Riesgos y Seguridad en Crypto

Por Pablo Sabbatella

ETH LATAM

ethereum foundation's Road to Devcon

defy EDUCATION

Agenda

- Seguridad informática
- Riesgos económicos
- Riesgos de smart contracts

Seguridad informática

- Confidencialidad: acceso a la información únicamente mediante autorización.
- Disponibilidad: la información debe permanecer accesible mediante autorización.
- Integridad: modificación de la información únicamente mediante autorización.
- No invertir más en seguridad que lo que se está asegurando.

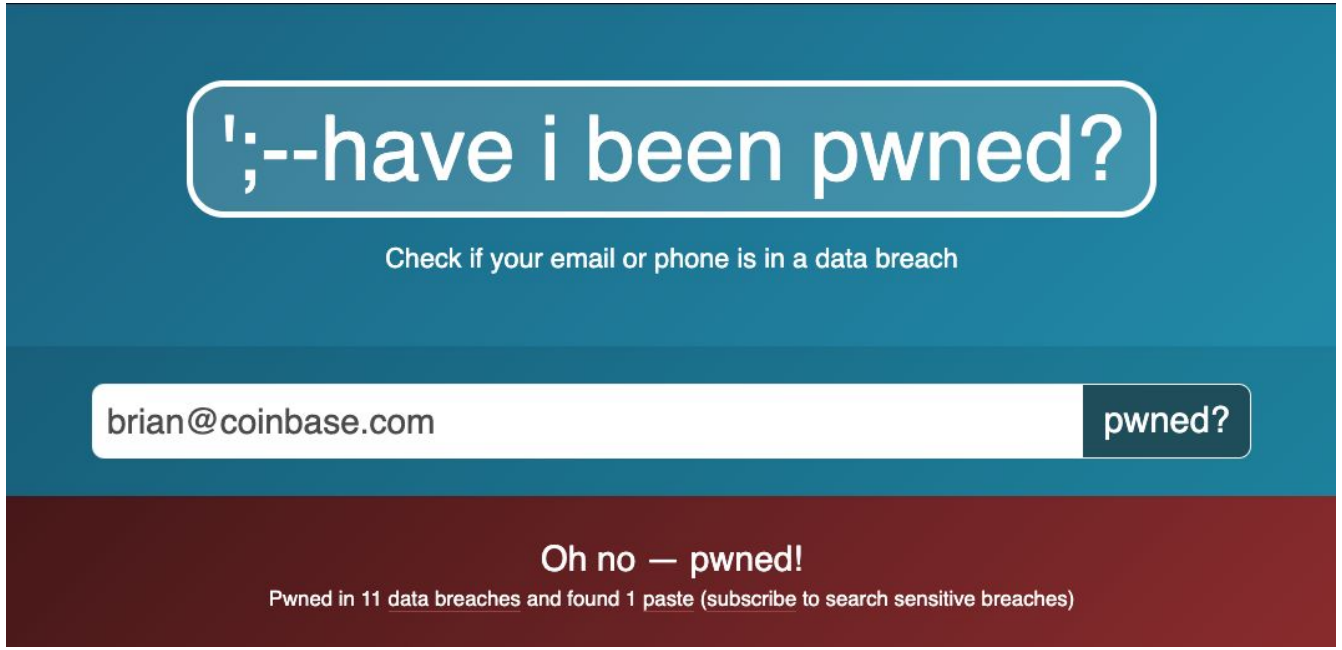
¿Cómo piensa y actúa un atacante?

Ataque a una cuenta CEX

- Recabar datos de la víctima
  - Email
  - Password
  - Número de celular
  - Segundo factor de autenticación

Contraseñas

- Conseguir contraseñas usadas por el target del ataque
- https://haveibeenpwned.com



defy EDUCATION

Sim-swap attack

- El atacante se presenta en una sucursal de la compañía telefónica o llama por teléfono y se hace pasar por la víctima
- Dice que le robaron la línea, por lo cual el chip de la víctima se da de baja
- Le otorgan al atacante un chip nuevo asociado a la línea de la víctima, por lo cual ahora tiene control total sobre la misma.
- Comienza a resetear accesos a servicios pidiendo códigos por sms

Ataque al buzón de voz

- El atacante espera a que la víctima esté durmiendo y pide código de reseteo por llamado de voz
- Al tener la víctima el teléfono apagado, el llamado entra al buzón de voz y queda grabado en el mismo
- El atacante llama a un número especial que tienen las telefónicas para levantar mensajes de voz de manera remota mediante un pin
- ¿Cual es el pin? Por defecto los últimos 4 números del celular :)

¿Y ahora qué hago?

Accionar

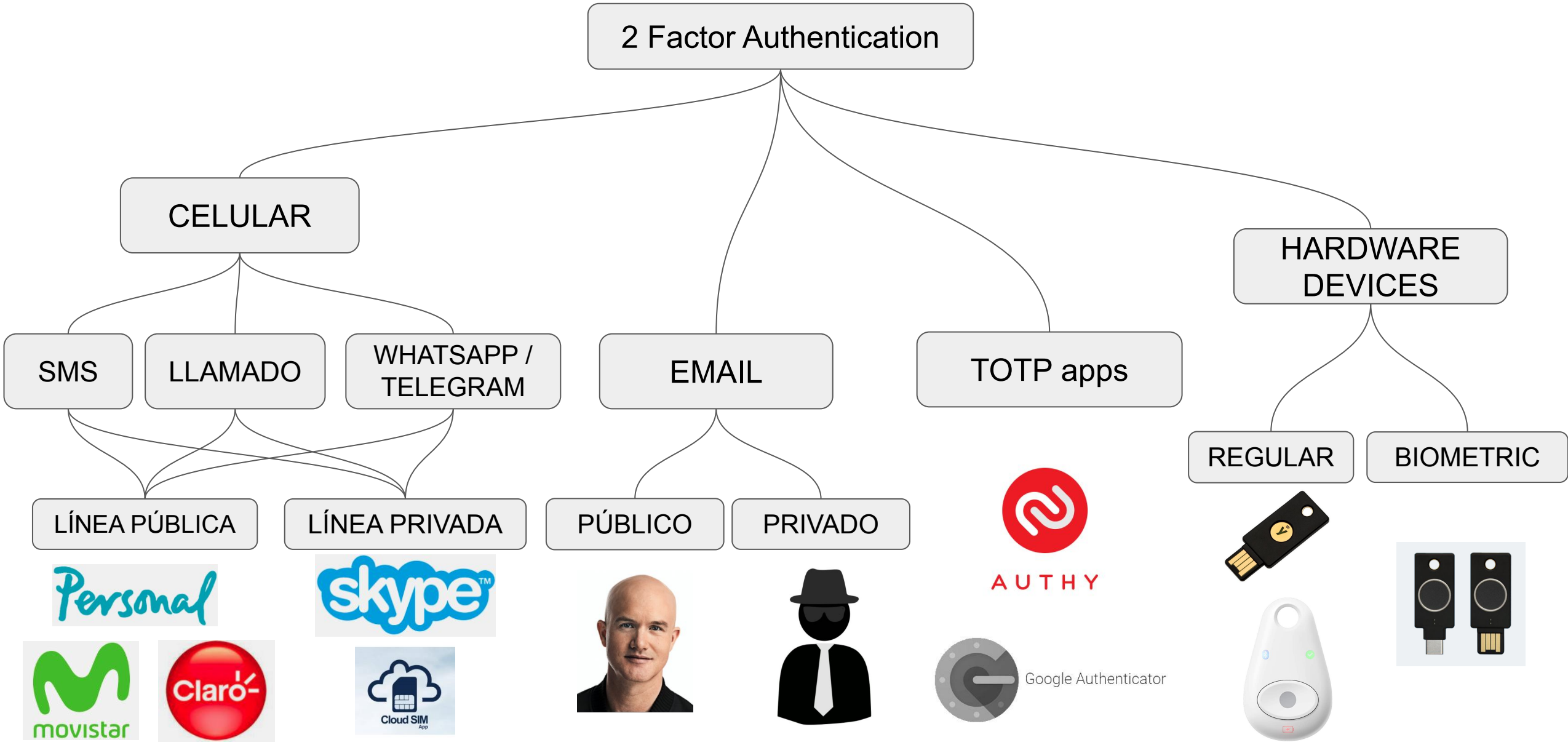
- Siempre configurar el segundo factor de autenticación, en todos los servicios.
- Evitar usar el SMS y el llamado como segundo factor.
- Utilizar aplicaciones TOTP (Time-based One Time Password) como Authy o Google Authenticator para generar estos códigos
- Siempre guardar impresos los códigos de backup al configurar 2FA
- Dispositivos 2FA físicos: Yubikey (https://www.yubico.com/), Fido multipass (https://www.ftsafe.com/Products/FIDO/Multi).

defy EDUCATION

Accionar

- Deshabilitar el buzón de voz del teléfono.
- Sacar una línea de celular privada vía Skype o Google Fi.
- Email exclusivo para crypto. Privado.
- Whatsapp > Settings > Account > Two-step verification > Configurar PIN y email.
- Telegram > Settings > Privacy and Security > Two-Step Verification > Activarlo

defy EDUCATION


2 Factor Authentication
CELULAR
SMS
LLAMADO
WHATSAPP / TELEGRAM
LÍNEA PÚBLICA
LÍNEA PRIVADA
EMAIL
PÚBLICO
PRIVADO
TOTP apps
AUTHY
Google Authenticator
HARDWARE DEVICES
REGULAR
BIOMETRIC
Personal
movistar
Claro
skype
Cloud SIM

Passwords

- Usar contraseñas complejas, creadas por un password manager
- Nunca repetir contraseñas
- Utilizar password manager:
  - 1Password: https://1password.com/
  - Lastpass: https://www.lastpass.com/
  - Bitwarden: https://bitwarden.com/
- Configurar 2FA en password manager
- Chequear nivel de exposición: https://haveibeenpwned.com/

¿Pensaron en qué va a pasar el día que les roben el celular desbloqueado?

Si no llevamos USD 2.000 en la billetera, ¿por qué lo hacemos en una app en el celular?

Celular

- Bloqueo automático
- Login mínimo de 6 dígitos o 6 puntos en caso de usar patrón
- Siempre sistema operativo actualizado. Si es viejo y no permite actualizarlo, cambiarlo.
- Configurarle pin al chip SIM
- Aplicaciones siempre actualizadas
- No bajar aplicaciones que no sean estrictamente necesarias
- Especial cuidado en el Google Play Store.
- Aplicaciones financieras y sensibles con bloqueo de pin o biométrico.
- Encriptar datos y bloquear desde el firmware

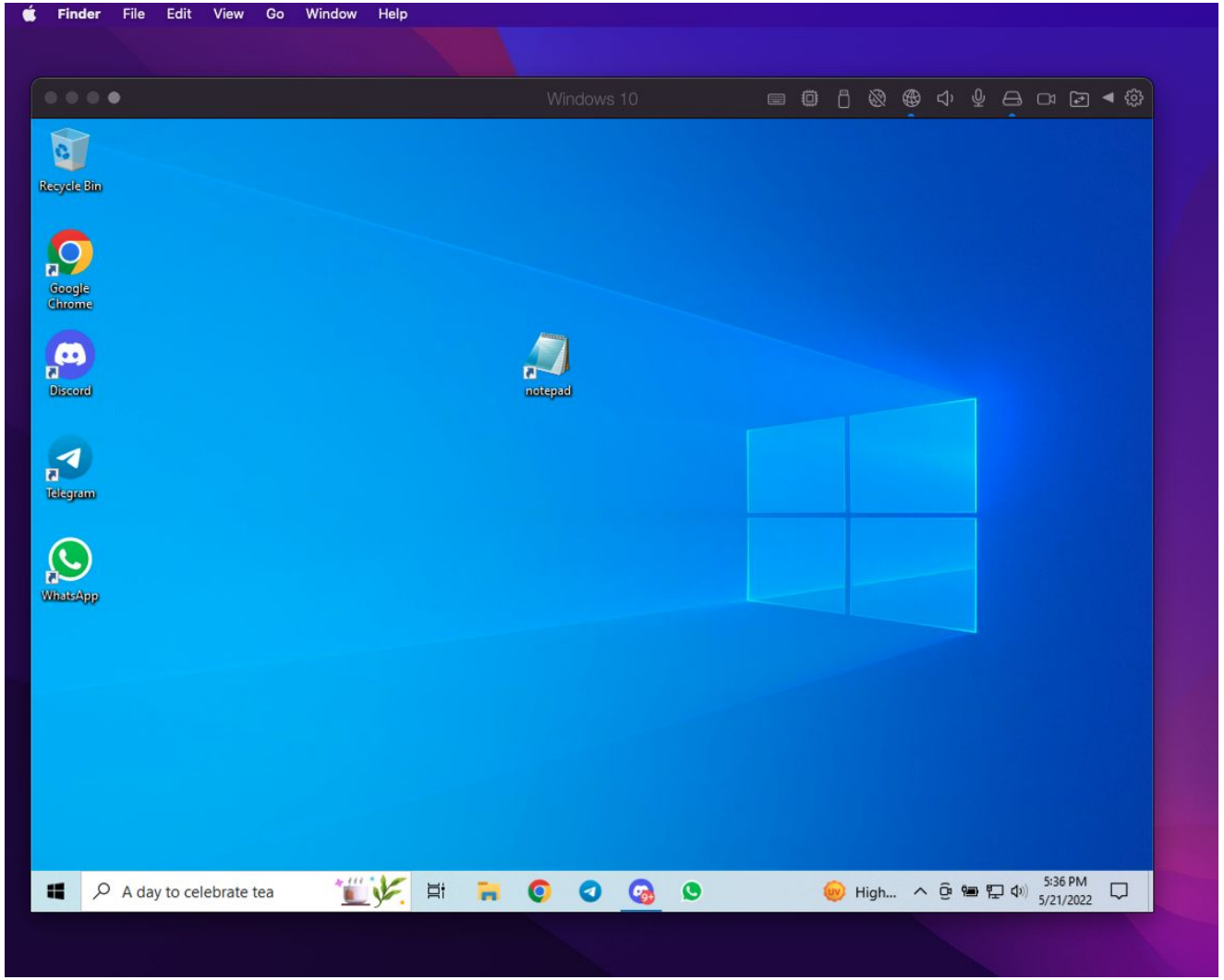
Laptop

- Siempre contraseña compleja en el login y bloqueo automático.
- Sistema operativo siempre actualizado. Prohibido Windows 7.
- Aplicaciones instaladas siempre actualizadas.
- No instalar aplicaciones que no sean estrictamente necesarias
- No instalar software crackeado o pirateado, en la gran mayoría de los casos trae Malware.
- Antivirus siempre actualizado en Windows. Task Explorer en Mac.
- Firewall. Lulu para Mac. Windows Defender Firewall para Windows
- Encriptar disco rígido: Windows > Bitlocker. Mac > FileVault
- State level > deshabilitar reseteo por Live o Apple ID.
- Configurar password en booteo. Windows y Mac: LINK

Laptop

- Navegador siempre actualizado
- Extensiones siempre actualizadas. Para forzar actualizaciones en Chrome > Settings > Extensions > Developer mode > Update
- No instalar extensiones de dudosa procedencia. Sólo lo esencial.
- Navegador separado para instalar Metamask u otras billeteras.
- De ser posible instalar una máquina virtual (Virtual Machine) para todo lo riesgoso: Twitter, Discord, Telegram, Whatsapp, porno, etc.
- Virtual Machine: Parallels para la Mac. VMware para Windows.
- Chequear links y archivos: Virus Total

Virtual Machine



Ingenieria social & phshing

- Nunca entregar información por teléfono, email, chat, discord, telegram, etc sin verificar quién está del otro lado. Ante la duda, cortar
- Cuidado ante la simulación de ser un amigo por Whatsapp, Facebook, Telegram, Discord, Twitter. Ante la duda, llamar.
- Discord y Telegram: bloquear todos los mensajes privados de quienes no conocen. Jamás seguir links ni indicaciones enviadas por ese medio.
- Phishing: no entrar a sitios buscando desde google ni desde emails que hayan recibido sin chequear que realmente sea el original. Tipear URL.

Toolkit de seguridad

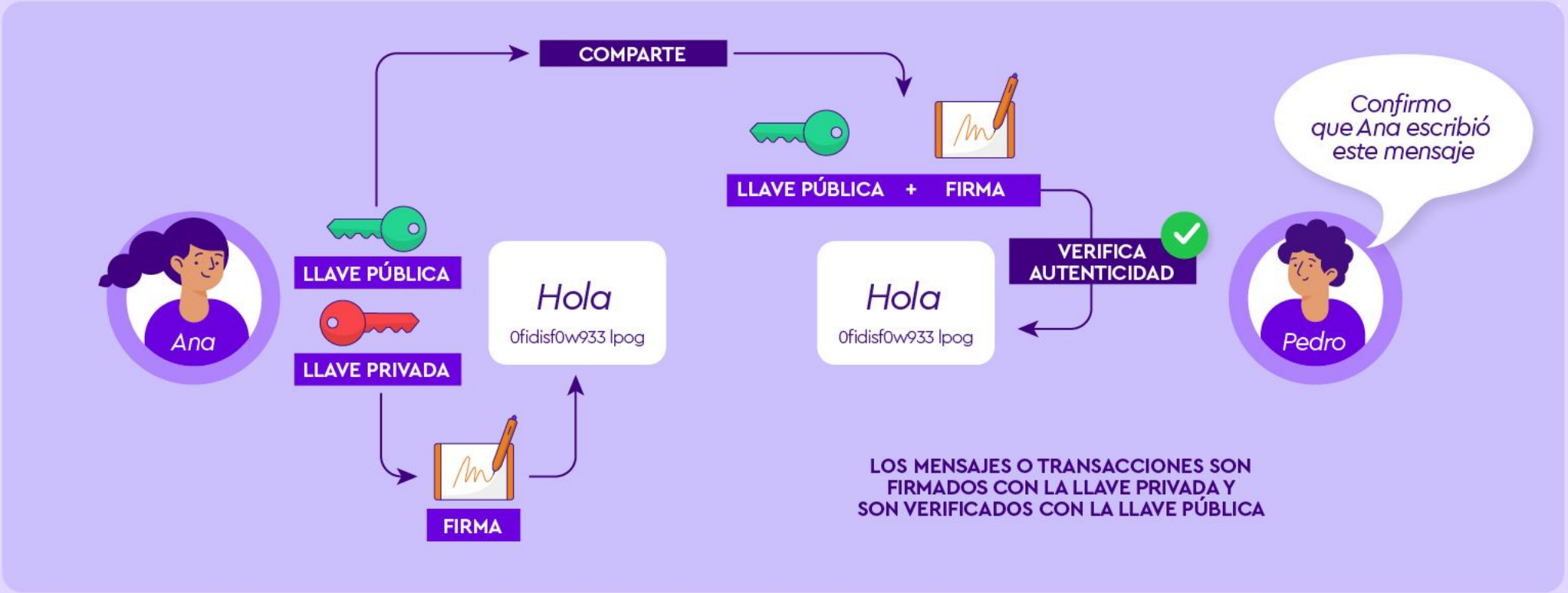
- Segundo Factor de autenticación (2FA):
  - Authy: https://authy.com/
  - Google Authenticator: Apple Store - Google Play Store
  - Yubico: https://www.yubico.com/
- Línea de teléfono alternativa:
  - Skype: https://skype.com/
  - Google Fi: https://fi.google.com/
- Bloqueo de apps con pin para Android:
  - Smart AppLock: Google Play Store
- Firewall:
  - Lulu (Mac): https://objective-see.com/products/lulu.html
- Task Explorer: https://objective-see.org/products/taskexplorer.html

Toolkit de seguridad

- Máquinas virtuales:
  - Parallels (Mac): https://www.parallels.com/es/
  - VMware (Windows): https://www.vmware.com/ar/products/workstation-player.html
- Encriptación computadora:
  - Bitlocker (Windows): https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-0c453637-bc88-5f74-5105-741561aae838
  - Filevault (Mac): https://support.apple.com/en-us/HT204837
- Disco virtual encriptado:
  - VeraCrypt: https://www.veracrypt.fr/code/VeraCrypt/

Wallets y llaves privadas

USANDO CRIPTOGRAFÍA PARA VERIFICAR INFORMACIÓN



defy EDUCATION

Diferentes tipos de

WALLETS

EXCHANGES

- KRAKEN
- BINANCE
- BELO
- BUENBIT
- BITFINEX
- BITTREX

CUSTODIAL WALLETS

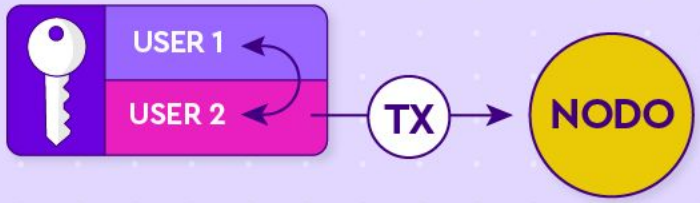
WALLET OF SATOSHI

- HOT WALLETS
  - METAMASK
  - TRUST WALLET
  - EXODUS
  - DEFIANT
- SMART CONTRACT WALLETS
  - ARGENT
  - MULTI-PARTY COMPUTATION
- WARM WALLETS
  - muun
  - MULTISIG WALLETS
    - GNOSIS SAFE
- COLD WALLETS
  - PAPER WALLETS
    - SHARE
    - SECRET
  - HARDWARE WALLETS
    - TREZOR
    - LEDGER
    - SAFEPAL

defy EDUCATION

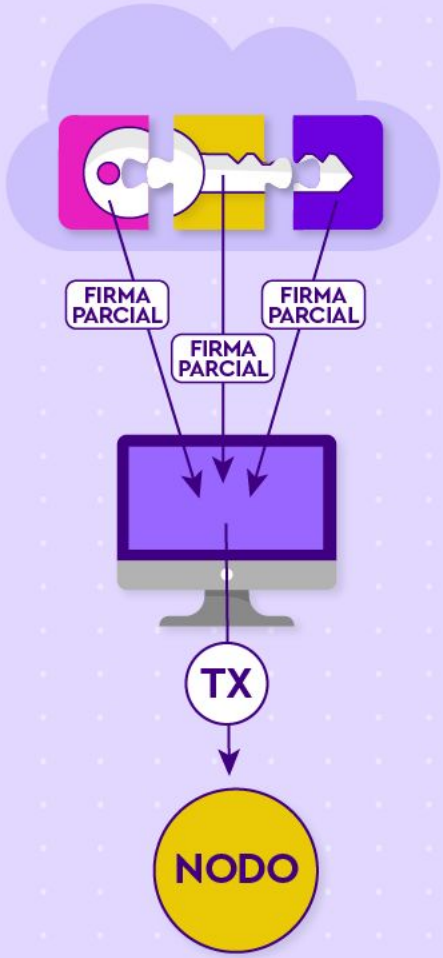
TIPOS DE WALLETS SEGÚN LA CUSTODIA DE LA LLAVE Y SUS INTERACCIONES

EXCHANGE
(Custodial wallet)

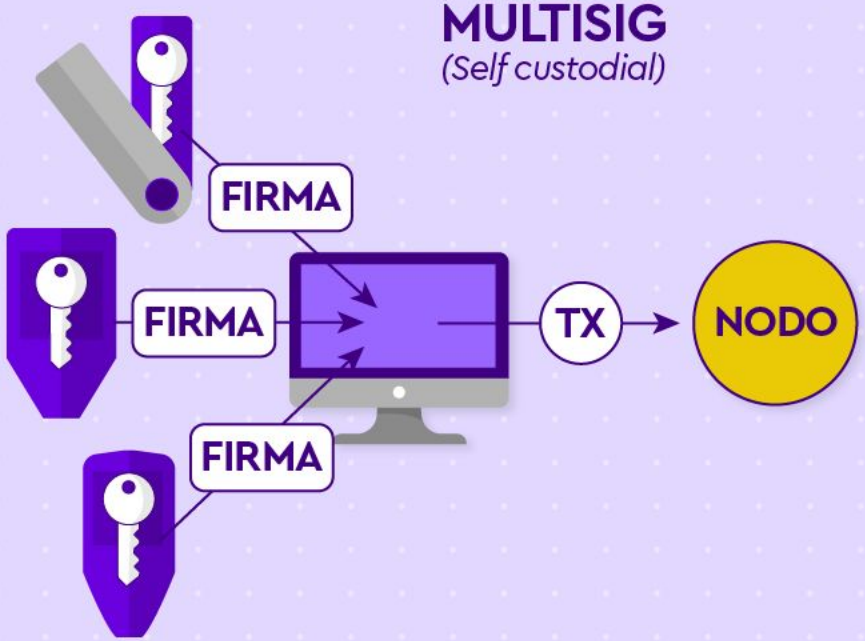


HOT WALLET
(Self custodial)

MULTI PARTY COMPUTATION
(Self custodial)



MULTISIG
(Self custodial)



HARDWARE WALLET
(Self custodial)

defy EDUCATION

CÓMO FUNCIONA UNA HARDWARE WALLET

La confirmación se realiza interactuando con el dispositivo de hardware y no con la computadora

La llave privada se mantiene almacenada en el dispositivo de hardware y aislada de la computadora

El dispositivo de hardware firma la transacción y solo envía esta firma hacia el software de la computadora que se encarga de enviar la transacción

defy EDUCATION

LAS HARDWARE WALLETS MÁS CONOCIDAS

Trezor T

Trezor One

Ledger Nano S

Ledger Nano X

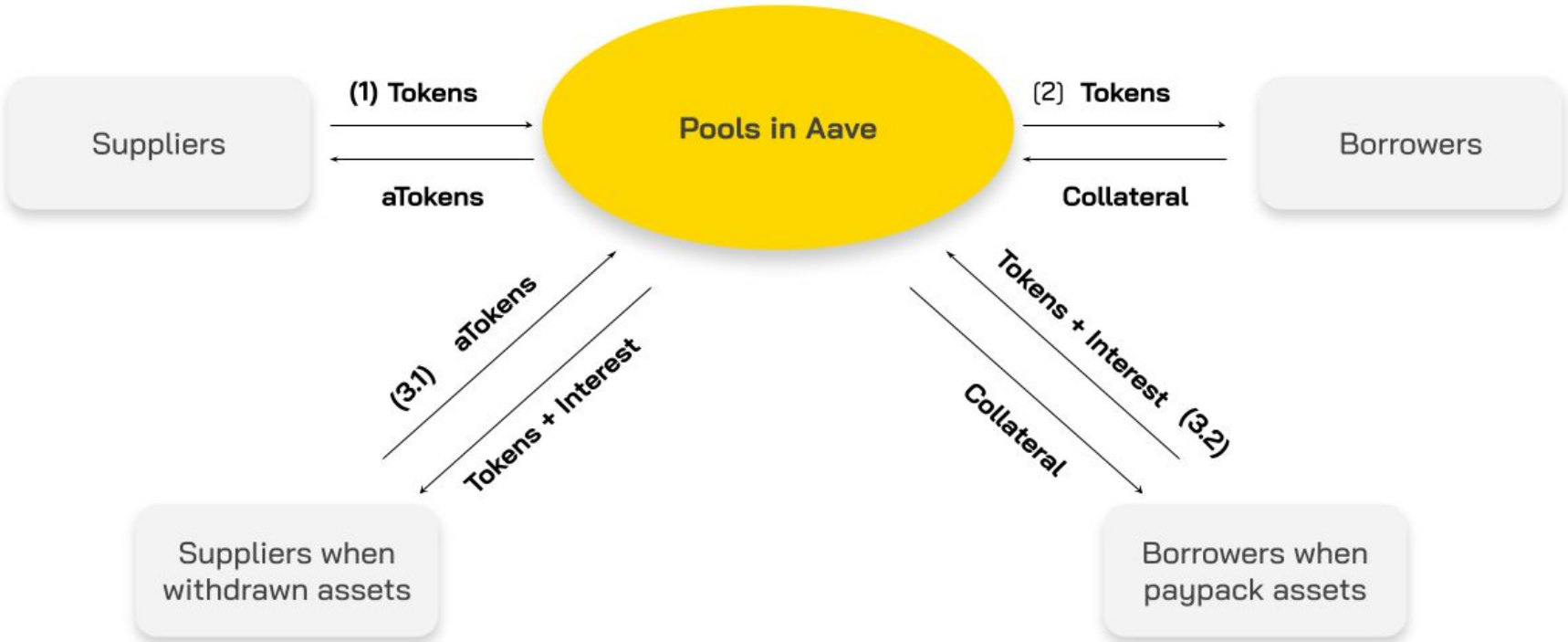
defy EDUCATION


DeFi - The Dark Forest

Riesgos en DeFi

- Mecanismo económico / financiero resiliente
- Riesgo de smart contract
  - Auditorías de seguridad
  - Contratos verificados
- Entorno de trabajo aislado
- Revocar permisos

Mecanismos económicos

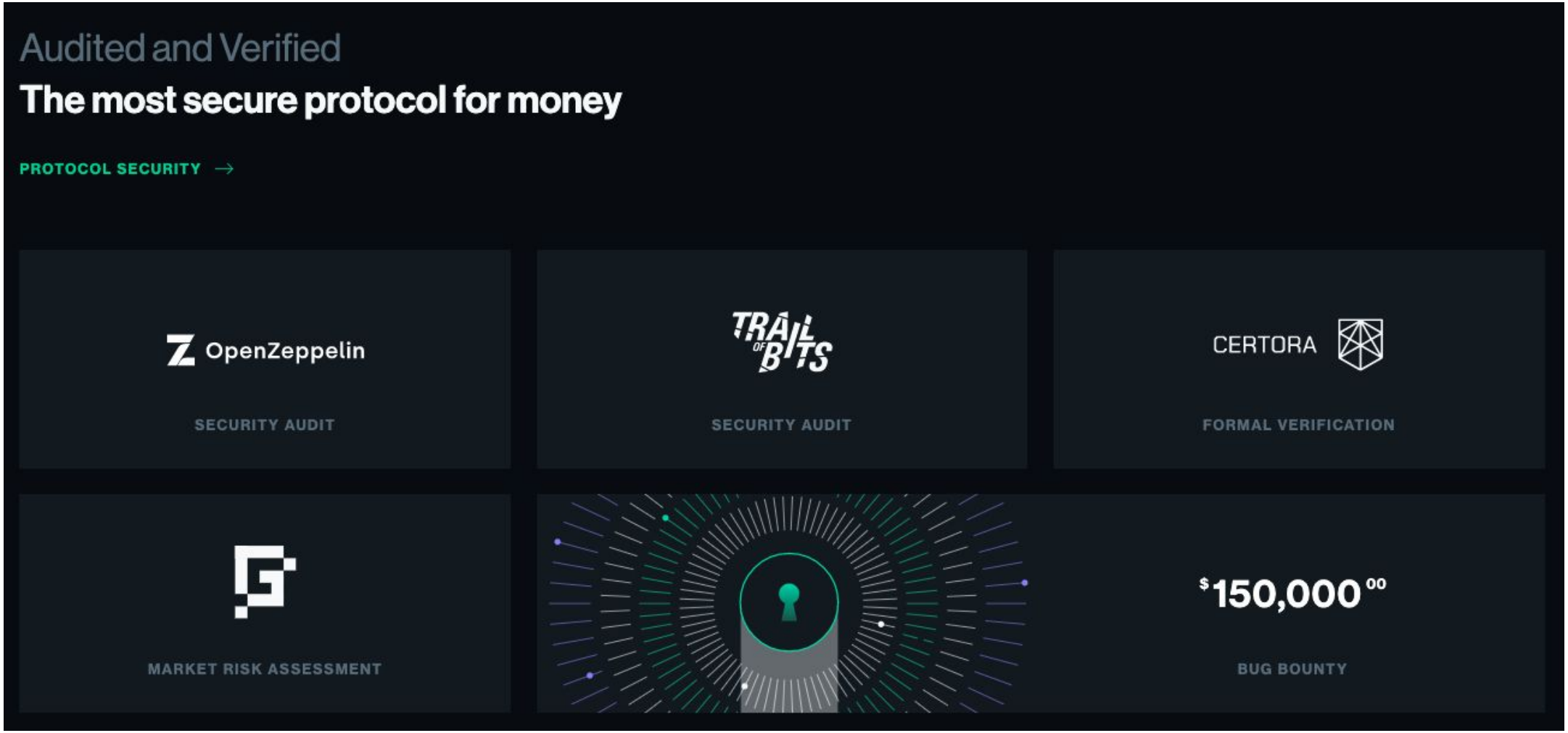


Mecanismos económicos

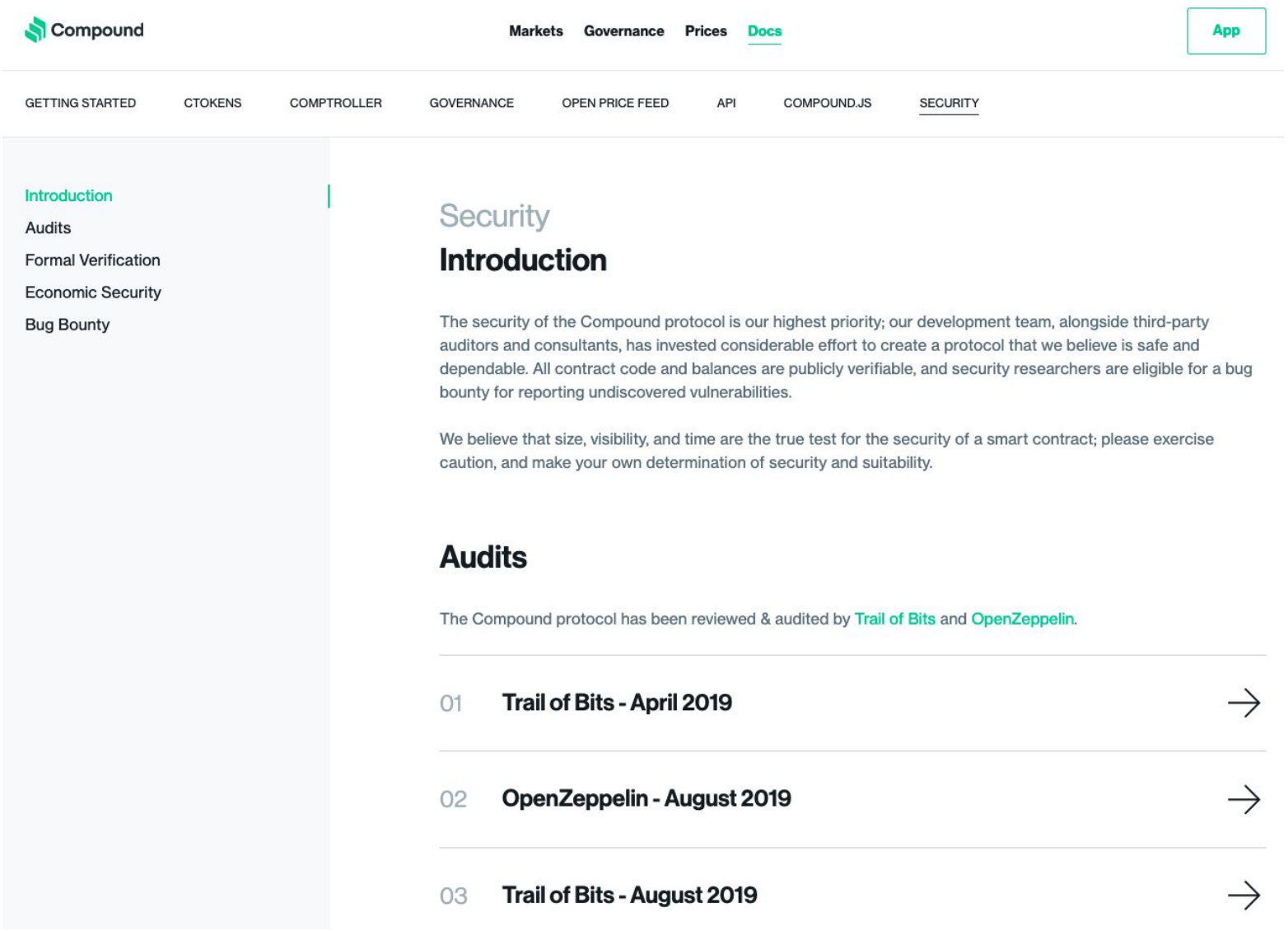
Crypto es un entorno adversarial. Si se puede romper, se va a romper

Mecanismos económicos

Auditorías de seguridad



Auditorías de seguridad



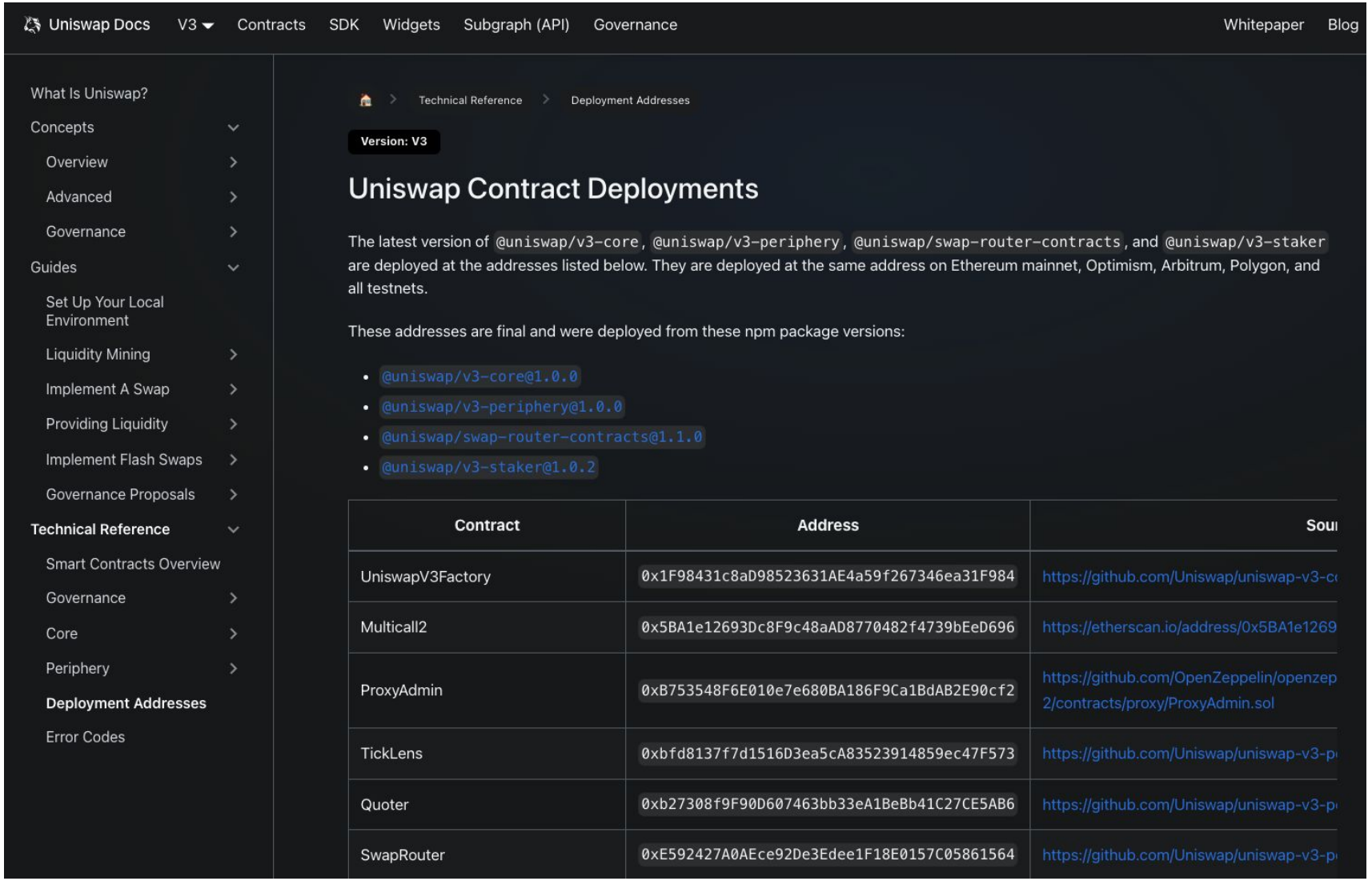
Rekt Leaderboard

rekt

1. **Ronin Network - REKT** *Unaudited*
   $624,000,000 | 03/23/2022
2. **Poly Network - REKT** *Unaudited*
   $611,000,000 | 08/10/2021
3. **Wormhole - REKT** *Neodyme*
   $326,000,000 | 02/02/2022
4. **BitMart - REKT** *N/A*
   $196,000,000 | 12/04/2021
5. **Beanstalk - REKT** *Unaudited*
   $181,000,000 | 04/17/2022
6. **Compound - REKT** *Unaudited*
   $147,000,000 | 09/29/2021
7. **Vulcan Forged - REKT** *Unaudited*
   $140,000,000 | 12/13/2021
8. **Cream Finance - REKT 2** *Unaudited*
   $130,000,000 | 10/27/2021
9. **Badger - REKT** *Unaudited*
   $120,000,000 | 12/02/2021
10. **Fei Rari - REKT 2** *Unaudited*
    $80,000,000 | 05/01/2022
11. **Qubit Finance - REKT** *Unaudited*
    $80,000,000 | 01/28/2022
12. **Ascendex - REKT** *Unaudited*
    $77,700,000 | 12/12/2021
13. **EasyFi - REKT** *Unaudited*
    $59,000,000 | 04/19/2021
14. **Uranium Finance - REKT** *Unaudited*
    $57,200,000 | 04/28/2021
15. **bZx - REKT** *Unaudited*
    $55,000,000 | 11/05/2021
16. **Cashio - REKT** *Unaudited*
    $48,000,000 | 03/23/2022
17. **PancakeBunny - REKT** *Unaudited*
    $45,000,000 | 05/19/2021
18. **Kucoin - REKT** *Internal audit*
    $45,000,000 | 09/29/2020
19. **Alpha Finance - REKT** *Quantstamp, Peckshield*
    $37,500,000 | 02/13/2021
20. **Vee Finance - REKT** *Slowmist, Certik*
    $34,000,000 | 09/21/2021
21. **Crypto.com - REKT** *Deloitte*
    $33,700,000 | 01/18/2022
22. **Meerkat Finance - BSC - REKT** *Unaudited*
    $32,000,000 | 03/04/2021
23. **MonoX - REKT** *Halborn, Peckshield*
    $31,400,000 | 11/30/2021
24. **Spartan Protocol - REKT** *Certik*
    $30,500,000 | 05/02/2021
25. **Grim Finance - REKT** *Solidity Finance*
    $30,000,000 | 12/18/2021
26. **StableMagnet - REKT** *Techrate*
    $27,000,000 | 06/23/2021
27. **Paid Network - REKT** *Unaudited*
    $27,000,000 | 03/05/2021
28. **Harvest Finance - REKT** *Haechi, Peckshield*
    $25,000,000 | 10/26/2020
29. **XToken - REKT** *Peckshield*
    $24,000,000 | 05/12/2021
30. **Elephant Money - REKT** *Solidity Finance*
    $22,200,000 | 04/12/2021
31. **Blizz Finance, Venus Protocol - REKT** *n/a*
    $21,800,000 | 05/13/2022
32. **Popsicle Finance - REKT** *Peckshield*
    $20,000,000 | 08/03/2021
33. **Pickle Finance - REKT** *Unaudited*
    $19,700,000 | 11/22/2020
34. **Cream Finance - REKT** *Unaudited*
    $18,800,000 | 08/30/2021

defy EDUCATION

Smart contracts verificados



Uniswap Docs V3 Contracts SDK Widgets Subgraph (API) Governance Whitepaper Blog

What Is Uniswap?
Concepts
Overview
Advanced
Governance
Guides
Set Up Your Local Environment
Liquidity Mining
Implement A Swap
Providing Liquidity
Implement Flash Swaps
Governance Proposals
Technical Reference
Smart Contracts Overview
Governance
Core
Periphery
Deployment Addresses
Error Codes

Technical Reference > Deployment Addresses

Version: V3

Uniswap Contract Deployments

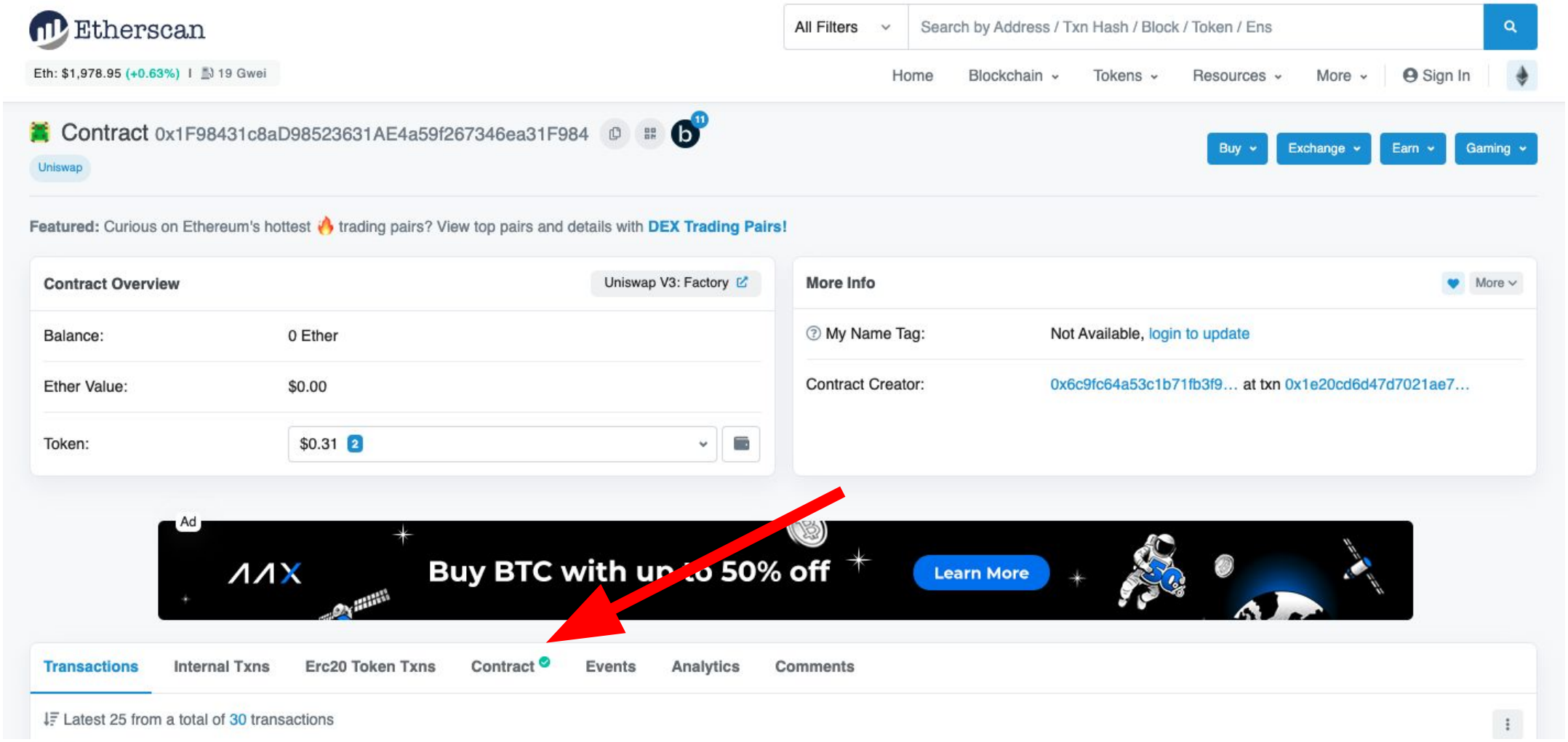
The latest version of `@uniswap/v3-core`, `@uniswap/v3-periphery`, `@uniswap/swap-router-contracts`, and `@uniswap/v3-staker` are deployed at the addresses listed below. They are deployed at the same address on Ethereum mainnet, Optimism, Arbitrum, Polygon, and all testnets.

These addresses are final and were deployed from these npm package versions:

- `@uniswap/v3-core@1.0.0`
- `@uniswap/v3-periphery@1.0.0`
- `@uniswap/swap-router-contracts@1.1.0`
- `@uniswap/v3-staker@1.0.2`

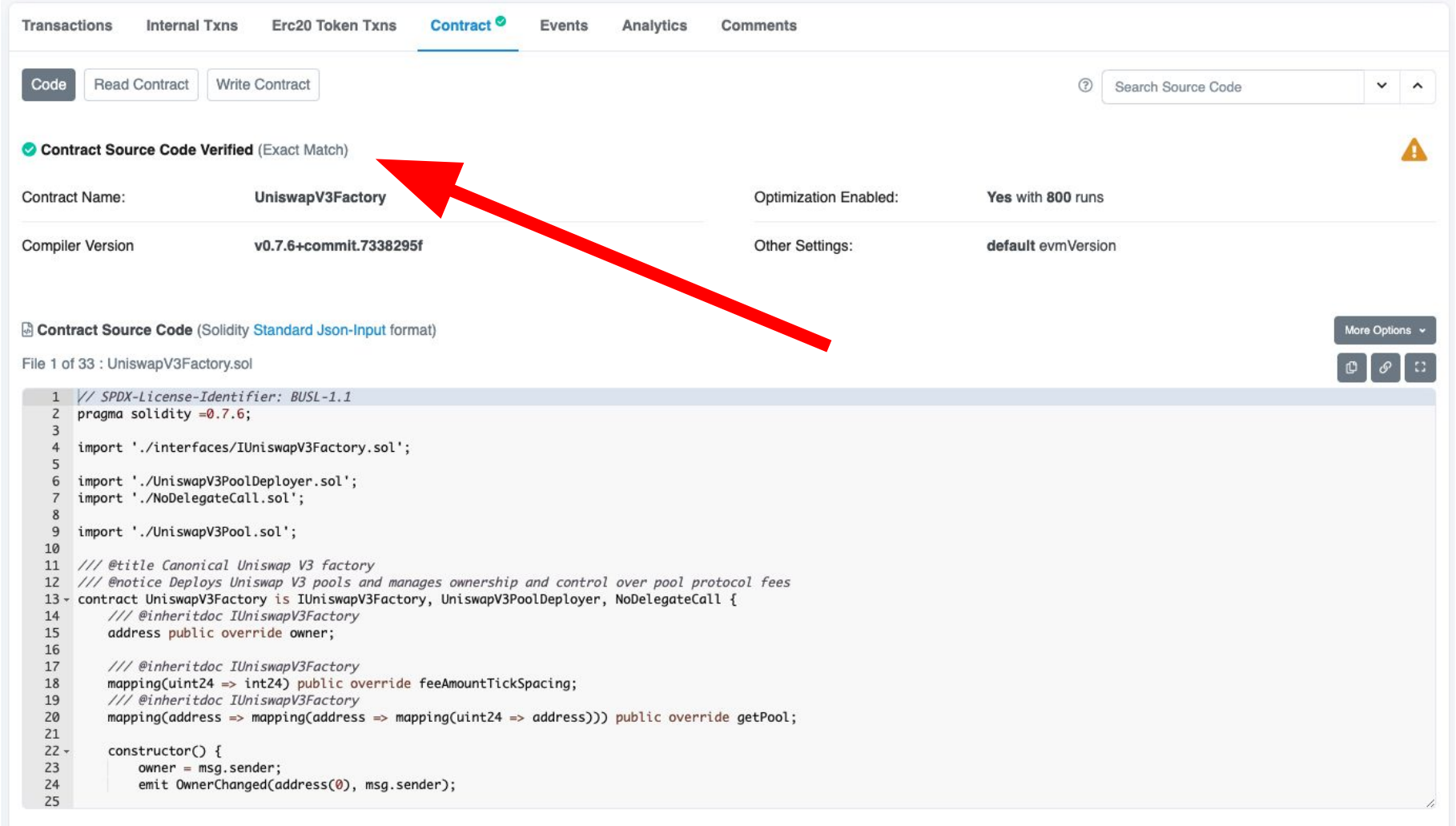
Contract	Address	Sou
UniswapV3Factory	`0x1F98431c8aD98523631AE4a59f267346ea31F984`	https://github.com/Uniswap/uniswap-v3-c
Multicall2	`0x5BA1e12693Dc8F9c48aAD8770482f4739bEeD696`	https://etherscan.io/address/0x5BA1e1269
ProxyAdmin	`0xB753548F6E010e7e680BA186F9Ca1BdAB2E90cf2`	https://github.com/OpenZeppelin/openzep 2/contracts/proxy/ProxyAdmin.sol
TickLens	`0xbfd8137f7d1516D3ea5cA83523914859ec47F573`	https://github.com/Uniswap/uniswap-v3-p
Quoter	`0xb27308f9F90D607463bb33eA1BeBb41C27CE5AB6`	https://github.com/Uniswap/uniswap-v3-p
SwapRouter	`0xE592427A0AEce92De3Edee1F18E0157C05861564`	https://github.com/Uniswap/uniswap-v3-p

Smart contracts verificados



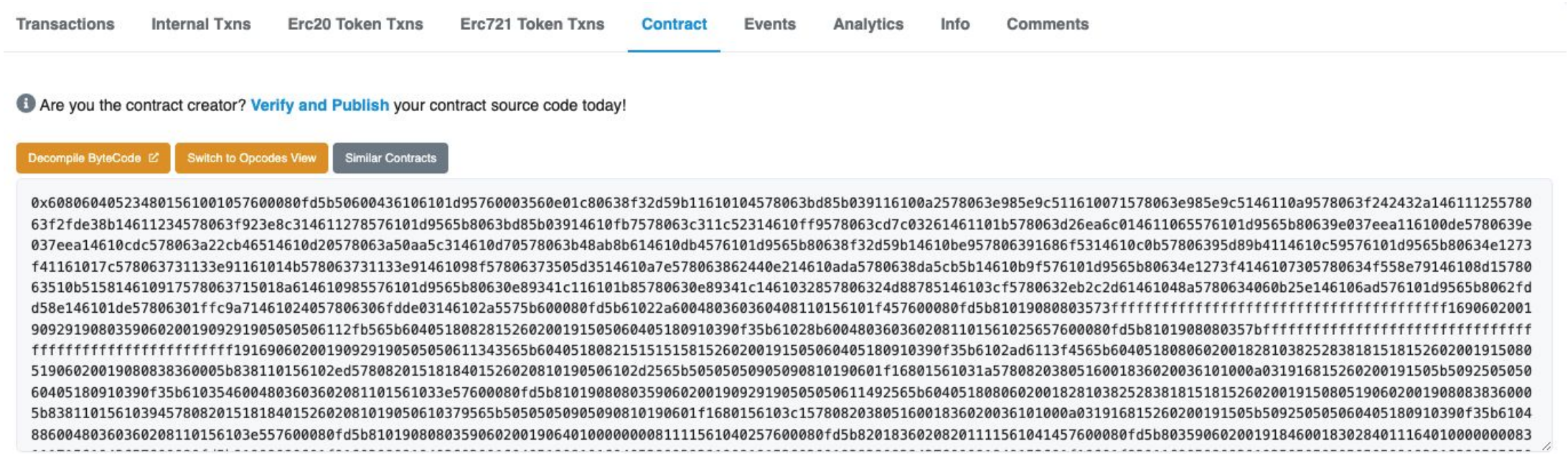
https://etherscan.io/address/0x1f98431c8ad98523631ae4a59f267346ea31f984#code

Smart contracts verificados

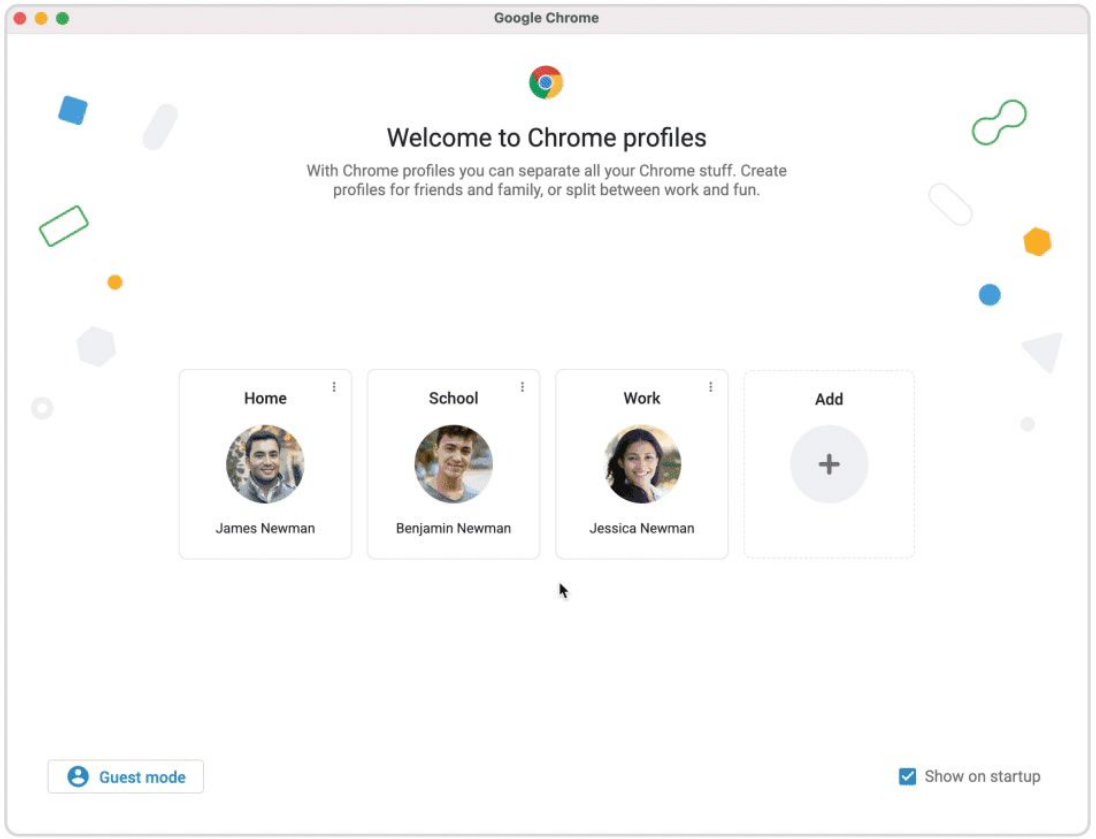


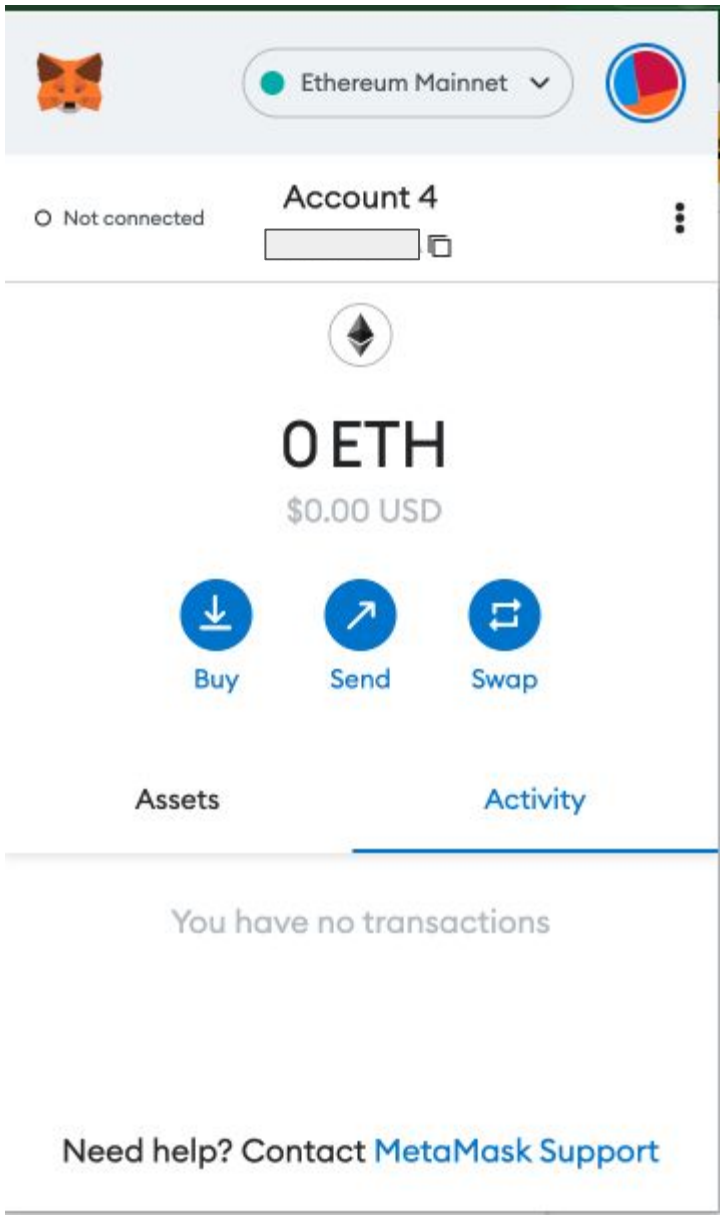
https://etherscan.io/address/0x1f98431c8ad98523631ae4a59f267346ea31f984#code

Smart contracts no verificados

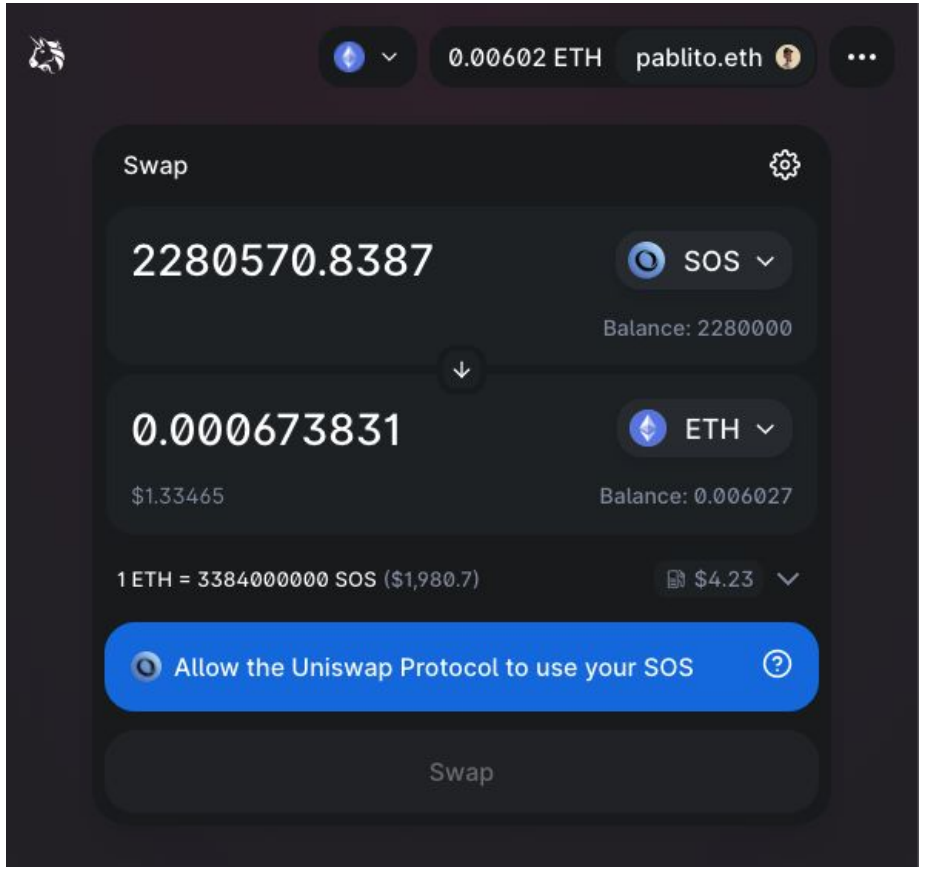


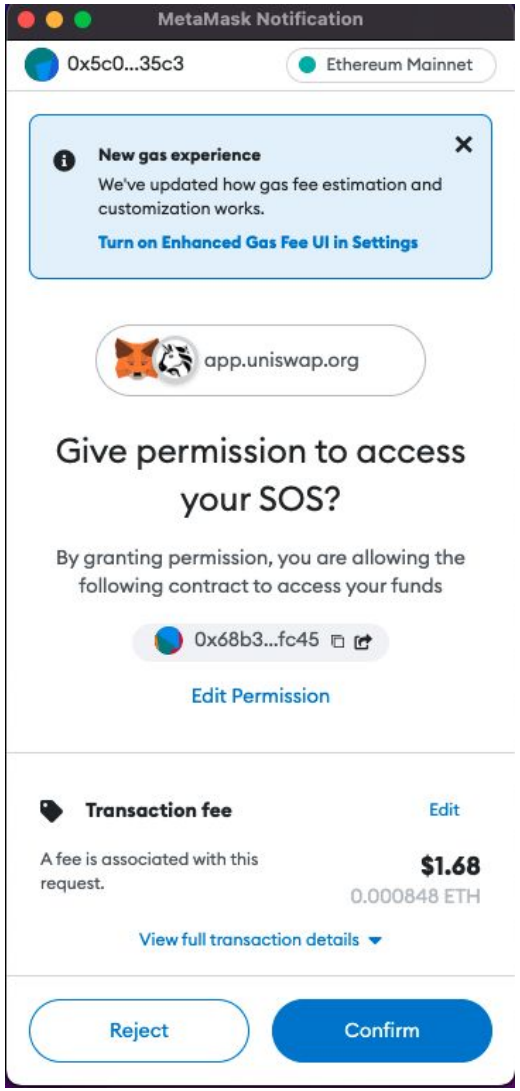
Nuevo navegador & wallet

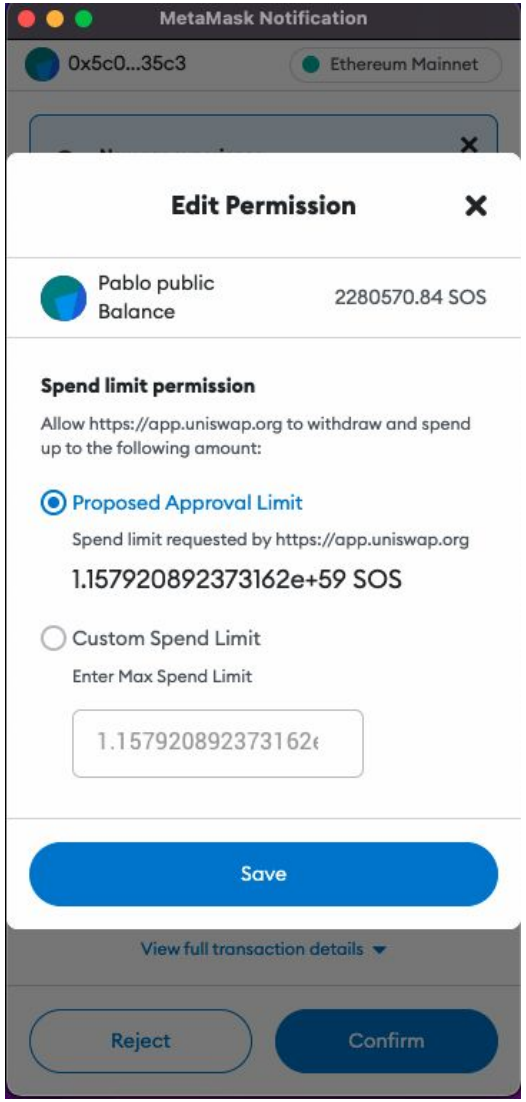




Contratos aprobados

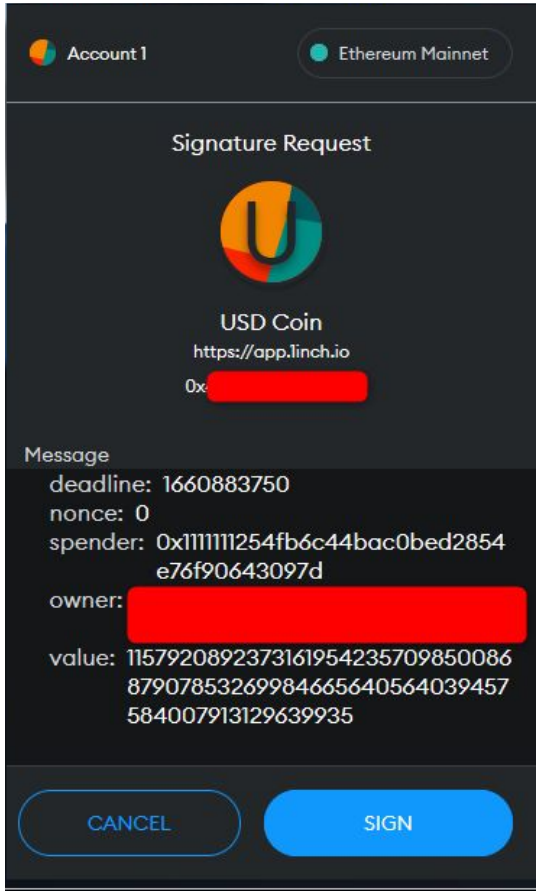






defy EDUCATION

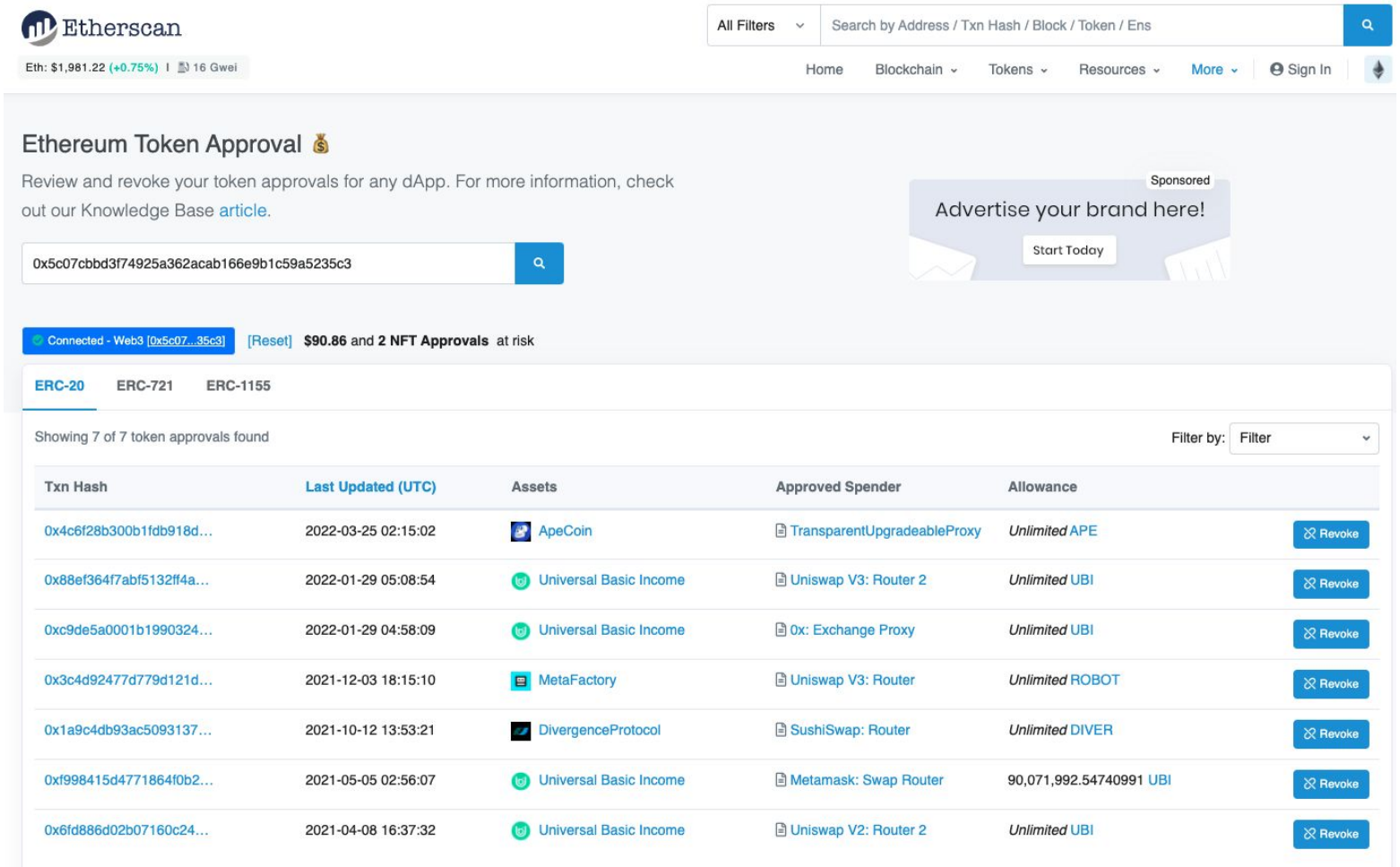
Contratos aprobados



Una firma off-chain puede drenar tu billetera.

defy EDUCATION

Approval checker



Link: https://etherscan.io/tokenapprovalchecker

defy EDUCATION

La seguridad es un estado mental

Wallets

Cada vez que te registres en un sitio, crees una contraseña, bajes una app, publiques algo en tus redes, te hablen por discord o telegram o des un dato por teléfono pensá:
¿Estoy seguro de lo que estoy haciendo? ¿Me estoy convirtiendo en un objetivo fácil de atacar?

¿Preguntas?

Gracias!

twitter.com/PabloSabbatella

defy EDUCATION