





# 內容

1. Web 3.0 是甚麼？
2. Web 3.0 相關的網路攻擊
3. 保安建議



# 國際

# 本地

交換保安事故和資訊

協調保安事故及發佈警示

## HKCERT 作為樞紐



# HKCERT 的服務和支援



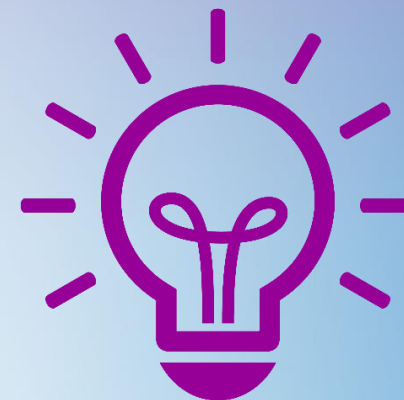
## 網絡監察

- 收集和分析攻擊模式
- 提供資訊保安警報



## 教育和技術建議

- 24小時免費事故報告熱線 ( 8105-6060 )
- 組織免費研討會和簡報
- 與本地業界、政府機構和全球CERT合作



## 研究和見解

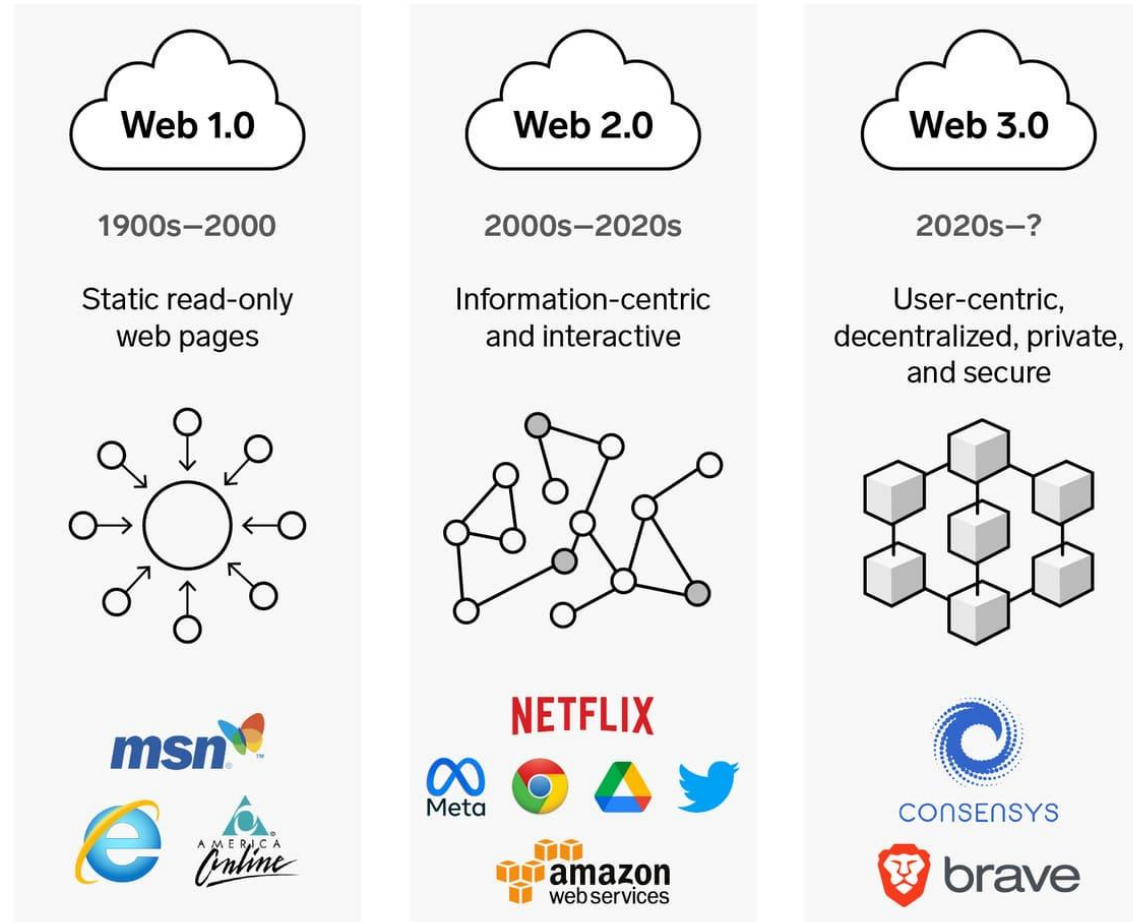
- 提供最佳實踐和指南
- 提供在線網絡安全自我評估工具

2

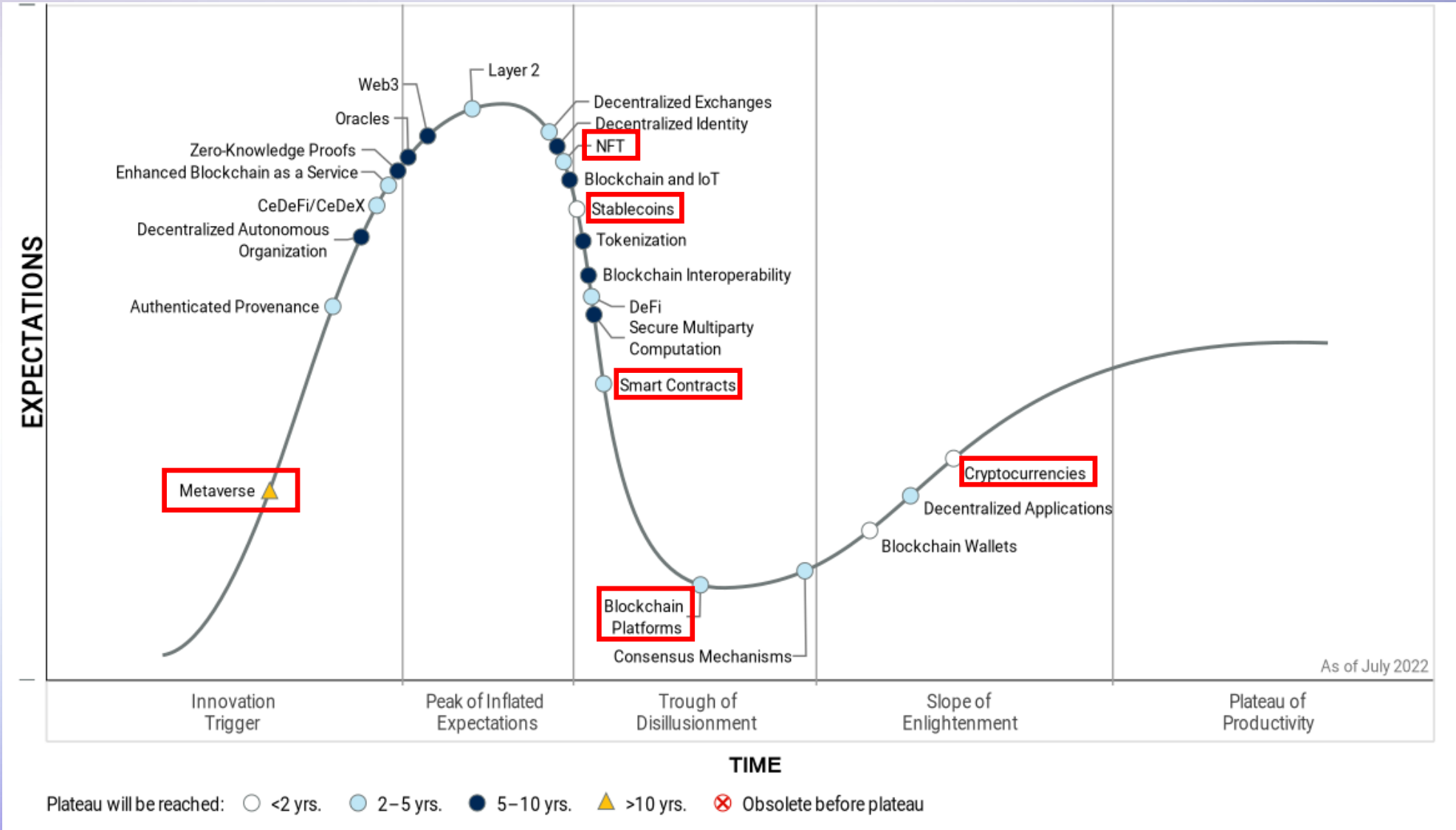
## Web 3.0 是甚麼？

# Web 3.0 的比較

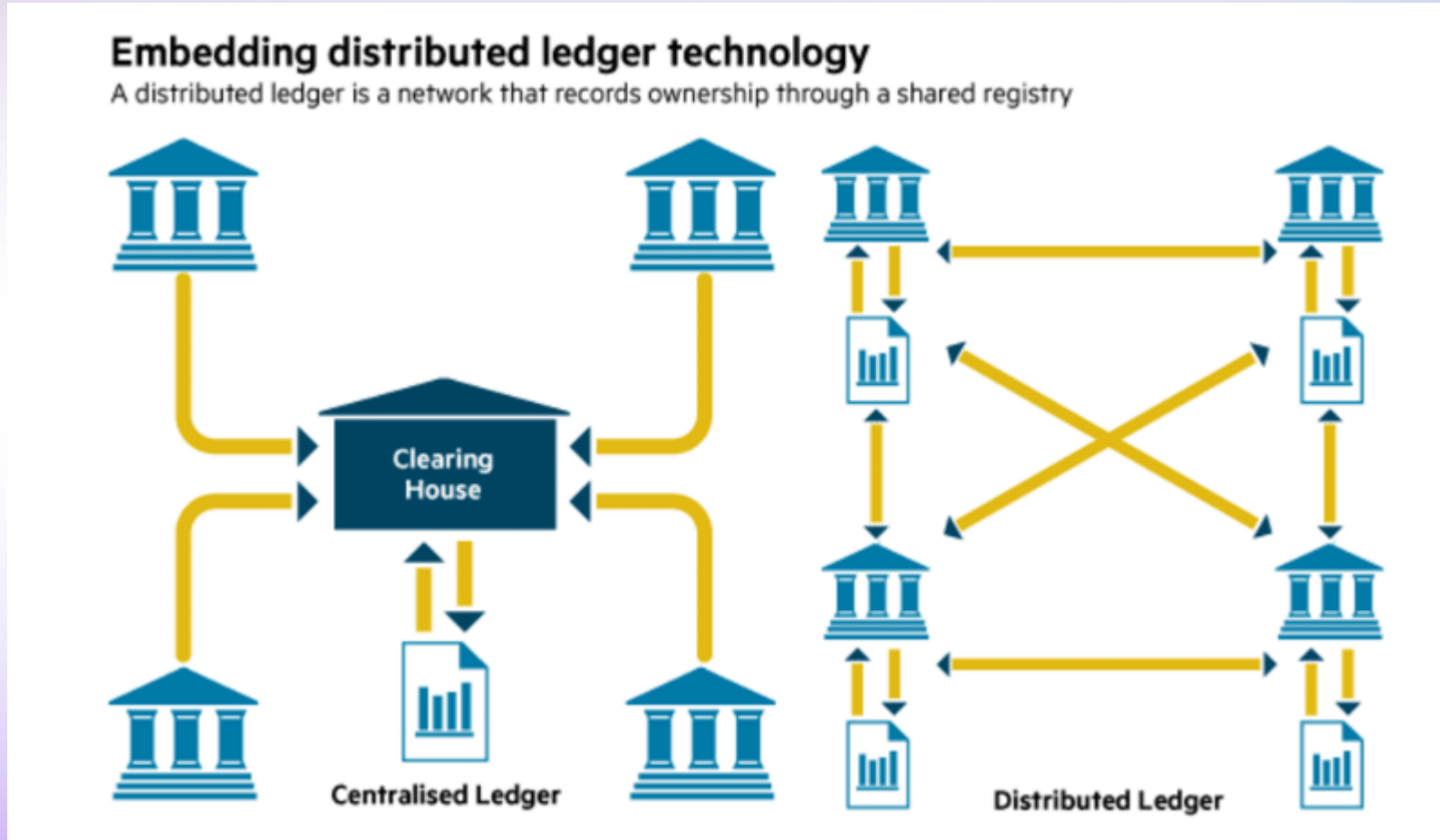
## Evolution of the web from 1.0 to 3.0



# Web 3.0 熱潮週期



# 區塊鏈的基本概念



- 區塊鏈作為分散式記帳冊
- 非中央權威架構
- 交易的有效性由對等節點驗證和審查

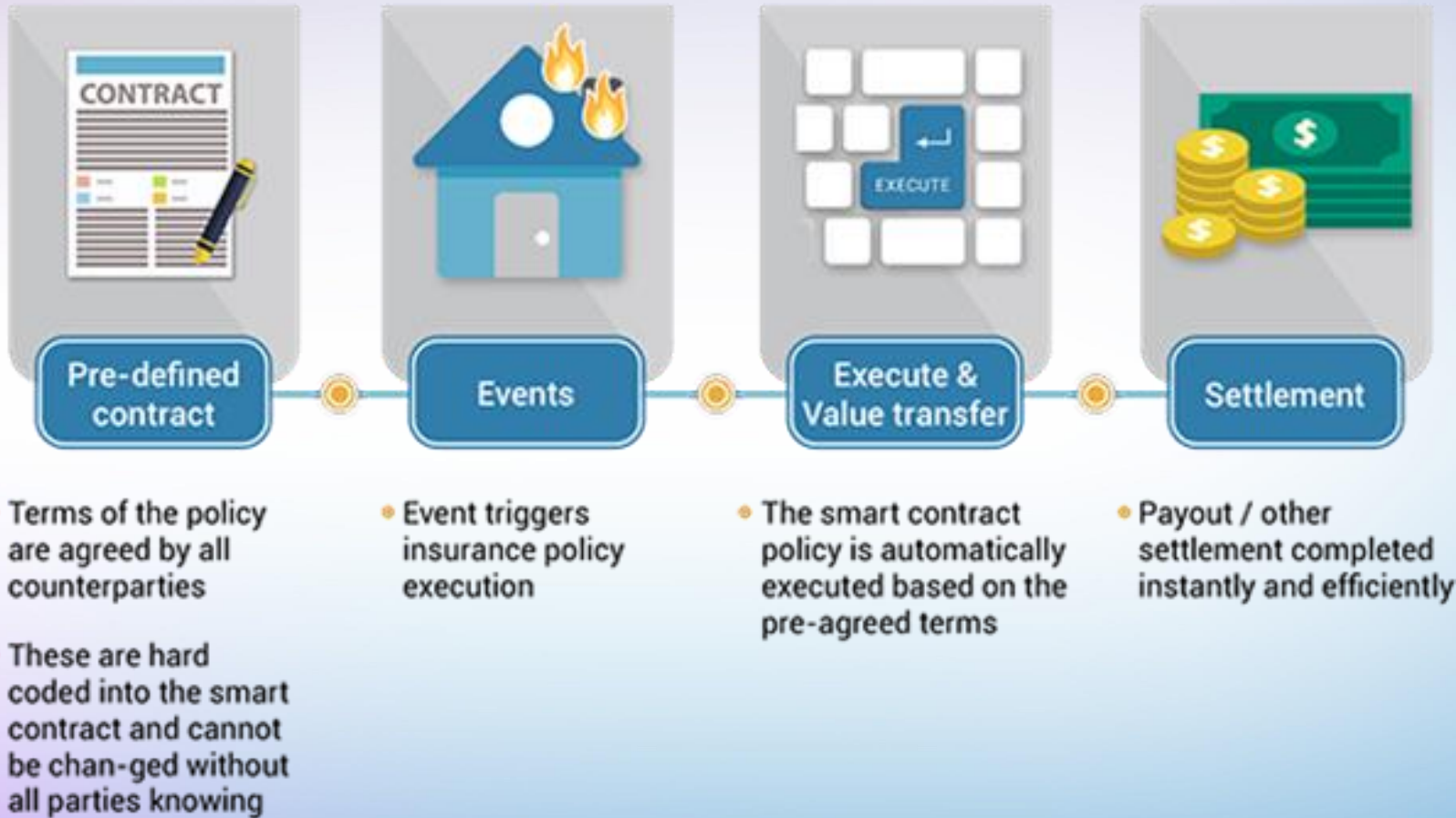


# 區塊鏈應用案例示例

NO MORE FAKES!!

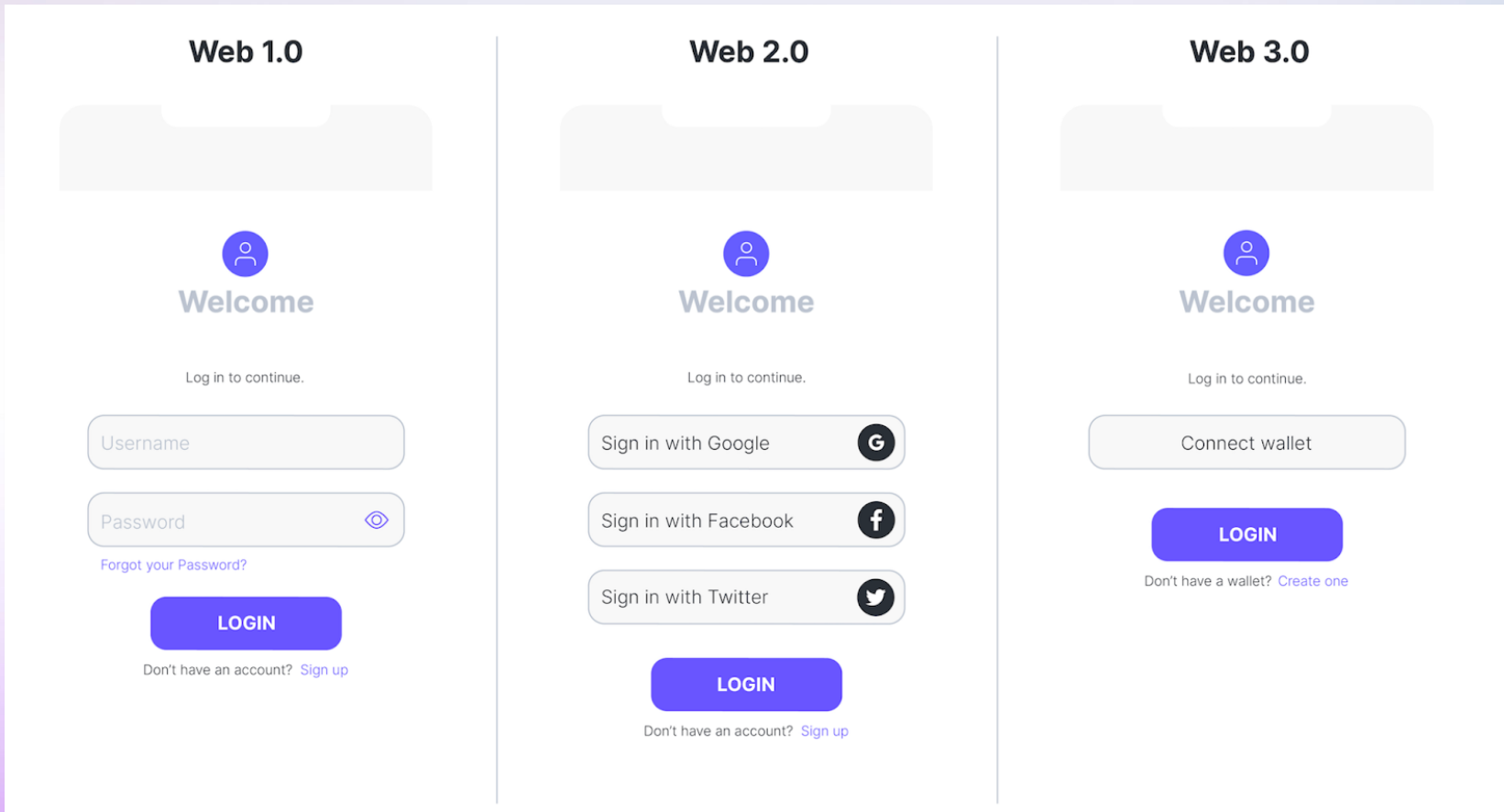


# 智能合約的基本概念



- 智能合約是儲存在區塊鏈上的**軟體程式**
- 當符合**預定條件**時，會自動觸發
- 簡單基本邏輯  
“**如果...，則...**”的陳述句

# Web 3.0 中的使用者身份識別



- 加密錢包是 Web 3.0 中代表您身份和宣稱所擁有的唯一密碼匙
- 加密錢包包含**私人密碼匙**，該私人密碼匙存儲在**錢包應用程式**（熱錢包）或專用硬件（冷錢包）中

# Web 3.0 中數字資產的例子



加密貨幣



NFT



虛擬實境地產



虛擬人物頭像



遊戲收藏品<sup>12</sup>

# Web 3.0 的總結

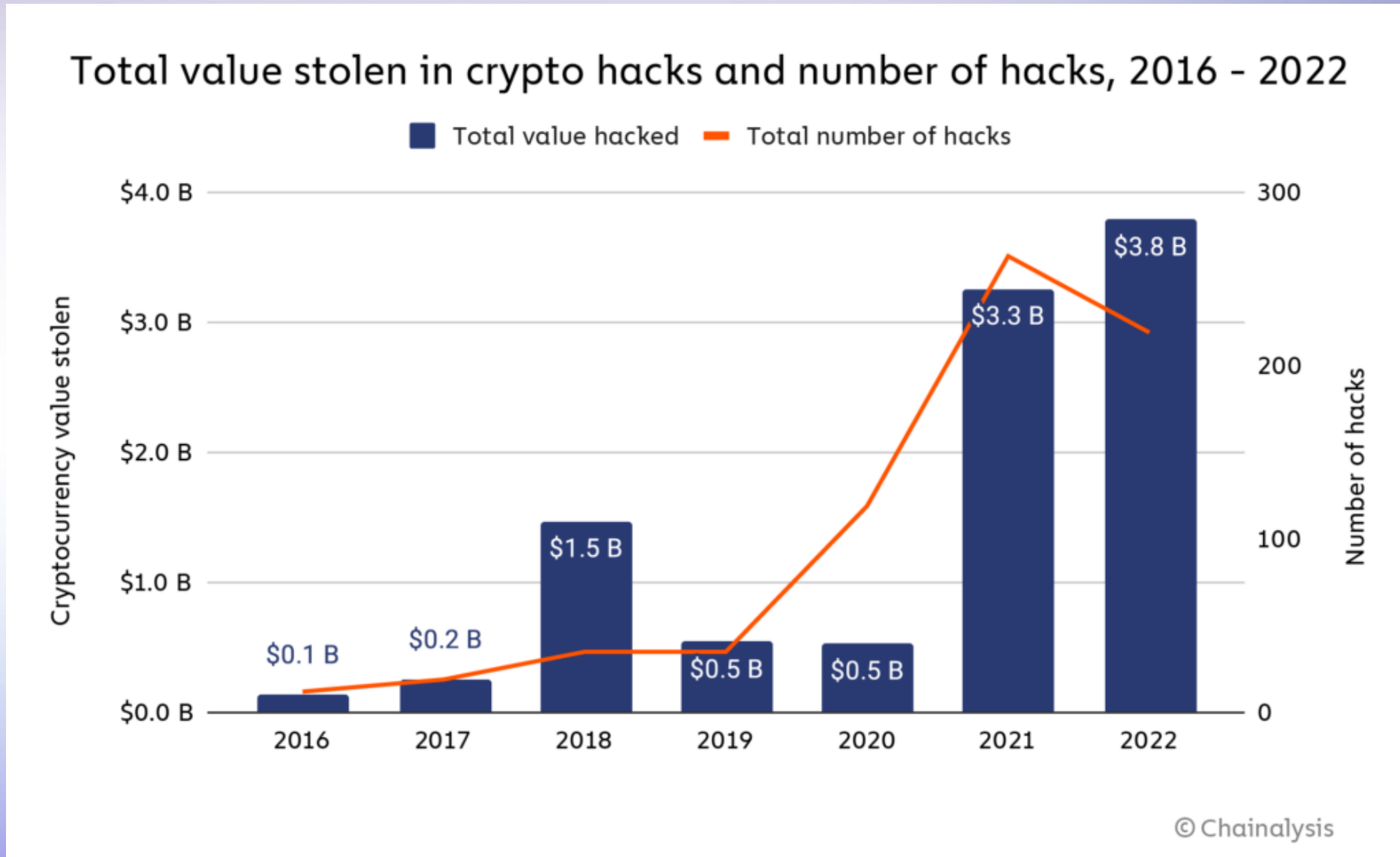
- 建立在**區塊鏈**技術之上
- 權威**分散化**，而非集中式機構
- 智能合約是一種**軟體程式**，當在區塊鏈中滿足某些條件時，會自動觸發。
- 用戶通過**加密錢包**進行身份驗證。
- **數字資產**的所擁權可以在區塊鏈中存儲和驗證（例如加密貨幣、NFT、Metaverse 中的數字資產等...）



2

# Web 3.0 相關的網路攻擊

# 加密貨幣受黑客攻擊的統計數據



# 加密錢包攻擊：假冒或欺詐應用程式

## FBI Warns Fake Cryptocurrency Apps Are Defrauding Investors

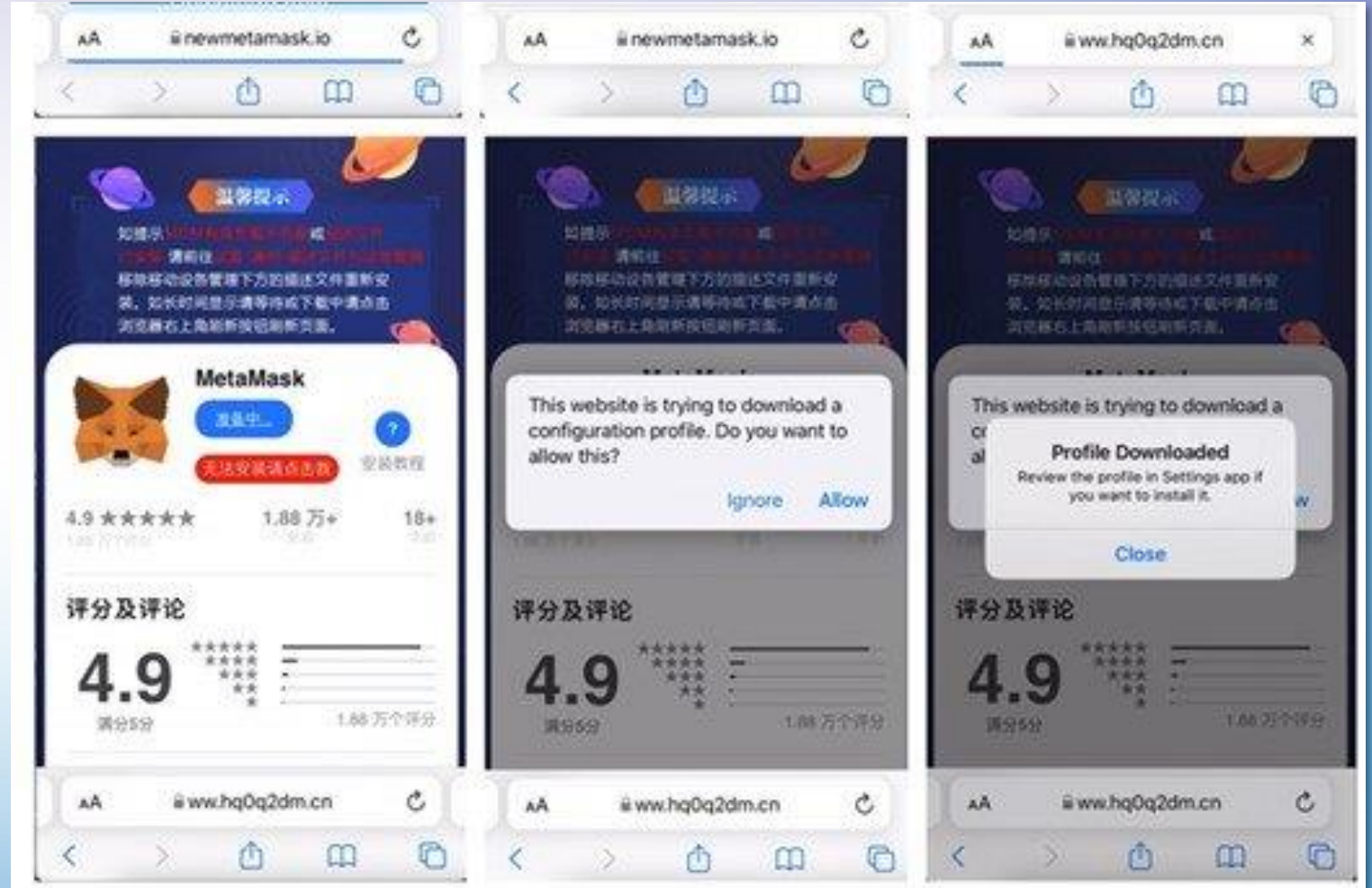
The fake mobile apps have duped investors out of an estimated \$42.7 million, says the FBI.

Alexandra Garrett  
July 18, 2022 9:06 a.m. PT



The FBI warns investors of fake crypto investing mobile apps.  
Miguel Candela/SOPA Images/LightRocket via Getty Images

Cybercriminals are creating fake cryptocurrency apps in an effort to defraud investors, according to a Monday warning from the FBI. The bureau's cyber division identified 244 victims that have been swindled by fraudulent apps, accounting for an estimated loss of \$42.7 million.







HKCE

# 加密錢包攻擊：錢包應用程式漏洞

## Coinbase Wallet 'Red Pill' flaw allowed attacks to evade detection

By Bill Toulas

March 21, 2023 10:45 AM 0



Coinbase wallet and other decentralized crypto apps (dapps) were found to be vulnerable to "red pill attacks," a method that can be used to hide malicious smart contract behavior from security features.

- 漏洞可能讓黑客，隱藏惡意代碼，在測試時**避開偵測**
- 當執行真正交易時才**換成有惡意的交易資料**

# 加密錢包遭受攻擊：釣魚攻擊

## MetaMask Issues Warning Following \$650K iCloud Phishing Scam

The DeFi wallet is advising users to disable iCloud backups to prevent future scams

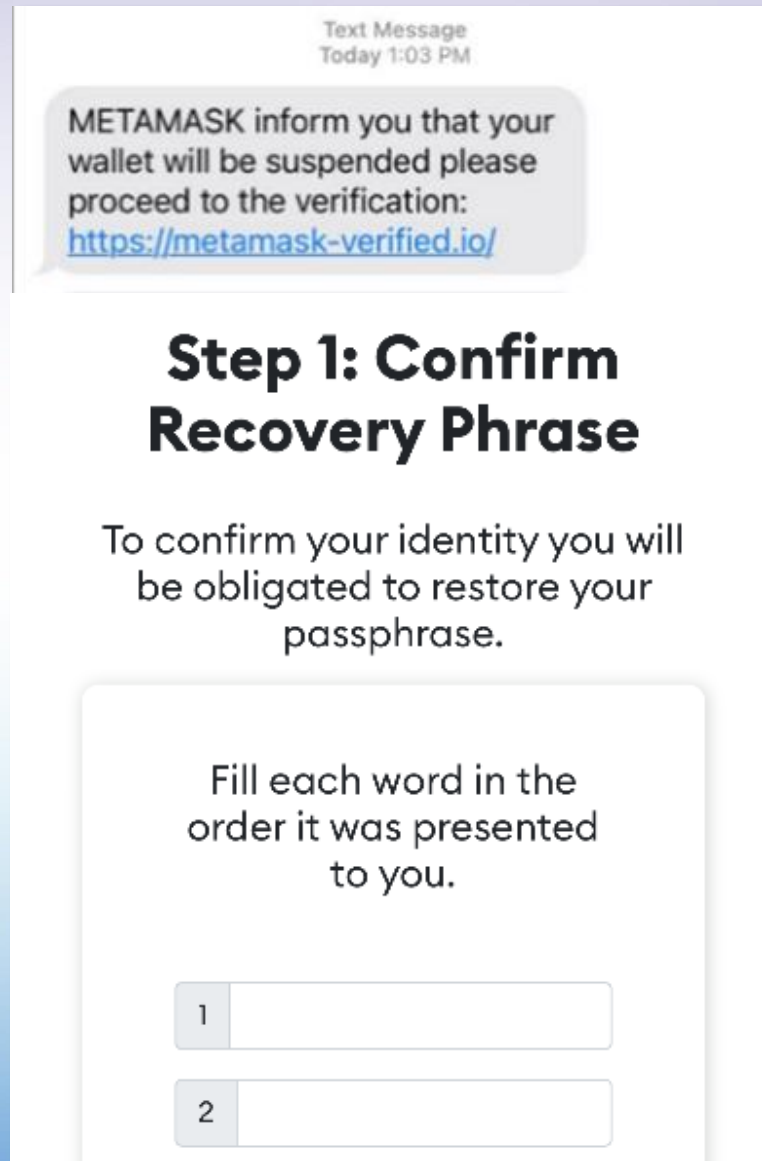
BY SEBASTIAN SINCLAIR / APRIL 19, 2022 05:10 AM



Source: Shutterstock

- 受害者遭釣魚攻擊，iCloud 帳戶被盜
- 黑客成功破解 iCloud 備份內加密錢包資料
- 最終令受害者蒙受巨額損失

# 加密錢包的其他攻擊形式



## 荔枝角虛擬貨幣劫案 21歲男遭拳打 被劫USB載價值\$15萬泰特幣



撰文：王譚揚 梁曉晴

出版：2023-01-02 22:34 更新：2023-01-02 22:48

荔枝角發生虛擬貨幣劫案，事主報稱損失價值約15萬港元的「泰特幣」。警方今晚（2日）約9時接報，一名21歲男子在荔枝角道863號泓景臺對開一個巴士站，與另一男子交收一隻載有價值約15萬港元泰特幣的USB時，被對方拳打後劫走USB，劫匪之後乘私家車逃去，事主被送往明愛醫院治理。警方將案件列作盜竊及襲擊致造成實際身體傷害處理，交深水埗警區刑事調查隊跟進，正追緝年約30多歲、肥身材疑犯。

# 利用人工智能的攻擊

## Immaculate AI images of Pope Francis trick the masses

Faux "puffy pontiff" AI image fools many in viral social media post.

BENJ EDWARDS - 3/28/2023, 5:41 AM



Enlarge / An AI-generated photo of Pope Francis wearing a puffy white coat that went viral on social media.

Over the weekend, an AI-generated image of Pope Francis wearing a puffy white coat went viral on Twitter, and apparently many people believed it was a real image. Since then, the puffy pontiff has inspired commentary on the deceptive nature of AI-generated images, which are now nearly photorealistic.

**MOTHERBOARD**  
TECH BY VICE

## How I Broke Into a Bank Account With an AI-Generated Voice

Banks in the U.S. and Europe tout voice ID as a secure way to log into your account. I proved it's possible to trick such systems with free or cheap AI-generated voices.



## ChatGPT Could Create Polymorphic Malware Wave, Researchers Warn

The powerful AI bot can produce malware without malicious code, making it tough to mitigate.



Dark Reading Staff  
Dark Reading

January 19, 2023



Source: Greg Guy via Alamy Stock Photo



The newly released ChatGPT artificial intelligence bot from OpenAI could be used to usher in a new dangerous wave of polymorphic malware, security researchers warn.

# 利用人工智能的攻擊




## No, Tom Cruise isn't on TikTok. It's a deepfake



A series of deepfake videos of Tom Cruise is confusing millions of TikTok users. See the convincing videos and learn how this technology could be used to spread misinformation.

01:26 - Source: CNN Business




Business Leader  
INSPIRE • INFORM • CONNECT

## AI start-up behind Tom Cruise deepfakes raises £7.5m to build out hyperreal metaverse experiences

Story by **Barney Cotton** January 26, 2022

VW TECH MONTH FUNDING SOUTH EAST TECHNOLOGY



A graphic showing a human head profile with a glowing brain, overlaid with a complex network of white lines and nodes, representing artificial intelligence or a metaverse.

# 利用人工智能的攻擊



## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



June 28, 2022

Alert Number  
**I-062822-PSA**

Questions regarding this  
PSA should be directed to  
your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

### Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

IC3 complaints also depict the use of stolen PII to apply for these remote positions. Victims have reported the use of their identities and pre-employment background checks discovered PII given by some of the applicants belonged to another individual.

#### **REPORT IT**

Companies or victims who identify this type of activity should report it to the IC3, [www.ic3.gov](http://www.ic3.gov).

If available, include any subject information such as IP or email addresses, phone numbers, or names provided.

# 利用聊天機械人的攻擊

丁客邦

新聞 ▾ 產品 ▾ 手機 遊戲/電競 評測 教學 影片 活動 ▾ 討論區 課程 #AI ChatGPT #iPhone 15 創業START印

首頁 > AI/大數據

## ChatGPT並非只有好處，報告指出生成式 AI 導致網路釣魚郵件攻擊增長 135%

cnBeta 發表於 2023年5月01日 06:30 | 收藏此文



根據網路安全公司 Darktrace 公佈的最新研究報告，攻擊者使用 ChatGPT 等度，讓社交工程攻擊量增加了 135%。



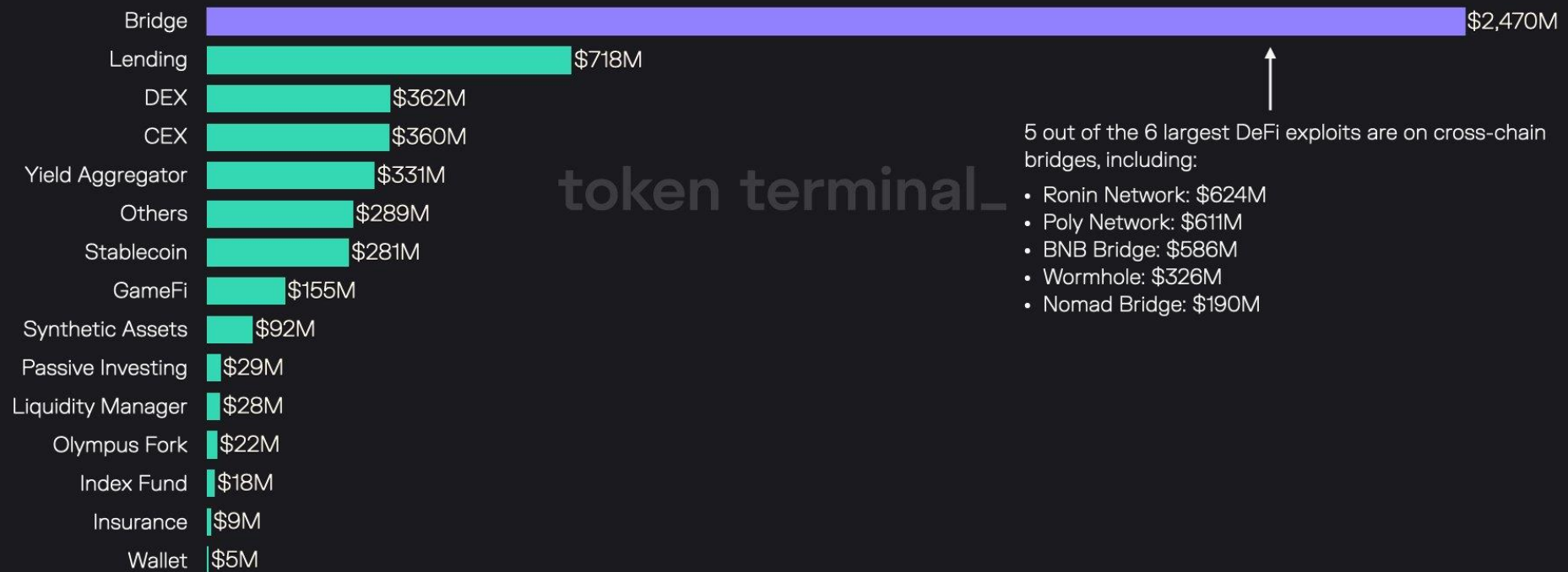
- 2023年1月至2月，新型社交工程攻擊增長 **135%**。
- 全球 **82%** 的員工擔心攻擊者使用生成式人工智能創建詐騙郵件
- 全球 **70%** 的員工注意到過去6個月詐騙郵件和短信的增加

資料來源：Darktrace

# 利用區塊鏈橋接漏洞的攻擊

Bridge exploits account for ~50% of all exploited funds in DeFi, totaling ~\$2.5B in lost assets

Funds lost in exploits per protocol type since September 2020





# 利用區塊鏈橋接漏洞的攻擊 : Binance

Crypto Hack; \$570 million stolen from Binance Bridge

© 7 OCTOBER 22



Hackers have reportedly stolen \$570 million worth of cryptocurrency from the Binance Bridge, issued by a popular crypto exchange.

The attack appears to have started at 2:30 pm EST today, with hackers receiving two transactions, each consisting of 1,000,000 BNB.

What are BSC and BNB?

Binance Smart Chain, or BSC, is a cryptocurrency platform for running decentralized apps. Binance Coin, or BNB, is the cryptocurrency issued by Binance.

- 漏洞可讓黑客生成任意BNB加密貨幣
- 導致有關服務及所有區塊鏈節點需即時暫停進行修復
- 損失高達5億7千萬美金

3

# 保安建議



# 加密錢包的安全風險

## 加密貨幣

### 「熱錢包」


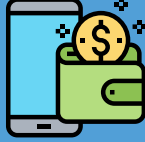
- 需要網絡連接
- 容易受到**網絡攻擊**或**資料外洩**

### 「冷錢包」

- 不需要網絡連接
- 有**遺失**或**損壞**儲存設備的風險



# 加密錢包 - 托管式和非托管式

	 托管式	 非托管式
用戶控制	<ul style="list-style-type: none"> <li>你並不擁有你的私人密碼匙</li> <li>控制由<b>第三方服務供應商</b>負責</li> </ul>	<ul style="list-style-type: none"> <li>你擁有你的私人密碼匙</li> <li>你擁有你的數字資產的<b>完全控制權</b></li> </ul>
訪問性	<ul style="list-style-type: none"> <li>對初學者更具可訪問性，作為加密貨幣交易所提供的服務的一部分</li> </ul>	<ul style="list-style-type: none"> <li>需要安全存儲私人密碼匙，因此對初學者來說不太容易訪問</li> </ul>
網絡安全	<ul style="list-style-type: none"> <li>由於<b>與互聯網連接</b>而容易受到黑客攻擊</li> </ul>	<ul style="list-style-type: none"> <li><b>沒有</b>互聯網連接，因此<b>減少</b>受網絡威脅，但用戶必須確保安全地存儲<b>私人密碼匙</b>和<b>恢復短語</b></li> </ul>
持有錢包費用	<ul style="list-style-type: none"> <li>取決於服務供應商</li> </ul>	<ul style="list-style-type: none"> <li>不需要</li> </ul>
提現錢包費用	<ul style="list-style-type: none"> <li>取決於服務供應商</li> </ul>	<ul style="list-style-type: none"> <li>不需要</li> </ul>
易用性	<ul style="list-style-type: none"> <li><b>較易用</b>，具有互動用戶界面 (UI) 和支援</li> </ul>	<ul style="list-style-type: none"> <li>需要技術知識和專業知識，<b>支援有限</b></li> </ul>

# 加密貨幣錢包保安建議

HKCERT  
Hong Kong Computer  
Emergency Response Team  
Coordinator Centre  
香港電腦緊急事故協調中心

ENG

主頁 > 刊物 > 保安博覽

## NFT熱潮下，如何保護自己的NFT資產

發佈日期: 2022年01月24日 | 10534 觀看次數



### 什麼是NFT

NFT全名是「非同質化代幣」(Non-Fungible Token)，是根據以太坊ERC721標準來發出的代幣，有別於其他虛擬貨幣，每一枚NFT代幣都會獲配一個獨有的數碼ID，所以不會重覆，而且交易時亦不可分割出售。



- 加密錢包應用程式
  - 備份你的錢包並設置密碼保護
  - 絕不向他人透露恢復短語
  - 啟用多重驗證
  - 啟用資產轉移白名單
  - 在簽署或授權所有交易之前仔細核對內容
  - 保持軟件更新
  - 使用冷錢包以獲得較好的安全性
- 平台管理的錢包帳戶
  - 啟用多重驗證
  - 啟用資產轉移白名單
  - 注意防範釣魚攻擊

# 利用人工智能進行社交工程攻擊的保安建議



- 採用零信任概念 - 核實所有事項
- 透過**其他途徑**（例如官方網站公告，客戶服務熱線）驗證**發送者**的身份和信息
- **不要打開**來源不明的文件、網頁連結和電子郵件
- 使用守網者 (Cyberdefender.hk) 的「**防騙視伏器**」，通過電子郵件、URL 或 IP 地址等方式以**評估詐騙及網絡安全風險**
- 在**提供個人或敏感信息**之前**三思而行**
- 警惕社交工程技倆（例如緊急、威脅、權威等）

# 智能合約的安全建議

主頁 > 刊物 > 保安博錄 >

## 簽吧。智能合約？

- ▶ 智能合約是將合約條文程式化並寫進區塊鏈中，有別於傳統合約的是它無需第三方介入，當滿足合約條件時，程式便會自動執行合約，而且無法更改。
- ▶ 過往有一些保安事故與智能合約有關，牽涉利用智能合約的程式設計漏洞，因此，不論是開發或使用智能合約時都要小心謹慎，以免程式執行結果與預期不同，同時要理解當中潛在的風險及相應的保安建議。

發佈日期: 2022年04月04日 | 7492 觀看次數



- 應先檢視智能合約內容才進行簽署
- 在交易平台或市場上使用官方智能合約進行交易
- 交易後，立即驗證加密資產的正確性
- 參考行業最佳實踐指南，以避免常見的攻擊方法
- 對智能合約進行安全評估或審計，檢查代碼是否存在安全問題

# 聊天機械人的良好作業模式



## 注意事項

- 私隱問題
- 偏見
- 錯誤和不準確的資訊
- 侵犯知識產權

## 良好作業模式

- 使用 AI 聊天機械人作為輔助工具
- 負責任地使用 AI 聊天機械人
- 緊記AI聊天機械人並非完美
- 保護私隱和數據





# 要點總結



- Web 3.0 和區塊鏈使用戶能夠在不同平台上**完全控制其數字資產的擁有權**
- 黑客會嘗試**各種攻擊技倆**以**獲取**你的加密貨幣錢包並盜取你的數字資產
- 越來越多的 Web 3.0 應用和案例正在發展
- 採用**零信任概念**，並**核實所有事項**以減少安全風險

# 訂閱HKCERT資訊保安警報服務

要對資訊保安風險保持警惕，請訂閱或追蹤：

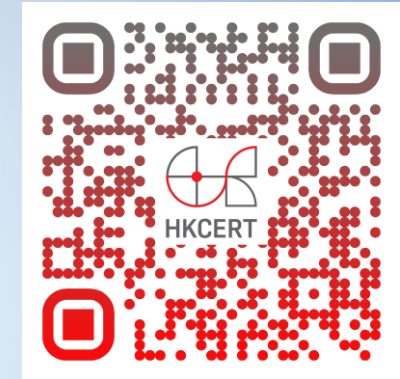
1. 免費保安公告及月報



2. 免費電話短訊警報



3. HKCERT的社交媒體平台（例如Facebook, LinkedIn及YouTube）



## 立即行動！

SUBSCRIBE

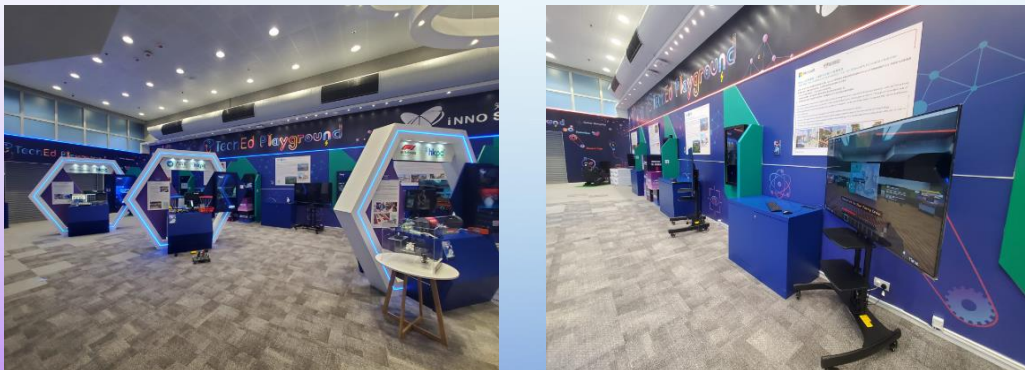
<https://www.hkcert.org/tc/form/subscribe/entry>

# 活動預告

## 流動車展覽 (Sep & Dec 2023)



## Smart & Secure City Exhibition @HKPC Building (2H 2023)



## Cyber Security Summit Hong Kong 2023 (11-12 Sep 2023)

<https://www.cssummit.hk>



## 香港網絡保安新生代 奪旗挑戰賽 (Nov 2023)





## Hong Kong Productivity Council 香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong  
香港九龍達之路78號生產力大樓  
+852 2788 5678 [www.hkpc.org](http://www.hkpc.org)

