



Cyber Security New Challenges in Web 3.0

Lawrence Law | Security Consultant, HKCERT





Agenda

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



International

Local

Exchange Incidents
and Information

HKCERT as a Hub

Coordinate incidents
and publish alerts

Global
Researchers



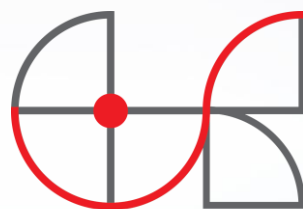
Global CERT Forum

APNIC

DOT ASIA
ORGANISATION



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

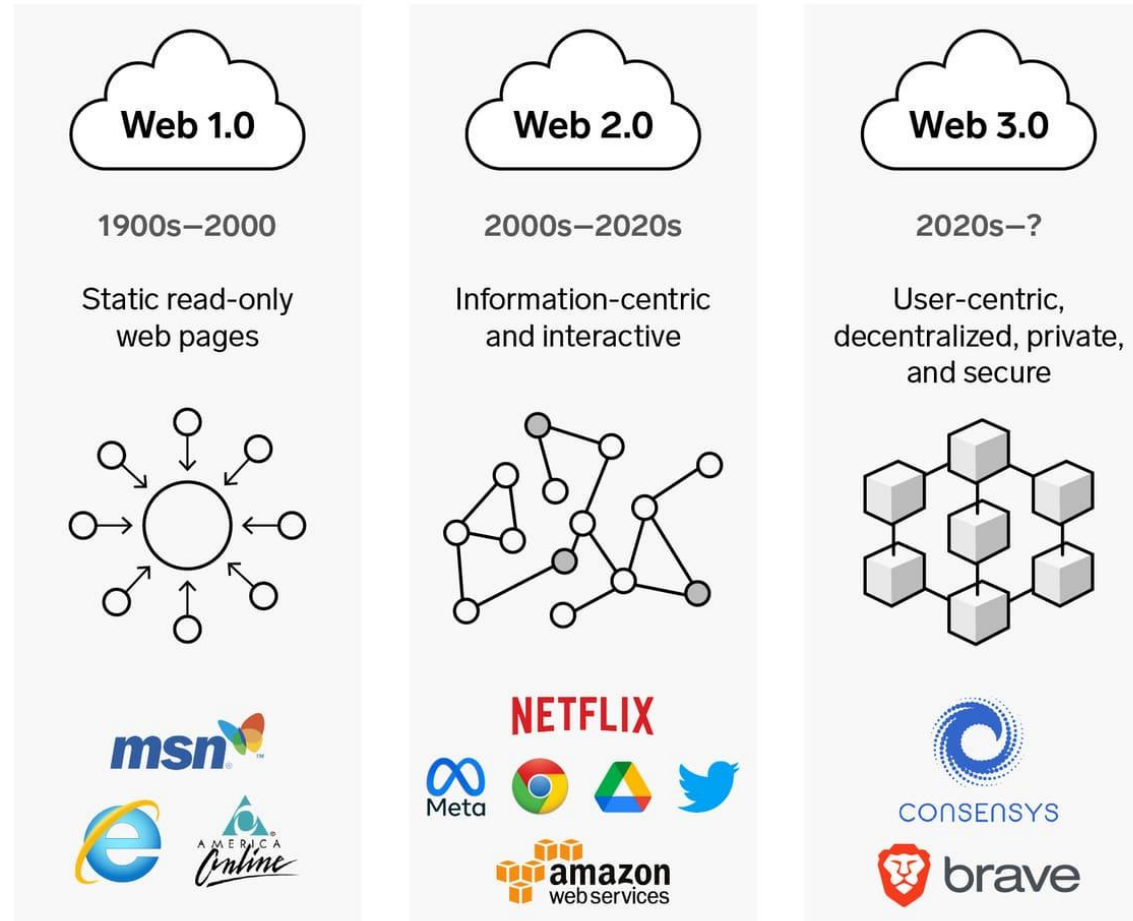
- Offer Best Practice and Guideline
- Provide Online Cyber Security Self-Assessment Tool

2






















What is Web 3.0?

Key Differences in Web 3.0

Evolution of the web from 1.0 to 3.0

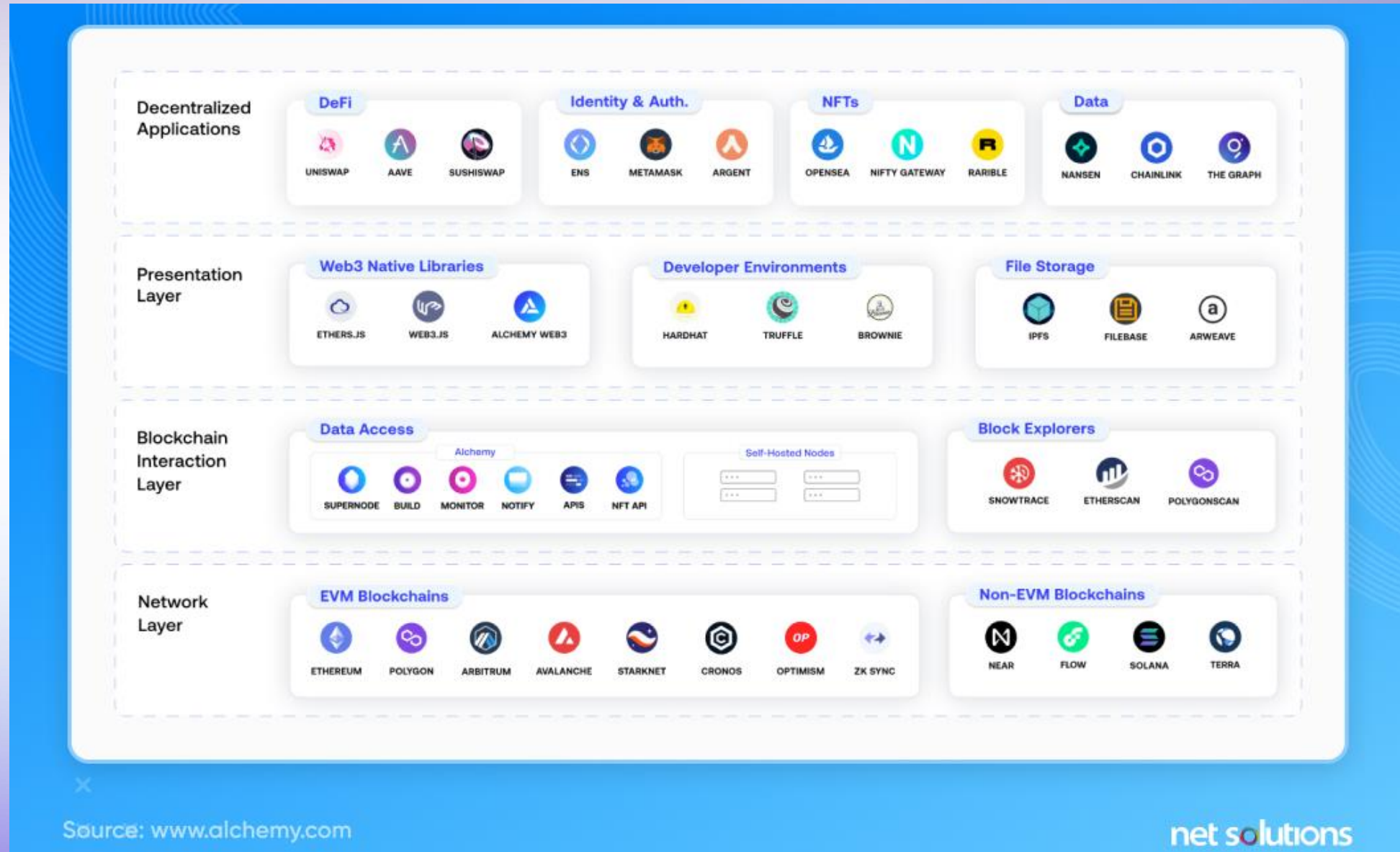


Example of Apps Leveraging Web 3.0 Technology

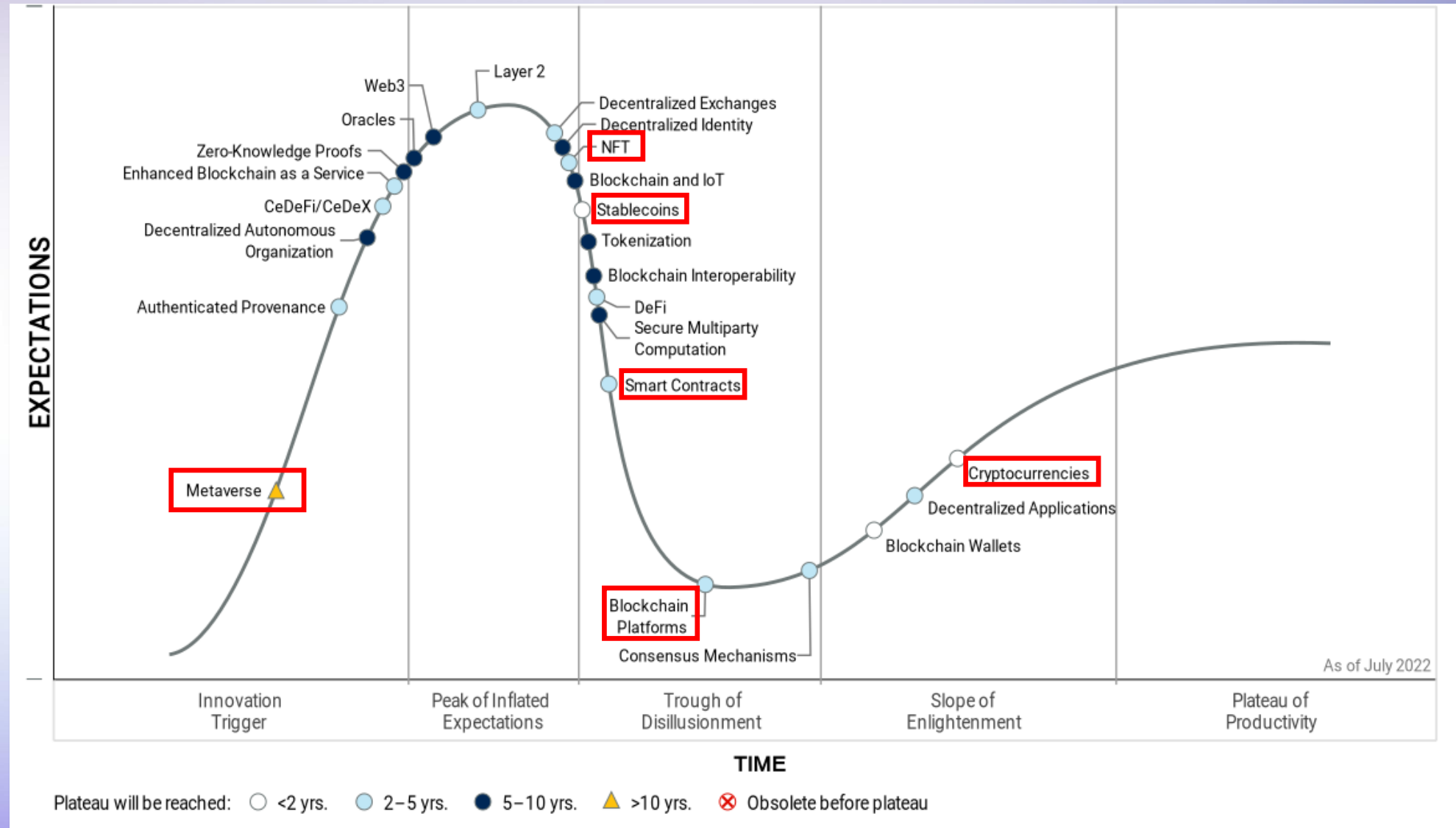
Emergence of apps based on blockchain		
	Web 2.0 apps	Web 3.0 apps (powered by blockchain)
Browser		 brave
Storage	 	  IPFS
Video and audio calls		 EXPERTY
Operating system	 	 
Social network	 	 
Messaging	 	 status
Remote job		

Source: Convergence Catalyst Research

Technology Landscape in Web 3.0



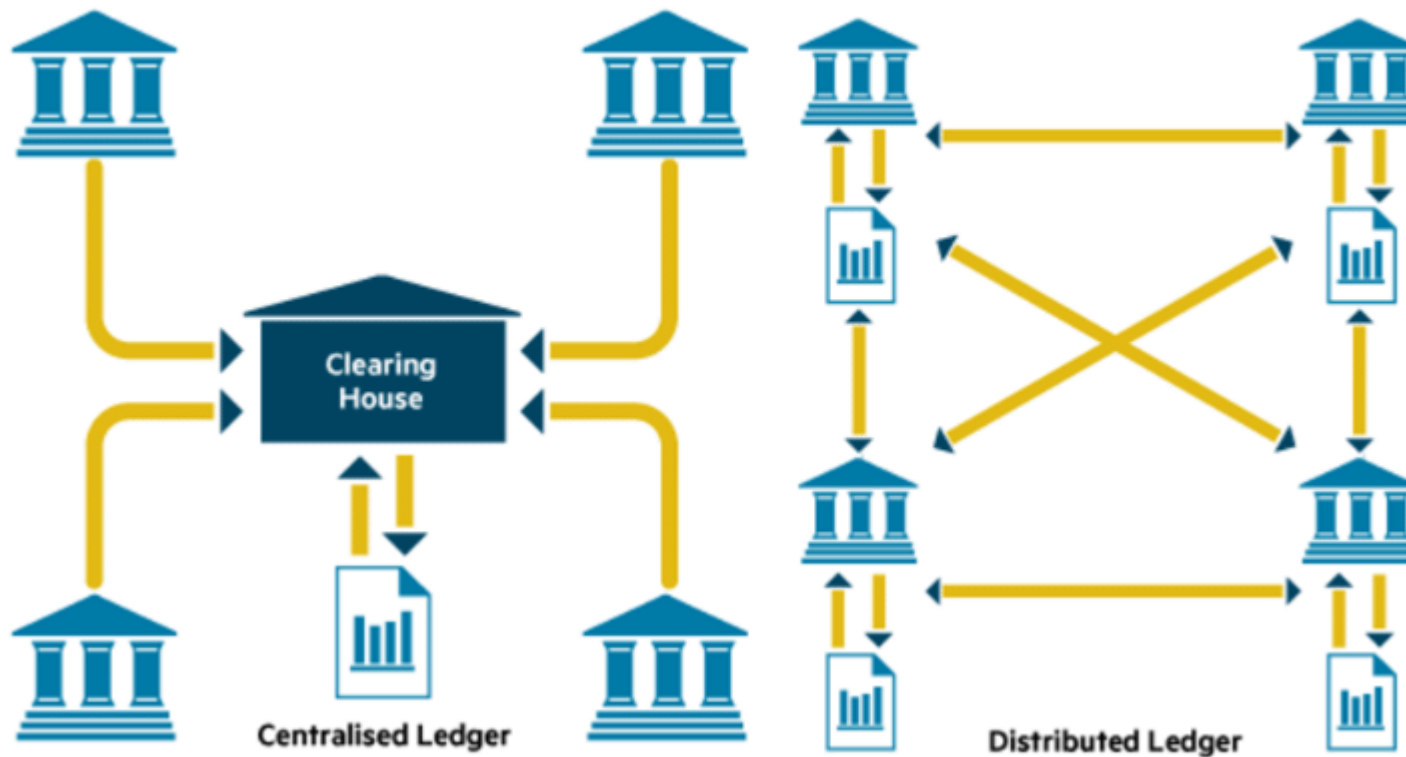
Web 3.0 Hype Cycle



The Basic Concept of Blockchain

Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



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

Example of Blockchain Use Case



Top Blockchain Platforms

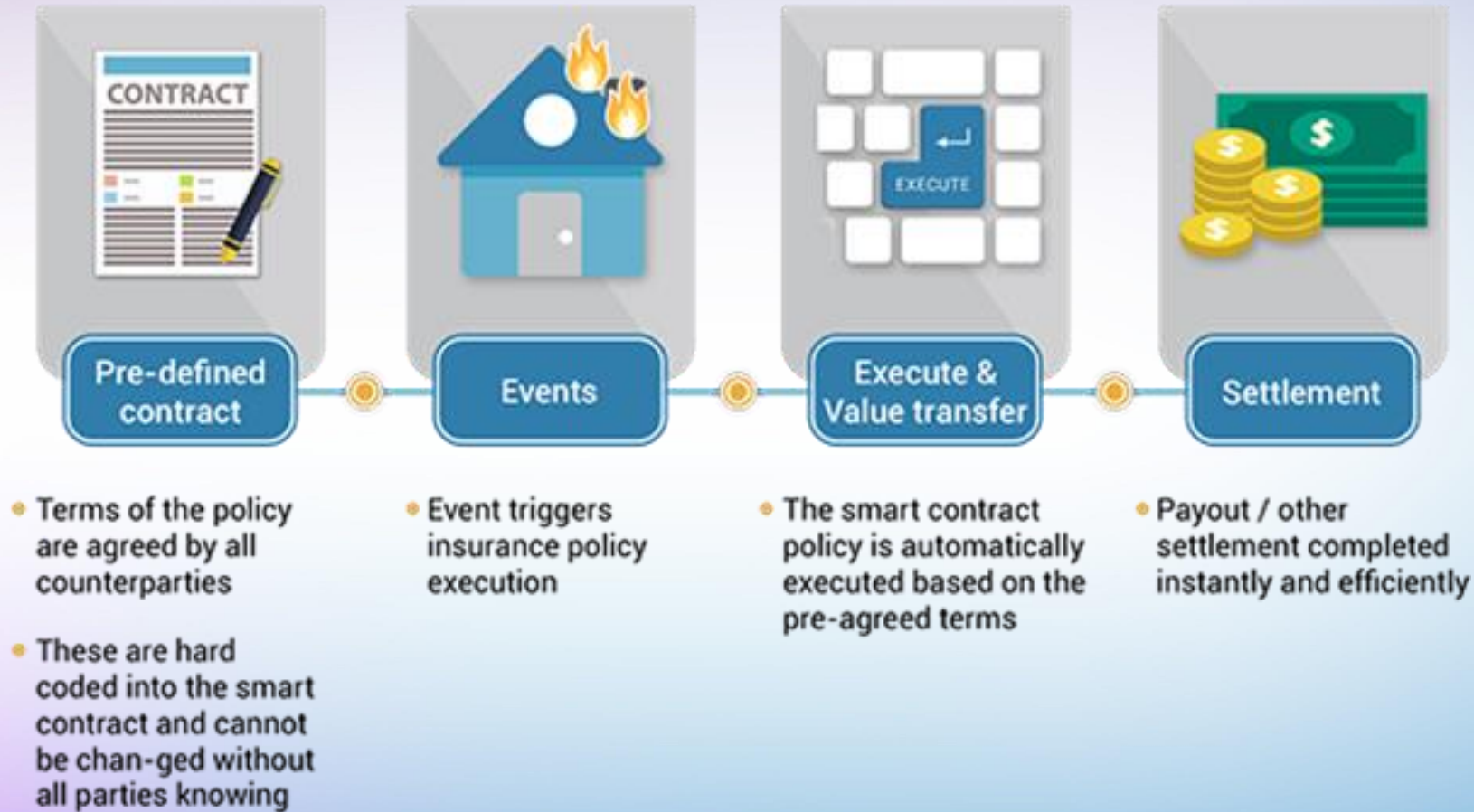


Comparison of top 10 blockchain platforms

(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

The Basic Concept of Smart Contract

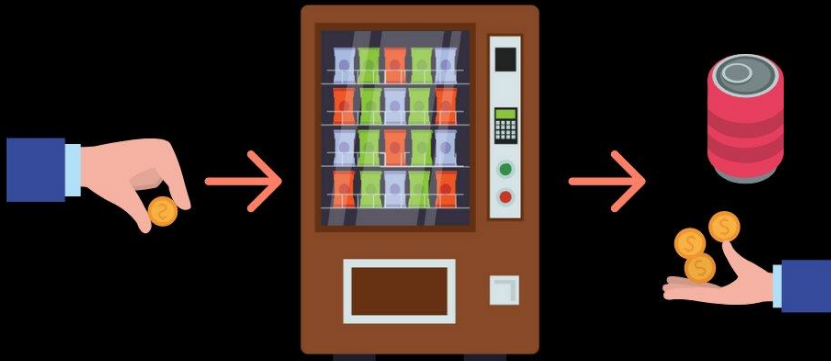


- Smart Contract simply **software programs** stored on a blockchain
- Auto triggered when **predetermined condition** are met
- Basic logic is simple **“if ..., then...”** statements

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

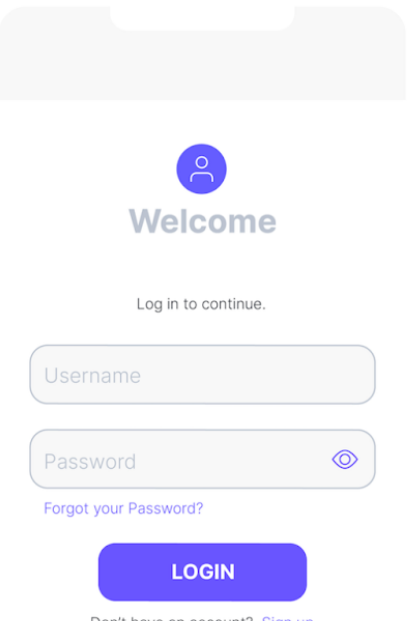
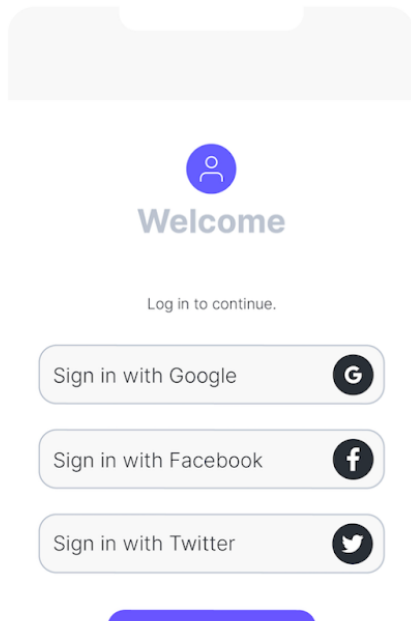
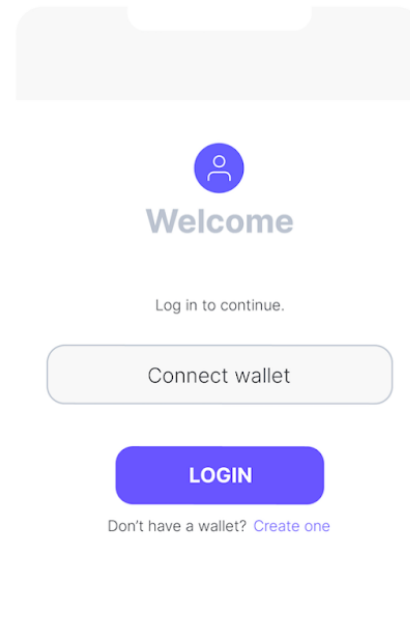


```

1  contract VendingMachine {
2
3      // Declare state variables of the contract
4      address public owner;
5      mapping (address => uint) public cupcakeBalances;
6
7      // When 'VendingMachine' contract is deployed:
8      // 1. set the deploying address as the owner of the contract
9      // 2. set the deployed smart contract's cupcake balance to 100
10     constructor() {
11         owner = msg.sender;
12         cupcakeBalances[address(this)] = 100;
13     }
14
15     // Allow the owner to increase the smart contract's cupcake balance
16     function refill(uint amount) public {
17         require(msg.sender == owner, "Only the owner can refill.");
18         cupcakeBalances[address(this)] += amount;
19     }
20
21     // Allow anyone to purchase cupcakes
22     function purchase(uint amount) public payable {
23         require(msg.value >= amount * 1 ether, "You must pay at least 1 ETH per cupcake");
24         require(cupcakeBalances[address(this)] >= amount, "Not enough cupcakes in stock ");
25         cupcakeBalances[address(this)] -= amount;
26         cupcakeBalances[msg.sender] += amount;
27     }
28 }
  
```

Predefined logic on how the application manipulates the transaction into blockchain

User Identity in Web 3.0

Web 1.0	Web 2.0	Web 3.0
 <p>Web 1.0 login form showing a 'Welcome' message, a 'Log in to continue.' prompt, and input fields for 'Username' and 'Password'. A 'LOGIN' button is present, along with a link for 'Forgot your Password?' and a 'Sign up' link for users who don't have an account.</p>	 <p>Web 2.0 login form showing a 'Welcome' message, a 'Log in to continue.' prompt, and social login options: 'Sign in with Google', 'Sign in with Facebook', and 'Sign in with Twitter'. A 'LOGIN' button is present, along with a 'Sign up' link for users who don't have an account.</p>	 <p>Web 3.0 login form showing a 'Welcome' message, a 'Log in to continue.' prompt, and a 'Connect wallet' button. A 'LOGIN' button is present, along with a link to 'Create one' for users who don't have a wallet.</p>

- Crypto wallet is the only **key** representing **your identity** and to **claim 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)

Example of Digital Asset in Web 3.0



Cryptocurrency



NFT



Virtual Real
Estate



Avatar



Game
Collectibles

Quick Summary on Web 3.0



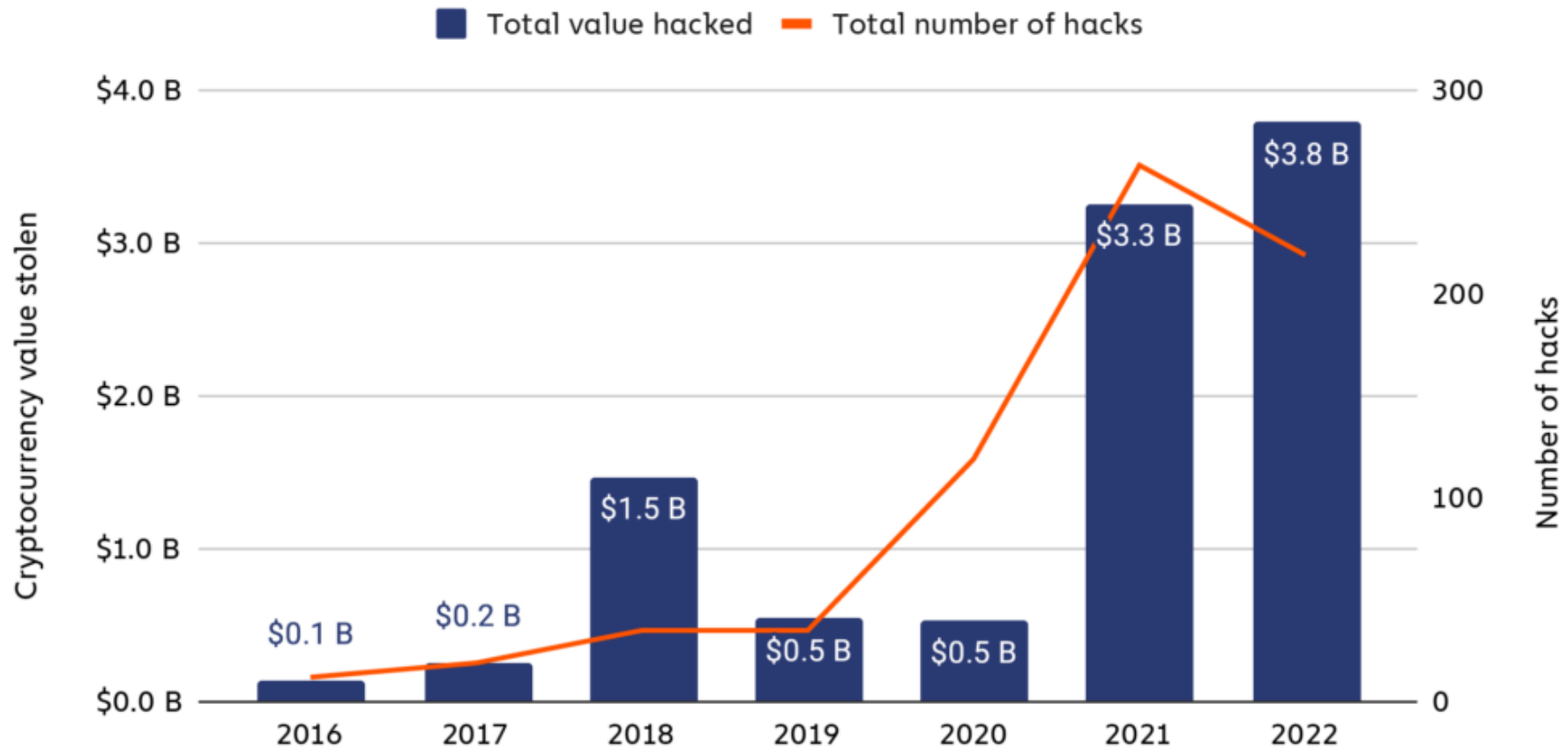
- Built on **blockchain** technology
- **Decentralized** rather than centralized authorities.
- Smart Contract is a **software program** triggered automatically when it meets certain condition in the blockchain
- Users authenticate by **crypto wallet**
- Ownership of **digital asset** can be stored and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

2

Cyber Attacks in Web 3.0

Statistics on Crypto Hacks

Total value stolen in crypto hacks and number of hacks, 2016 - 2022



© Chainalysis

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

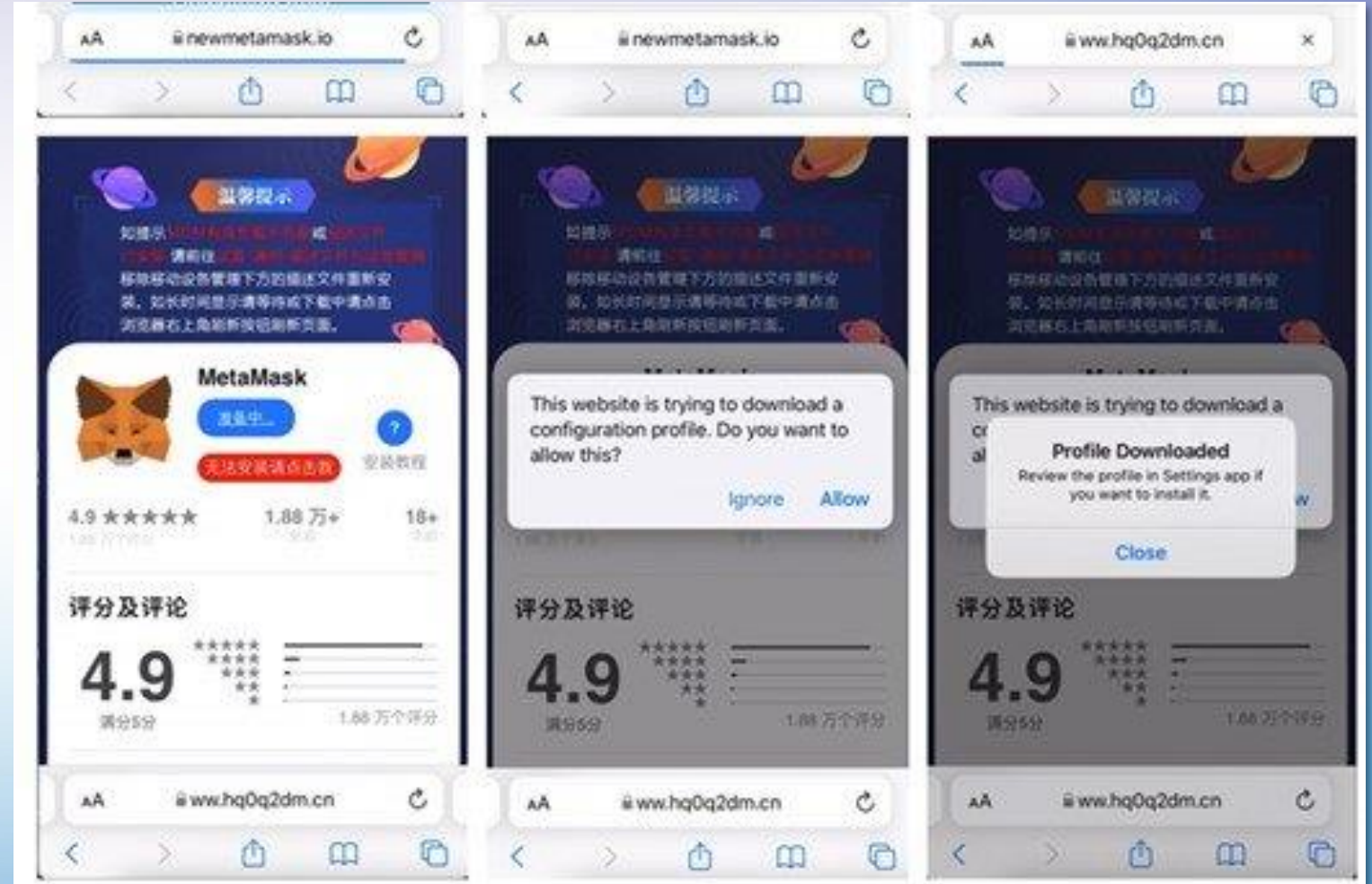
July 18, 2022 9:06 a.m. PT



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.





HKCE

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.”

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

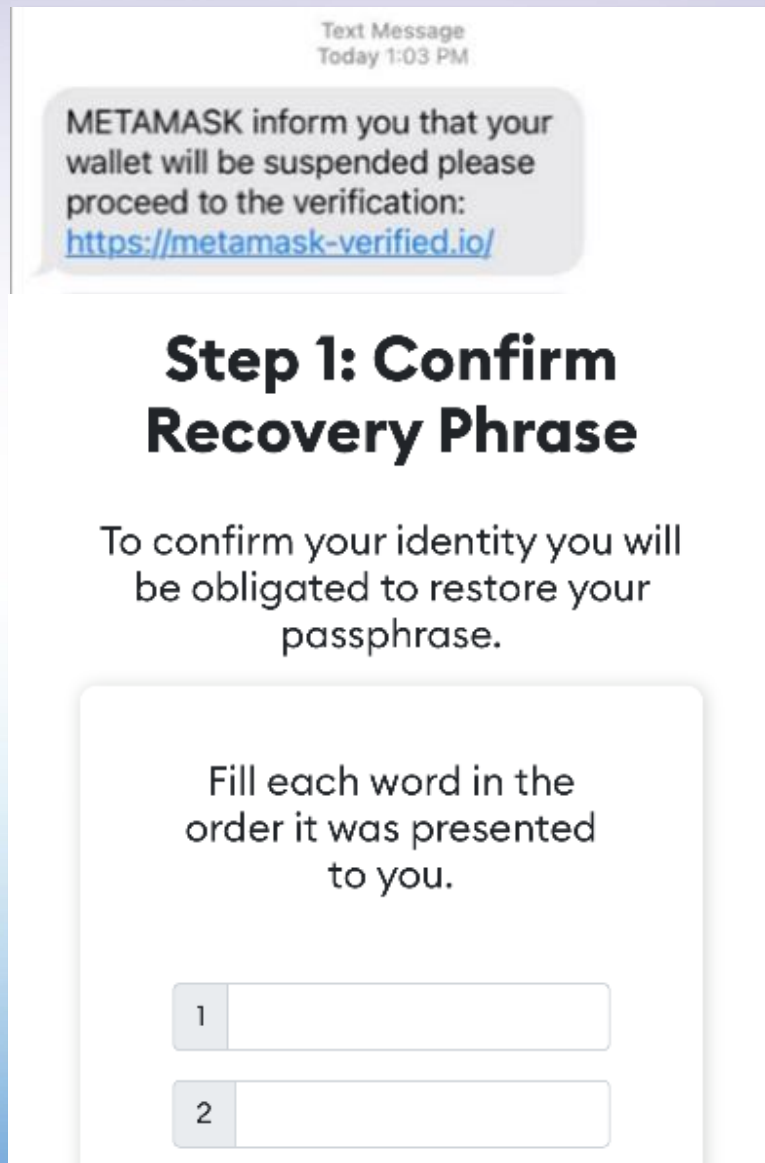


Source: Shutterstock

“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.

Other Forms of Attacks on Crypto Wallet



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。

Attacks Utilising A.I.

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.

Attacks Utilising A.I.

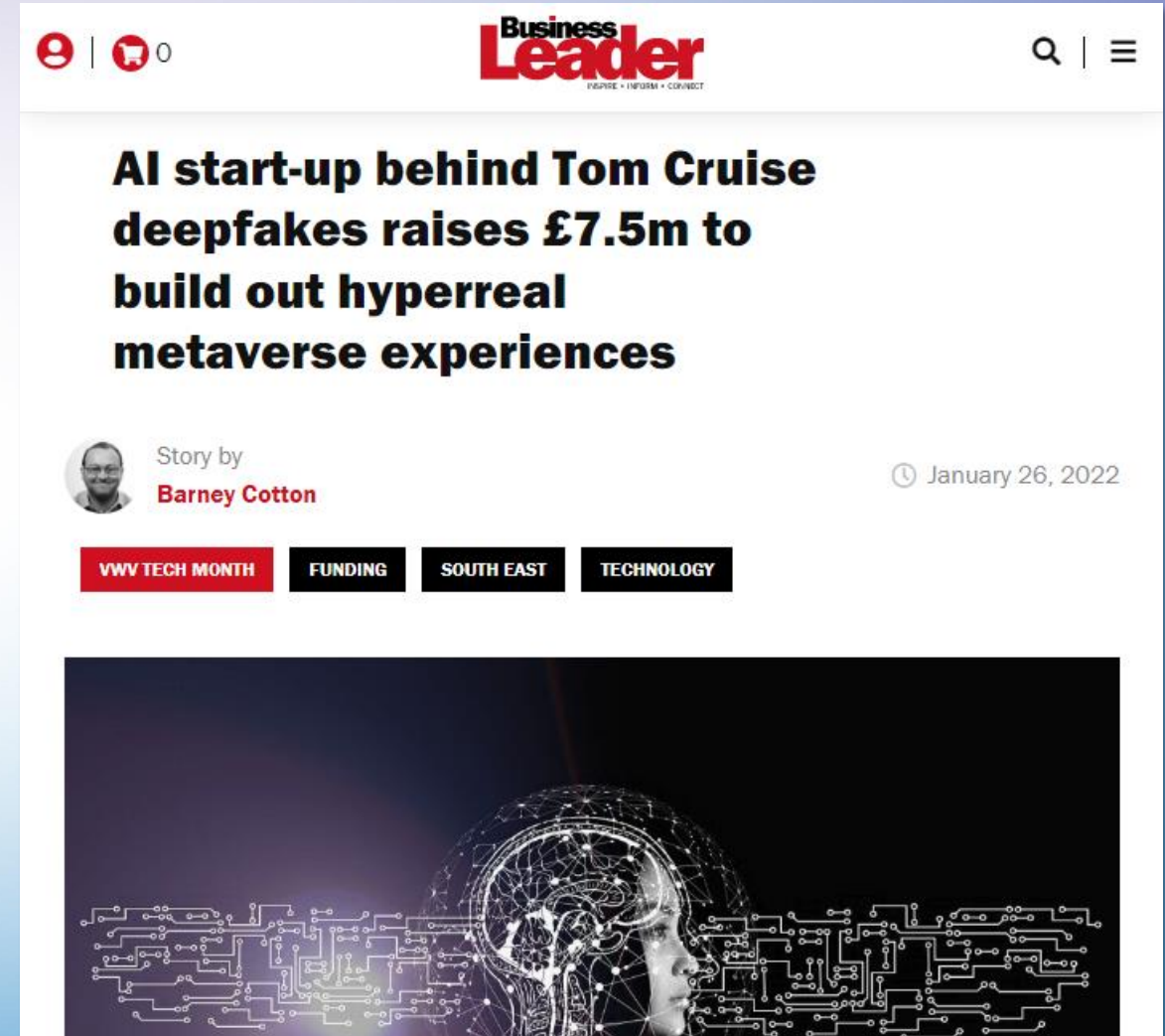


No, Tom Cruise isn't on TikTok. It's a deepfake



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



Attacks Utilising A.I.



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

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

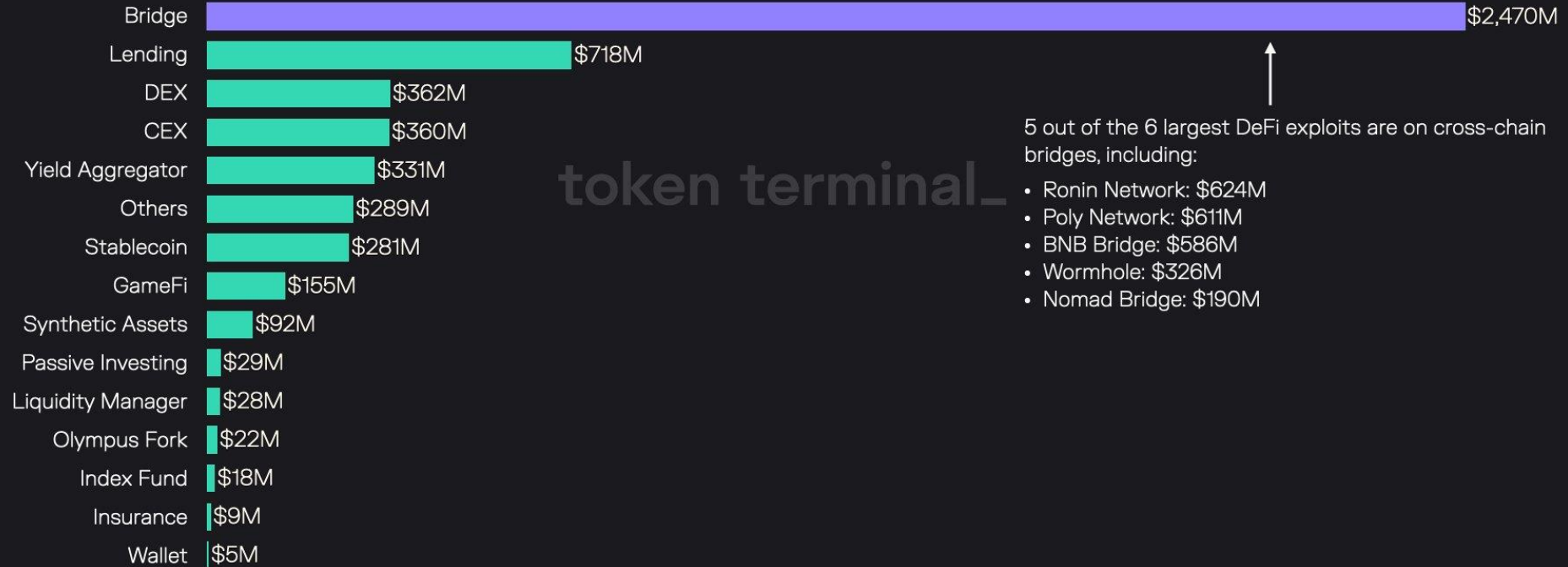
Companies or victims who identify this type of activity should report it to the IC3, www.ic3.gov.

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

Exploiting Vulnerabilities in Blockchain Bridge

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



token terminal_

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”

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.”

3

Security Advice



Security Risks of Crypto Wallet

Cryptocurrency

“Hot wallet”

- Requires an internet connection
- Vulnerable to **cyber attacks** or **data breach**


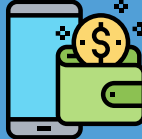


“Cold wallet”

- Does NOT require an internet connection
- At risk of **physical loss or damage**, **storage device malfunction**



Crypto Wallet - Custodial vs Non-custodial

	 Custodial	 Non-custodial
User control	<ul style="list-style-type: none"> You do not own your private keys Control is undertaken by third-party service provider 	<ul style="list-style-type: none"> You own your private keys You have total control over your digital assets
Accessibility	<ul style="list-style-type: none"> More accessible to beginners as part of a service provided by cryptocurrency exchanges 	<ul style="list-style-type: none"> Less accessible to beginners who need to store private keys securely
Cybersecurity	<ul style="list-style-type: none"> Vulnerable to hackers due to its connectivity to the Internet 	<ul style="list-style-type: none"> Secure from cyber threats with no Internet connection, but users must ensure storage of private keys and recovery phrases
Wallet fees for holding	<ul style="list-style-type: none"> Depends on provider 	<ul style="list-style-type: none"> No
Wallet fees for withdrawing	<ul style="list-style-type: none"> Depends on provider 	<ul style="list-style-type: none"> No
Ease of use	<ul style="list-style-type: none"> User-friendly with interactive UI and support 	<ul style="list-style-type: none"> Requires technical knowledge and expertise with limited support

Security Advice on Crypto Wallet



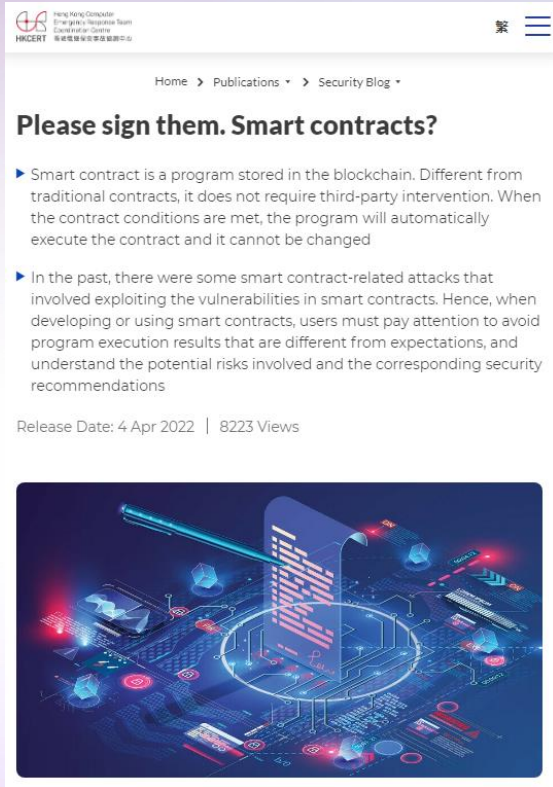
- Wallet Apps
 - **Back up** your wallet and set a password for protection
 - **Never disclose** the **recovery phrase** to others
 - Enable **Multi-factor Authentication**
 - Enable asset transfer **whitelist**
 - **Verify carefully** the content before signing or authorising all transactions
 - Keep 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**

Security Advice on Social Engineering Attacks Utilising A.I.



- 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 links 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 cautious of **social engineering tactics** (e.g. appeal to urgency, threatening, authority, etc.)

Security Advice on Smart Contracts



- **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.

Decentralisation vs Regulation

Virtual Asset

- **Virtual assets** should be regarded as “**objects**” that can be “**stolen**”?
- Or **access to computer** with criminal or dishonest intent **under criminal law**?
- **Cross-border issues** may arise?
- Will the **transfers of NFTs** constitute **taxable** transactions?

“Ownership” of Lands

- **Smart contract** templates provided by the transaction platform is **very simple form**, merely contain **monetary obligations** and term limitations.
- Necessary to improve the **legal protection to the owners** of the land in the metaverse

Payment

- By agreeing to complete the transaction of bitcoins, the parties involved **automatically accept the terms and conditions** provided by such platform
- Possible to have a **universal law** to **regulate** all payment disputes in this virtual world?
- If doing so, does it simply frustrate the **decentralised concept** of blockchain technologies?

Key Takeaway



- Web 3.0 and blockchain enables user to have **total control** over their **ownership of digital assets** across platforms
- Hacker tries **various attack tactics** to **gain access** to your crypto wallet and steal your digital assets
- More Web 3.0 use cases and Apps are **emerging**
- Adopt **Zero-Trust Concept** and **verify everything** to minimise security risks



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

