HKCERT

Cyber Security New Challenges in Web 3.0

Lawrence Law | Security Consultant, HKCERT

WFH Digital Certificate
Security Awareness DDoS
Malware Password Sniffing
Exploitation Virtual
Worm Domain Hijack
DeepFake
Anti-spyware Unencrypted
Hacker QR Code
IP Address AI Fruads
Data Breach Webinar
HTTPS VPN
Robotics
Information Security Web Meeting
Remote Work Distance Learning Social networking
HKCERT Cyberspace
Automatic updates
Digital Transformation Network Black Hat Phishing
Cybercrime Sensitive Information
Data Leakage System Overload Confidentiality
Extortion Data protection
Vulnerabilities Scams Distance Learning
Trojan Virus Blacklist Internet Browsing Webmail BYOD
Authentication
Backdoor Digital copyrights Keystrokes Activity Monitoring
Coding Antivirus Data Loss Prevention
Spear Phishing Activity Monitoring Privacy Identity check Ransomcloud
Online Shopping Ransomware
Cyber Attack Cloud Sharing Firewalls Clickjacking

HKCERT

Agenda

1. What is Web 3.0?
2. Cyber Attacks in Web 3.0
3. Security Advice

WFH Digital Certificate
Security Awareness DDoS
Malware Password Sniffing
Exploitation
Virtual
Worm Domain
Hijack
DeepFake
Anti-spyware
Unencrypted
Hacker
QR Code
IP Address
AI Fruads
Data Breach
Webinar
HTTPS
VPN
Robotics
Information Security Web Meeting
Remote Work Distance Learning Social networking
HKCERT Cyberspace
Automatic updates
Digital Transformation
Network Black Hat Phishing
Cybercrime
Sensitive Information
Data Leakage System Overload
Confidentiality
Extortion Data protection
Scams Distance Learning
Vulnerabilities
Trojan Virus Blacklist Internet
Browsing Webmail BYOD
Authentication
Backdoor Digital copyrights
Keystrokes Activity Monitoring
Coding Antivirus Data Loss Prevention
Spear Phishing Activity Monitoring Privacy Identity check Ransomcloud
Online Shopping Ransomware
Cyber Attack Cloud Sharing Firewalls Clickjacking

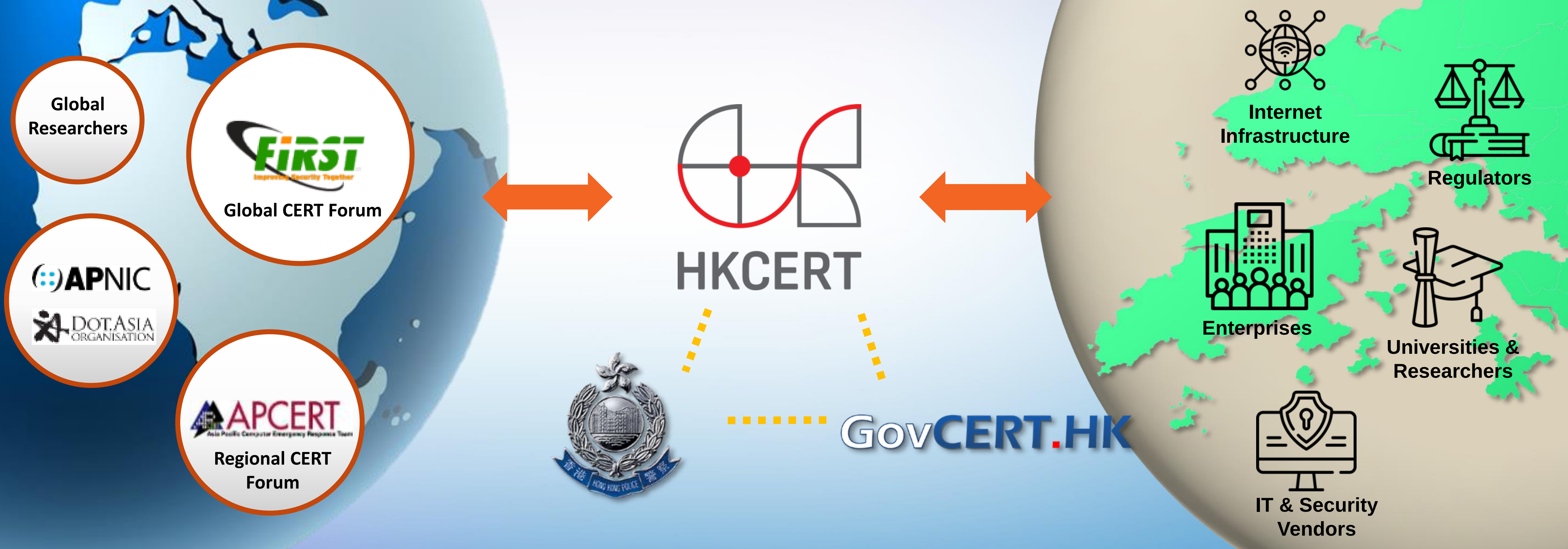
International

Local

Exchange Incidents and Information

HKCERT as a Hub

Coordinate incidents and publish alerts



Global Researchers

FIRST
Improving Security Together
Global CERT Forum

APNIC
DOT.ASIA ORGANISATION

APCERT
Asia Pacific Computer Emergency Response Team
Regional CERT Forum

HKCERT

GovCERT.HK

Internet Infrastructure

Regulators

Enterprises

Universities & Researchers

IT & Security Vendors

Service and Support by HKCERT

Monitoring

- Collect and Analyse Attack Patterns
- Provide Early Information Security Alerts

Education and Technical Advice

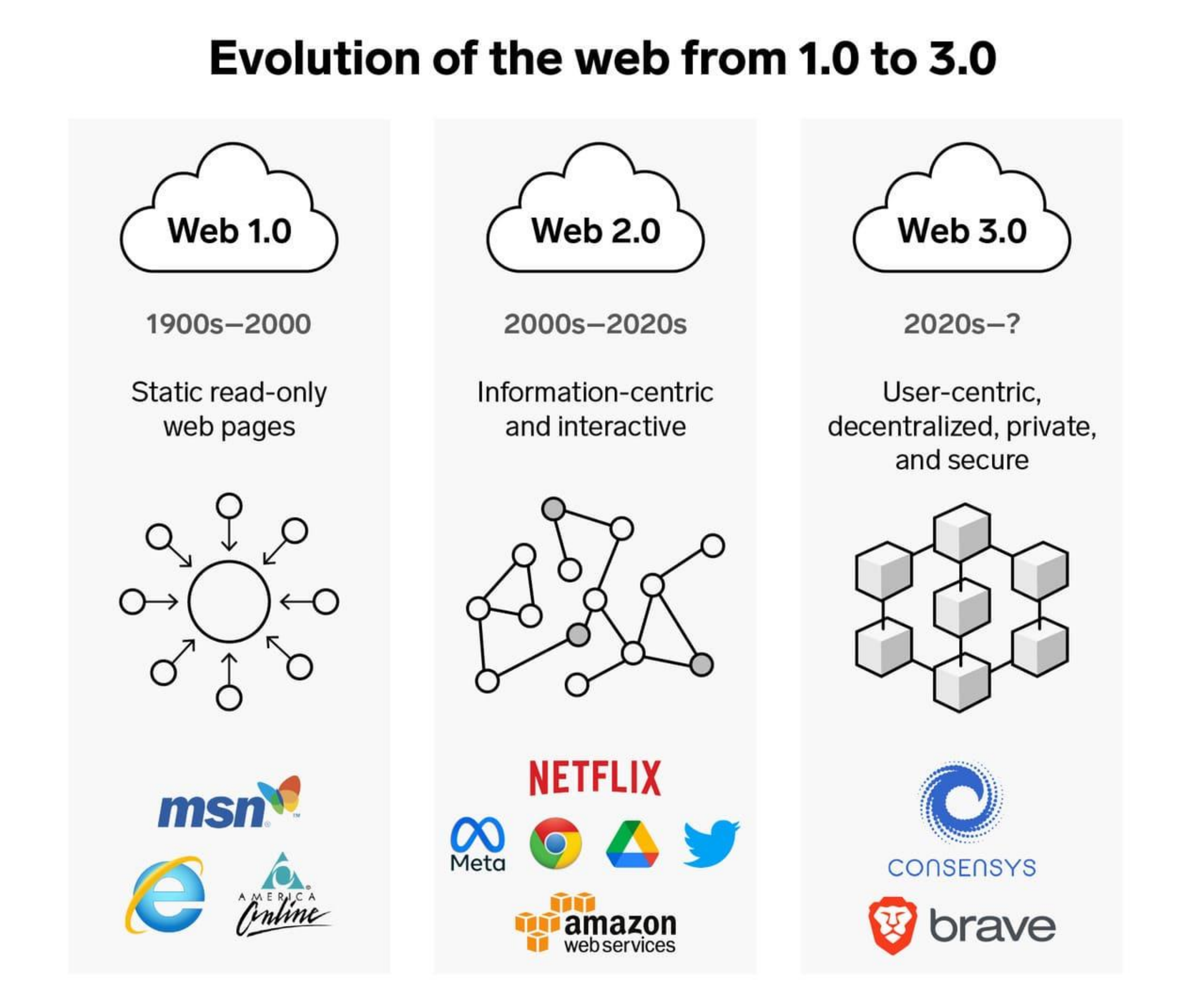
- 24-hours Free Incident Report Hotline (8105-6060)
- Organise Free Seminars and Briefings
- Collaborate with Local Industry, Government Agencies, and Global CERTs

Research and Insights

- Offer Best Practice and Guideline
- Provide Online Cyber Security Self-Assessment Tool

2 What is Web 3.0?

Key Differences in Web 3.0

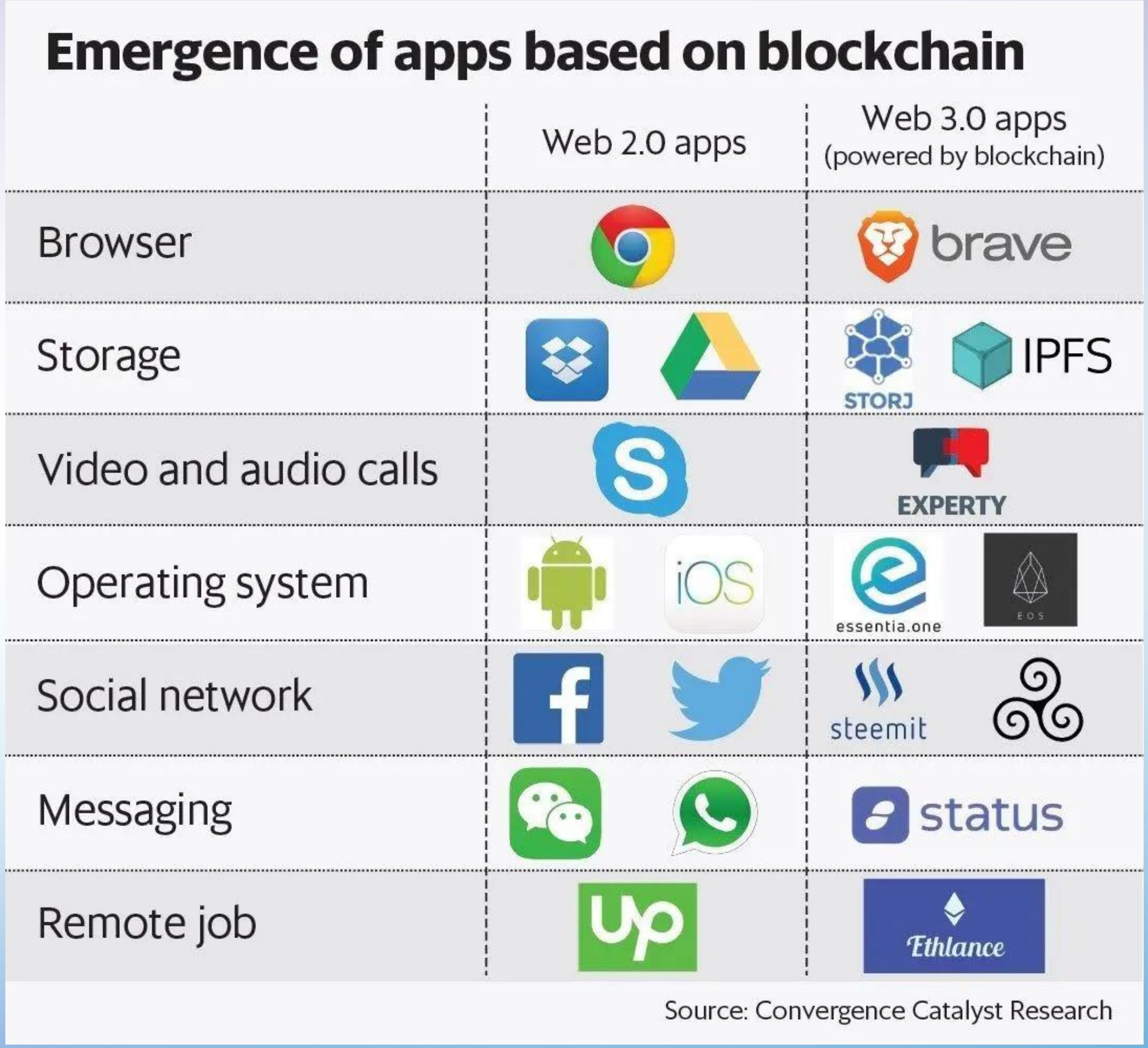


Evolution of the web from 1.0 to 3.0

Web 1.0	Web 2.0	Web 3.0
1900s–2000	2000s–2020s	2020s–?
Static read-only web pages	Information-centric and interactive	User-centric, decentralized, private, and secure

Source: https://www.theinsaneapp.com/2022/08/web3.html

Example of Apps Leveraging Web 3.0 Technology



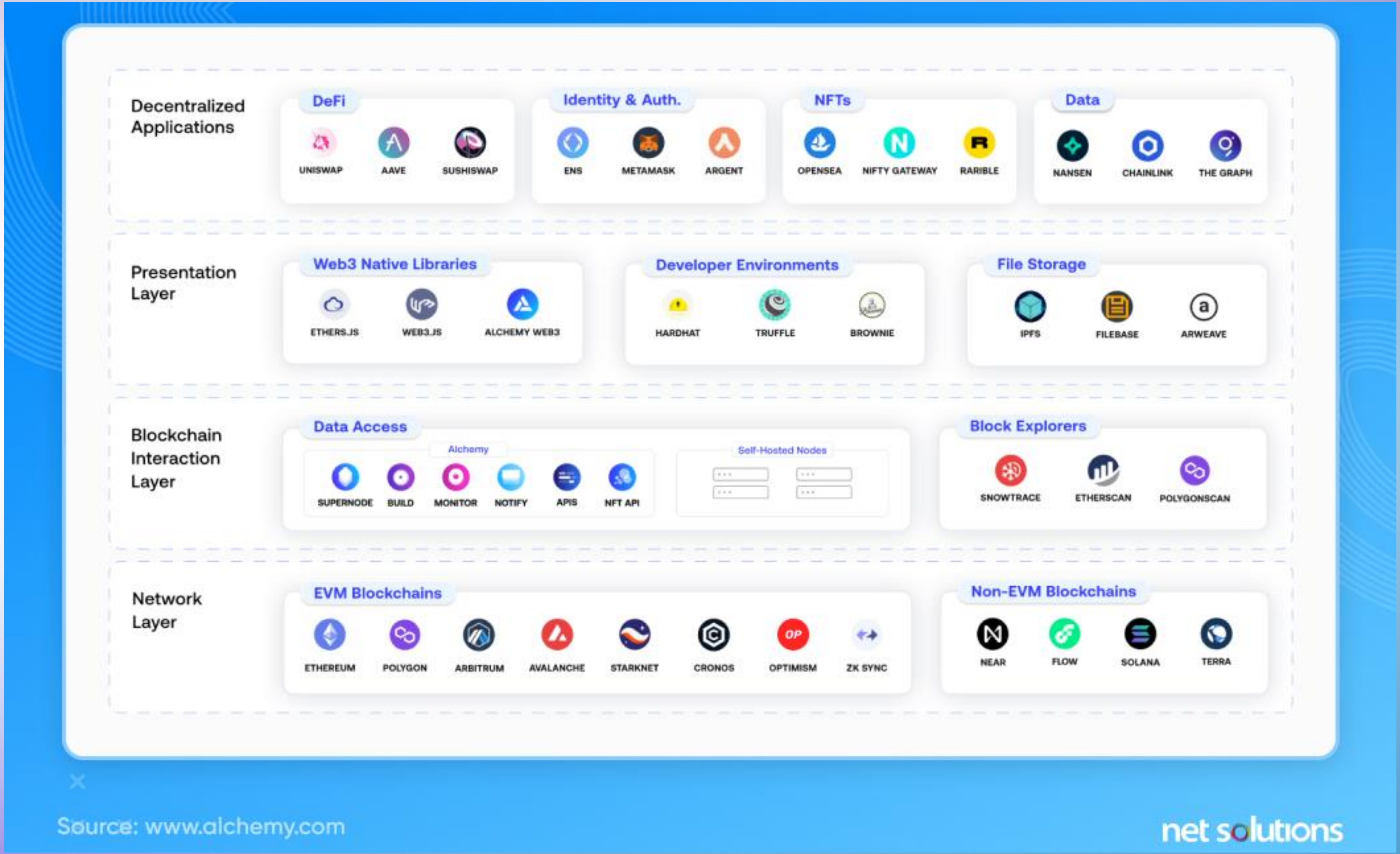
Emergence of apps based on blockchain

	Web 2.0 apps	Web 3.0 apps (powered by blockchain)
Browser		brave
Storage		STORJ IPFS
Video and audio calls	S	EXPERTY
Operating system	iOS	essentia.one EOS
Social network	f	steemit
Messaging		status
Remote job	Up	Ethlance

Source: Convergence Catalyst Research

Source: https://anric.blatt.com/blockchain/the-emergence-of-apps-based-on-blockchain-web-3-0/

Technology Landscape in Web 3.0



Decentralized Applications
- DeFi: UNISWAP, AAVE, SUSHISWAP
- Identity & Auth.: ENS, METAMASK, ARGENT
- NFTs: OPENSEA, NIFTY GATEWAY, RARIBLE
- Data: NANSEN, CHAINLINK, THE GRAPH

Presentation Layer
- Web3 Native Libraries: ETHERS.JS, WEB3.JS, ALCHEMY WEB3
- Developer Environments: HARDHAT, TRUFFLE, BROWNIE
- File Storage: IPFS, FILEBASE, ARWEAVE

Blockchain Interaction Layer
- Data Access: Alchemy: SUPERNODE, BUILD, MONITOR, NOTIFY, APIS, NFT API; Self-Hosted Nodes
- Block Explorers: SNOWTRACE, ETHERSCAN, POLYGONSCAN

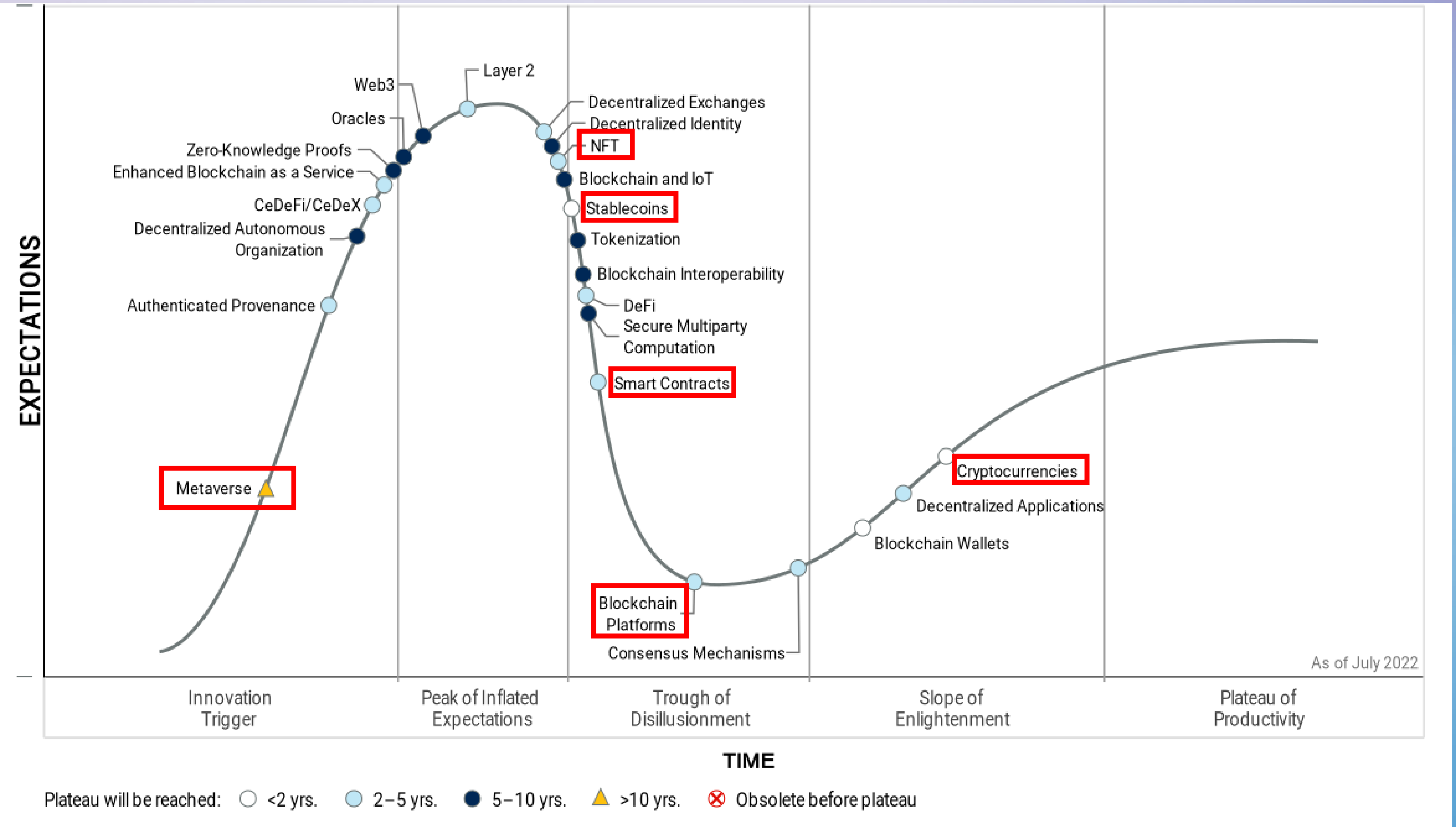
Network Layer
- EVM Blockchains: ETHEREUM, POLYGON, ARBITRUM, AVALANCHE, STARKNET, CRONOS, OPTIMISM, ZK SYNC
- Non-EVM Blockchains: NEAR, FLOW, SOLANA, TERRA

Source: www.alchemy.com

net solutions

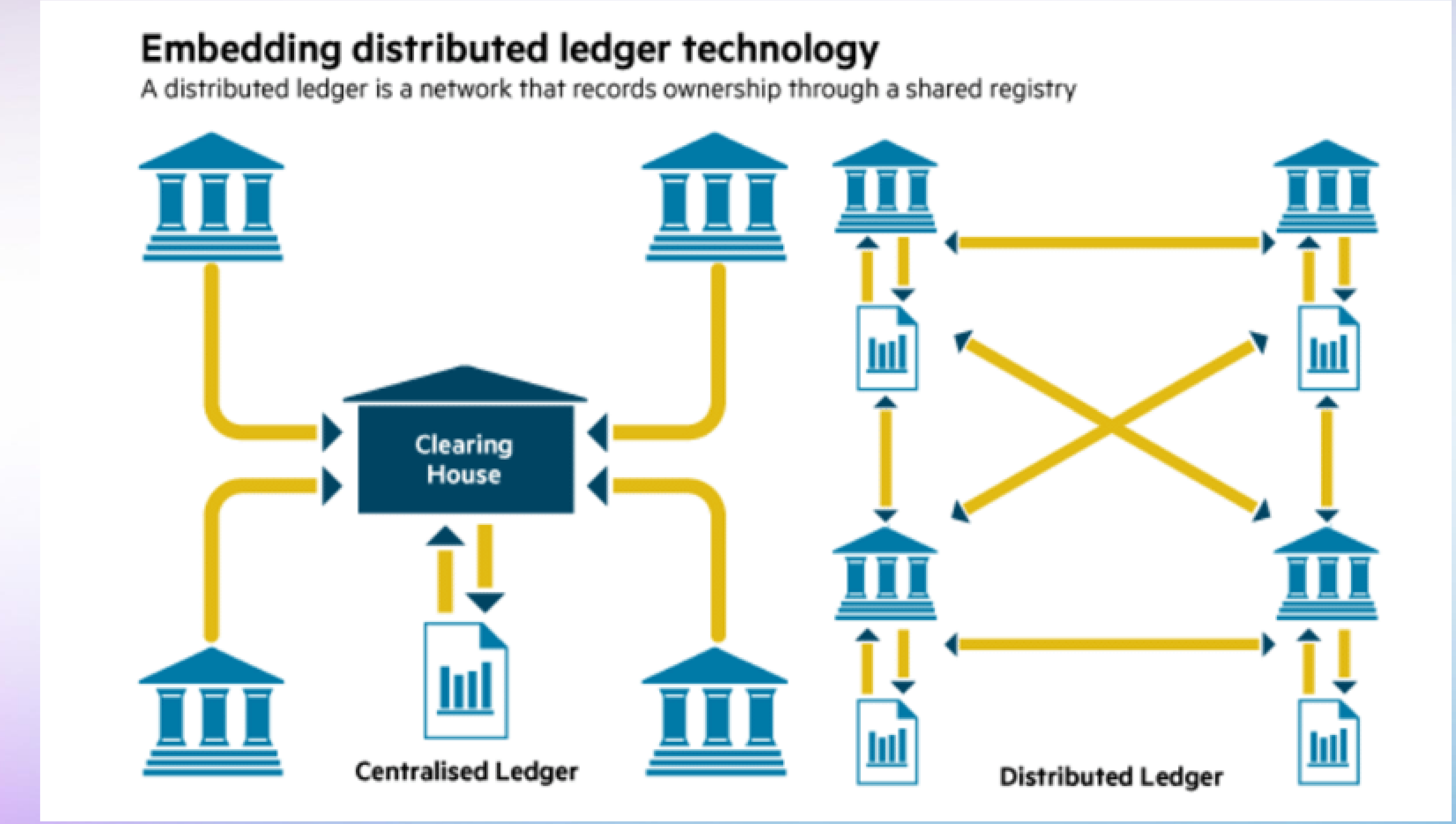
Source: https://www.netsolutions.com/insights/what-is-web-3-0-why-does-it-matter/

Web 3.0 Hype Cycle



Source: https://www.gartner.com/en/newsroom/press-releases/2022-08-30-metaverse-web3-and-crypto-separating-blockchain-hype-from-reality

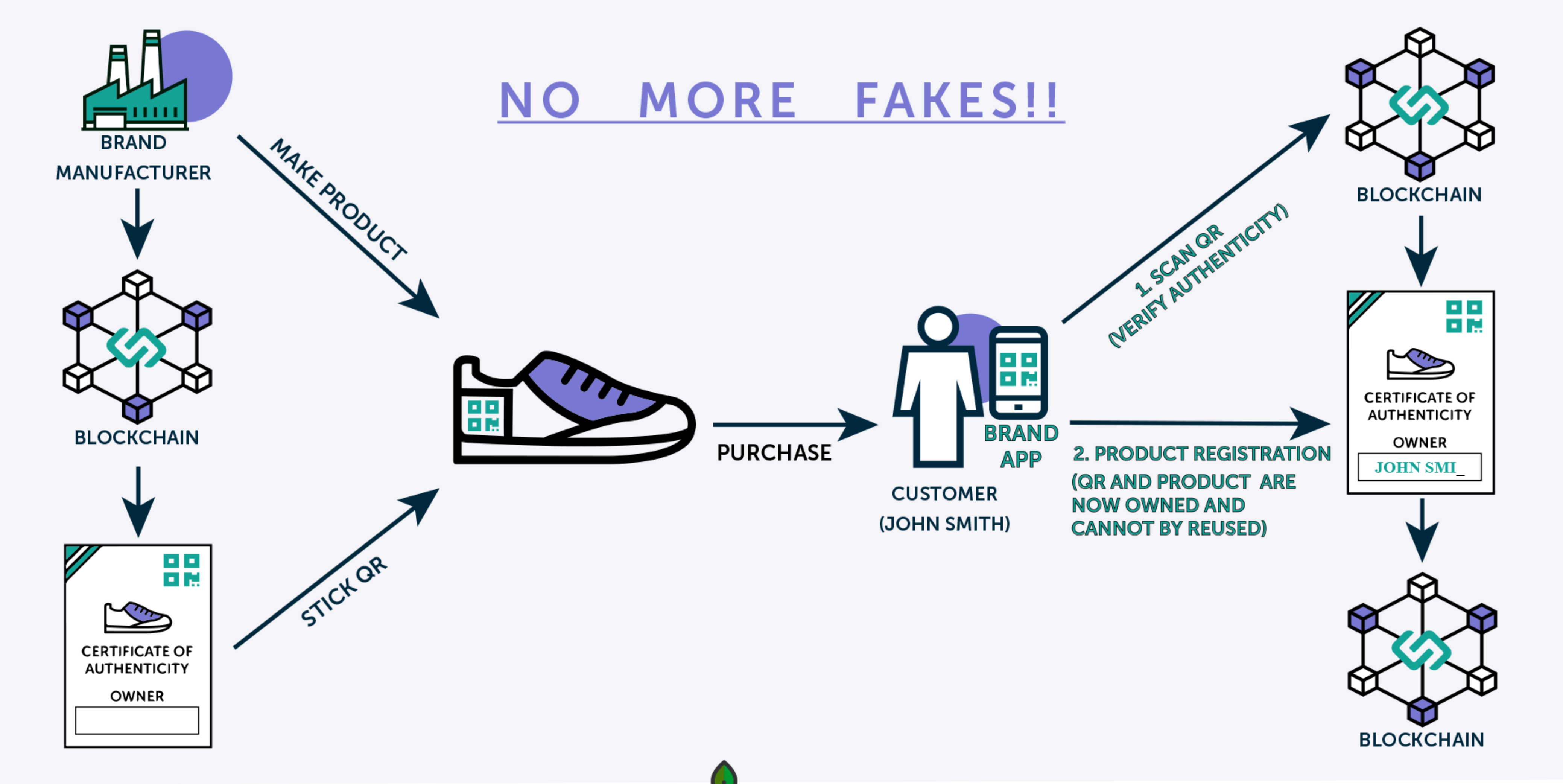
The Basic Concept of Blockchain


Embedding distributed ledger technology
A distributed ledger is a network that records ownership through a shared registry
Clearing House
Centralised Ledger
Distributed Ledger

- Blockchain works as Distributed Ledger
- Not central authority architecture
- Validity of transaction is verified and censored by peer node

Source: https://www.researchgate.net/figure/Two-examples-of-ledgers-a-centralized-and-a-distributed-one-From-10ZTalk_fig1_334626679

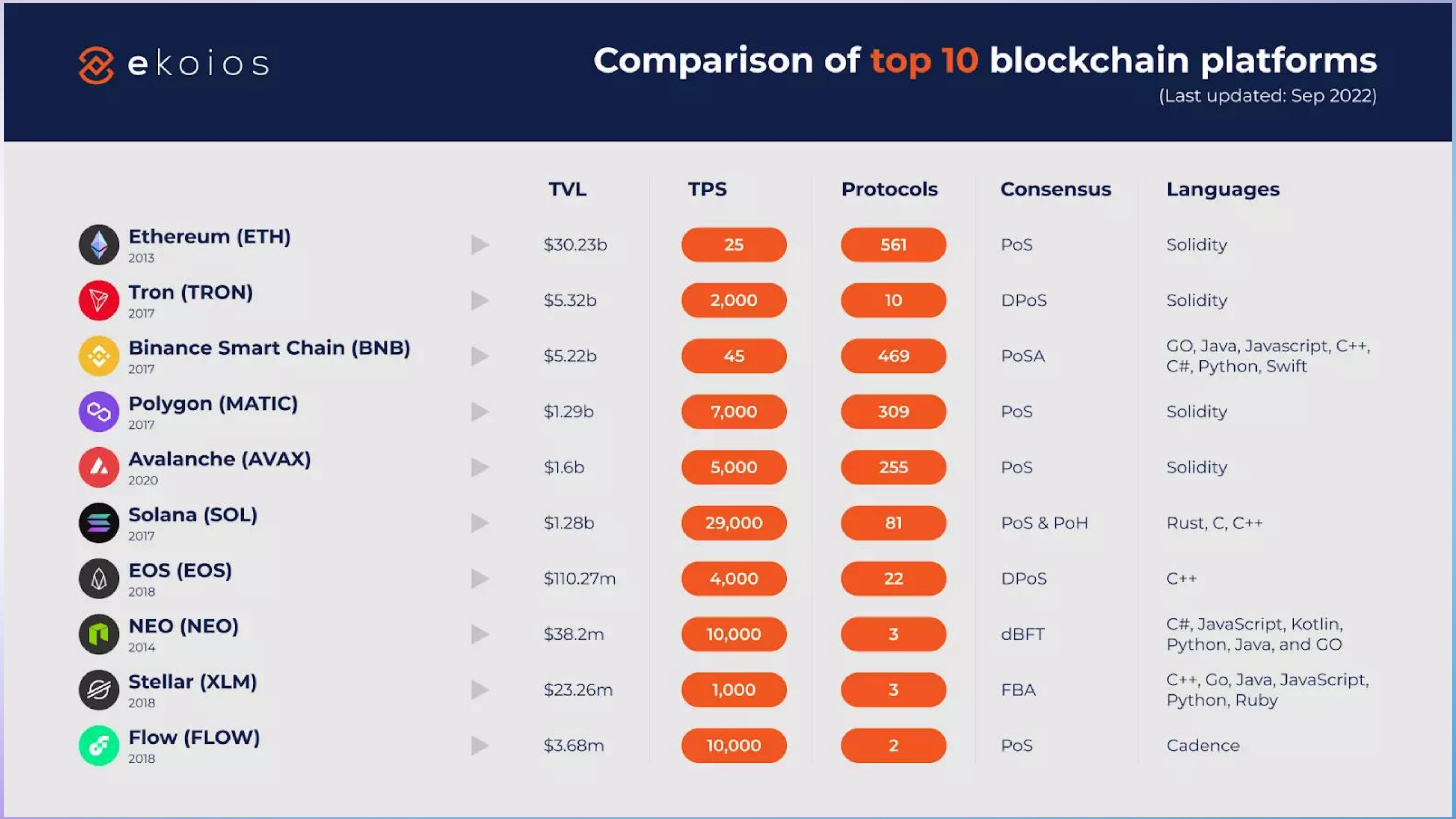
Use Case of Blockchain



ethereum æternity RSK SMARTER BITCOIN ethereum classic HYPERLEDGER FABRIC

Source: https://www.blockm3.com/en/certinchain/

Top Blockchain Platforms



ekoios

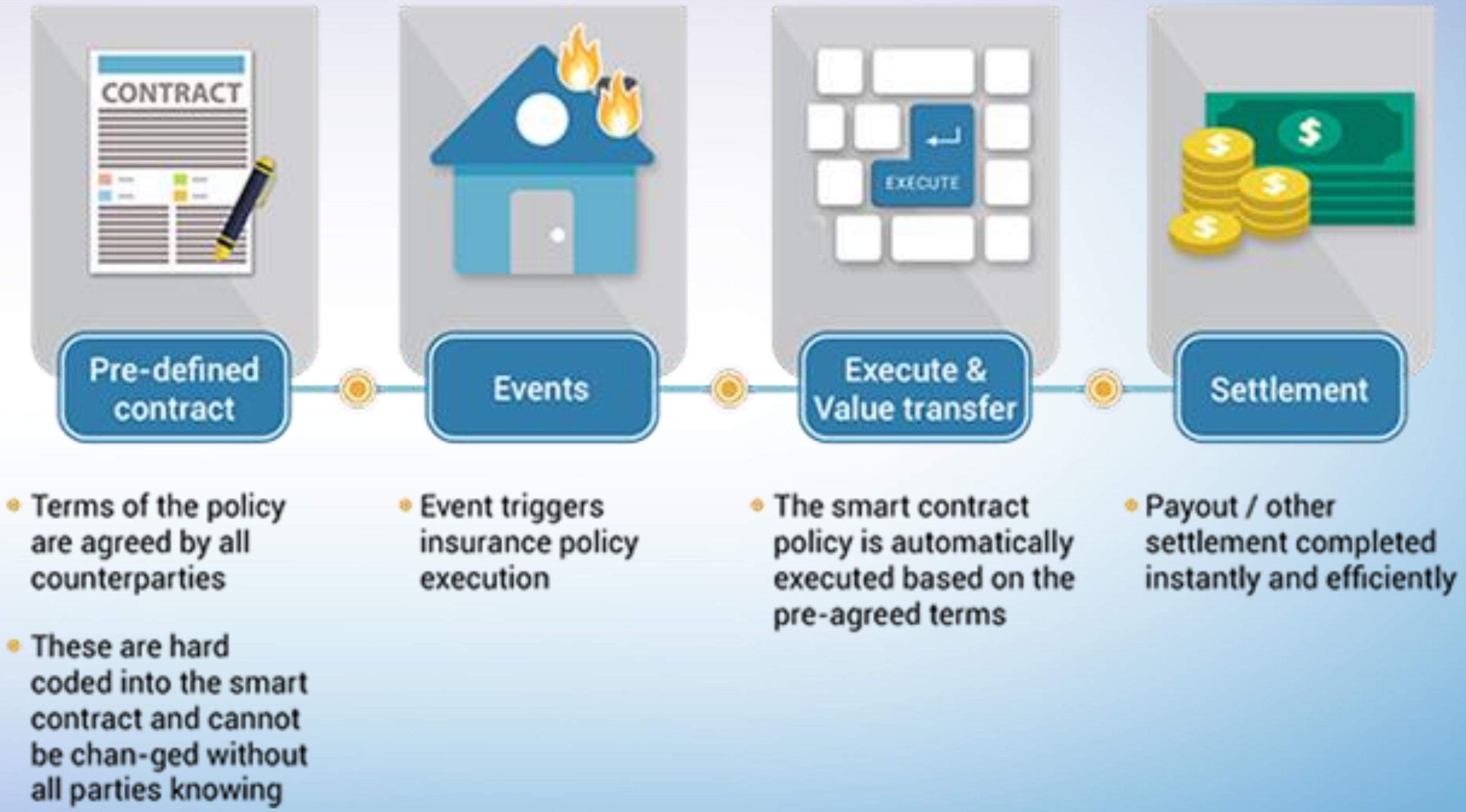
Comparison of top 10 blockchain platforms

(Last updated: Sep 2022)

	TVL	TPS	Protocols	Consensus	Languages
Ethereum (ETH) 2013	$30.23b	25	561	PoS	Solidity
Tron (TRON) 2017	$5.32b	2,000	10	DPoS	Solidity
Binance Smart Chain (BNB) 2017	$5.22b	45	469	PoSA	GO, Java, Javascript, C++, C#, Python, Swift
Polygon (MATIC) 2017	$1.29b	7,000	309	PoS	Solidity
Avalanche (AVAX) 2020	$1.6b	5,000	255	PoS	Solidity
Solana (SOL) 2017	$1.28b	29,000	81	PoS & PoH	Rust, C, C++
EOS (EOS) 2018	$110.27m	4,000	22	DPoS	C++
NEO (NEO) 2014	$38.2m	10,000	3	dBFT	C#, JavaScript, Kotlin, Python, Java, and GO
Stellar (XLM) 2018	$23.26m	1,000	3	FBA	C++, Go, Java, JavaScript, Python, Ruby
Flow (FLOW) 2018	$3.68m	10,000	2	PoS	Cadence

Source: https://ekoios.vn/top-10-blockchain-platforms-of-2020-and-their-applications

The Basic Concept of Smart Contract



- Terms of the policy are agreed by all counterparties
- These are hard coded into the smart contract and cannot be chan-ged without all parties knowing

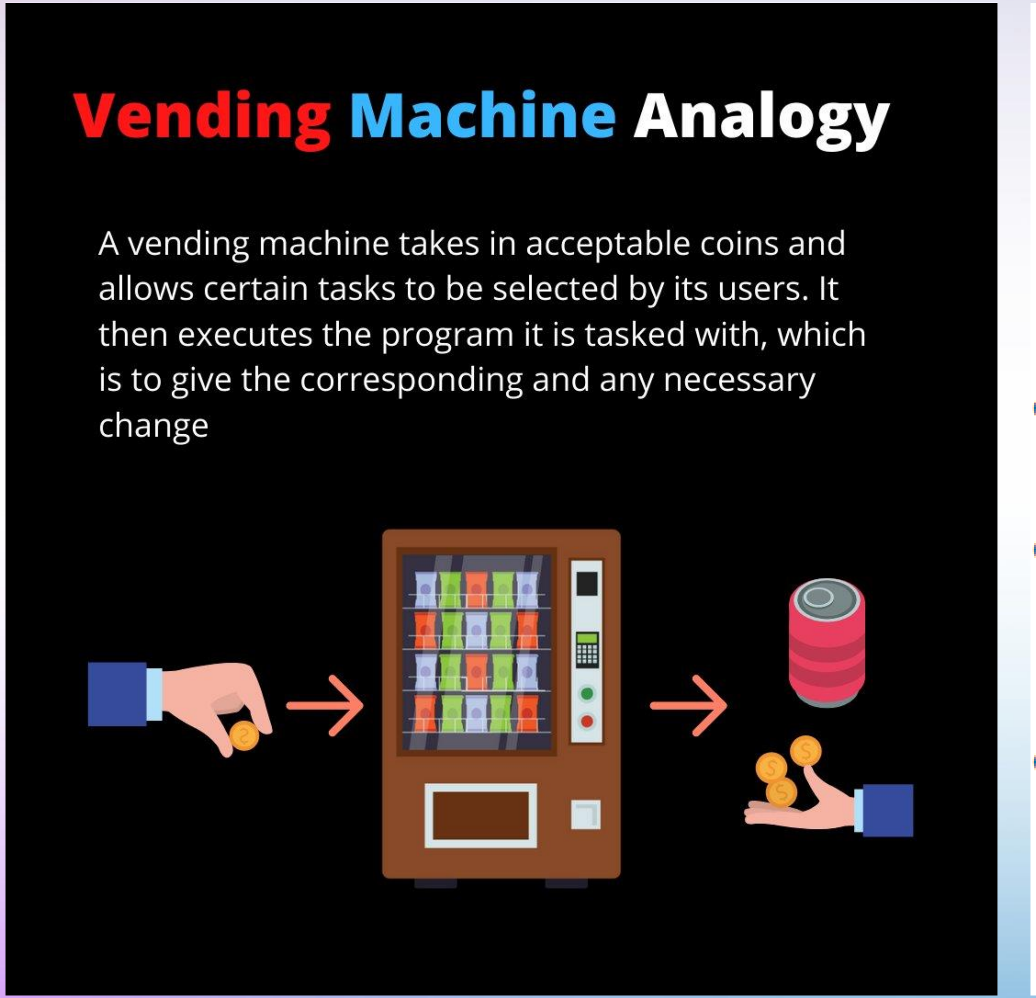
- Event triggers insurance policy execution

- The smart contract policy is automatically executed based on the pre-agreed terms

- Payout / other settlement completed instantly and efficiently

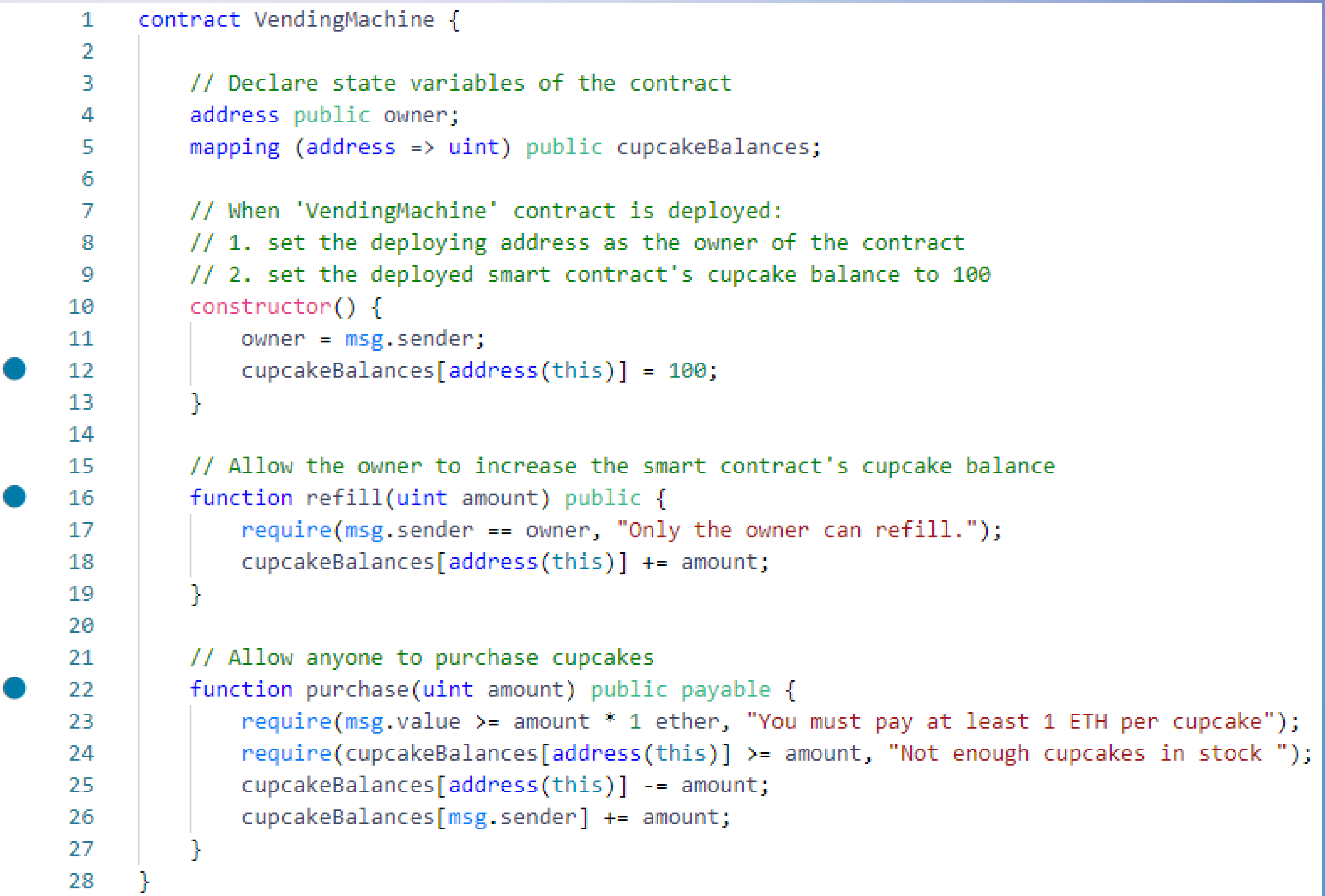
Source: https://www.nicepng.com/ourpic/u2w7y3t4w7a9e6i1_smart-contracts-in-insurance-policies-history-of-smart/

Smart Contract in Real Life Example



Vending Machine Analogy

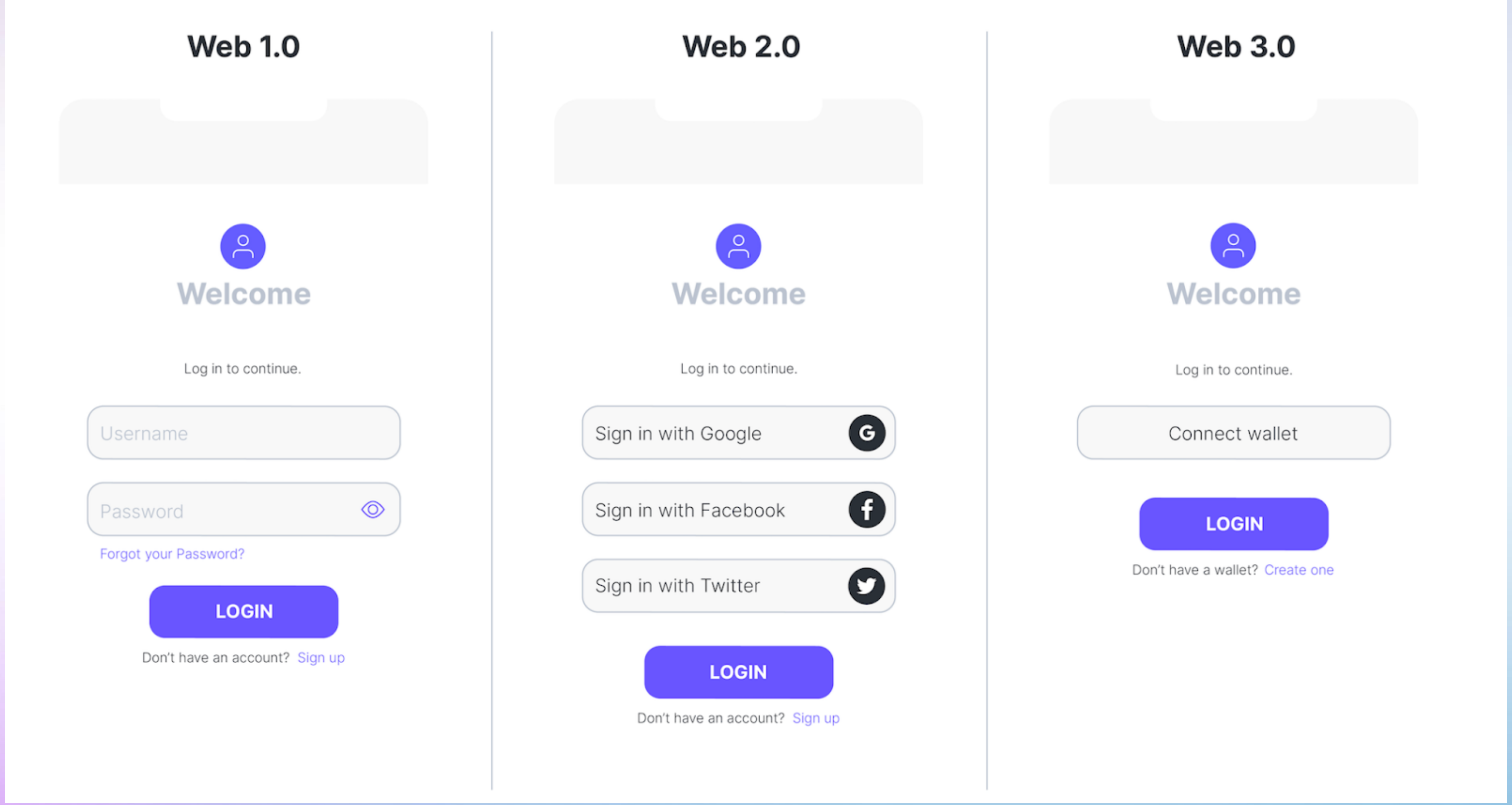
A vending machine takes in acceptable coins and allows certain tasks to be selected by its users. It then executes the program it is tasked with, which is to give the corresponding and any necessary change



```
contract VendingMachine {

    // Declare state variables of the contract
    address public owner;
    mapping (address => uint) public cupcakeBalances;

    // When 'VendingMachine' contract is deployed:
    // 1. set the deploying address as the owner of the contract
    // 2. set the deployed smart contract's cupcake balance to 100
    constructor() {
        owner = msg.sender;
        cupcakeBalances[address(this)] = 100;
    }

    // Allow the owner to increase the smart contract's cupcake balance
    function refill(uint amount) public {
        require(msg.sender == owner, "Only the owner can refill.");
        cupcakeBalances[address(this)] += amount;
    }

    // Allow anyone to purchase cupcakes
    function purchase(uint amount) public payable {
        require(msg.value >= amount * 1 ether, "You must pay at least 1 ETH per cupcake");
        require(cupcakeBalances[address(this)] >= amount, "Not enough cupcakes in stock ");
        cupcakeBalances[address(this)] -= amount;
        cupcakeBalances[msg.sender] += amount;
    }
}
```

Source: https://twitter.com/ETHKL1/status/1384504003434668036/photo/1
https://ethereum.org/en/developers/docs/smart-contracts/

User Identity in Web 3.0



- Crypto wallet is the only key representing your identity and to access what you own in Web 3.0

- Crypto wallet contains private key which is stored in Wallet Apps (Hot wallet) or dedicated hardware (Cold wallet)

Source: https://auth0.com/blog/identity-and-web3/

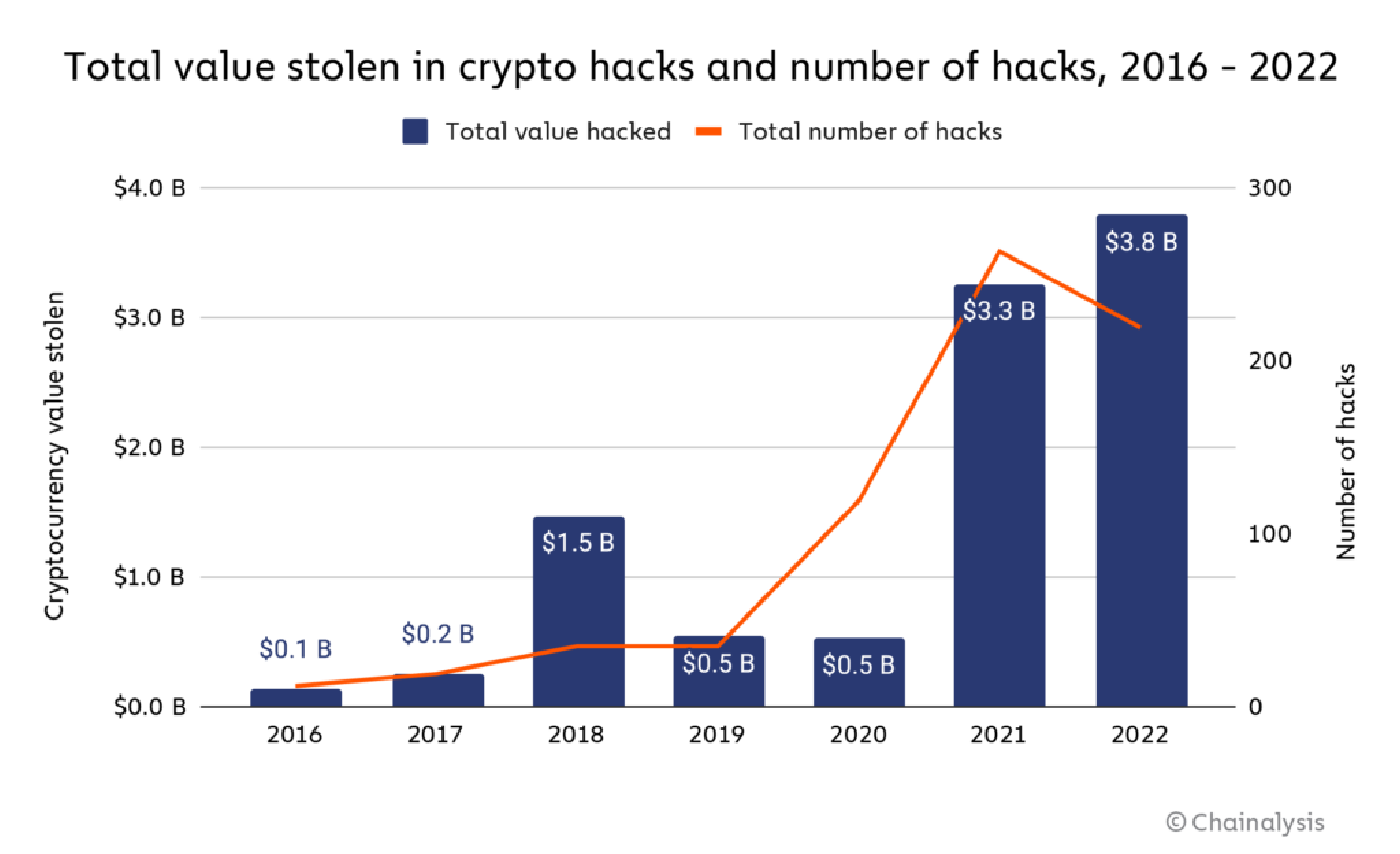
Quick Summary on Web 3.0

- Built on blockchain technology
- Decentralized rather than centralized authorities.
- Smart Contract is a program triggered automatically when it meets certain condition in the blockchain
- Users authenticate by crypto wallet
- Ownership of digital asset can be stored and verified in blockchain
  (e.g. Cryptocurrency, NFT, digital asset in metaverse)

2 Cyber Attacks in Web 3.0

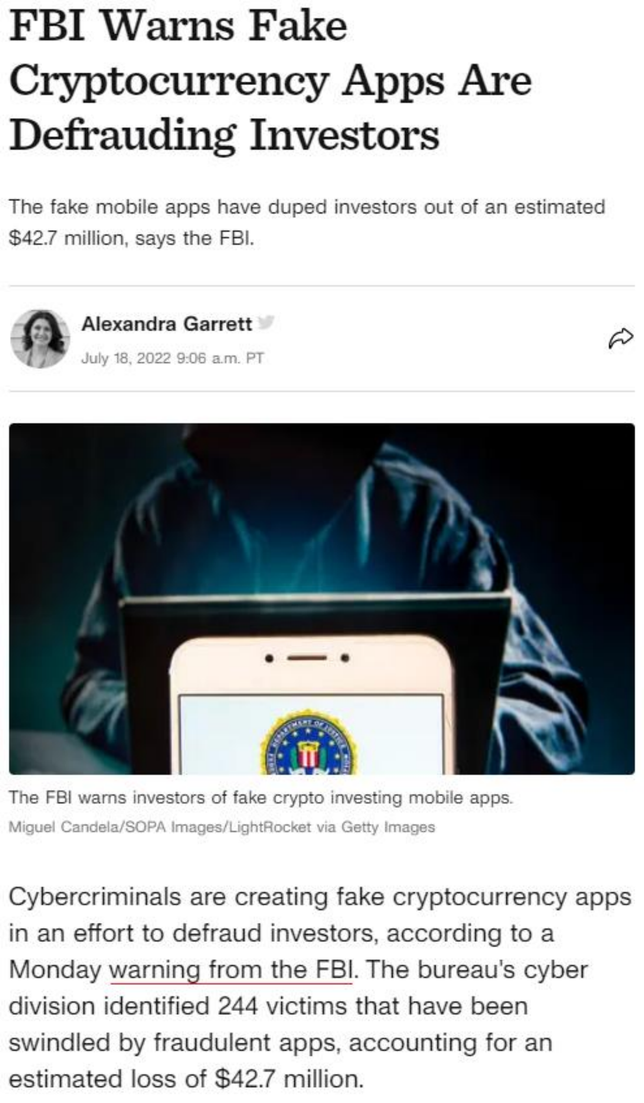
HKCERT

Statistics on Crypto Hacks



Source: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

Attacks on Crypto Wallet: Fake or Fraudulent Apps



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.

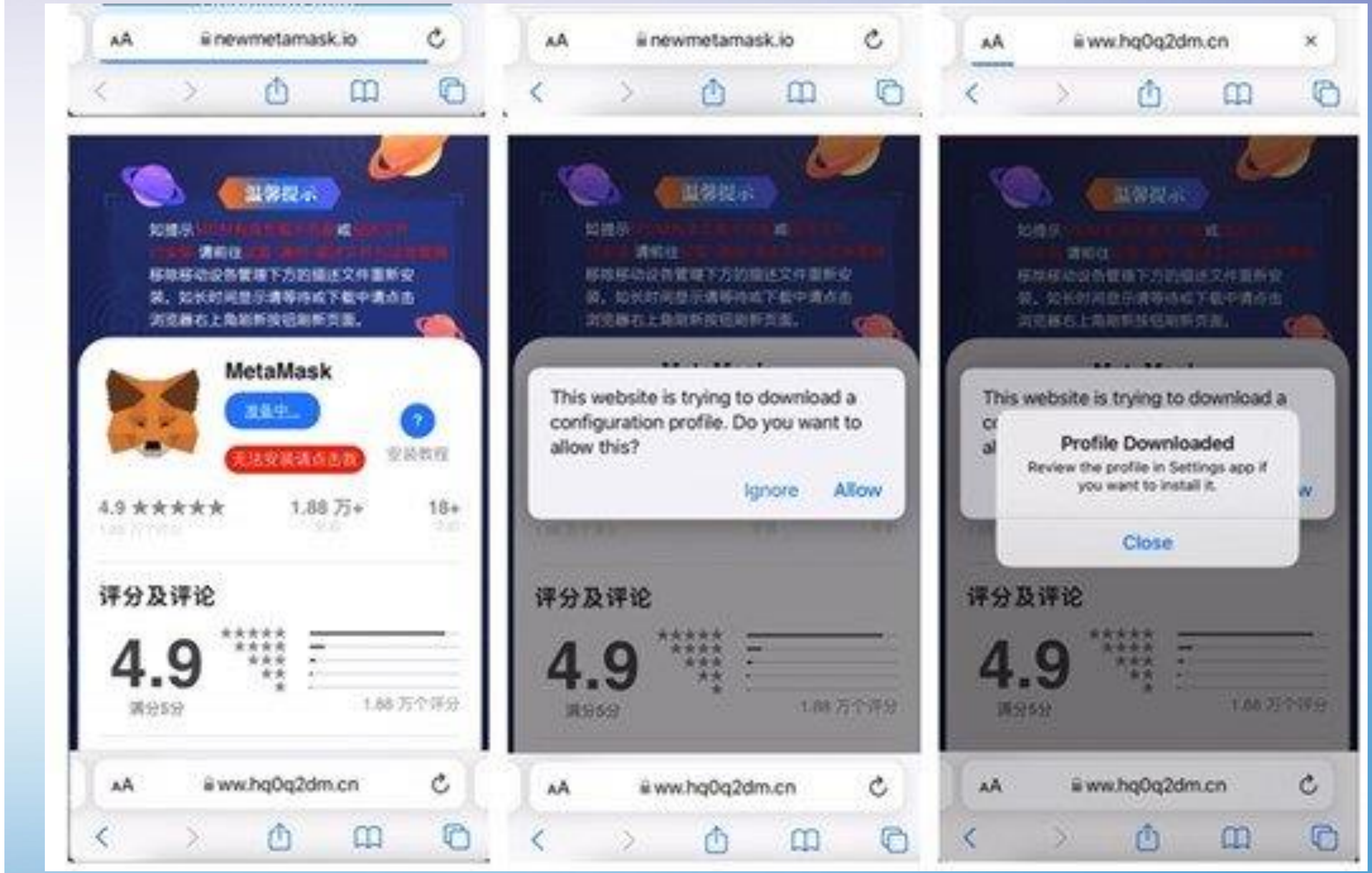
Alexandra Garrett

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.



如提示 [illegible] 或 [illegible] 请前往 [illegible] 移除移动设备管理下方的描述文件重新安装。如长时间显示请等待或下载中请点击浏览器右上角刷新按钮刷新页面。

This website is trying to download a configuration profile. Do you want to allow this?

Ignore Allow

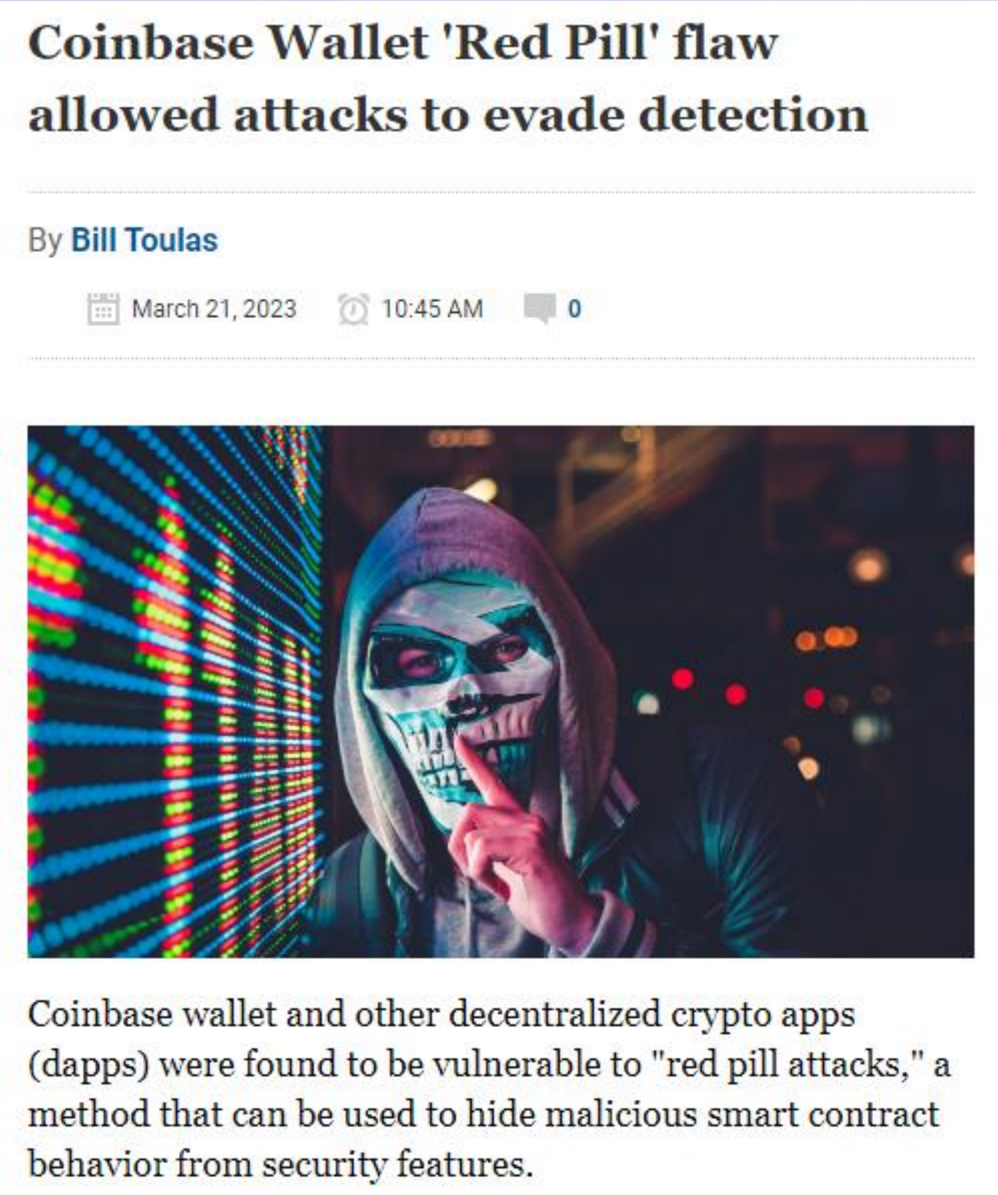
Profile Downloaded

Review the profile in Settings app if you want to install it.

Close

Source: https://www.cnet.com/personal-finance/crypto/fbi-warns-fake-cryptocurrency-apps-are-defrauding-investors/

Attacks on Crypto Wallet: Vulnerability in Wallet Apps



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

By Bill Toulas

March 21, 2023 10:45 AM 0

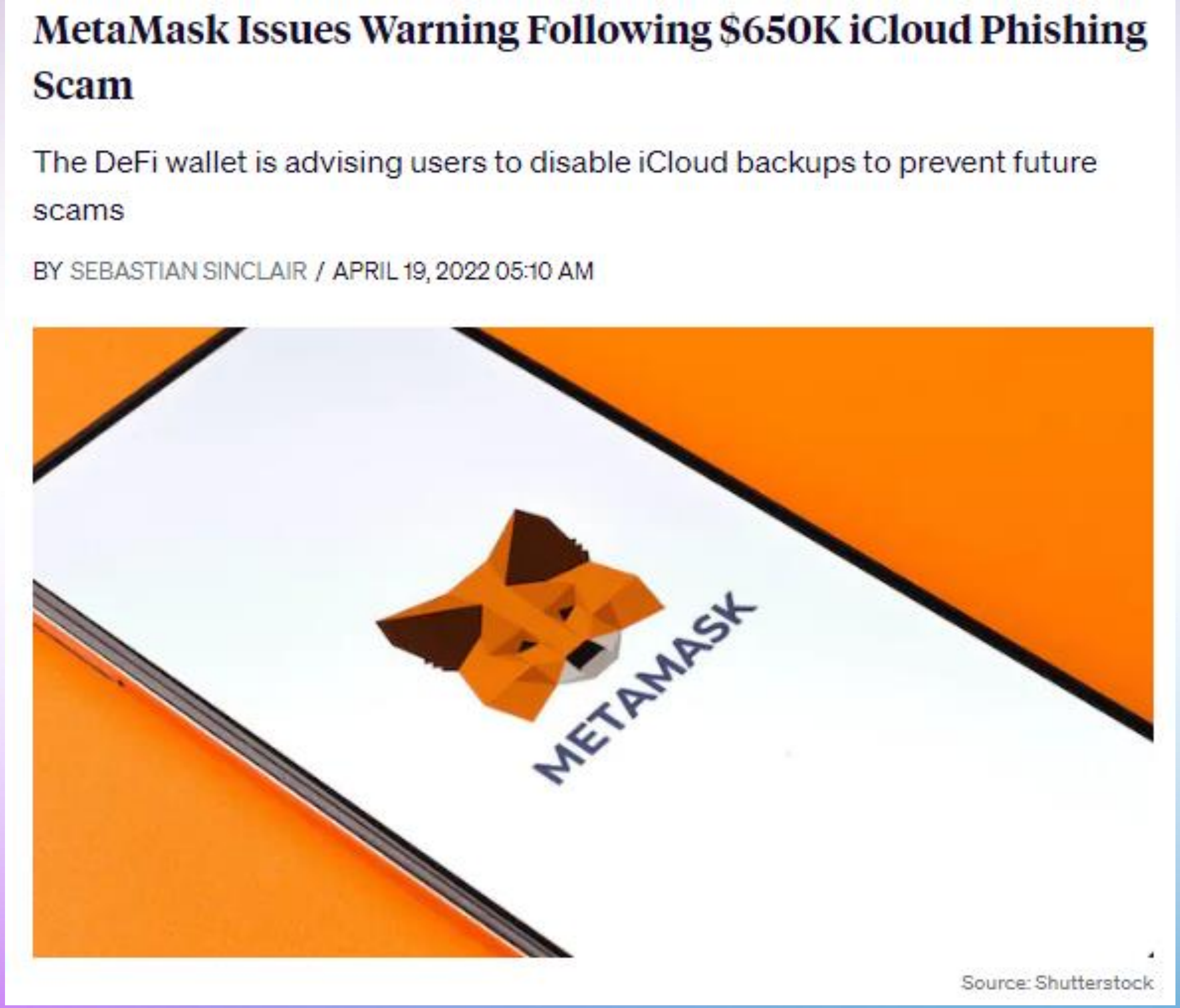
Coinbase wallet and other decentralized crypto apps (dapps) were found to be vulnerable to "red pill attacks," a method that can be used to hide malicious smart contract behavior from security features.

"…vulnerable to a new attack that allows smart contracts to hide malicious behavior during transaction simulations. "

"…This attack is conducted by filling variables in a smart contract with "safe" data during simulations and then swapping it with "malicious" data during a live transaction."

Source: https://www.bleepingcomputer.com/news/security/coinbase-wallet-red-pill-flaw-allowed-attacks-to-evade-detection/

Attacks on Crypto Wallet: Phishing Attack



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

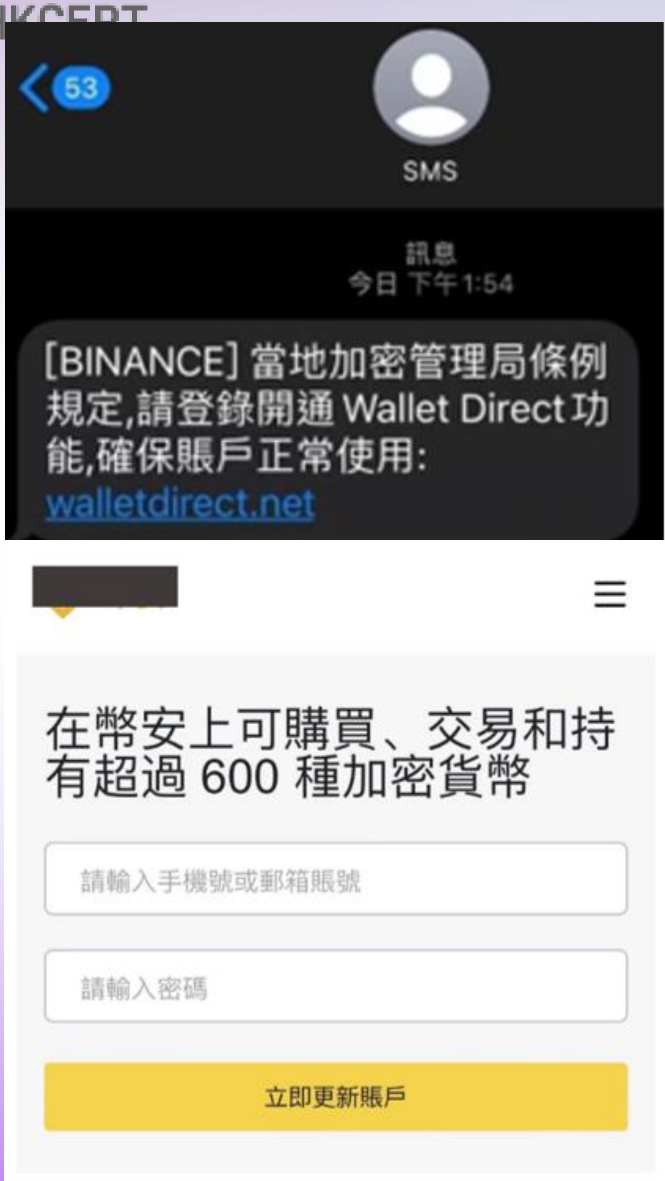
Source: Shutterstock

"The DeFi wallet provider said Sunday users who have iCloud enabled for iPhone application data were susceptible to hackers because the backups include their password-encrypted MetaMask vault."

"If your password isn't strong enough and someone phishes your iCloud credentials, this can mean stolen funds," MetaMask tweeted.

Source: https://blockworks.co/news/metamask-issues-warning-following-icloud-phishing-scam

Other Forms of Attacks on Crypto Wallet



訊息
今日 下午1:54

[BINANCE] 當地加密管理局條例規定,請登錄開通 Wallet Direct功能,確保賬戶正常使用: walletdirect.net

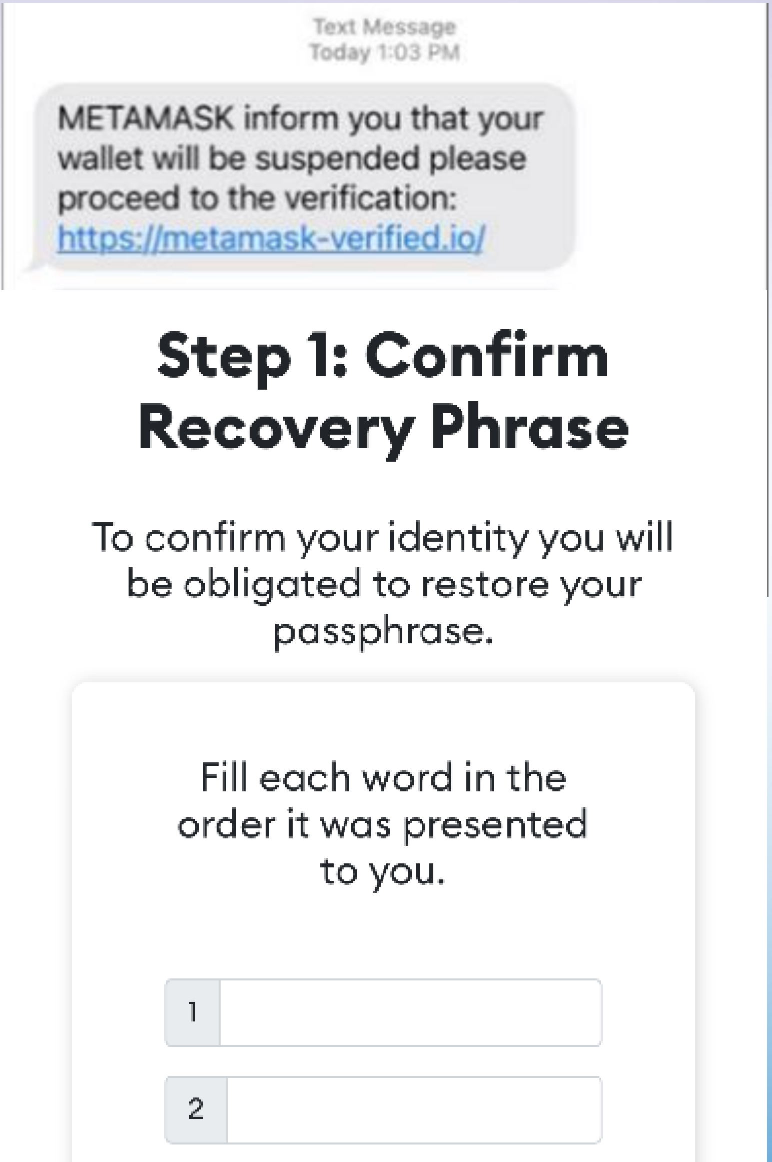
[redacted]

在幣安上可購買、交易和持有超過 600 種加密貨幣

請輸入手機號或郵箱賬號

請輸入密碼

立即更新賬戶


Text Message
Today 1:03 PM

METAMASK inform you that your wallet will be suspended please proceed to the verification: https://metamask-verified.io/

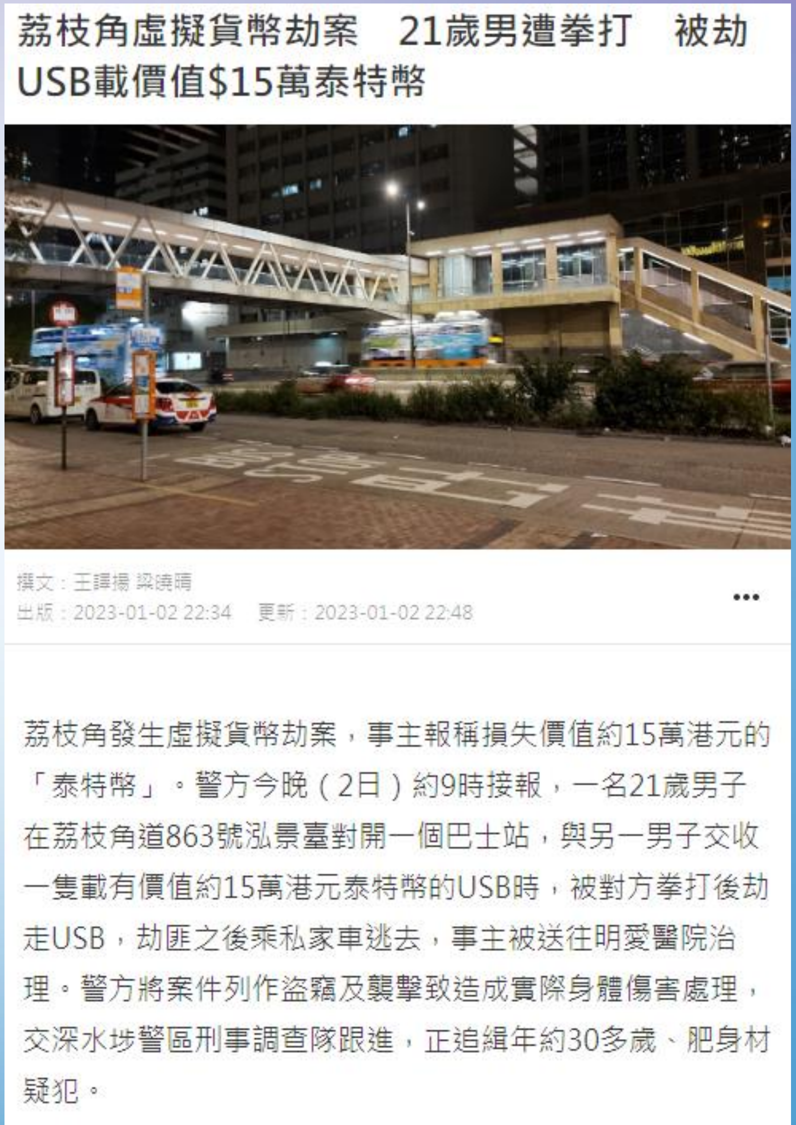
Step 1: Confirm Recovery Phrase

To confirm your identity you will be obligated to restore your passphrase.

Fill each word in the order it was presented to you.

1

2

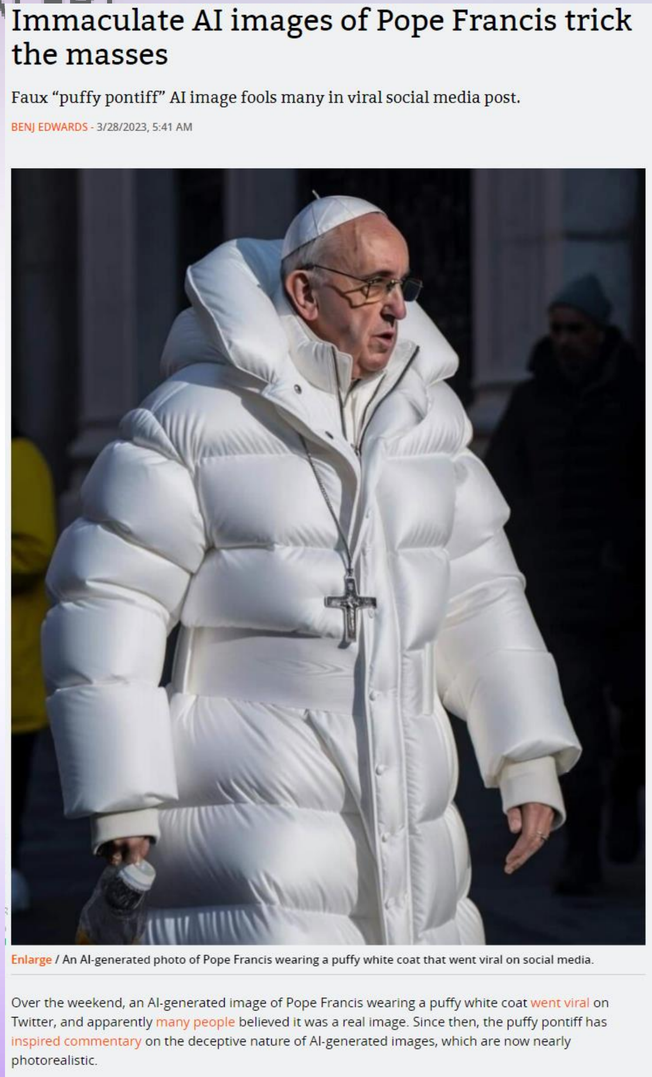

荔枝角虛擬貨幣劫案　21歲男遭拳打　被劫USB載價值$15萬泰特幣

撰文：王譯揚 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。

Source: https://www.hk01.com/%E7%AA%81%E7%99%BC/853038/%E8%8D%94%E6%9E%9D%E8%A7%92%E8%99%9B%E6%93%AC%E8%B2%A8%E5%B9%A3%E5%8A%AB%E6%A1%88-21%E6%AD%B2%E7%94%B7%E9%81%AD%E6%8B%B3%E6%89%93-%E8%A2%AB%E5%8A%ABusb%E8%BC%89%E5%83%B9%E5%80%BC-15%E8%90%AC%E6%B3%B0%E7%89%B9%E5%B9%A3

AI Assisted Cyber Attacks on the Rise



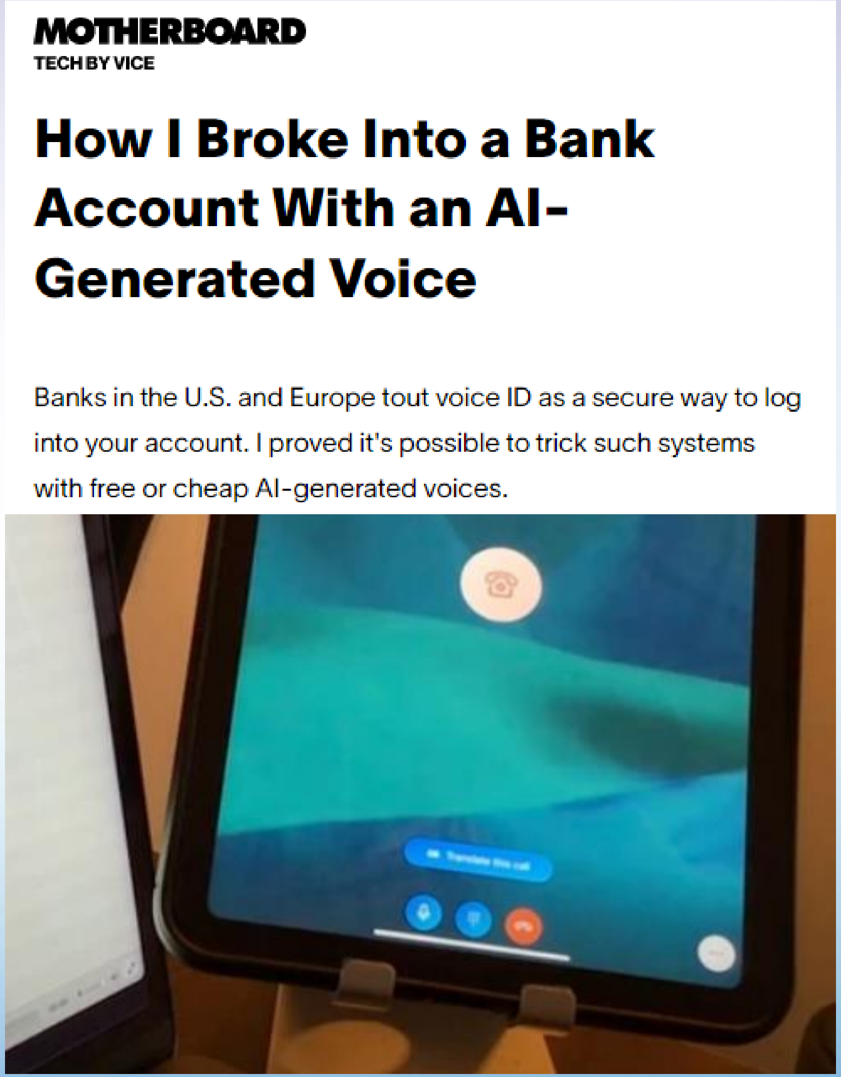
Immaculate AI images of Pope Francis trick the masses

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.

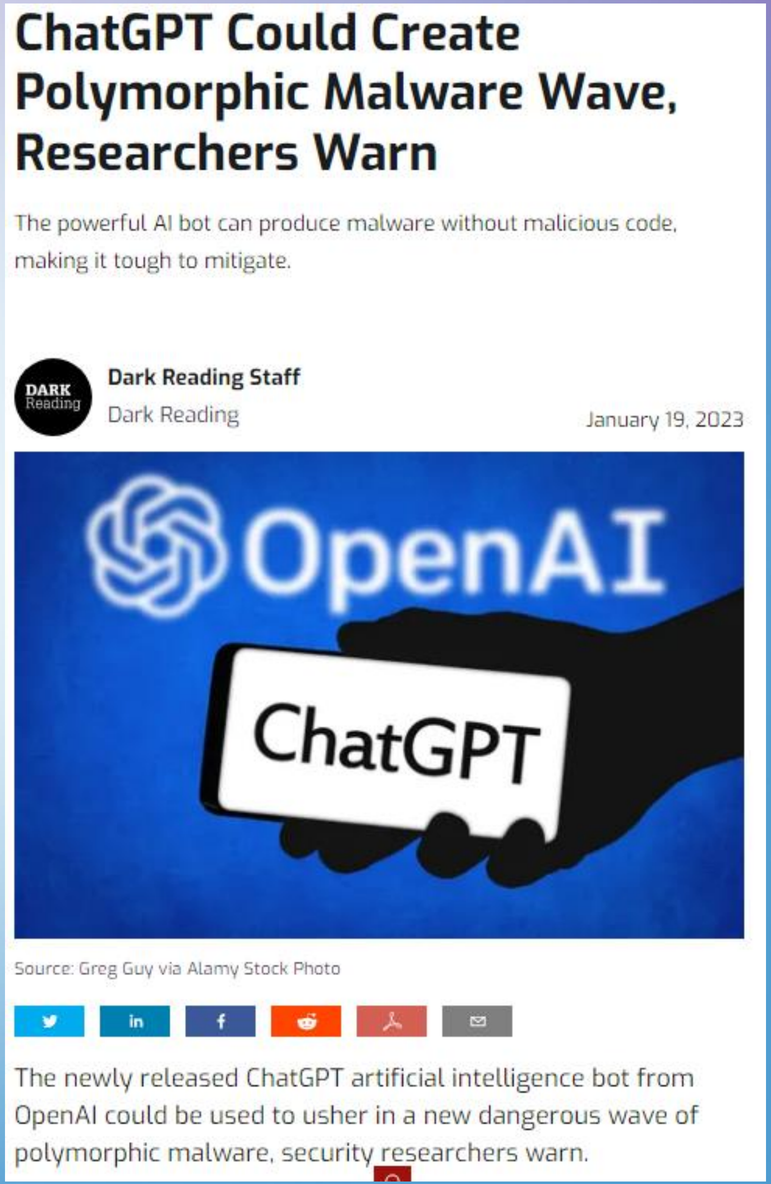
Over the weekend, an AI-generated image of Pope Francis wearing a puffy white coat went viral on Twitter, and apparently many people believed it was a real image. Since then, the puffy pontiff has inspired commentary on the deceptive nature of AI-generated images, which are now nearly photorealistic.



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

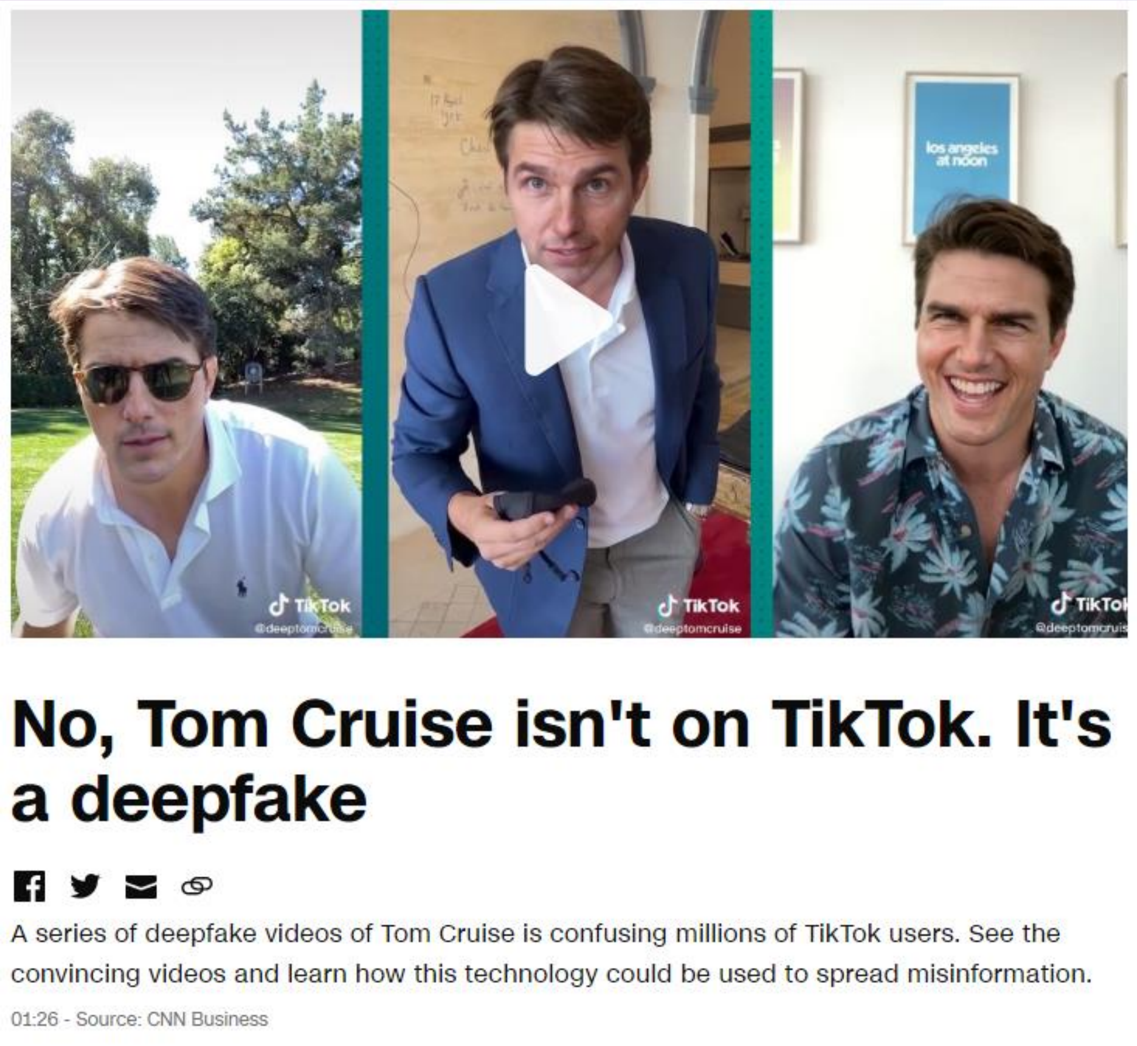
January 19, 2023

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.

Source: https://www.vice.com/en/article/dy7axa/how-i-broke-into-a-bank-account-with-an-ai-generated-voice
https://www.darkreading.com/threat-intelligence/chatgpt-could-create-polymorphic-malware-researchers-warn
https://arstechnica.com/information-technology/2023/03/the-power-of-ai-compels-you-to-believe-this-fake-image-of-pope-in-a-puffy-coat/

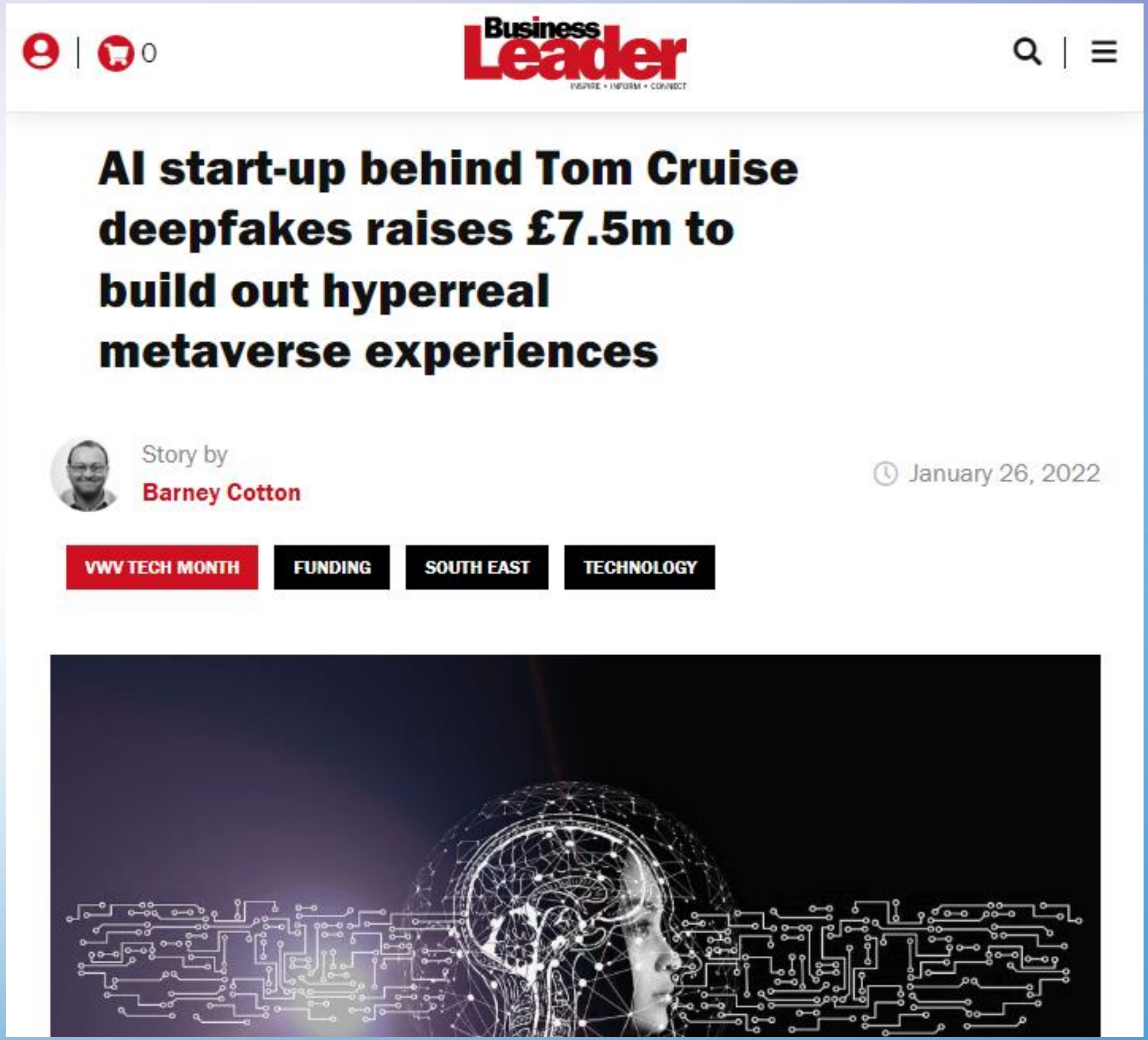
AI Assisted Cyber Attacks on the Rise



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



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

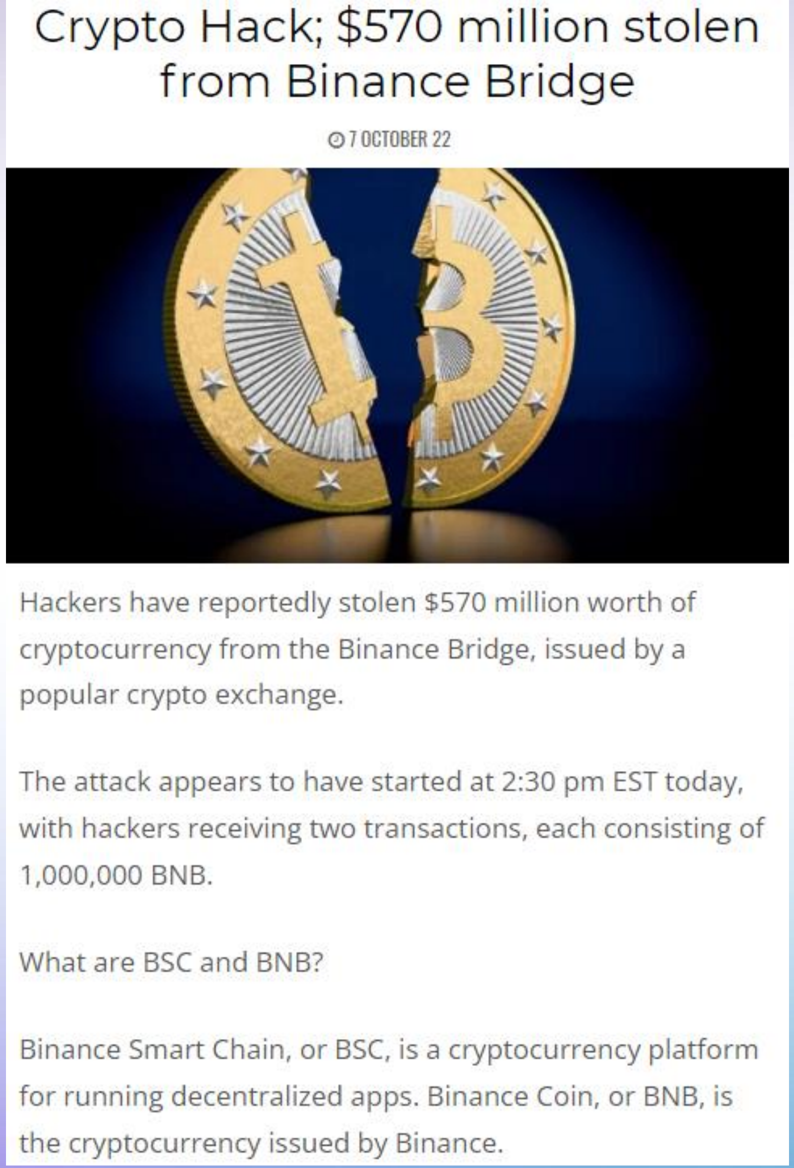
Story by
Barney Cotton

January 26, 2022

VWV TECH MONTH | FUNDING | SOUTH EAST | TECHNOLOGY

Source: https://edition.cnn.com/videos/business/2021/03/02/tom-cruise-tiktok-deepfake-orig.cnn-business
https://www.businessleader.co.uk/ai-start-up-behind-tom-cruise-deepfakes-raises-7-5m-to-build-out-hyperreal-metaverse-experiences/

Exploiting Vulnerabilities in Blockchain Bridge: 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?

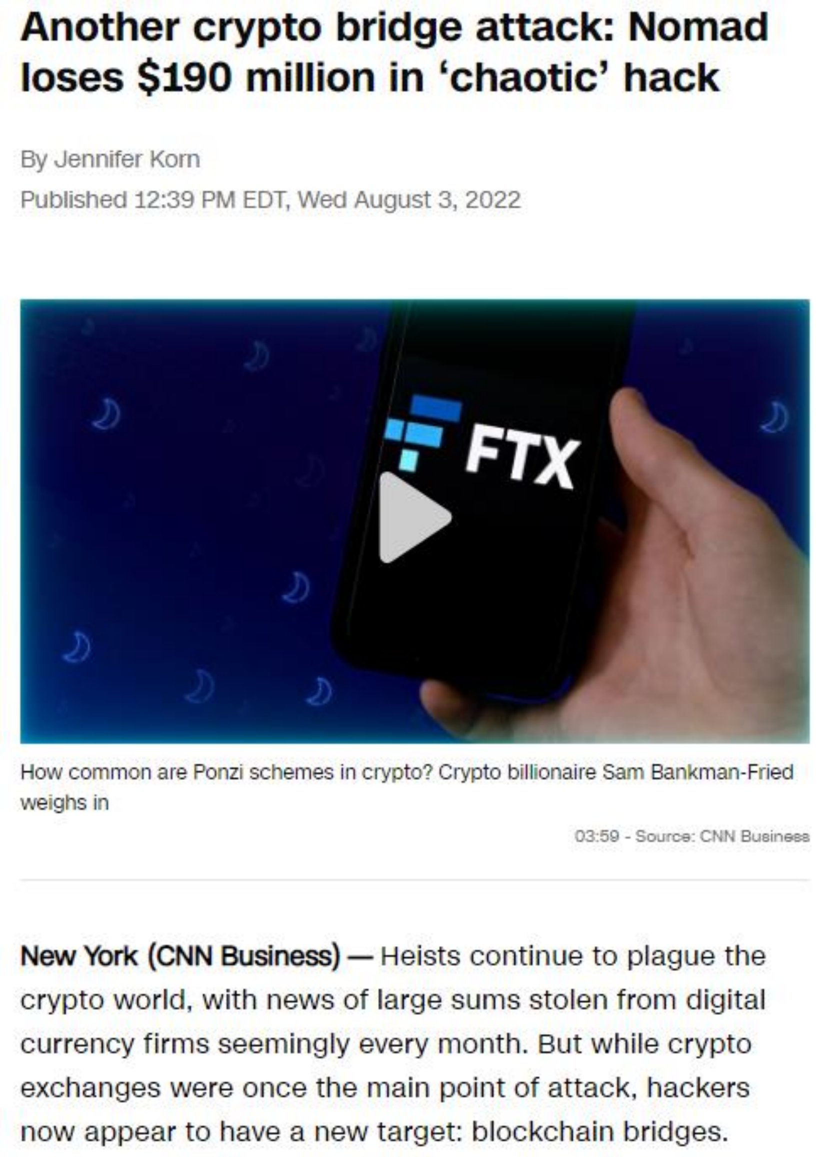
Binance Smart Chain, or BSC, is a cryptocurrency platform for running decentralized apps. Binance Coin, or BNB, is the cryptocurrency issued by Binance.

"According to samczsun's analysis, the attacker leveraged a bug in the BSC Token Hub to forge arbitrary, allowing them to mint (create) BNB coins out of thin air."

"An exploit on a cross-chain bridge, BSC Token Hub, resulted in extra BNB. We have asked all validators to suspend BSC temporarily. The issue is contained now. Your funds are safe. We apologize for the inconvenience and will provide further updates accordingly"

Source: https://securereading.com/crypto-hack-570-million-stolen-from-binance-bridge/

Exploiting Vulnerabilities in Blockchain Bridge: Nomad



Another crypto bridge attack: Nomad loses $190 million in 'chaotic' hack

By Jennifer Korn

Published 12:39 PM EDT, Wed August 3, 2022

How common are Ponzi schemes in crypto? Crypto billionaire Sam Bankman-Fried weighs in

03:59 - Source: CNN Business

New York (CNN Business) — Heists continue to plague the crypto world, with news of large sums stolen from digital currency firms seemingly every month. But while crypto exchanges were once the main point of attack, hackers now appear to have a new target: blockchain bridges.

"…However, the transactions to the bridge only called the process() within Replica.sol without proving validity."

"In an upgrade to the protocol, Nomad decided to initialize the value of trusted roots to 0x00. While this is common practice, it also matches the value for an untrusted root, so all messages are automatically viewed as proven."

"This exploit demonstrates the importance of performing a comprehensive security audit on smart contract code before deployment."

Source: https://securereading.com/crypto-hack-570-million-stolen-from-binance-bridge/
https://www.halborn.com/blog/post/explained-the-nomad-hack-august-2022

HKCERT

3 Security Advice

Security Advice on Crypto Wallet

HKCERT Hong Kong Computer Emergency Response Team Coordination Centre 香港電腦保安事故協調中心

Home > Publications > Security Blog

NFT Boom, How to Protect Your NFT Assets

Release Date: 24 Jan 2022 | 12371 Views

- Wallet Apps
  - Back up your wallet and set a password for protection
  - Never disclose the recovery phrase to others
  - Enable multi-factor authentication
  - Enable asset transfer whitelist
  - Verify carefully the content before signing or authorising all transections
  - Keep software up-to-date
  - Use of Cold Wallet for maximum security
- Platform Managed Wallet Account
  - Enable Multi-factor Authentication
  - Enable asset transfer whitelist
  - Beware of phishing attack

https://www.hkcert.org/blog/nft-boom-how-to-protect-your-nft-assets

Security Advice on AI Assisted Social Engineering Attacks

- Adopt a Zero-Trust Concept – Verify Everything

- Verify the sender’s identity and the information by another channel (e.g. Official website announcement, customer service hotline)

- Do not open unknown files, web pages and emails

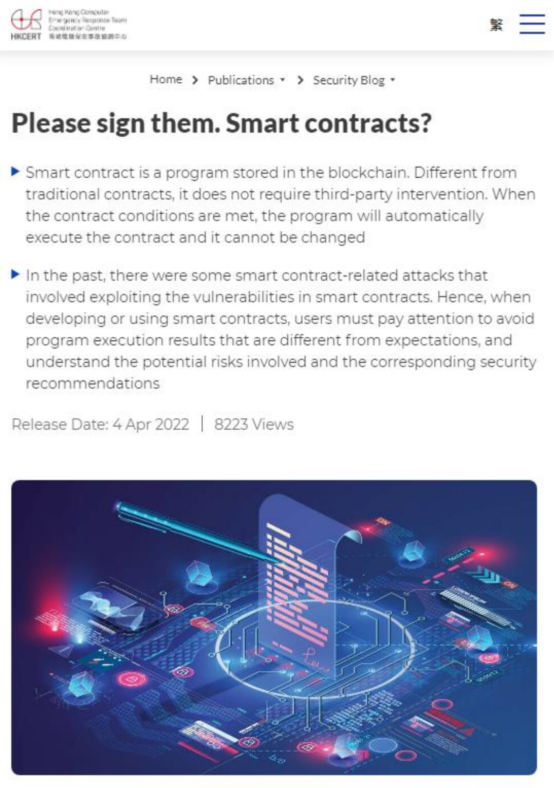
- Use the “Scameter” of Cyberdefender.hk to identify frauds and online pitfalls through email, URL or IP address, etc.

- Think twice before providing personal or sensitive information

- Be cautions of social engineering tactics (e.g. appeal to urgency, threatening, authority, etc.)

https://cyberdefender.hk/en-us/scameter/

Security Advice on Smart Contracts


Hong Kong Computer Emergency Response Team Coordination Centre
HKCERT 香港電腦保安事故協調中心
繁
Home > Publications > Security Blog

Please sign them. Smart contracts?

- Smart contract is a program stored in the blockchain. Different from traditional contracts, it does not require third-party intervention. When the contract conditions are met, the program will automatically execute the contract and it cannot be changed
- In the past, there were some smart contract-related attacks that involved exploiting the vulnerabilities in smart contracts. Hence, when developing or using smart contracts, users must pay attention to avoid program execution results that are different from expectations, and understand the potential risks involved and the corresponding security recommendations

Release Date: 4 Apr 2022 | 8223 Views

- Review before signing a smart contract
- Use the official smart contracts on the trading platform or marketplace for transactions
- After the transaction, verify the correctness of the crypto asset immediately
- Refer to the industry best practice guidelines to avoid common attack methods, such as reentrancy, denial of service attacks
- Conduct security assessment or auditing against smart contracts to examine the code for security issues.

https://www.hkcert.org/blog/please-sign-them-smart-contracts

HKCERT

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