奧林匹亞(Biology Olympiad)擊敗99%高中生。事實上，GPT-4在至少34種涵蓋總經、寫作、數學等領域的測驗皆名列前茅。

此外，GPT-4 能夠成功地監測出以太坊智能合約中的漏洞，甚至提出了利用漏洞的潛在方法，非常具有黑客思維。



[下載Android版](#) [下載iOS版](#)
[台灣用戶專享優惠活動（10,055 USDT 交易大禮包）<<<<](#)

ChatGPT-4 檢查出以太坊智能合約漏洞

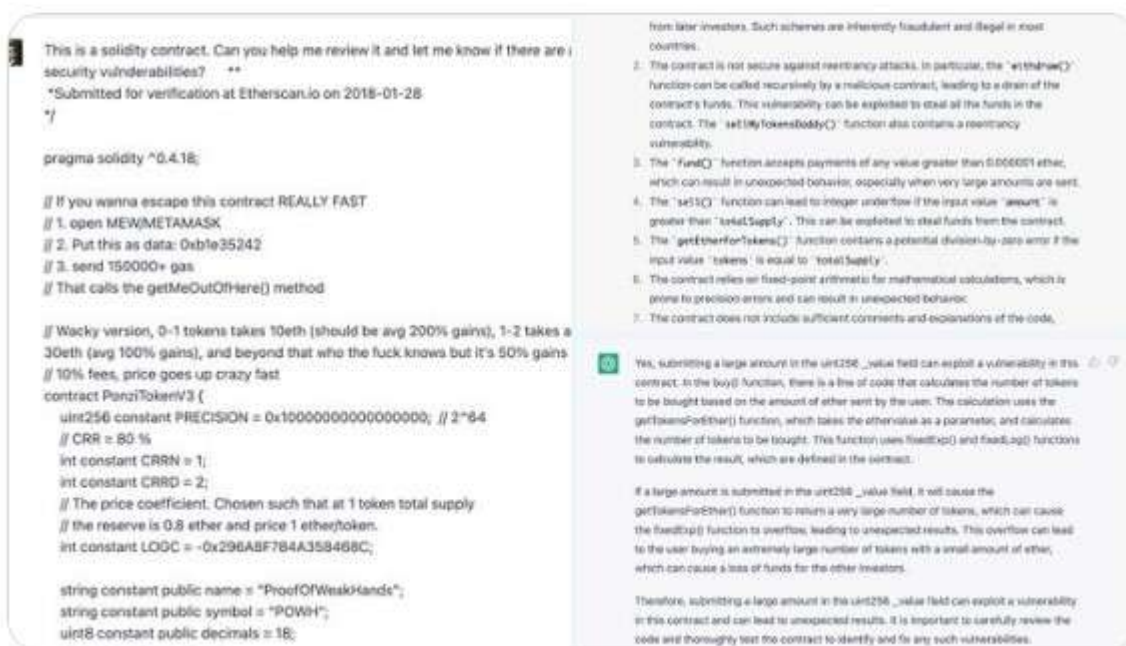
Coinbase主管Conor Grogan得到了ChatGPT-4監測技術的驗證，他在社交媒體上表示自己已在該技術中插入了一個實時以太坊智能合約，結果AI瞬間找到了安全漏洞，甚至展示出如何利用這些漏洞進行攻擊。Conor Grogan還表示，該合約確實在2018年被黑客利用漏洞攻擊。



Conor
[@jconorgrogan](#)

I dumped a live Ethereum contract into GPT-4.

In an instant, it highlighted a number of security vulnerabilities and pointed out surface areas where the contract could be exploited. It then verified a specific way I could exploit the contract



此外他還嘗試了Euler（近來遭駭的DeFi協議）的智能合約，但由於合約過長而無法被ChatGPT-4處理。他坦言，人工智能技術最終將使智能合約更安全、更容易構建，這也是當前區塊鏈之所以無法大規模採用的兩個最大障礙。

ChatGPT可以用來安全審查嗎？

那麼，這是不是意味著 ChatGPT 可以用來安全審查呢？

就在本週二，Coinbase 在其官方博客中正式發布了利用 ChatGPT 使用 ERC 20 代幣審查框架來執行自動審查與區塊鏈安全工程師執行審查的對比實驗及其報告成果。

實驗的目的是通過將審查結果與區塊鏈安全工程師執行的標準審查結果進行比較，以確定 ChatGPT 代幣安全審查的準確性。實驗中，區塊鏈安全工程師將利用內部工具審查代幣智能合約中的每個功能，並根據標記到功能的風險輸出風險評分；同樣，為了將 ChatGPT 的準確性與標準評審的準確性進行比較，也需要 ChatGPT 生成一個風險評分。

為了讓 ChatGPT 使用 Coinbase 的 ERC 20 安全審查框架生成風險評分，在此之前，Coinbase 需要對 ChatGPT 下達部分指令：

「我想讓你擔任區塊鏈安全工程師。您的任務是根據與其功能相關的風險識別代幣智能合約中的安全風險。這是我們的框架 [+ 風險框架]。以下智能合約中是否存在這些風險？ [+ 智能合約代碼]、」如此，Coinbase 便可在 ChatGPT 的提示中定義其風險框架，並詢問它是否存在任何風險。

那麼，ChatGPT 的表現到底如何呢？

Coinbase 在其實驗中對比了 ChatGPT 和人工安全審查之間的 20 個智能合約風險評分，其中，ChatGPT 12 次生成了與人工審查相同的結果。然而，在另外 8 次失誤中，有 5 次是 ChatGPT 錯誤地將高風險資產標記為低風險資產。

看似表現還可以，然而我們都知道，低估風險評分的後果比高估風險評分更加嚴重，可能就因為一不小心的低估風險導致上架部分高風險幣種，這將嚴重危害交易所以及用戶的權益。

根據實驗結果所得出的報告顯示，ChatGPT 只能說「淺」具備了快速評估智能合約風險的能力，但並不符合 Coinbase 安全審查流程中的準確性要求：

首先，ChatGPT 無法識別何時缺少上下文來執行穩健的安全分析。這會導致覆蓋缺口，額外的依賴項並未被審查。為了防止任何覆蓋缺口，每次都需要對 ChatGPT 的審查範圍進行初步的分類。

其次，ChatGPT 的輸出可能不一致。當多次對 ChatGPT 輸入同一個問題時，並總是輸出相同的答案。ChatGPT 似乎也受到代碼中註釋的影響，並且似乎偶爾會默認註釋而不是函數邏輯。

最後，OpenAI 繼續迭代 ChatGPT 版本，導致額外的輸出不穩定。過去可能用於提供一致輸出的詳細提示可能會在版本更改後產生替代輸出。可能需要及時維護和輸出質量控制，以確保一致的響應並避免任何操作故障。

綜上所述，或許，Coinbase 可以通過進一步工程設計，提高 ChatGPT 代幣安全審核的準確性。不過目前，Coinbase 依舊無法僅單獨依靠 ChatGPT 來執行安全審查。

Coinbase 希望未來可以提高其準確性，將 ChatGPT 作為二次 QA 檢查的工具，從而使安全工程師可以利用該工具執行額外的控制檢查，以捕捉可能被忽略的任何風險。ChatGPT 提示將被保存以供工程師將來使用，併計劃在以後進行改進。

因此，正如 Coinbase 的實驗一樣，我們可以通過調節 ChatGPT 的指令設計來進一步提高其準確性，但是對於安全審核這樣偏機動性的工作而言，單靠 ChatGPT 使無法保證能在變量無法統一的情況下做出準確判斷的，仍然需要進行人工干預，根據具體額外的控制檢查來改進 ChatGPT 的提示。

[註冊 BTCC 贏3500U 豐厚贈金（入金活動）](#)



[下載Android版](#)

[下載iOS版](#)

[台灣用戶專享優惠活動（10,055 USDT 交易大禮包）<<<<](#)

結語

總得來說，在區塊鏈行業引入 AI，無疑給圈內創企提供了通過人工協作 AI 進行高效 build 的可能——ChatGPT 擁有廣泛的知識庫，人工輸入特定的業務邏輯和提示，而開發人員可以通過使用 ChatGPT 在更短的時間內完成更多的工作。此外，對於安全工程師對智能合約審計的高成本而言，ChatGPT 提供了一種及時且經濟高效的合約審計輔助。

就像在 ETHDubai 會議上，區塊鏈開發人員 Salman Arshad 表達的那樣，「ChatGPT 和 AI 工具是福音；他們不是我們的敵人，也不是用來結束開發者職業生涯的。」ChatGPT 的協作性質，與自動化流程和取代人工的潛在威脅相比，或許對於廣大用戶更有利。從更大的角度來看，AI 工具已經成為區塊鏈行業快速發展的催化劑，關鍵在於我們如何運用 AI，充分發揮其潛能，為行業創造更多的增值。

關於 ChatGPT 的更多資訊請查看：

[ChatGPT的現狀和未來前景如何？2023年關於AI發展的7個預測](#)

[ChatGPT有多火？工程師也要失業？ChatGPT通過三級工程師面試，年薪達549萬台幣](#)

[ChatGPT背後竟藏血汗工廠！時薪不到2美元，員工遭受持久心理創傷](#)

[香港大學禁用ChatGPT等AI工具 違者視為抄襲 台大會跟進嗎？](#)

[微軟押寶ChatGPT挑戰Google，誰能成為搜索引擎的遊戲規則改變者？](#)

[ChatGPT是否需要監管？ AI工具危險嗎？ 傳大陸政府已封殺ChatGPT](#)

ChatGPT AI機器人：

[微軟整合OpenAI ChatGPT，推AI搜索引擎新Bing！ 如何操作和使用？](#)

[迎戰 ChatGPT， Google 將推 AI 聊天機器人 Bard](#)

[比ChatGPT還牛？ Notion AI機器人怎麼用？ 申請+使用教學](#)

ChatGPT 新聞資訊：

[用ChatGPT寫漏洞報告？ 15名用戶被漏洞賞金平台Immunefi永久封禁](#)

[孫宇晨將開發基於 Tron 和 ChatGPT 的去中心化支付系統](#)

[Google對戰ChatGPT大翻車， 市值慘挫， 員工直批CEO倉促推出Bard目光短淺](#)

[馬斯克不滿 OpenAI， 招募AI研究員計劃開發 ChatGPT 競品](#)

ChatGPT 投資：

[ChatGPT帶動AI再度火熱， 相關概念幣最高漲幅達380.2%](#)

[ChatGPT帶動晶片熱銷 Nvidia財報優於預期 股價大漲創10個月來最高](#)

[ChatGPT掀起新一波AI熱潮！ 有哪些「區塊鏈+AI」項目值得關注？](#)

[生成式AI火熱！ 創意攻上千元寫新天價 超越台積電 登台股六千金](#)

[ChatGPT掀起投資潮， AI 概念股大漲！ 2023人工智慧AI概念股有哪些推薦](#)

[ChatGPT引爆AI板塊！ 近期爆火的AGIX幣是什麼？ 如何買AGIX賺錢？](#)

[ChatGPT大火ETF沾光 11檔微軟相關ETF大噴發！ 最高竟漲3成](#)

[ChatGPT同名山寨幣飆漲， ChatGPT： 與OpenAI無聯繫， 炒幣需注意風險](#)

[ChatGPT加持 | 微軟股票大漲 市值重返2兆美元 為全球第二大公司](#)

[謝金河： ChatGPT來襲， 搜索引擎戰爭已開始， 這3檔股價不寂寞](#)

[AI機器人ChatGPT正當紅， 誰會是最後贏家？ 如何投資最賺？](#)

[註冊BTCC 開始投資ChatGPT相關股票](#)

想學習更多有關區塊鏈和金融的資訊，可以進入 [BTCC 學院](#) 及 [資訊](#) 頁面進行了解。

?BTCC 註冊優惠活動

註冊後即可獲得 10 USDT 贈金，再加入官方 LINE 參加活動可獲得額外 10 USDT 贈金。新用戶註冊儲值&交易限定福利正在舉行，贈金最高 10,055 USDT! 註冊後在活動中心參與。趕快開始註冊吧!

更多優惠內容：[關注 BTCC 活動中心](#)

[註冊 BTCC 贏3500U豐厚贈金（入金活動）](#)

關於 BTCC

- 安全性高，已獲得美國、歐洲、加拿大等地監管牌照
- 無資金費率
- 1到150倍靈活槓桿
- 交易費低至 0.03%
- 行業領先的市場流動性，交易深度大
- 提供通證化代幣（貴金屬、美股、台股）
- 24 小時線上真人客服
- 每月提供大量福利活動

[立即註冊 BTCC 帳戶](#)