



# AADAP'Tate

(O te levantarán la cartera)

# DeFi 101



Bob envía dinero a Alice **a través** de su banco



Sistema Bancario  
Centralizado



Alice recibe el dinero **en su** banco

Los bancos de Bob y Alice tienen la custodia de los fondos y de las trasferencias entre ellos



Bob envía dinero a Alice a través de blockchain



BlockChain



Alice recibe el dinero en su dirección pública

Blockchain transfiere el dinero entre cuentas, sin un tercero de confianza que tenga la custodia

# North Korean hackers cash out hundreds of millions from \$1.5bn ByBit hack

10 March 2025

Share  Save **Joe Tidy**

Cyber correspondent, BBC World Service



Get

Hackers thought to be working for the North Korean regime have successfully converted at least \$300m (£232m) of their record-breaking \$1.5bn crypto heist to unrecoverable funds.



Alejandro Ramos (@aramosf)

💰 ~6.113 millones de dólares robados en cripto: y... ¿hemos aprendido algo? Voy a volver a repetir el número, por que reducido parece algo más pequeño: ¡¡¡6.113.000.000 \$!!!

### 1 Vulnerabilidades en Smart Contracts y protocolos

Errores en lógica, validaciones o puentes cross-chain:

- The DAO (2016): Reentrada en withdraw() (~\$50M)
- Parity (2017):
- Poly Network: validación y c...
- Euler (2023):
- Radiant (2024):

💰 Total: ~2.170

### 2 Compromiso de Claves y Malware (Ingeniería Social)

Acceso mediante phishing, malware o errores humanos:

De Mt. Gox (2011) a Nobitex (2025): claves robadas, phishing dirigido, claves API comprometidas o wallets controladas por malware:

2024 (récord) - Volumen ilícito total estimado en USD **51 mil millones**

2025 S1 – Superados los USD **2,17 mil millones**. Se estima alcanzar los **4,3**

### 3 Fallos de Infraestructura

Errores de arquitectura:

Desde Bitfloor (2012) a DMM Bitcoin (2024): backups sin cifrar, wallets sin aislamiento, multisig mal configurado:

- Coincheck (2018): hot wallet sin multifirma (~\$534M)
- Bitfinex (2016): multisig mal integrado (~\$70.5M)

💰 Total: ~1.426M USD



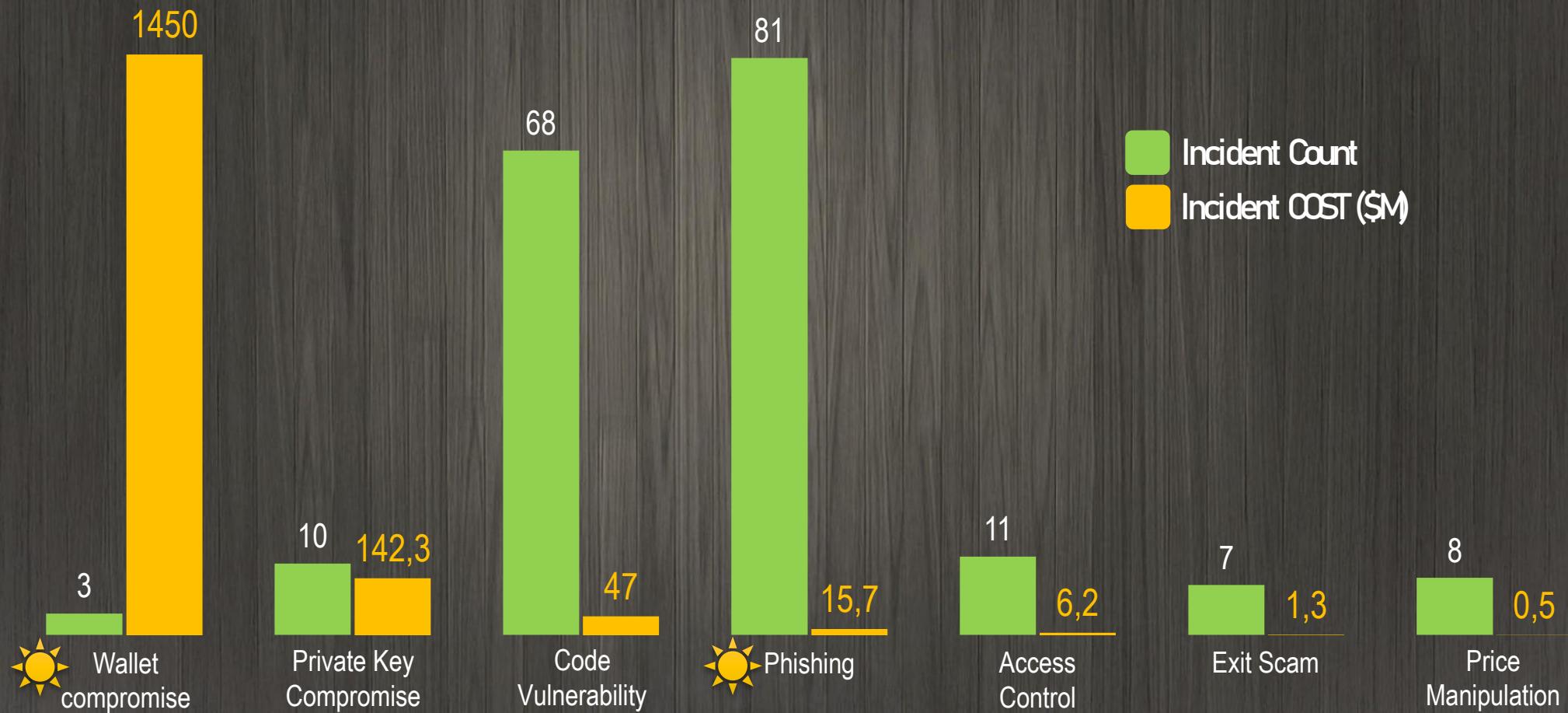
**PIB ESP=USD1,62 mil millones**

- Sheep Marketplace, BitGrail, Multichain: fondos retirados por fundadores o ejecutivos con acceso privilegiado.

💰 Total: ~\$396M USD

Desde 2021 ha habido más de 1.000 ataques documentados contra objetivos de criptomonedas y plataformas descentralizadas financieras (DeFi), con un resultado de **\$12,5 billion** de pérdidas

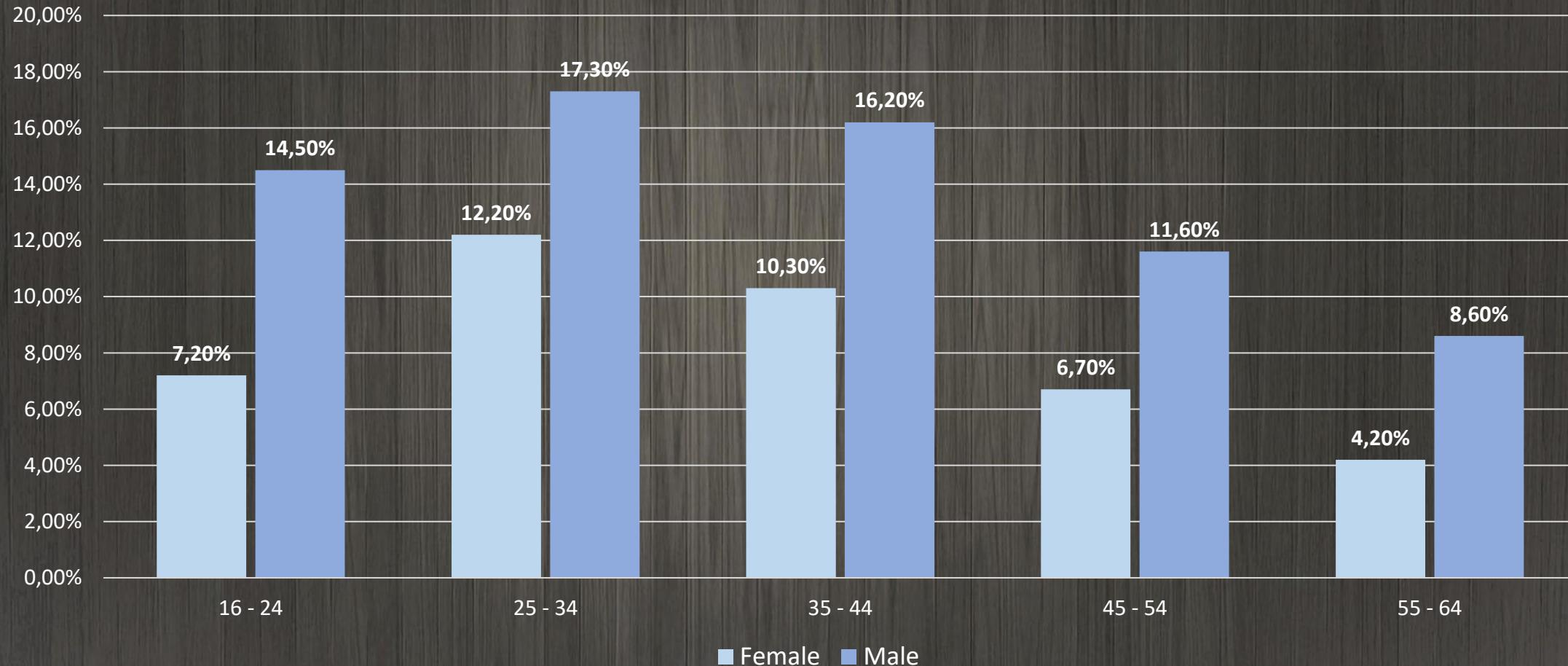
Chainalysis: The 2025 Crypto Crime Report



JAN  
2023

# OWNERSHIP OF CRYPTOCURRENCY

PERCENTAGE OF INTERNET USERS WHO OWN SOME FORM OF CRYPTOCURRENCY



# MITRE ADAPT



MITRE  
ATT&CK™

CAPEC

CVE®

ATLAS 

DEFEND



III  
MITRE  
ENGENUITY.

CALDERA 

# MITRE AADAPT

Adversarial Actions in Digital Asset Payment Technologies

Reconnaissance	Resource Development	Initial Access	Execution	Privilege Escalation	Defense Evasion	Credential Access	Lateral Movement	Collection	Impact	Fraud
Channel Wormholing	Acquire Accounts	Exploit External Services	Exploit Blockchain Technology Specific Vulnerabilities	Exploit Smart Contract Hierarchical Ownership	Circumvent Account Limits	Exploit External Services	Exploit Gas-Free RPCs	Aggregate Private Key Generation Data	Burn Wallets	Chain Reorganization
Smart Contract Implementation Analysis	Flash Loan	Exploit Obsolete Device	Exploit Consensus Logic		Cross-Chain Swaps (Hopping)	Unsecured Credentials &	Insider-Assisted Access	Intercept API Communication	Chain Reorganization	Eclipse Attack
		Insider-Assisted Access	Exploit Smart Contract Implementation		Siphon Funds			Scrape Blockchain Data	Induce Legal and Regulatory Penalties	Exploit Consensus Logic
			Fault-Injection Attack		Use Anonymizing Services			Scrape KYC Data	Market Manipulation	Generate Counterfeit Tokens
			Quantum Efficient Factorization						Reputation Damage	Manipulate Transaction History
			Side-Channel Attack							Partial Payments Attack
										Siphon Funds

11 TÁCTICAS  
38 TÉCNICAS

# MITRE AADAPT

Persistencia	Descubrimiento	C2	Exfiltración							
Reconocimiento	Desarrollo de recursos	Acceso inicial	Ejecución	Escalada de privilegios	Evasión de defensa	Acceso a credenciales	Movimiento lateral	Recopilación	Impacto	Fraude
Channel Wormholing	Adquisición de cuentas	Explotar servicios externos	Explotar las vulnerabilidades específicas de Blockchain	Aprovechar la jerarquía de los Smart Contracts	Evitar los límites de la cuenta	Explotar servicios externos	Explotar RPC sin gas	Datos agregados de generación de claves privadas	Quemar carteras	Reorganización de la Cadena
Análisis de la implementación de Smart Contracts	Préstamo Flash	Explotar dispositivo obsoleto	Explotar la lógica del consenso		Swaps entre cadenas (Hopping)	Credenciales no seguras &	Acceso asistido o por insider	Interceptar las comunicaciones de un API	Reorganización de la cadena	Ataque de eclipse
		Acceso asistido o por insider	Explotar la implementación de Smart Contracts		Desvío de Fondos			Extraer datos de blockchain	Inducir sanciones legales y reglamentarias	Explotar la lógica del consenso
			Inyección de fallas		Utilice servicios de anonimización			Extraer datos KYC	Manipulación del mercado	Generar tokens falsificados
			Factorización cuántica eficiente						Daño a la reputación	Manipular el historial de las transacciones
			Ataque de canal lateral							Ataque de pagos parciales
										Desvío de fondos

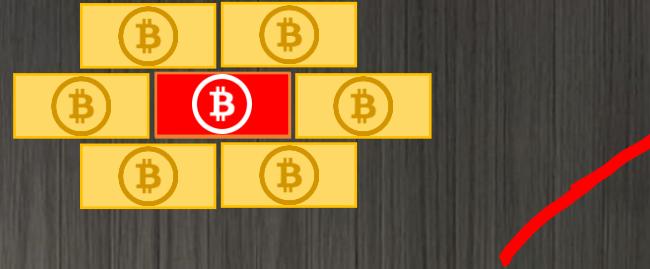
# Cómo funciona Blockchain (101)

trc



# Chain Reorganization

(Reorganización de la BlockChain)



- Incorrecto: Una vez que un bloque se acepta, *no* es immutable de inmediato.
- Correcto: Un bloque es considerado "provisional" hasta que pasan suficientes confirmaciones (más bloques después de él).

Consiste en **reescribir el historial reciente de bloques** para anular transacciones previas y sustituirlas por otras nuevas

Ocurre cuando alguien con suficiente poder de minado o validación (atacante) ...

1. Crea en secreto una cadena alternativa (con transacciones omitidas o modificadas).
2. La va extendiendo más allá de la cadena pública oficial.
3. Una vez tiene más bloques, la publica de golpe.
4. La red, siguiendo su lógica, acepta esta nueva cadena como válida, anulando transacciones anteriores.

# Chain Reorganization

Escenario teórico

Supongamos una red estilo Bitcoin o Ethereum:

Cadena oficial actual:

A → B → C → D → E

↑ última cabeza de la cadena

Imaginemos que un atacante comienza a minar en secreto una cadena alternativa desde el bloque 'C':

Cadena atacante (oculta):

A → B → C → X → Y → Z

(3 bloques frente a 2 desde C)

Cuando el atacante revela su cadena, los nodos de la red reorganizan su cadena y adoptan la del atacante:

Cadena nueva aceptada:

A → B → C → X → Y → Z ✓

A → B → C → D → E ✗ (descartada)

Los bloques D y E quedan "huérfanos" (orphaned blocks) y sus transacciones pueden desaparecer de la historia oficial.

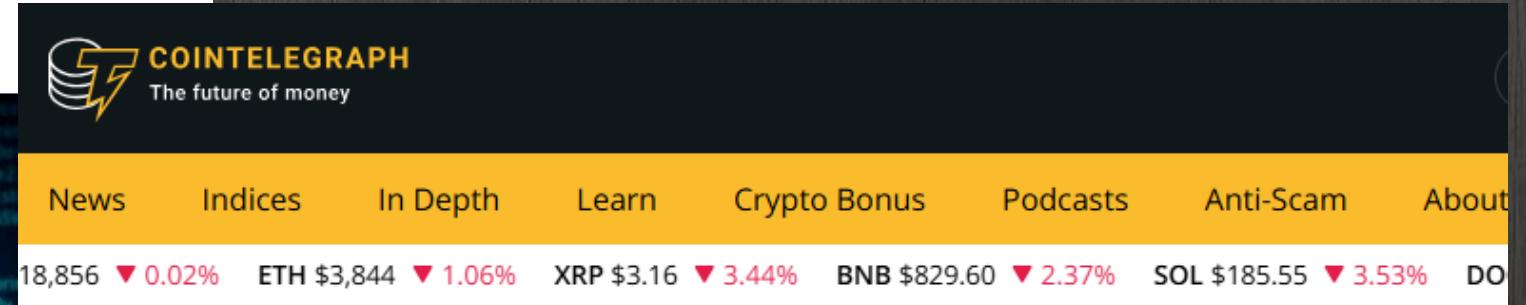
 Emilia David 30 ago 2020

## Ethereum Classic sufre otro ataque del 51%

Es el tercer ataque de este mes.



 La red de Ethereum Classic (ETC) se vio afectada por otro ataque del 51% el pasado 29 de agosto, lo que provocó la reorganización de más de 7,000 bloques solo unas semanas después de proponer actualizaciones de seguridad.



COINTELEGRAPH The future of money

News Indices In Depth Learn Crypto Bonus Podcasts Anti-Scam About

18,856 ▼ 0.02% ETH \$3,844 ▼ 1.06% XRP \$3.16 ▼ 3.44% BNB \$829.60 ▼ 2.37% SOL \$185.55 ▼ 3.53% DO

Safer transactions with Web3 Antivirus. Scan risks before you send 

 Brian Quarmby May 26, 2022

## Ethereum Beacon Chain experiences 7 block reorg: What's going on?

"This reorg is not an indicator of a flawed fork choice, but a non-trivial segmentation of updated vs out of date client software" suggested Core Ethereum developer Preston Van Loon.

# Chain Reorganization: consecuencia



Blockchain	Tiempo por bloque	Confirmaciones recomendadas	Tiempo para "finalidad segura"	Notas
Bitcoin (BTC)	~10 minutos	6	~60 minutos	Estándar en comercio y exchanges
Ethereum (PoS)	~12 segundos	2–3 epochs (64–96 bloques)	~2–4 minutos	Usa <i>finality checkpoints</i> (via Casper/FFG)
Ethereum Classic	~13 segundos	2,500+	~12 horas	Vulnerable a reorganizaciones
Litecoin (LTC)	~2.5 minutos	12	~30 minutos	Basado en Bitcoin
Polygon (PoS)	~2 segundos	100–150	~3–5 minutos	Finalidad probabilística
Avalanche (C-Chain)	~2 segundos	3	~6 segundos	Finalidad casi instantánea
BNB Smart Chain	~3 segundos	15	~45 segundos	Compatible con Ethereum
Polkadot	~6 segundos	1 block	~6 segundos	Finalidad inmediata por GRANDPA

# Flash Loan

(préstamo instantáneo)

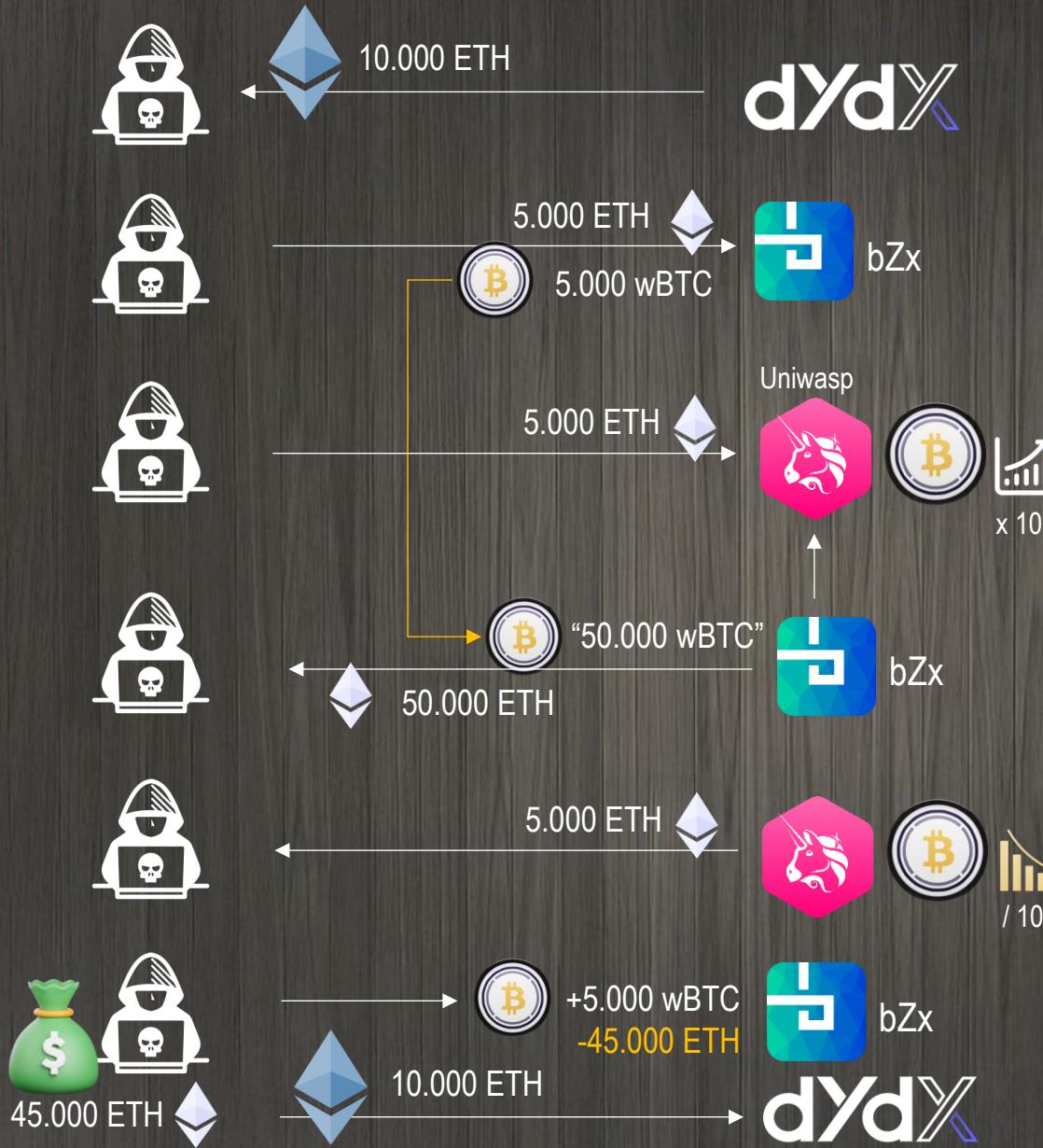


- Es un tipo especial de **préstamo** que solo existe dentro de **una única transacción** en blockchain.
- Puedes pedir prestada una gran cantidad de dinero (criptomonedas).
- **No necesitas garantías** (*collateral*).
- Pero debes devolverlo **dentro de esa misma transacción**.
- Si no puedes devolverlo en ese mismo bloque, la transacción entera se cancela automáticamente.



## The bZx Flash Loan Attack

# The bZx Flash Loan Attack



Solicita un Flash Loan: pide prestados 10.000 ETH desde dYdX.

Deposita 5.000 ETH en bZx como garantía de 5.000 wBTC

Invierte 5.000 ETH en wBTC en el DEX de Uniswap, incrementando el precio del wBTC x10

bZx usa Uniswap como oráculo, cree que wBTC vale mucho más de lo que realmente vale.  
El atacante pide un crédito por el valor de su garantía (con un valor incrementado artificialmente).

El atacante recupera los ETH y baja el precio del mercado

Devuelve el ‘valor’ de la garantía. bZx pierde 45.000 ETH  
Devuelve el Flash Loan a dYdX.  
Se queda con la ganancia.

## 8 Smart contract

```
function executeFlashLoanAttack() external {
    // 1. Solicitar un flash loan de 10,000 ETH desde dYdX
    dydx.flashLoan(address(this), asset, amount, params);
}

function callFunction(sender, account) external {
    // 2. Convertir parte del ETH a wBTC
    uint256 wbtcAmount = swapETHforWBTC(5_500 ether);
    // 3. Manipular el precio del wBTC en Uniswap
    buyWBTCConUniswap(1_300 ether);
    // 4. Usar los wBTC sobrevalorados como colateral
    depositCollateralInBZx(wbtcAmount);
    // Pedir un préstamo en ETH contra el colateral
    uint256 borrowedETH = borrowETHfromBZx();
    // 5. Vender los wBTC para restablecer el precio de mercado
    sellWBTCConUniswap(wbtcAmount);
    // 6. Devolver el flash loan a dYdX
    repayFlashLoan(10_000 ether);
    // 7. Atacante se queda con la ganancia en ETH
    uint256 profit = address(this).balance;
    withdraw(profit, attackerWallet);
}
```

### ¿Por qué?

Muchos contratos inteligentes en DeFi:

- No están preparados para cambios bruscos de precio.
- No verifican si los precios son reales o manipulados.
- Confían en oráculos que pueden ser manipulables temporalmente.

# Sphon Funds



(desvío de fondos)

Consiste en aprovechar vulnerabilidades en contratos inteligentes para **redirigir o robar activos** sin que los usuarios se den cuenta inmediatamente.

Esto implica redireccionar tokens que deberían ir a una dirección legítima, hacia una controlada por el atacante

Paso 1: Alice tiene recompensas  
`balances[Alice] = 10 ETH`

Paso 2: Bob llama a `withdrawReward()` desde un contrato malicioso  
`msg.sender = Alice` (suplantado)  
`recipient = Bob's wallet`

Paso 3: El contrato transfiere fondos  
`balances[Alice] = 0`  
Enviar 10 ETH → Bob

Resultado final:  
Bob recibe fondos de Alice sin autorización real

```
// SPDX-License-Identifier: MIT. // pragma solidity ^0.8.0;
RewardVault
contract {mapping(address => uint256) public balances;

// Los usuarios ganan recompensas
function depositReward(address user, uint256 amount) public {
    balances[user] += amount;
}

// Vulnerabilidad: permite cualquier dirección como destino
function withdrawReward(address recipient) public {
    uint256 amount = balances[msg.sender];
    require(amount > 0, "No rewards");

    balances[msg.sender] = 0;

    // 🔥 Riesgo: los fondos no necesariamente van a msg.sender
    (bool success, ) = recipient.call{value: amount}("");
    require(success, "Transfer failed");
}

// Recibir ETH
receive() external payable {}

}
```

# Una especie de resumen

## En mercados tradicionales...



- Algunas prácticas como manipular precios, usar información privilegiada o aprovecharse de errores del sistema **son ilegales y están reguladas** por organismos como la CNMV o la SEC.
- Pero otras formas de arbitraje o movimientos rápidos de capital **son legales** y parte del juego

## En DeFi...

El término "ataque" se usa cuando el actor:



- **Explota una debilidad técnica** en un contrato inteligente (no es solo moverse rápido en el mercado).
- Genera un **comportamiento anómalo** o no deseado **del protocolo**, que los diseñadores no anticiparon
- La operación se ejecuta **sin** que haya una **oferta y demanda real** → atacante NO corre riesgo.



Groucho Marx

“¡Hay muchas cosas en la vida, mucho  
más importantes que el dinero! ...  
... ¡Pero cuestan tanto!”



Emilio Rico Ruiz

Security Advisor at 



@Emilio\_RR



Emilio Rico Ruiz

muchas  
GRACIAS