



CYBERSEC 2022 臺灣資安大會

CHANGE

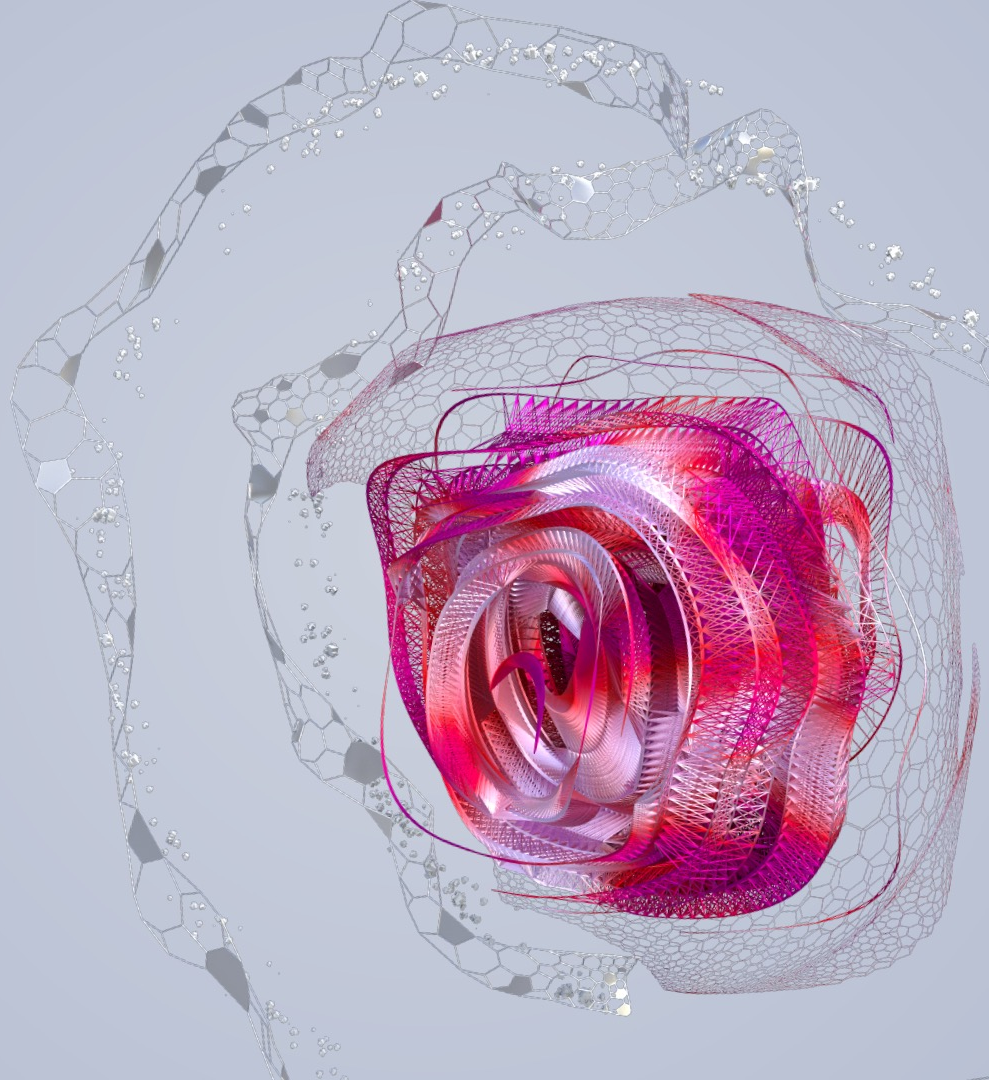
數位轉型 資安升級

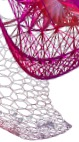
SEP. 20-22 臺北南港展覽二館



Attack Surface on Metaverse

Trend Micro Metaverse Security Dept.
Sam Ku





Agenda

- Metaverse 是什麼?
- Attack surface on metaverse
 - Blockchain
 - A.I. Deepfake
 - VR/AR
- 腦洞大開的想像
- 結論





Metaverse 是什麼?

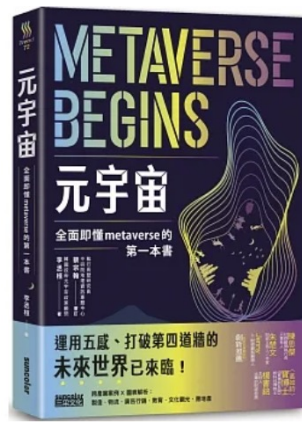
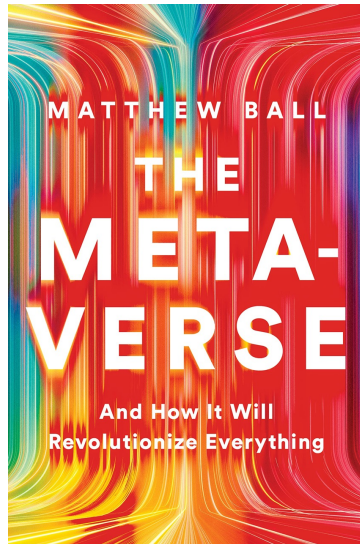
Metaverse 是什麼?

Matthew Ball

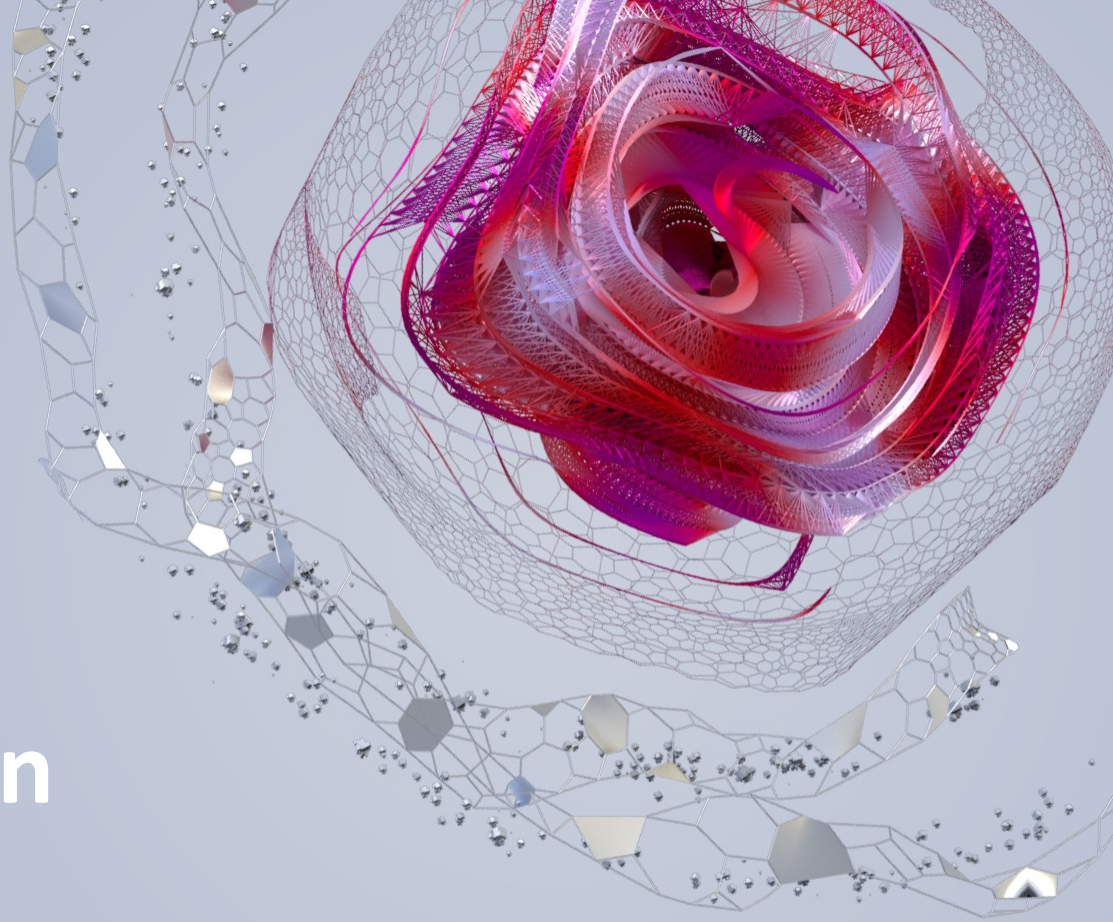
- Real-time render
- 3D 虛擬世界
- 大規模、可互通的網路
- 無限的使用者
- 同步以及持續性的體驗
- 存在感
- 各種資料也具有連續性

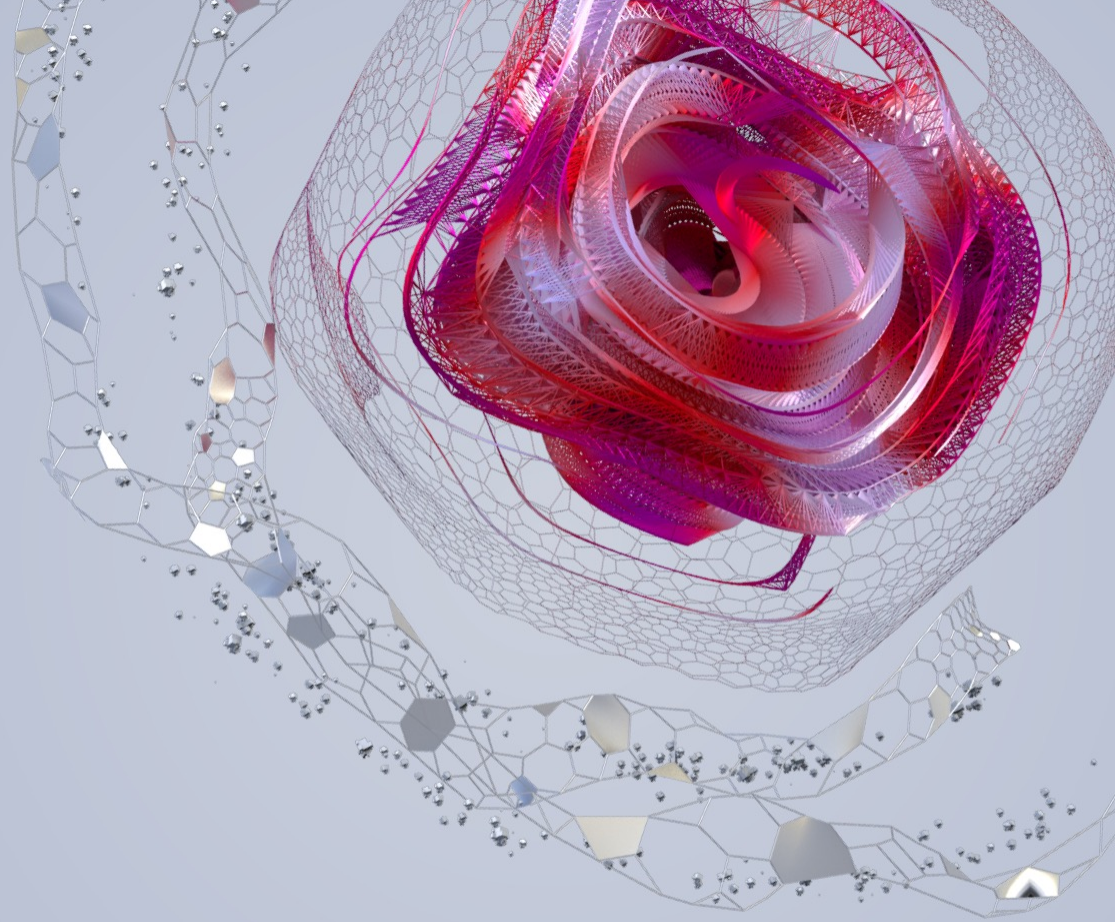
<https://youtu.be/4S-4mTvK4cl>

The metaverse explained in 14 minutes | Matthew Ball



Attack surface on metaverse





區塊鏈

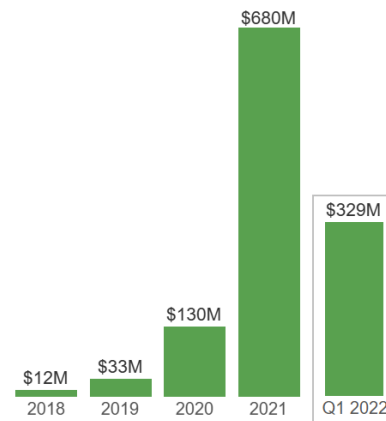
攻擊總是出現在最有利益的地方

- Over \$100 million worth of NFTs are reportedly stolen through scams




Reported cryptocurrency fraud losses by year

January 2018 - March 2022



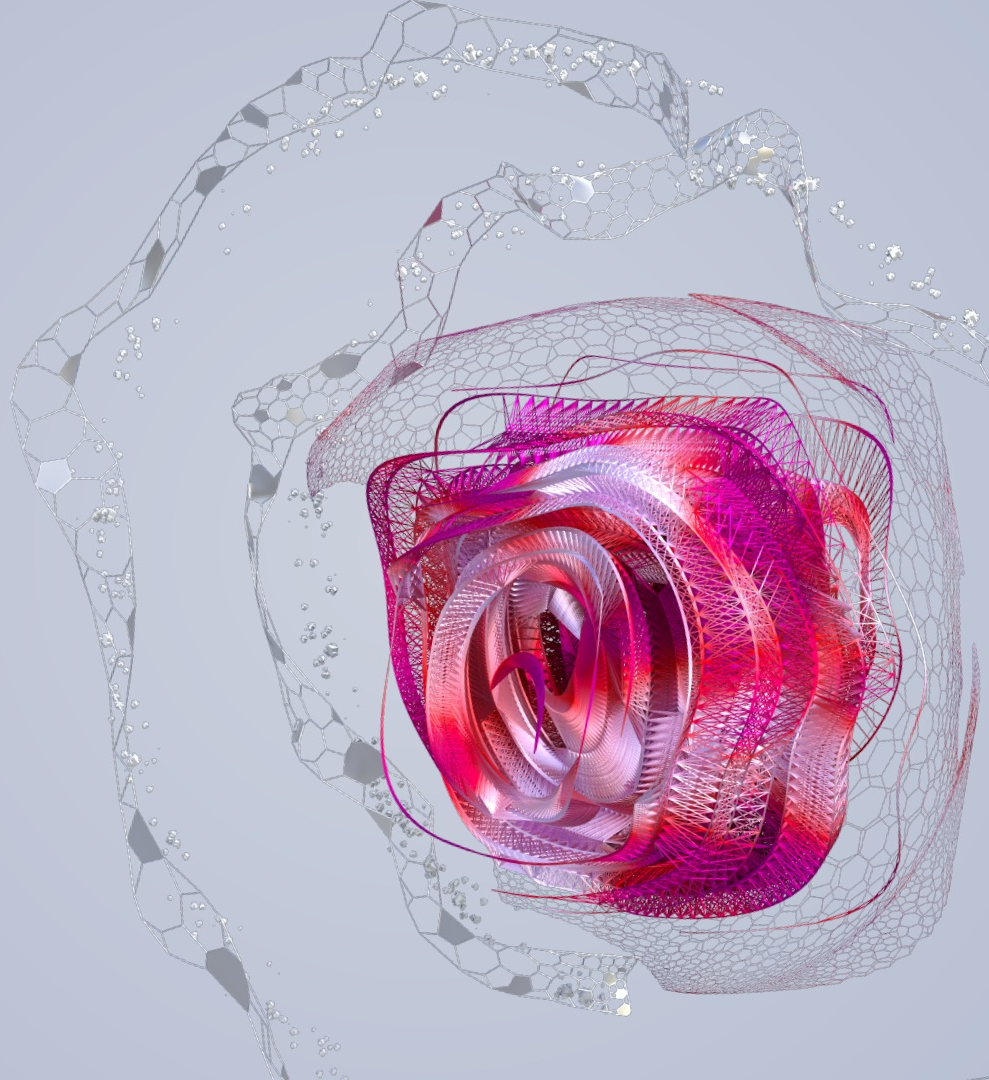
These figures are based on fraud reports to the FTC's Consumer Sentinel Network indicating cryptocurrency as the payment method. Reports provided by Sentinel data contributors are excluded.



**Web3 is new. They
don't have a good
enough security
design.**



使用者的資安挑戰





Ellen 是一個 NFT 的小白買家，他想要購買 NFT

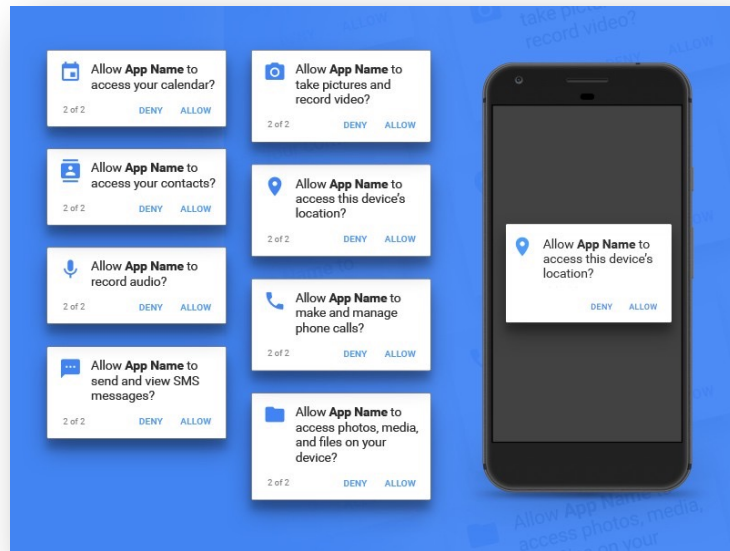
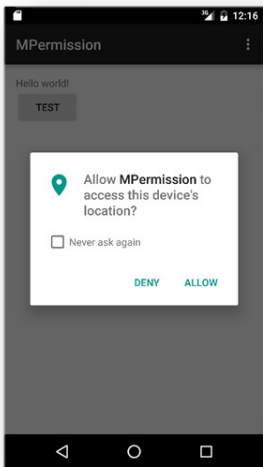
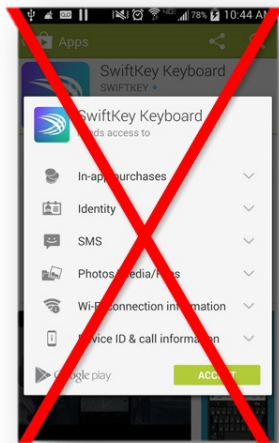
1. 申請交易所
2. 安裝錢包，產生助憶詞 (private key) (!)
3. 從交易所買幣
4. 轉帳到錢包 (!)
5. 瀏覽 NFT 網站/NFT marketplace (!)
6. 連接錢包及簽名 (!)
7. 選擇手續費策略
8. Mint NFT、允許權限、扣除 gas fee (!)
9. 等待結果
10. 得到 NFT



對使用者來說

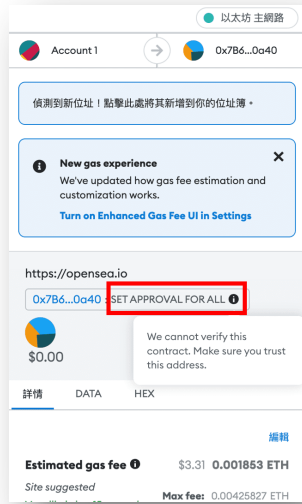
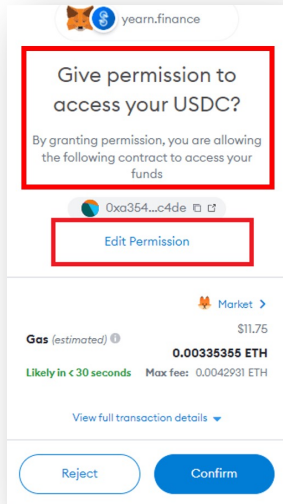
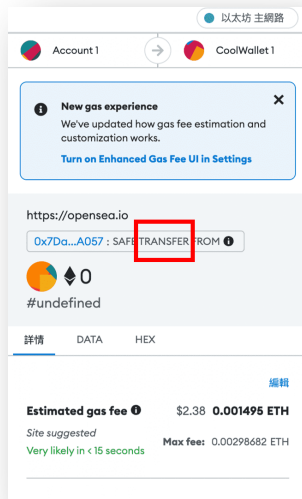
- 最容易被忽略的安全門檻
 - 權限問題

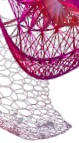
以前手機也有這樣的時光



最容易被忽略的安全門檻

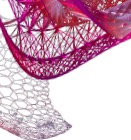
- 權限問題
 - 請允許我移動你的加密貨幣 (ERC20)
 - 請允許我移動你的 NFT (ERC721,1155)





釣魚手法

- 釣魚網站
- 假帳號，盜帳號
- 駭入 Discord server



- 私人訊息
- +
- Pednaq
 - Hassie80
 - MidJourney Bot
 - TzuTzu
 - bean
 - announcement | Slep...
 - GM Squad
 - RandyBrown
 - JoaoPedroLucPer
 - FrankWrightEpic
 - INFO TheNovatar's se...
 - sabbs
 - hiramosca
 - ХЛЕБОУТКА
 - Trenton | STEP
 - Dyciel_Snow
 - Asics x SteP.N
 - tangearar
 - Gamer123



Pednaq

這是在與 @Pednaq 私人訊息記錄的開頭。



1 個伺服器

封鎖

2022年6月8日



Pednaq 昨天 19:27

GoblinTownWTF - FREE MINT (EXCLUDING GAS FEES)! 🚩

AAAAAAUUUUUGGGHHHHH goblins goblins GOBLINNNNNNNNs wekm ta goblintown, @samku! 🎉



We are reserving 1,000 goblins. Because we want to.



Hurry up ugly goblin, first come, first served!

Goblin Town Announcement | Raffle ID: G-BIYq2H

GoblinTown Free Mint Is Now Live! 🎉

<https://goblintown.wtf/>

🎁 We are reserving 1,000 goblins. Because we want to. 🎁

● 1 free + gas mint per wallet.
Don't be fucking greedy.
That's how we got ourselves here.

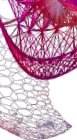
● No roadmap. No Discord. No utility. CC0. Contract wasn't actually written by goblins.
#GOBLINFOLLOWGOBLIN

First come, first served.
Good luck to all participants!

👉 GoblinTown Team







Collab.Land



MetaMask

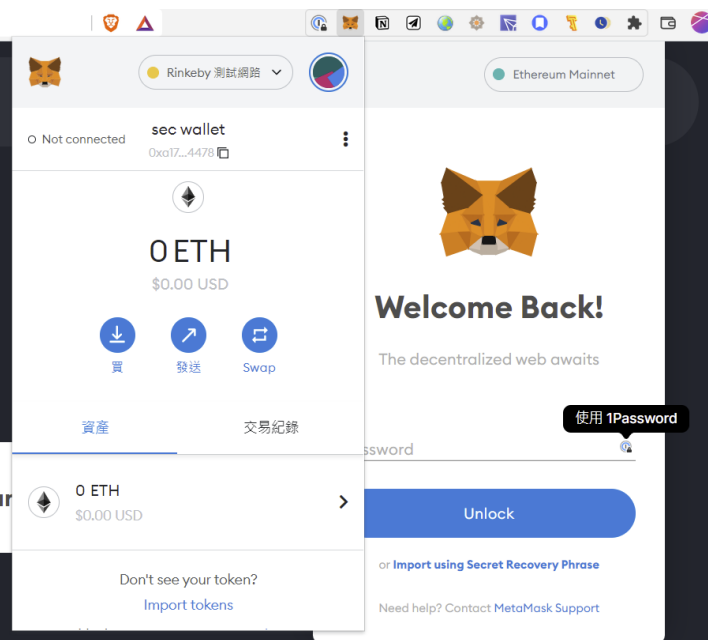


WalletConnect



Talisman

Show All



Beeple推特遭駭、發假 LV NFT 抽獎！駭客詐走 43.8 萬鎊，含MAYC、Otherdeeds...



by Joe — 2022-05-23 in nft, 加密貨幣市場, 安全, 犯罪

0



38
SHARES



分享至Facebook



分享至Twitter



Follow

beeples ✓

@beeples

BEEPLE X VUITTON COLLECTION_1: BEEPLES
Official Raffle Below.

beeples-vuitton.com Joined April 2009

675 Following 672.2K Followers



Followed by OnChainMonkey (🐵, 🐵),
dontkwon.eth | hamer.eth, Dre Dogue, and 27...

Tweets

Tweets & replies

Media

Likes



Pinned Tweet



beeples ✓ @beeples · 31m

Been working on this with LV for a long time behind the scenes. 1000 total unique pieces.

BEEPLE x VUITTON COLLECTION_1:
BEEPLES

Official Raffle Below.

1 ETH = 1 Raffle Entry.

All non-winning entries are refunded post raffle.

Good luck :)

Azuki 投資者中招！詐騙仔駭入Twitter藍勾勾帳號，假冒官方空投 BEANZ NFT 釣魚

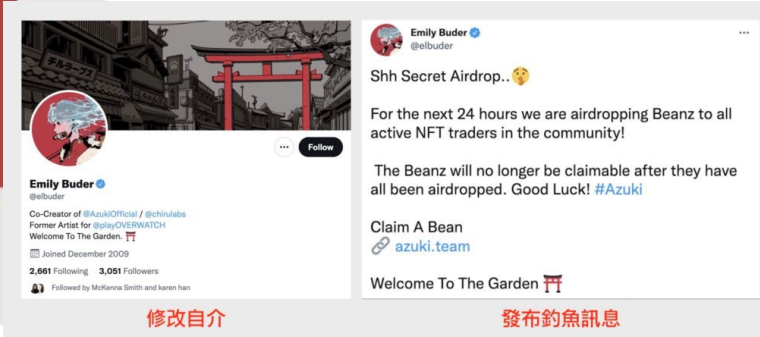
 by **Joe** — 2022-04-10 in nft, Web3.0, 即時新聞, 投資分析, 犯罪

0



修改自介

發布釣魚訊息



修改自介

發布釣魚訊息

222
SHARES

 分享至Facebook

 分享至Twitter



73 NFT DISCORDS COMPROMISED

1-Aug-22	Miningverse	13-Aug-22	Alpha Blocks	22-Aug-22	Solana Warriors
1-Aug-22	Degen Goat Coinflip	13-Aug-22	SaphireNFT	23-Aug-22	Lucid NFT
1-Aug-22	LittleMaMi Label Club	13-Aug-22	Sushi Cats Fam	23-Aug-22	ChubbyLand
1-Aug-22	Gas Guzzlers NFT	13-Aug-22	DAISUKI (2nd time)	23-Aug-22	Secret Project
1-Aug-22	Vibe Kingdom	13-Aug-22	Gotterhavn	23-Aug-22	Dininho NFT
1-Aug-22	UghaBugha	13-Aug-22	D.A.I.F	24-Aug-22	Aotuverse
2-Aug-22	BotBuddyz	13-Aug-22	Alpha Gorillas	24-Aug-22	Hameer's Hideout (2nd time)
2-Aug-22	CYBER CREW NFT	13-Aug-22	Alpha Mutants	24-Aug-22	Duckish
2-Aug-22	dTweenies	14-Aug-22	DigiKong	25-Aug-22	Hello Moon
4-Aug-22	Shinsekai	14-Aug-22	Pirate Apes	25-Aug-22	Space Punks Club
4-Aug-22	Fuk Bois	15-Aug-22	Rebel Racoons	26-Aug-22	OVR NFT
4-Aug-22	Fearless Bulls	15-Aug-22	Pixel Guild	26-Aug-22	Kaitu
5-Aug-22	Famous Fox Federation	16-Aug-22	Mutarium Universe	26-Aug-22	Meta Legends
5-Aug-22	The Doge Capital	17-Aug-22	BigFoot Town	26-Aug-22	DigiKong (2nd time)
5-Aug-22	AI Roulette	17-Aug-22	Degenerate Gods	27-Aug-22	Splinterlands
5-Aug-22	ChainMyth	17-Aug-22	RuggPullFinder	27-Aug-22	Sui by Mysten Labs
6-Aug-22	GOLD SQUAD	17-Aug-22	456 Collectors Club	27-Aug-22	Cosmic Clones
6-Aug-22	ETHJETS	17-Aug-22	Azra Games	28-Aug-22	Flippin Rabbits
7-Aug-22	Mooncatz	17-Aug-22	Legendary Owls	29-Aug-22	Floaties
9-Aug-22	TheLost4444	18-Aug-22	The Humanoids	30-Aug-22	Decentral Games
10-Aug-22	TipsyTikiDao	20-Aug-22	Hameer's Hideout	31-Aug-22	TheTrollsNFT
10-Aug-22	Otaku Club	21-Aug-22	Llamaverse	31-Aug-22	Jelly eSports NFT
11-Aug-22	Mogul Productions	21-Aug-22	PGodjira		
11-Aug-22	Heroes Of Astron	21-Aug-22	CETS ON KREK		
13-Aug-22	Aptos Labs	21-Aug-22	SMS Solana.FM		
13-Aug-22	Martian Wallet				

* dated 1 sep 2022, data & source: @NFTherder



OKHotshot
@NFTherder

73 #NFT discords have been exploited in August through social engineering including big projects like Llamaverse, PGodjira and Humanoids

Millions continue to be stolen. These are REAL crimes with real victims. Stay vigilant 🙋

翻譯推文

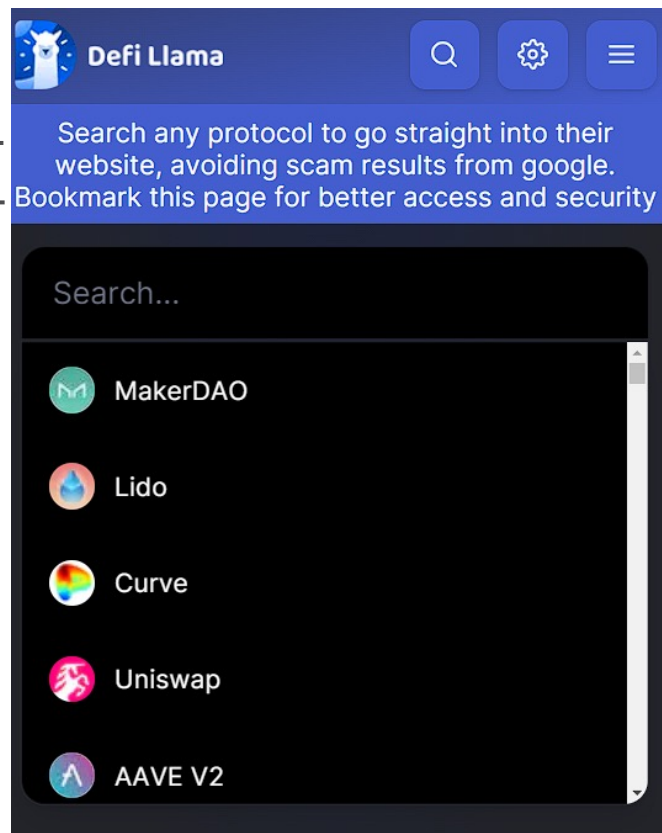
下午9:05 · 2022年9月1日 · Twitter Web App

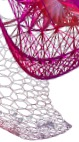
2 引用的推文 3 個喜歡



難道大家都不知道官網在哪裡嗎?

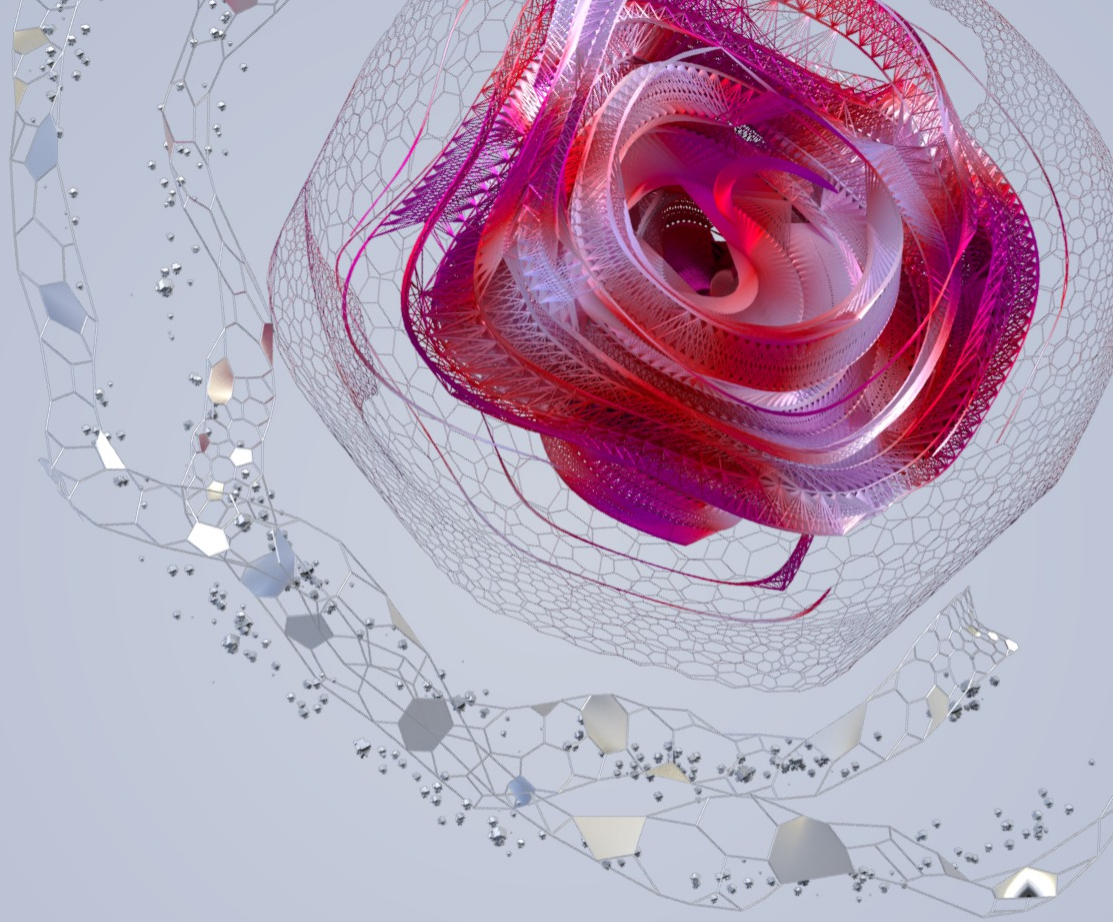
- 對喔，嚴重到
Defi Llama 的新功能是直
列出來 O.O



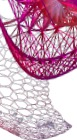



如何防治?


- Whois 是你的好朋友
 - 通常最近才註冊的網站都很有問題
 - 憑證逾期時間太快
- 安裝防詐騙的 Browser extension
- 仔細的檢查你的交易
- 取消掉所有不必要的授權
 - <https://etherscan.io/tokenapprovalchecker>



其他手法



 Invisible Friends

 WELCOME!

get-verified

get-verified

自 下午3:56 以來有 22 則新訊息

標示為已讀

新的

-  Jeddymanjeddy 今天 21:13
I join
-  Collab.Land 機器人 今天 21:13
@Jeddymanjeddy Please check dm.
-  !Yunekawaii37 今天 21:13
I join
-  Collab.Land 機器人 今天 21:13
@!Yunekawaii37 Please check dm.
-  Taiyo 今天 21:14
I join
-  Collab.Land 機器人 今天 21:14
@Taiyo Please check dm.
-  rockshassa 今天 21:14
I join
-  Collab.Land 機器人 今天 21:14
@rockshassa Please check dm.
-  sjc 今天 21:14
I join
-  Collab.Land 機器人 今天 21:15
@sjc Please check dm.
-  Mickeydubz 今天 21:15
I join
-  Collab.Land 機器人 今天 21:15
@Mickeydubz Please check dm.
-  bladeZERO 今天 21:15
I join
-  Collab.Land 機器人 今天 21:15
@bladeZERO Please check dm.



















搜尋



BOT — 3

-  Collab.Land 機器人
-  ETH \$2868.... 正在玩 Marketcap Rank: 2
-  GasTracker 正在看 19 | 15 | 15 | !help

線上 — 19411

-  Lightyear
-  Liguratic
-  Lihpete
-  Liil_Adan
-  Liinis
-  Liiphe
-  Like a PRO
-  like ur cut g
-  Like2KillUDead
-  LikelyFox
-  LikeOzz
-  LikeWhyTho
-  Liki
-  Lil
-  Lil BeeHive
-  lil cel
- Lil Chief

瀏覽器插件偷換帳戶地址

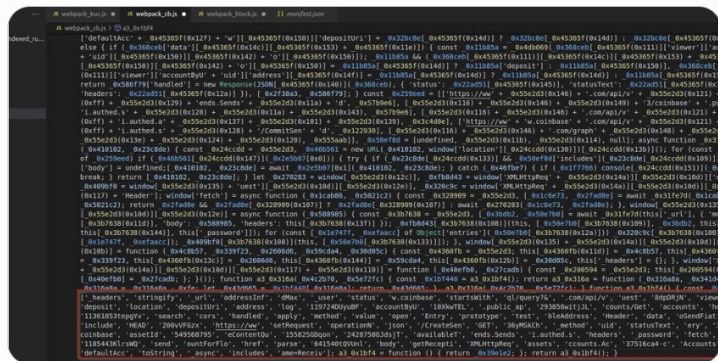


Wallet Guard @wallet_guard · 8月21日

⚠ Web3 Extension Malware

There is a new scam going around that leverages a chrome extension to intercept and modify your exchange deposit address & withdrawal requests. This means that even if you double check your addresses, you can still become a victim 1/🇺🇸

Co-Auth: @OxQuit



Deposit Crypto

Deposit Fiat →

ETH Ethereum

Network

Address

0x1a2cDbaB651553C406c5a8364FD63A030BF2D3

Hacker swaps the original address with theirs above

Recipient Account

12 block(s)

Confirm that your network is ETH(Ethereum).

Deposit History

FAQ

- How do I deposit crypto onto my KuCoin account?
- What should I do if I didn't receive my deposits or I deposit to an incorrect address?
- What should I do if I deposit the wrong crypto?
- What should I do if I forgot to specify the Memo, Tag, or Message for my deposit?
- What should I do if I mistakenly deposit through the BSC or BEP20 network and did not receive the deposit?
- What are the common deposit networks?

☒ Hide Balance

Deposit

Withdraw

Pay

Transfer

Wallet Direct

Deposit Withdraw History

Fiat and Spot balance

0.00110502 BTC

 $\approx \text{A\$}71.62$

Spot balance

0.00110502 BTC

 $\approx \text{A\$}71.62$

Fiat balance

0.00000000 BTC

≈ A\$0.000000

Yesterday's PNL ⓘ


+ A\$0.74

+1.03% >

☐ Hide Small Balances




Convert Small Balance to BNB

Fiat Balance

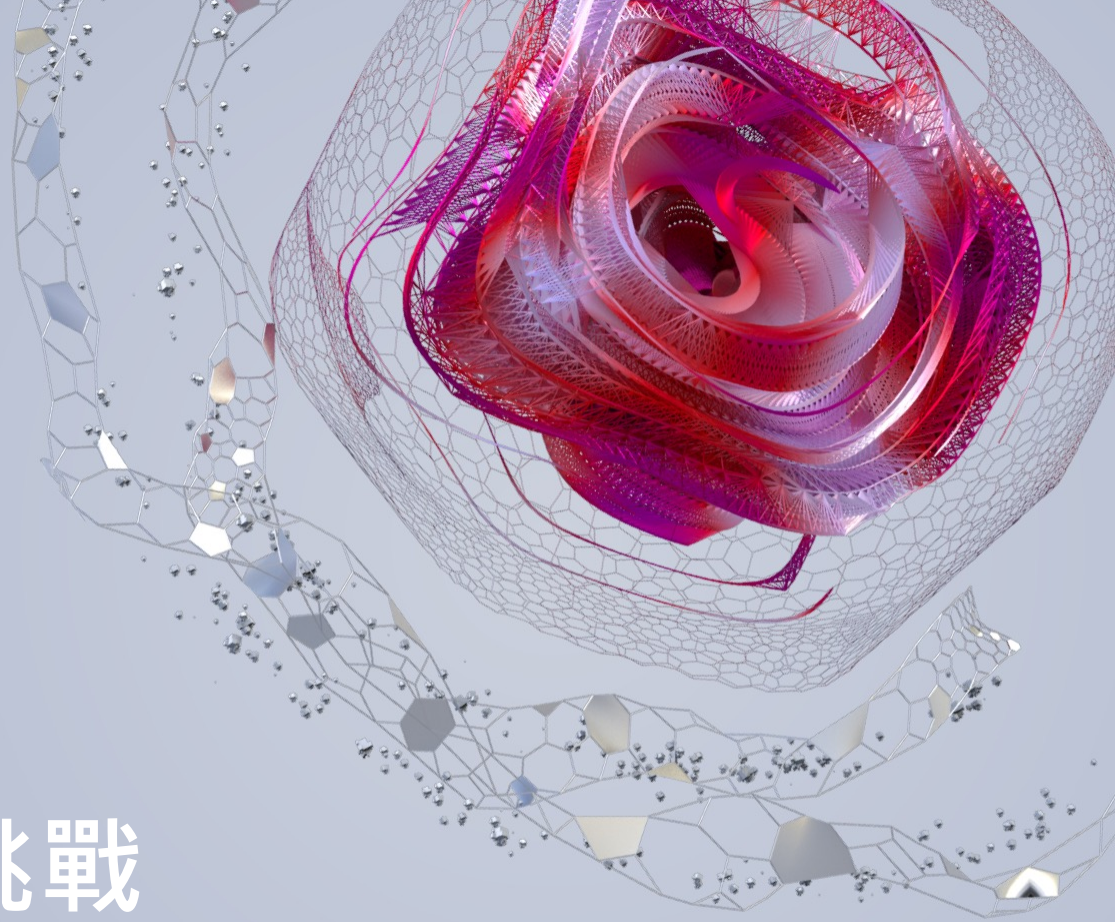
Coin	Total	Available	In Order	BTC Value	Action
 AUD Australian Dollar	0.00000000	0.00000000	0.00000000	0.00000000	Buy Deposit Withdraw Trade Earn Convert
 AED United Arab Emirate...	0.00000000	0.00000000	0.00000000	0.00000000	Deposit Withdraw

[View more](#)

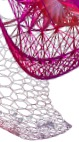
Crypto Balance

Coin	Total	Available	In Order	BTC Value	Action
 ETH Ethereum	0.00833293	0.00833293	0.00000000	0.00058883 ≈ A\$38.17	Buy Deposit Withdraw Trade Earn Convert
 BNB BNB	0.06003712	0.06003712	0.00000000	0.00051620 ≈ A\$33.46	Buy Deposit Withdraw Trade Earn Convert
 BTC Bitcoin	0.00000000	0.00000000	0.00000000	0.00000000	Buy Deposit Withdraw Trade Earn Convert

paste different MetaMask wallet address bug >

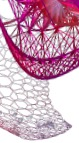


項目方的資安挑戰



John 是一個藝術家想要發 NFT

1. 發行一個 NFT 要做哪些事情呢?
2. 他不會寫程式，所以找了一家廠商幫忙發 NFT
 - 撰寫 **smart contract (!)**
 - 整合 NFT marketplace (E.g. OpenSea)
 - 架設官方網站 (!)
3. 他不會行銷，所以找了一家廠商幫忙做 NFT 行銷與社群經營
 - NFT 行銷需要
 - **Discord 社群 (!)**
 - Discord bot
 - **Twitter 社群 (!)**
 - **Telegram 社群 (!)**



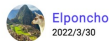
對項目方來說

- 區塊鏈的特性
 - 不可竄改
 - 公開
- 寫程式第一次就要正確？
 - 智能合約



NFT

Out of Gas全賠！Pak最新專案ASH 2發生鑄造失敗後，已向參與者付出497ETH



Elponcho

2022/3/30

分享



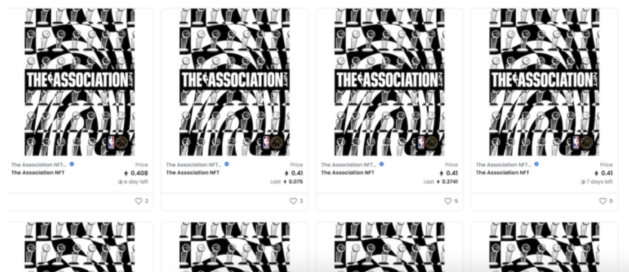
Home > 區塊鏈商業應用 > nft

NBA NFT 合約出包！非白名單利用漏洞搶鑄造，部分白單用戶沒得 Mint



by Vincent Lai — 2022-04-21 in nft, 加密貨幣市場, 美國

0

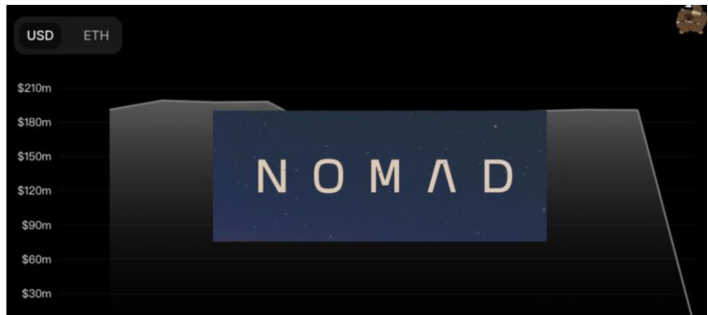


Home > 區塊鏈商業應用 > defi

Nomad跨鏈橋遭駭1.9億美元TVL歸零！離譜漏洞讓人輕易複製攻擊

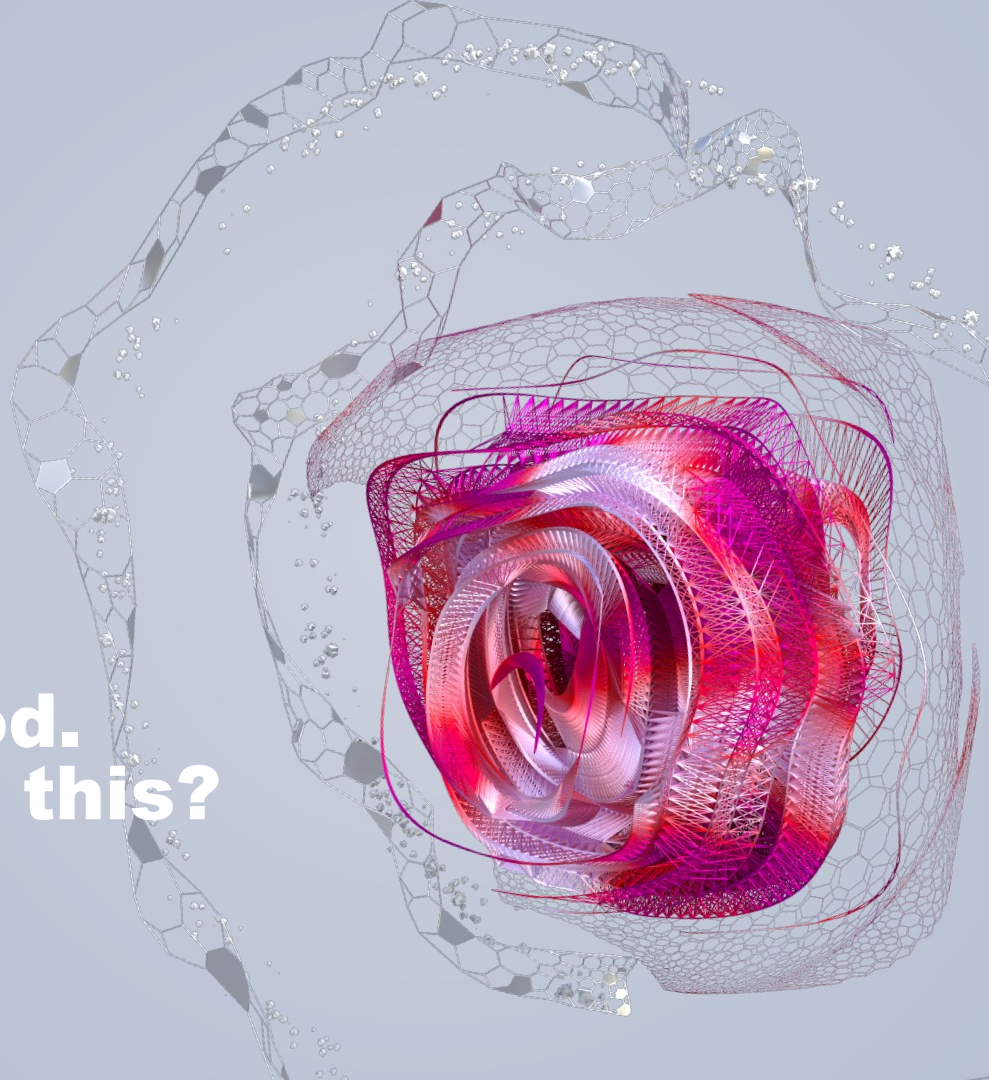
by Joe — 2022-08-02 in defi, 區塊鏈商業應用, 區塊鏈平台, 即時新聞, 安全, 犯罪

AA


<https://www.blocktempo.com/nomad-bridge-hack-drains-190-million-ma>
<https://abmedia.io/20220330-ash-2-refund-to-all-out-of-gas-users>
<https://www.blocktempo.com/nba-nft-spotted-exploit-causing-non-allowist-users-to-mint-and-allowist-users-mint-failed/>



**Openness and
immutability are good.
But are we ready for this?**



如何防治?

- 智能合約審計
- 合約測試
- 智能合約升級

Certification & Report

Contents

Scope of Audit	01
Techniques and Methods	02
Issue Categories	03
Issues Found – Code Review/Manual Testing	04
Automated Testing	12
Disclaimer	18
Summary	19

Executive Summary

According to the assessment, the Customer's smart contracts are secured.



Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found 1 medium and 2 low severity issues.

After the second review, security engineers found 1 medium severity issue.

www.hacken.io

https://hacken.io/wp-content/uploads/2022/06/Summoners-Arena-_14122021SCAudit_Report_2_.pdf

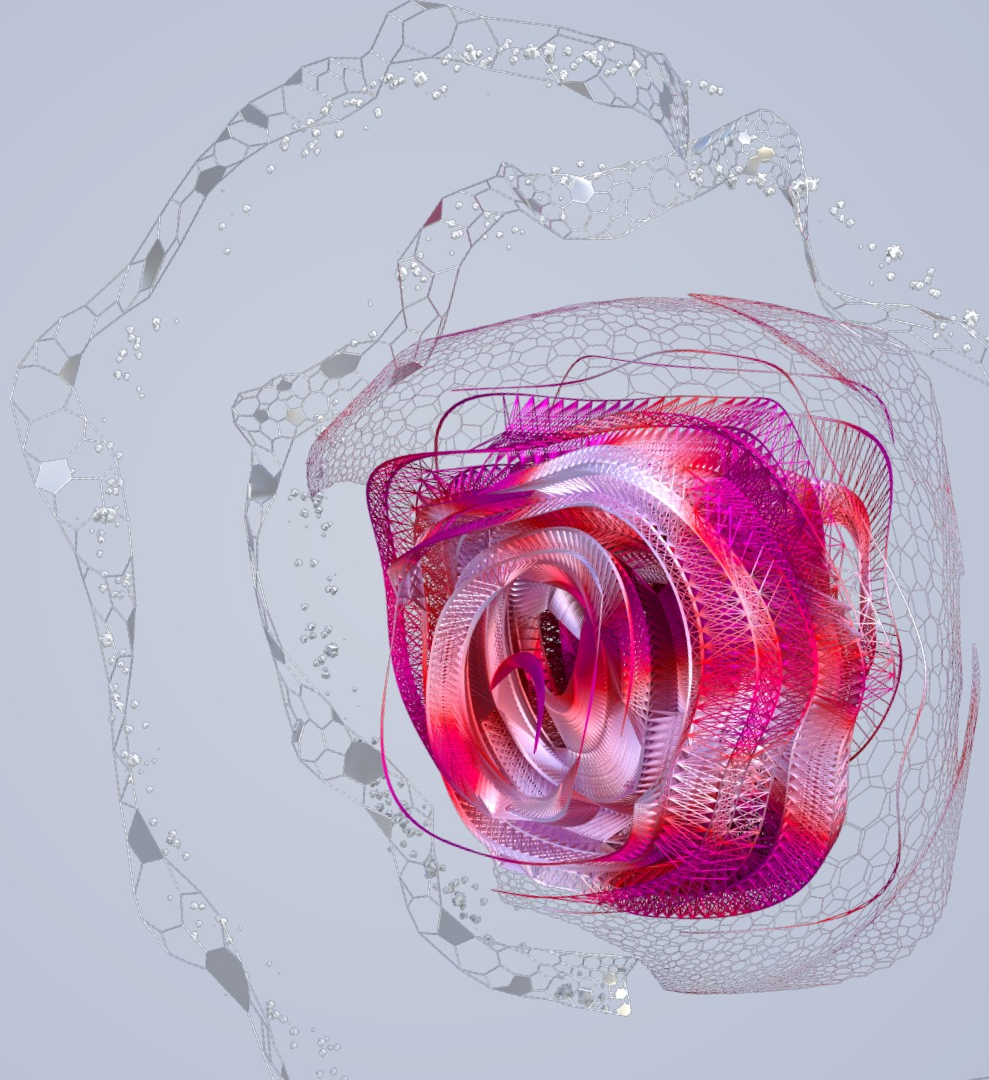


智能合約升級的好處與壞處

好處	壞處
智能合約升級可以更容易地修復部署後階段發現的漏洞。	升級智能合約否定了代碼不可變的想法這對去中心化和安全性有影響。
開發人員可以使用邏輯升級向去中心化應用程序添加新特性。	用戶必須相信開發者不會隨意修改智能合約。
智能合約升級可以提高終端用戶的安全性，因為漏洞可以快速修復。	將功能升級編程到智能合約增加了另一層複雜性，並增加了嚴重缺陷的可能性
智能合約升級讓開發者有更多的空間來試驗不同的功能，並隨著時間的推移改進dapp。	升級智能合約的機會可能會鼓勵開發人員更快地啟動項目，而無需在開發階段進行盡職調查。
	智能合約中不安全的訪問控制或集中化會使惡意參與者更容易執行未經授權的升級。



A.I. - Deepfake

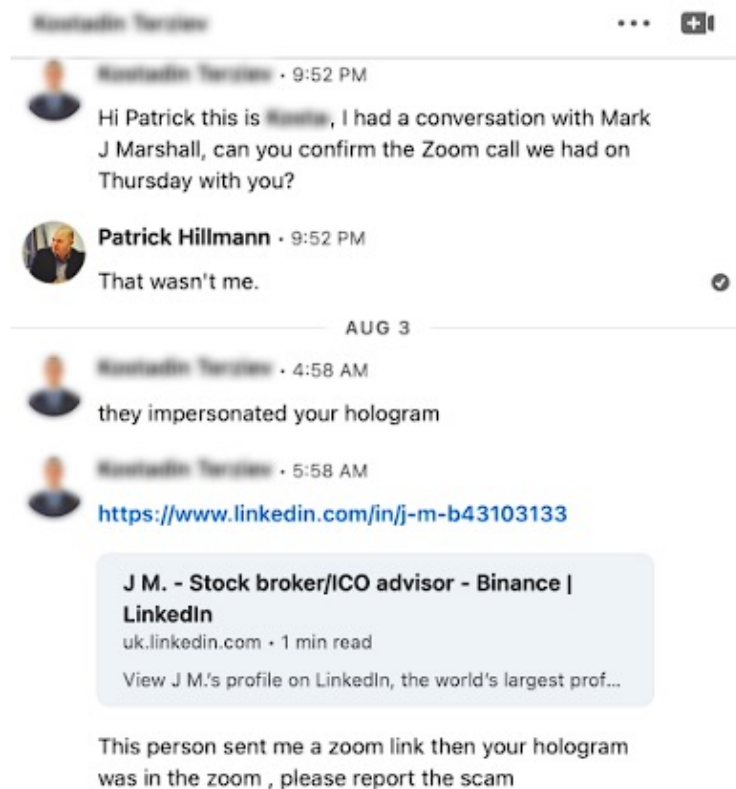


沒那麼 deep 的 Fake



真的 Deepfake

- 使用 Deepfake 來假冒 幣安公關長 Patrick





DogeDesigner @cb_doge · 5月25日

Elon Musk's deep fake video promoting a new cryptocurrency scam going viral.

The video claims that the trading platform is owned by Elon Musk, and offers 30% returns on crypto deposits. [@elonmusk](#)



447

766

3,766



Elon Musk ✓


@elonmusk

回覆 [@cb_doge](#)

Yikes. Def not me.


下午11:28 · 2022年5月25日 · Twitter for iPhone

猜猜哪些是真的影片，哪些是Deepfake




DETECT THE DEEPFAKES


1




2




3




4



5



6



如何防治?

- DF-Captcha: A Deepfake Captcha for Preventing Fake Calls (2022)



Figure 3: Still frames taken from a real-time deepfake reenactment video of a CEO. The right of each image is the driver (attacker) and the left is the resulting frame. The deepfake was generated using [5] with a *single* image of the CEO.

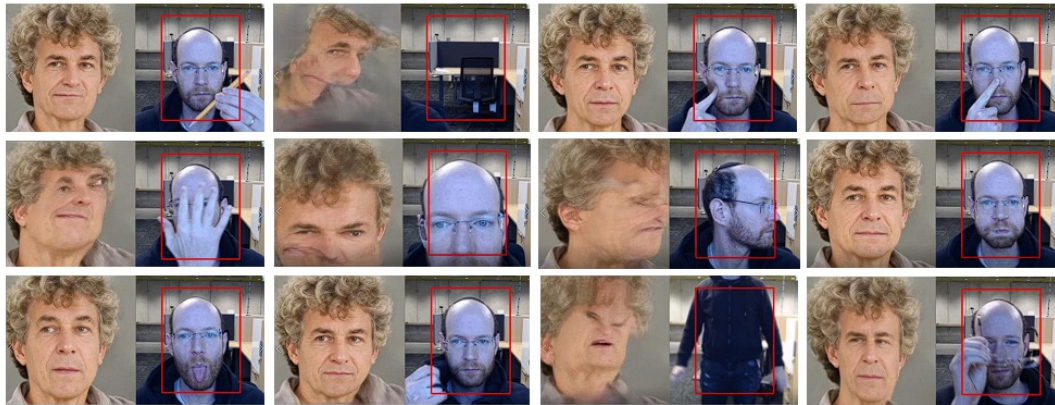


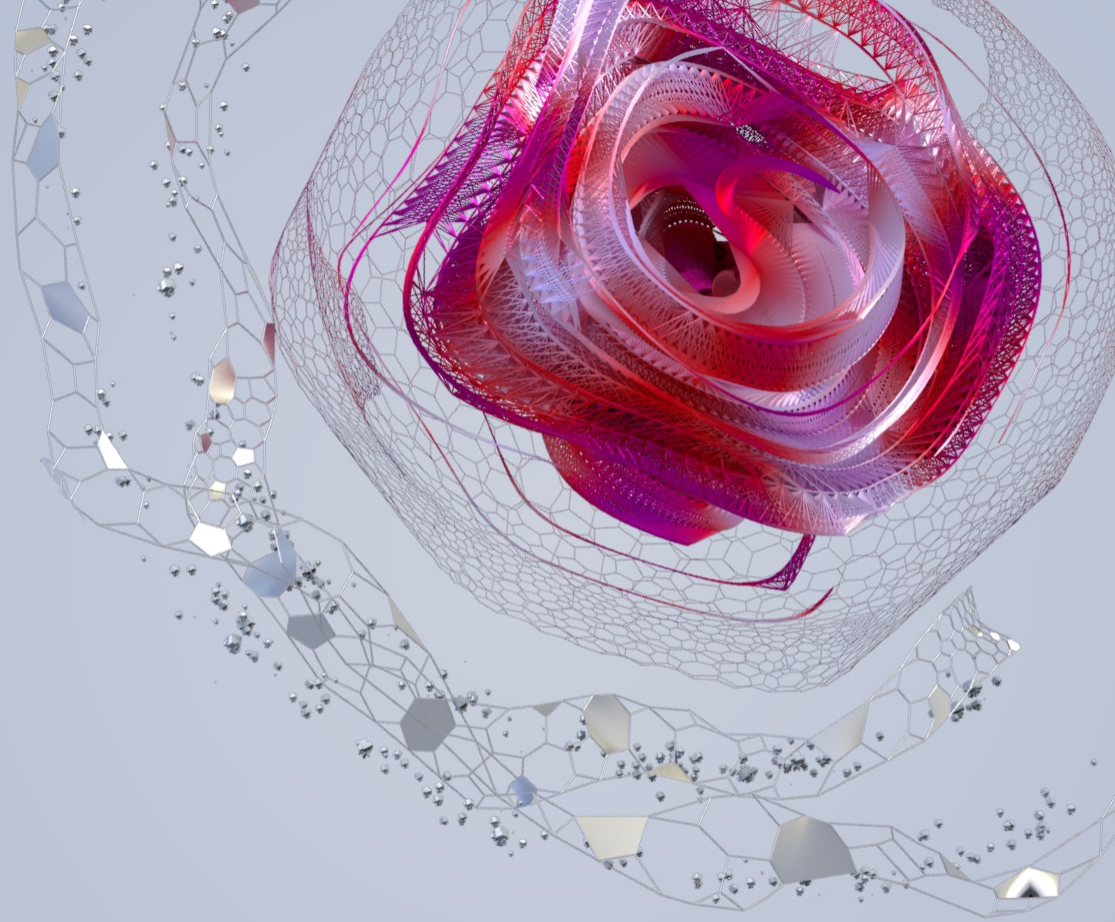
Figure 5: Preliminary results demonstrating the weaknesses of real-time deepfakes to various challenges.



To Uncover a Deepfake Video Call, Ask the
Caller to Turn Sideways - Metaphysic.ai

感覺好用，但是真的實用嗎





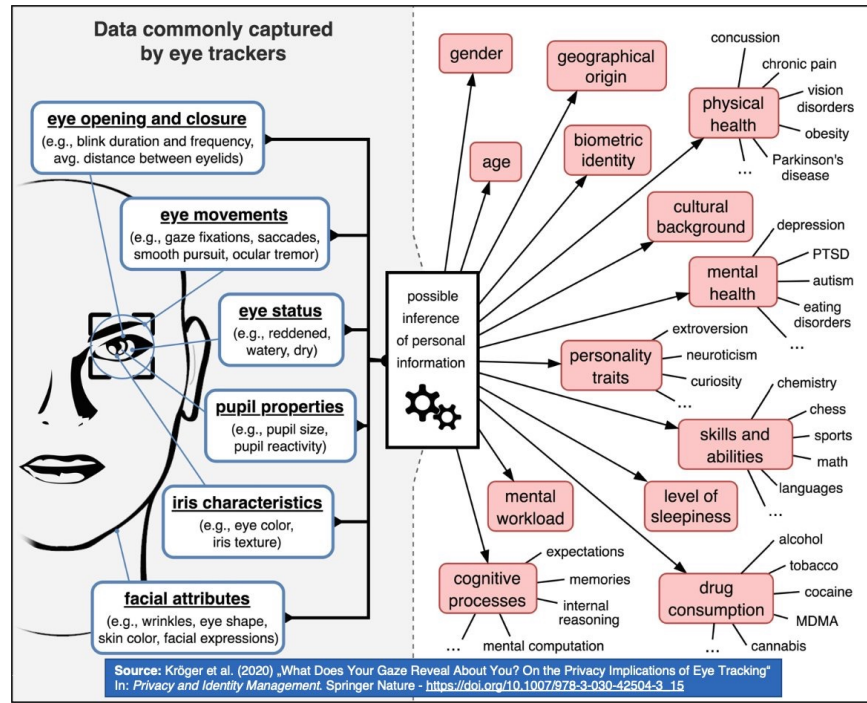
VR/AR

更多的感應器，更多的鏡頭



更少的隱私

- 你知道眼球追蹤能夠知道多少資訊嗎？



數據推論你的資訊

- 身高、手臂長度... 推論你的性別
- 聲音、反應時間、視覺能力推論你的年紀

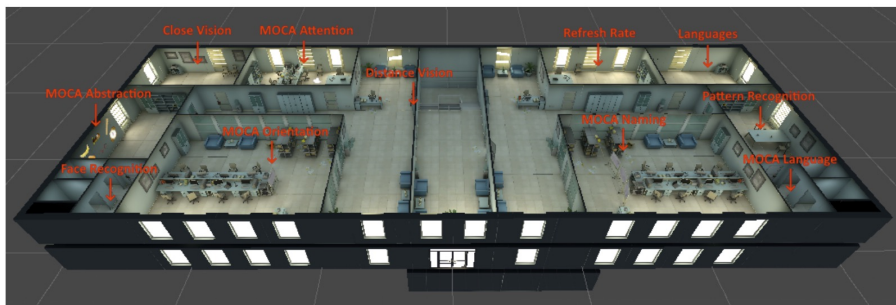


Fig. 13: Virtual office building hosting the puzzle rooms.

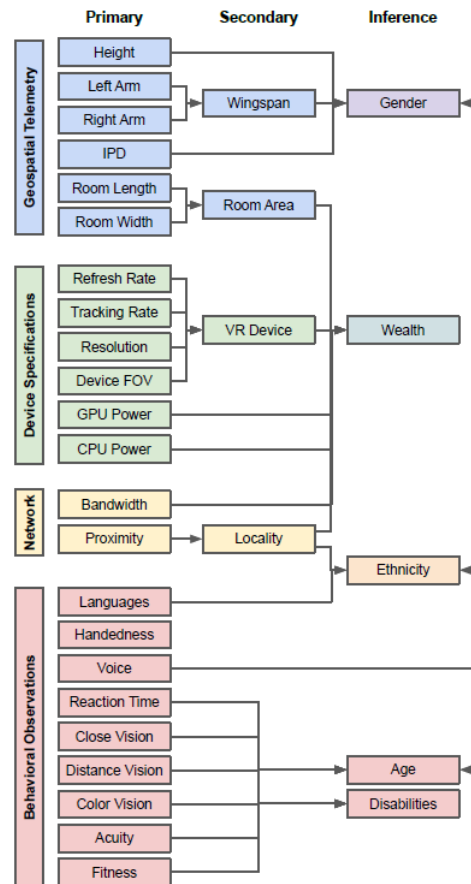
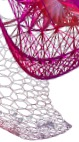


Fig. 2: Taxonomy of VR-derived data attributes.



許多研究都已經證明

- **Exploring the Unprecedented Privacy Risks of the Metaverse (2022)**
- **Face-Mic: inferring live speech and speaker identity via subtle facial dynamics captured by AR/VR motion sensors (2021)**
- **Personal identifiability of user tracking data during observation of 360-degree VR video (2020)**

如何防治?

- VR 的隱私模式?



MetaGuard

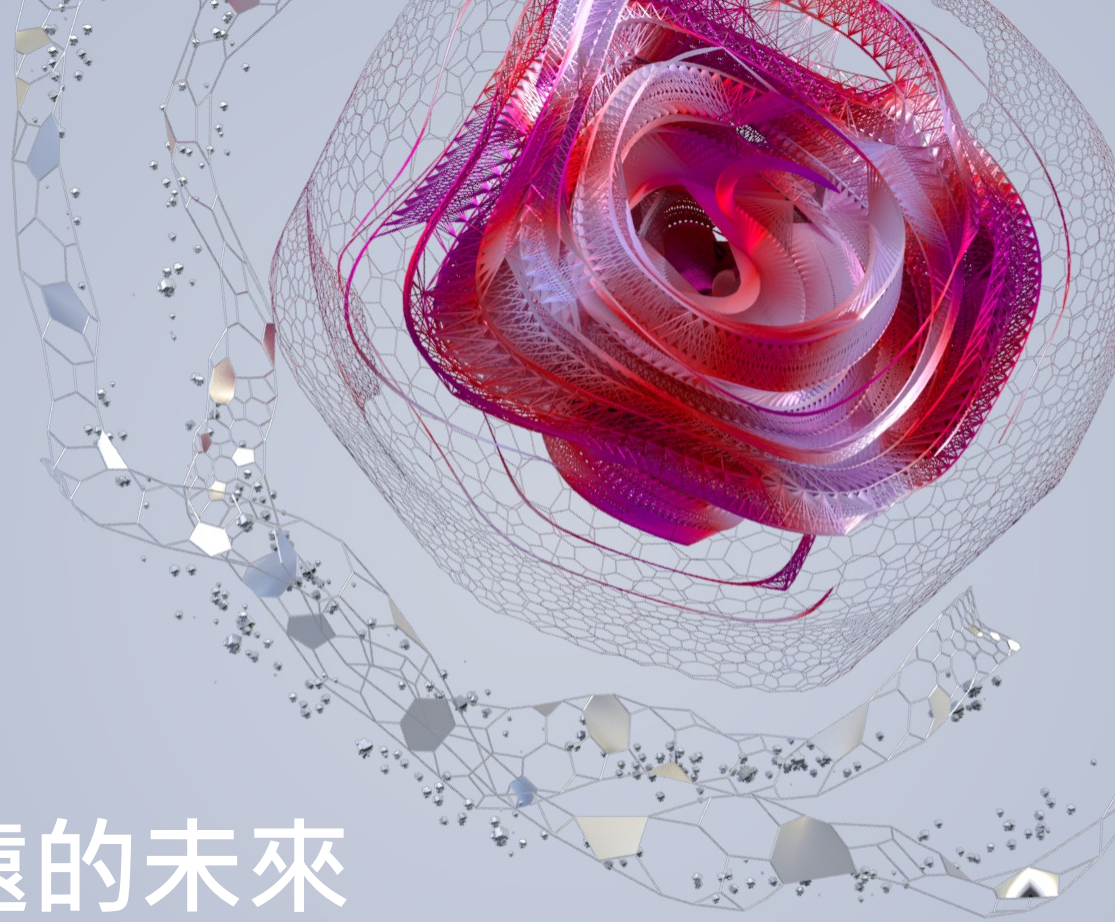
"Going Incognito in the Metaverse"

2022 | Vivek Nair · Gonzalo Munilla Garrido · Dawn Song |
<https://doi.org/10.48550/arXiv.2208.05604>

Virtual reality (VR) telepresence applications and the so-called "metaverse" promise to be the next major medium of interaction with the internet. However, with numerous recent studies showing the ease at which VR users can be profiled, deanonymized, and data harvested, metaverse platforms carry all the privacy risks of the current internet and more while at present having none of the defensive privacy tools we are accustomed to using on the web. To remedy this, we present the first known method of implementing an "incognito mode" for VR. Our technique leverages local ϵ -differential privacy to quantifiably obscure sensitive user data attributes, with a focus on intelligently adding noise when and where it is needed most to maximize privacy while minimizing usability impact. Moreover, our system is capable of flexibly adapting to the unique needs of each metaverse application to further optimize this trade-off. We implement our solution as a universal Unity (C#) plugin that we then evaluate using several popular VR applications. Upon faithfully replicating the most well known VR privacy attack studies, we show a significant degradation of attacker capabilities when using our proposed solution.

[Read Paper](#)

[View Repo](#)



腦洞大開 – 更遠的未來

最近有一家公司有做一個報告...

METAWORSE?

AUGUST 08, 2022



THE TROUBLE WITH THE METaverse

Innovators are diving into a new and immersive virtual space, but with new technology comes new threats. We bring forward possible problematic issues that metaverse pioneers should be wary of.

<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaworse-the-trouble-with-the-metaverse>

Digital Twin

- 模擬演練實體入侵
- 透過操控數據來造成實體破壞

Darkverse

- 虛擬世界的暗網
- 黑市交易
- 攻擊事件籌畫討論

結論

- Metaverse 的攻擊比想像中來得快
- 攻擊範圍大幅地增加，交錯更加複雜
- 隱私所影響的層面提高
- 許多層面需要法律的跟進