

Riesgos y Seguridad en Crypto



Por Pablo Sabbatella



BUENOS AIRES 2022



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.

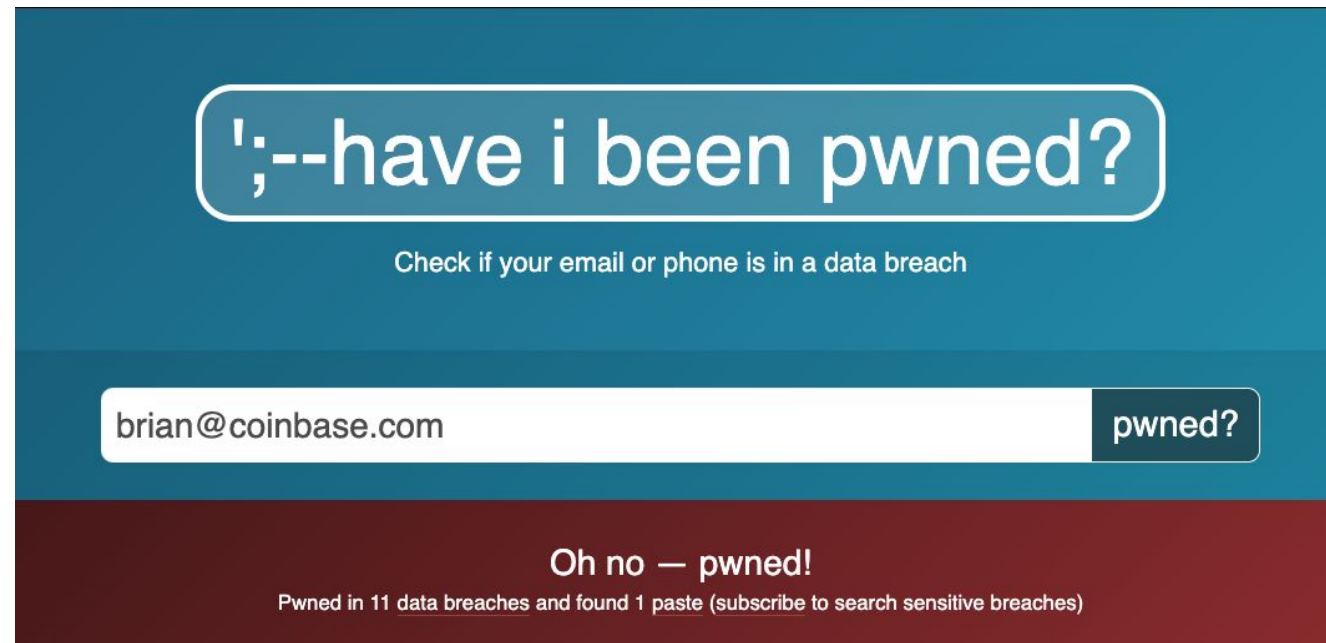
¿Cómo piensa y actúa un atacante?

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>



';--have i been pwned?

Check if your email or phone is in a data breach

brian@coinbase.com pwned?

Oh no — pwned!

Pwned in 11 data breaches and found 1 paste (subscribe to search sensitive breaches)



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 :)

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>).

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

2 Factor Authentication

CELULAR

SMS

LLAMADO

WHATSAPP /
TELEGRAM

LÍNEA PÚBLICA

LÍNEA PRIVADA

Personal

skype™



EMAIL

PÚBLICO

PRIVADO



TOTP apps



AUTHY

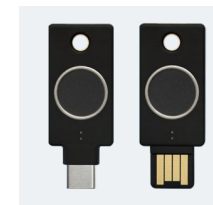


Google Authenticator

HARDWARE DEVICES

REGULAR

BIOMETRIC



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 5.000 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

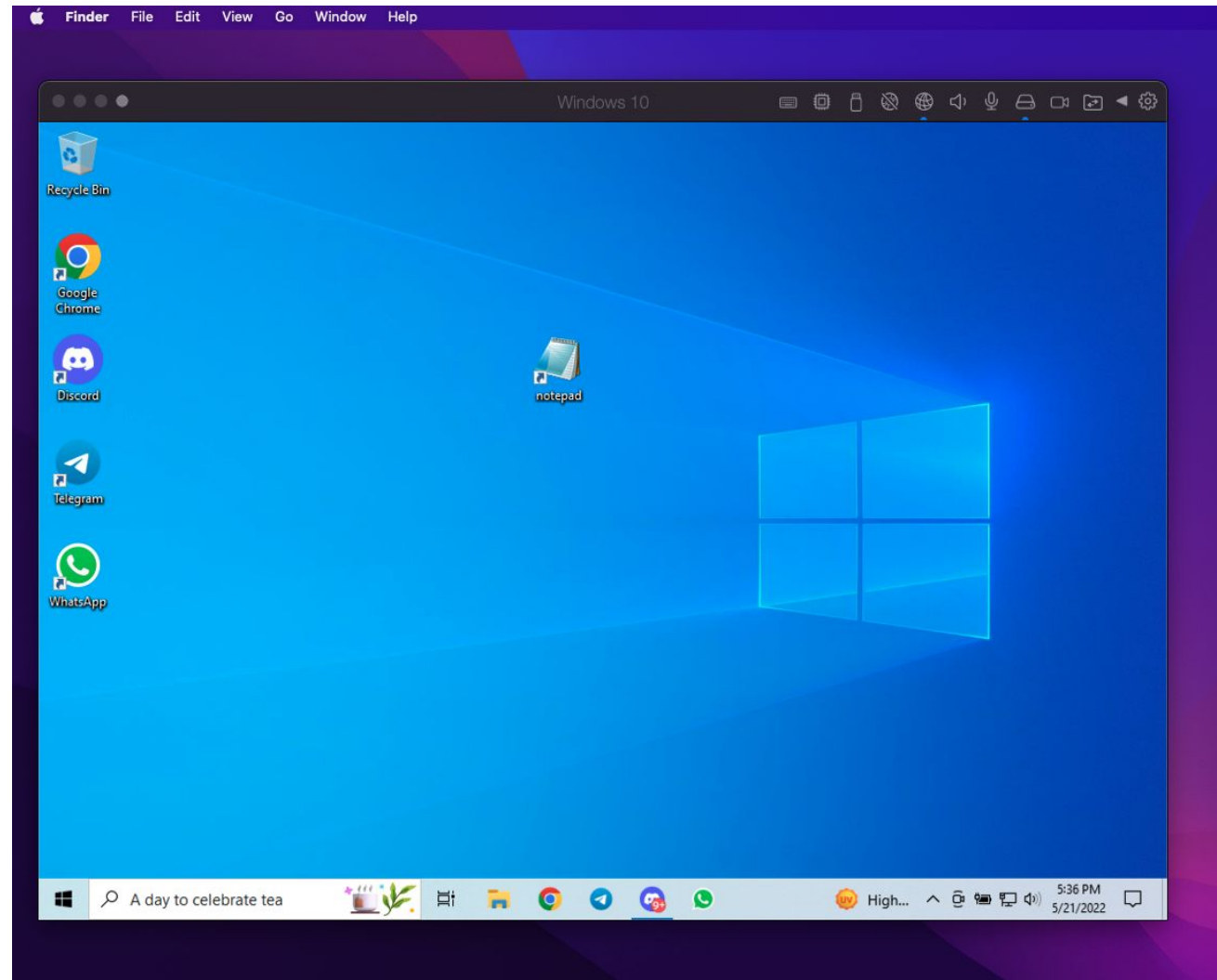
Laptop

- 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 - VM) para todo lo peligroso: Twitter, Discord, Telegram, Whatsapp, porno, etc.
- Virtual Machine: Parallels para la Mac. VMware para Windows.

Virtual Machine



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

Diferentes tipos de WALLETS



CUSTODIAL

EXCHANGES



KRAKEN



BINANCE



BELO



BUENBIT



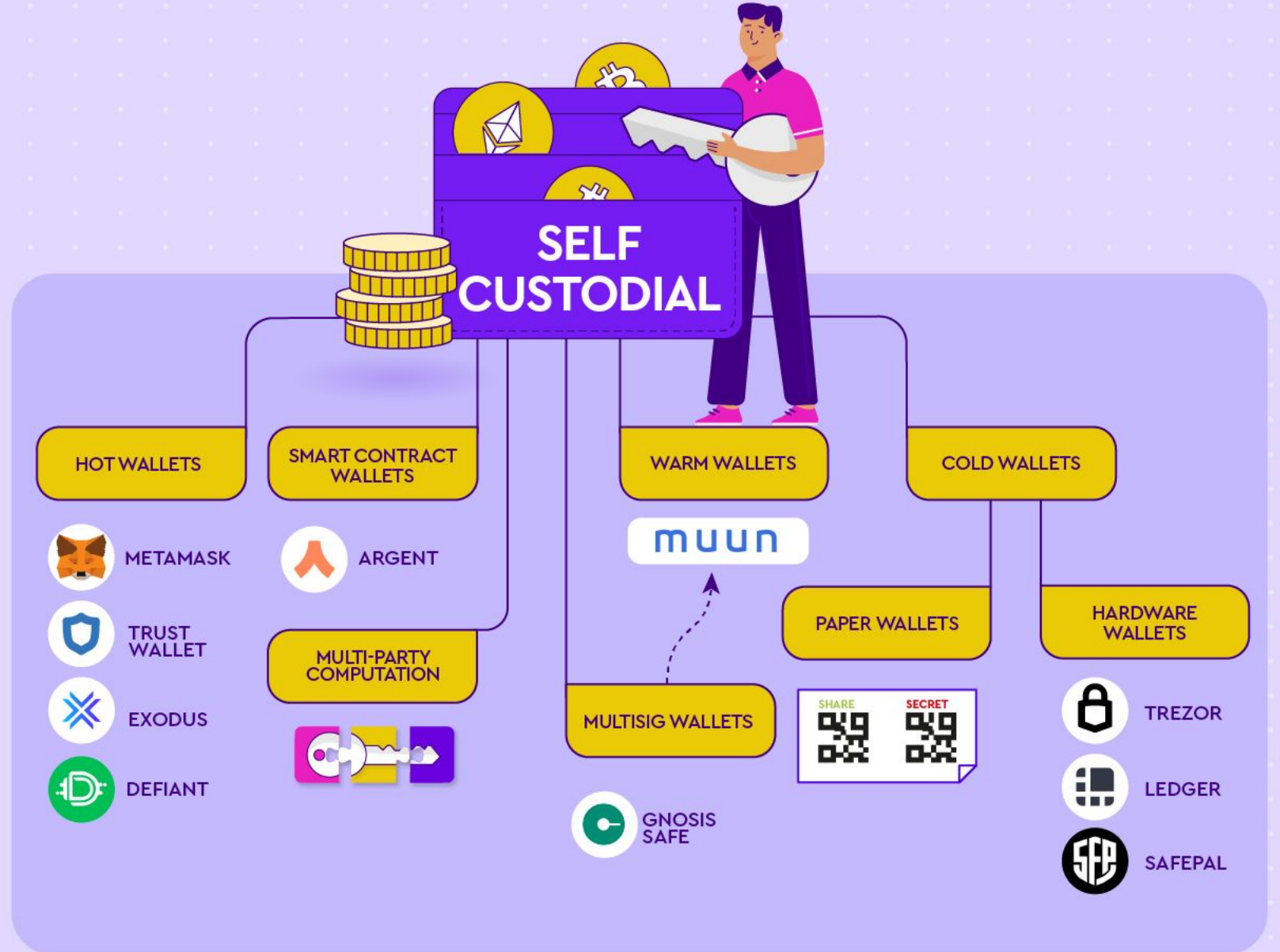
BITFINEX



BITTREX

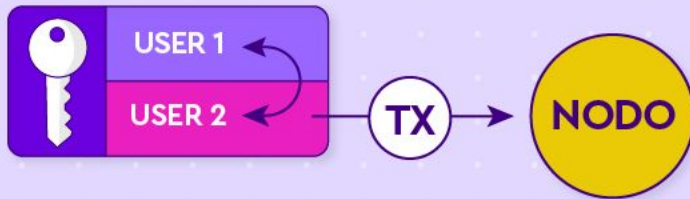
CUSTODIAL WALLETS

WALLET
OF SATOSHI



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

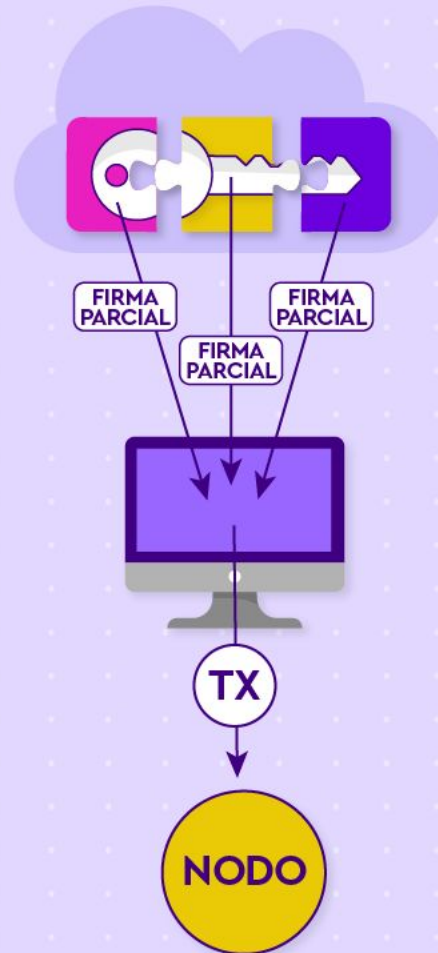
EXCHANGE *(Custodial wallet)*



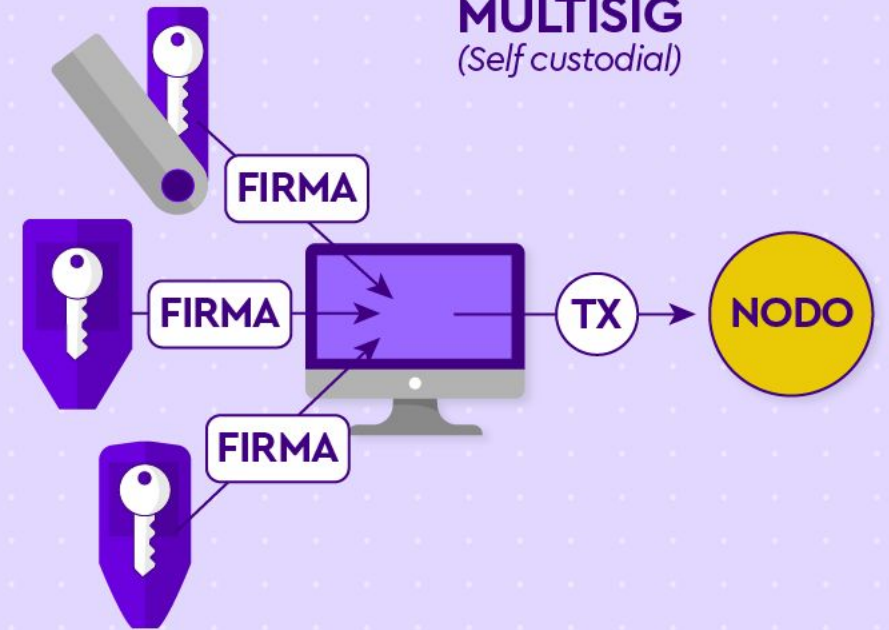
HOT WALLET *(Self custodial)*



MULTI PARTY COMPUTATION *(Self custodial)*



MULTISIG *(Self custodial)*



HARDWARE WALLET *(Self custodial)*

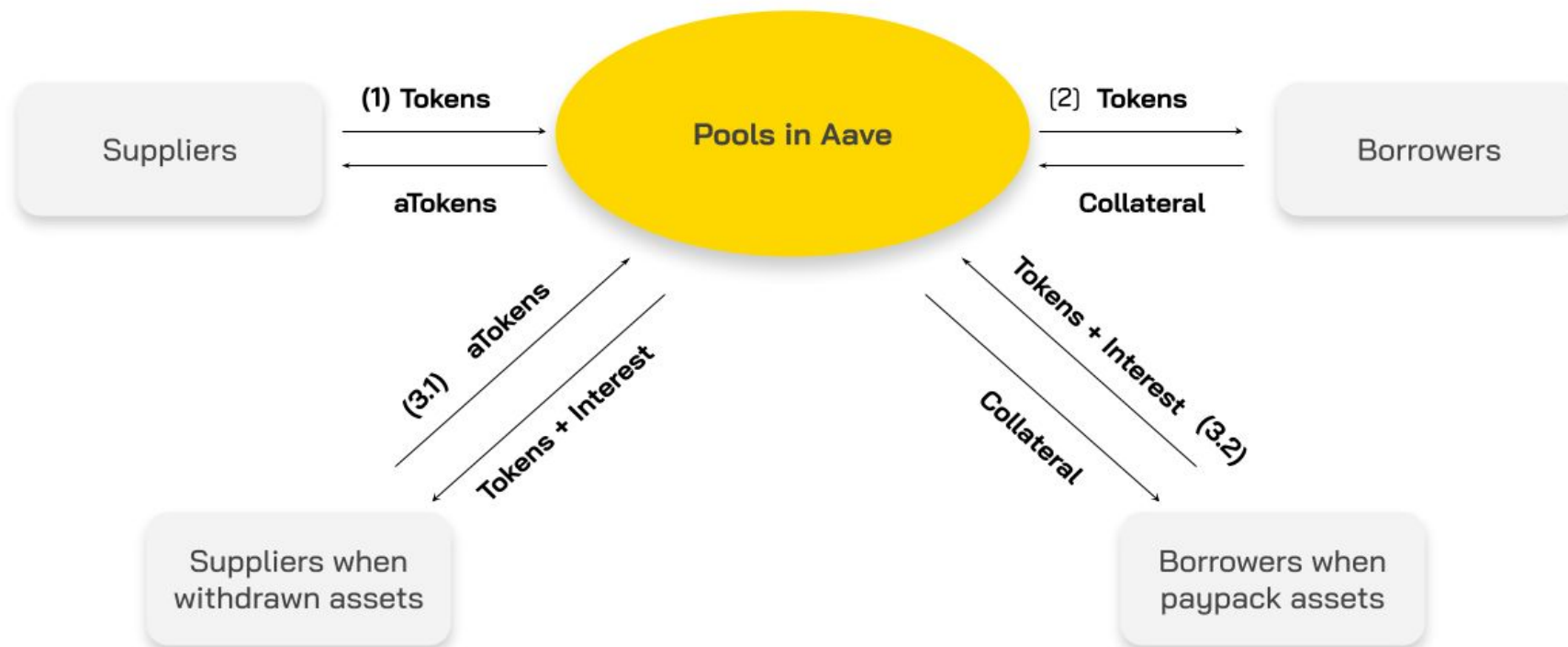


DeFi - The Dark Forest

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

Audited and Verified

The most secure protocol for money

PROTOCOL SECURITY →

 OpenZeppelin

SECURITY AUDIT



SECURITY AUDIT

CERTORA



FORMAL VERIFICATION



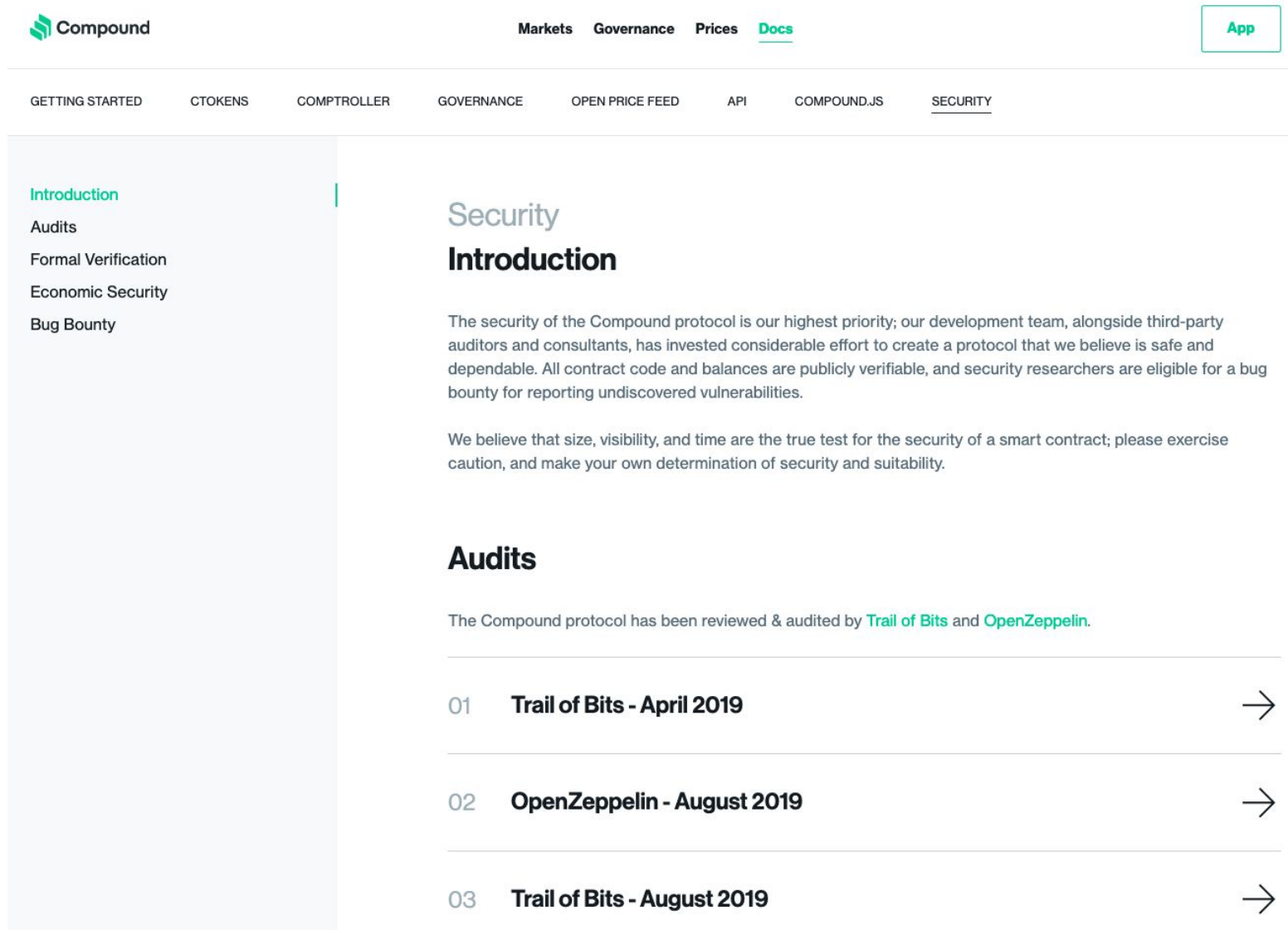
MARKET RISK ASSESSMENT



\$150,000⁰⁰

BUG BOUNTY

Auditorías de seguridad



The screenshot shows the Compound website's documentation page for security. The top navigation bar includes the Compound logo, links for Markets, Governance, Prices, and Docs (which is highlighted), and an App button. Below this is a secondary navigation bar with links for GETTING STARTED, CTOKENS, COMPROLLER, GOVERNANCE, OPEN PRICE FEED, API, COMPOUND.JS, and SECURITY (which is underlined). The left sidebar contains a list of navigation items: Introduction (highlighted), Audits, Formal Verification, Economic Security, and Bug Bounty. The main content area features a 'Security' section with an 'Introduction' sub-section. The introduction text states that the security of the Compound protocol is the highest priority and that the development team, along with third-party auditors, has invested significant effort to ensure the protocol is safe and dependable. It also mentions a bug bounty program for reporting vulnerabilities. Below this, a paragraph emphasizes the importance of size, visibility, and time in testing smart contract security. The 'Audits' section follows, listing three audits: Trail of Bits - April 2019, OpenZeppelin - August 2019, and Trail of Bits - August 2019, each with a right-pointing arrow.

Compound Markets Governance Prices Docs [App](#)

GETTING STARTED CTOKENS COMPROLLER GOVERNANCE OPEN PRICE FEED API COMPOUND.JS SECURITY

[Introduction](#)
Audits
Formal Verification
Economic Security
Bug Bounty

Security

Introduction

The security of the Compound protocol is our highest priority; our development team, alongside third-party auditors and consultants, has invested considerable effort to create a protocol that we believe is safe and dependable. All contract code and balances are publicly verifiable, and security researchers are eligible for a bug bounty for reporting undiscovered vulnerabilities.

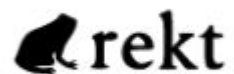
We believe that size, visibility, and time are the true test for the security of a smart contract; please exercise caution, and make your own determination of security and suitability.

Audits

The Compound protocol has been reviewed & audited by [Trail of Bits](#) and [OpenZeppelin](#).

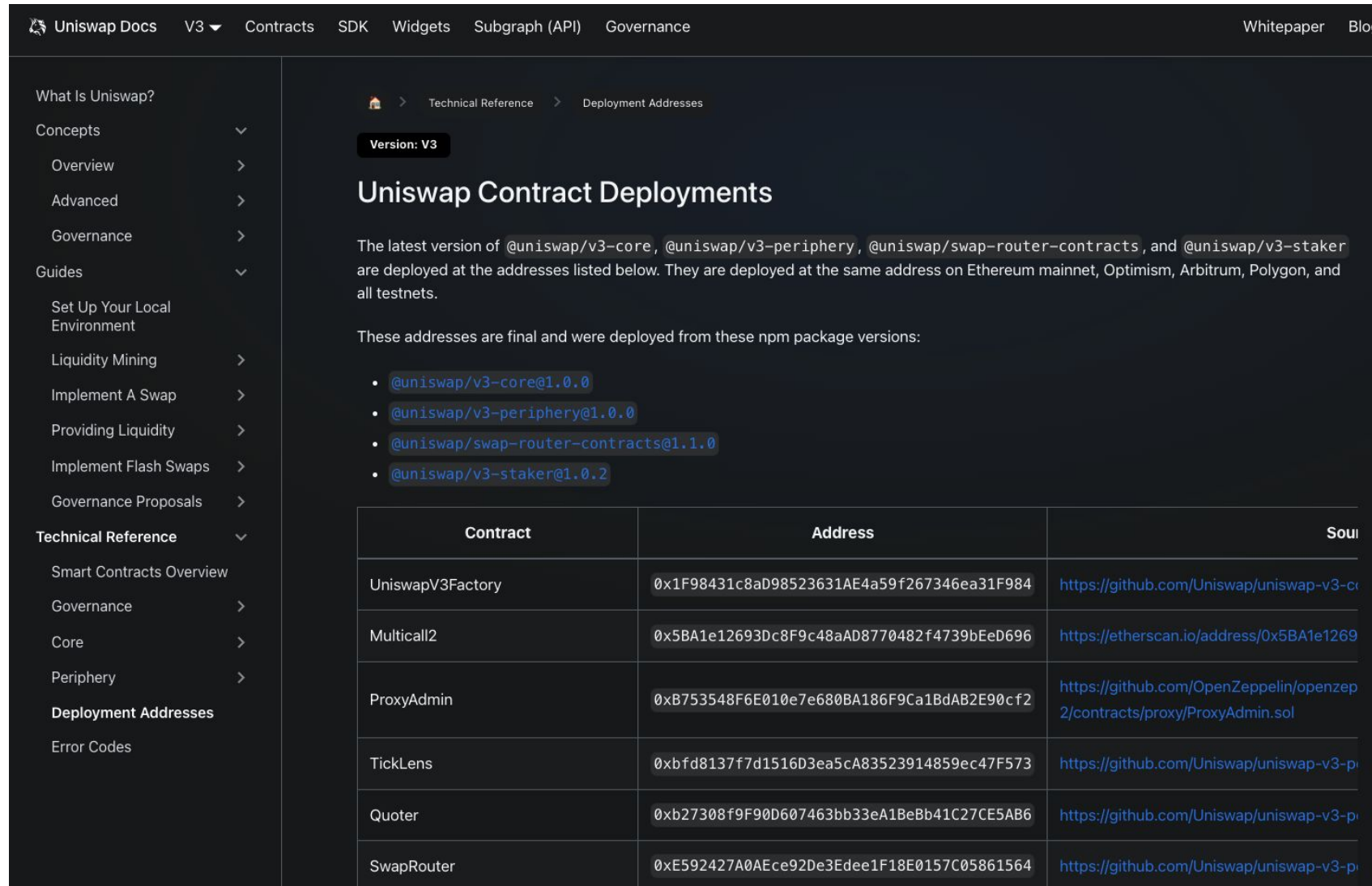
- 01 **Trail of Bits - April 2019** →
- 02 **OpenZeppelin - August 2019** →
- 03 **Trail of Bits - August 2019** →

Rekt Leaderboard



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

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

Home > 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-core
Multicall2	0x5BA1e12693Dc8F9c48aAD8770482f4739bEed696	https://etherscan.io/address/0x5BA1e12693Dc8F9c48aAD8770482f4739bEed696
ProxyAdmin	0xB753548F6E010e7e680BA186F9Ca1BdAB2E90cf2	https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/proxy/ProxyAdmin.sol
TickLens	0xbfd8137f7d1516D3ea5cA83523914859ec47F573	https://github.com/Uniswap/uniswap-v3-periphery
Quoter	0xb27308f9F90D607463bb33eA1BeBb41C27CE5AB6	https://github.com/Uniswap/uniswap-v3-periphery
SwapRouter	0xE592427A0AEce92De3Edee1F18E0157C05861564	https://github.com/Uniswap/uniswap-v3-periphery


Smart contracts verificados

The screenshot shows the Etherscan interface for a smart contract. At the top left is the Etherscan logo and the current price of ETH: \$1,978.95 (+0.63%) with 19 Gwei gas price. A search bar at the top right allows filtering by address, transaction hash, block, token, or ENS. The main header identifies the contract as 'Contract 0x1F98431c8aD98523631AE4a59f267346ea31F984' and 'Uniswap V3: Factory'. Navigation buttons for 'Buy', 'Exchange', 'Earn', and 'Gaming' are visible. A featured banner promotes 'DEX Trading Pairs!'. The 'Contract Overview' section shows a balance of 0 Ether, an ether value of \$0.00, and a token value of \$0.31. The 'More Info' section shows the contract creator's address. A large red arrow points from the 'Contract' tab in the 'Transactions' section to the 'Contract Overview' section. The 'Transactions' section shows a list of transactions, with the 'Contract' tab selected.


Smart contracts verificados

Transactions Internal Txns Erc20 Token Txns **Contract** Events Analytics Comments

Code Read Contract Write Contract Search Source Code

Contract Source Code Verified (Exact Match) 

Contract Name:	UniswapV3Factory	Optimization Enabled:	Yes with 800 runs
Compiler Version:	v0.7.6+commit.7338295f	Other Settings:	default evmVersion

 **Contract Source Code** (Solidity [Standard Json-Input](#) format) More Options

File 1 of 33 : UniswapV3Factory.sol

```
1 // SPDX-License-Identifier: BUSL-1.1
2 pragma solidity =0.7.6;
3
4 import './interfaces/IUniswapV3Factory.sol';
5
6 import './UniswapV3PoolDeployer.sol';
7 import './NoDelegateCall.sol';
8
9 import './UniswapV3Pool.sol';
10
11 /// @title Canonical Uniswap V3 factory
12 /// @notice Deploys Uniswap V3 pools and manages ownership and control over pool protocol fees
13 contract UniswapV3Factory is IUniswapV3Factory, UniswapV3PoolDeployer, NoDelegateCall {
14     /// @inheritdoc IUniswapV3Factory
15     address public override owner;
16
17     /// @inheritdoc IUniswapV3Factory
18     mapping(uint24 => int24) public override feeAmountTickSpacing;
19     /// @inheritdoc IUniswapV3Factory
20     mapping(address => mapping(address => mapping(uint24 => address))) public override getPool;
21
22     constructor() {
23         owner = msg.sender;
24         emit OwnerChanged(address(0), msg.sender);
25     }
```

Smart contracts no verificados

Transactions Internal Txns Erc20 Token Txns Erc721 Token Txns **Contract** Events Analytics Info Comments

i Are you the contract creator? [Verify and Publish](#) your contract source code today!

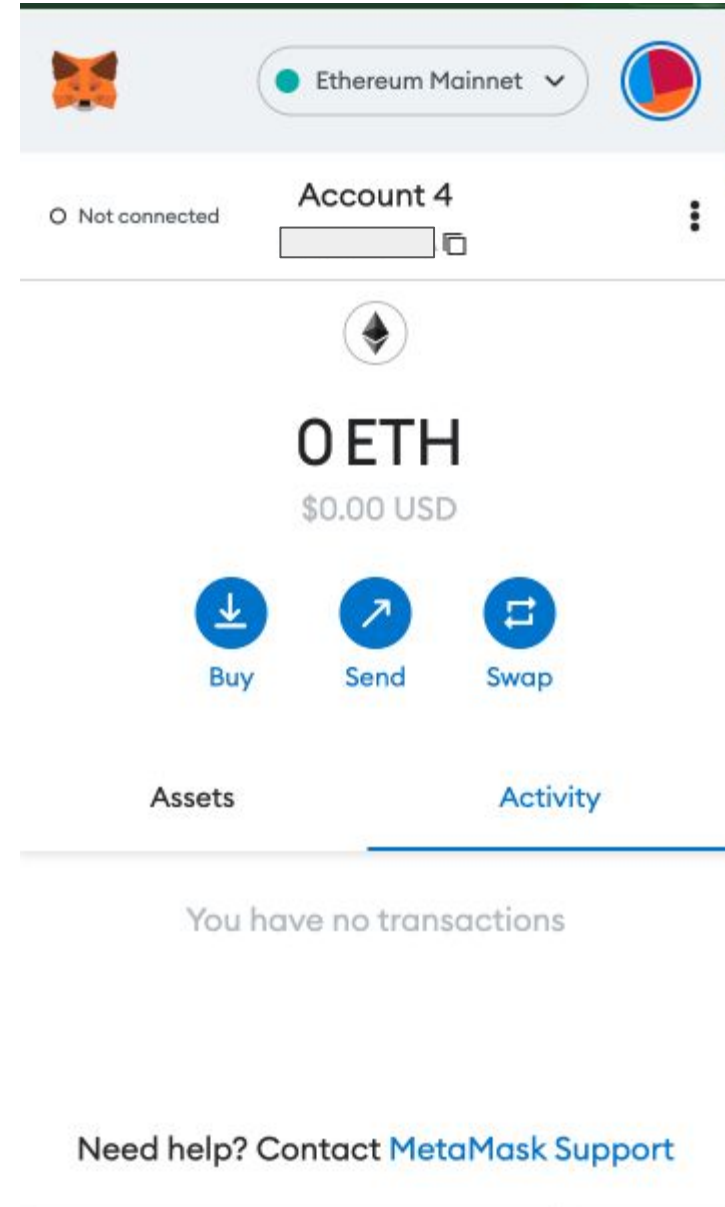
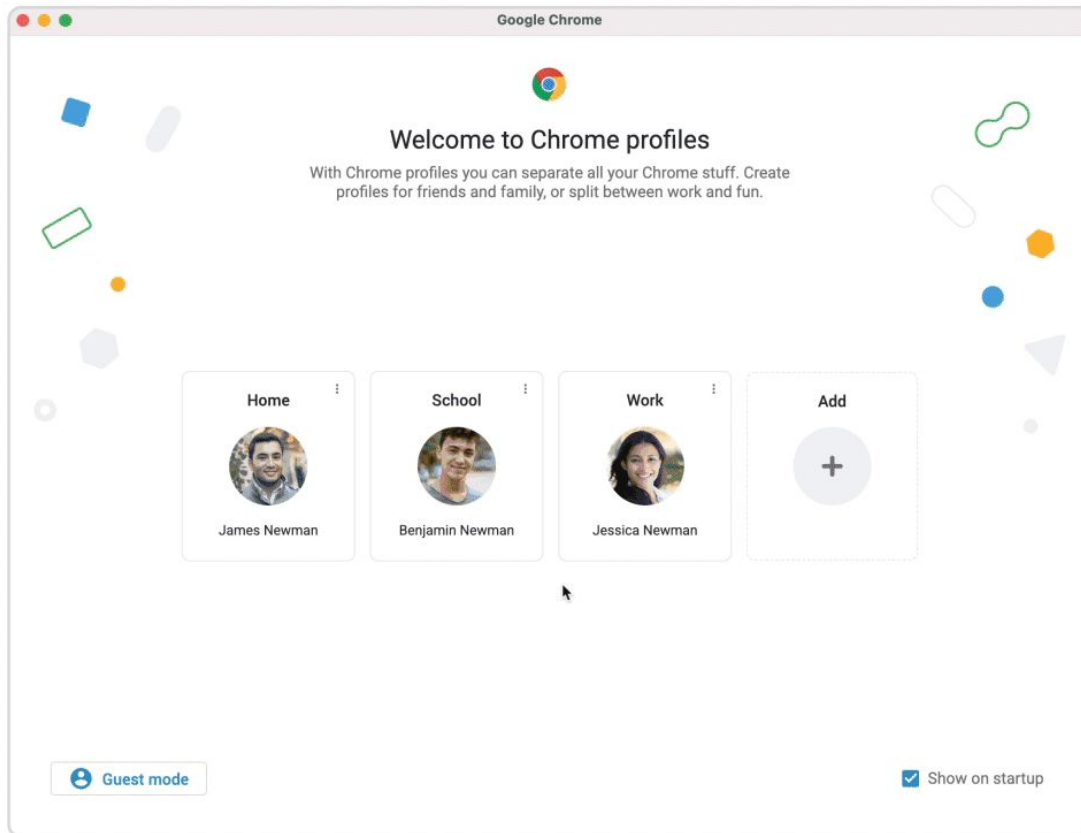
Decompile ByteCode 

Switch to Opcodes View

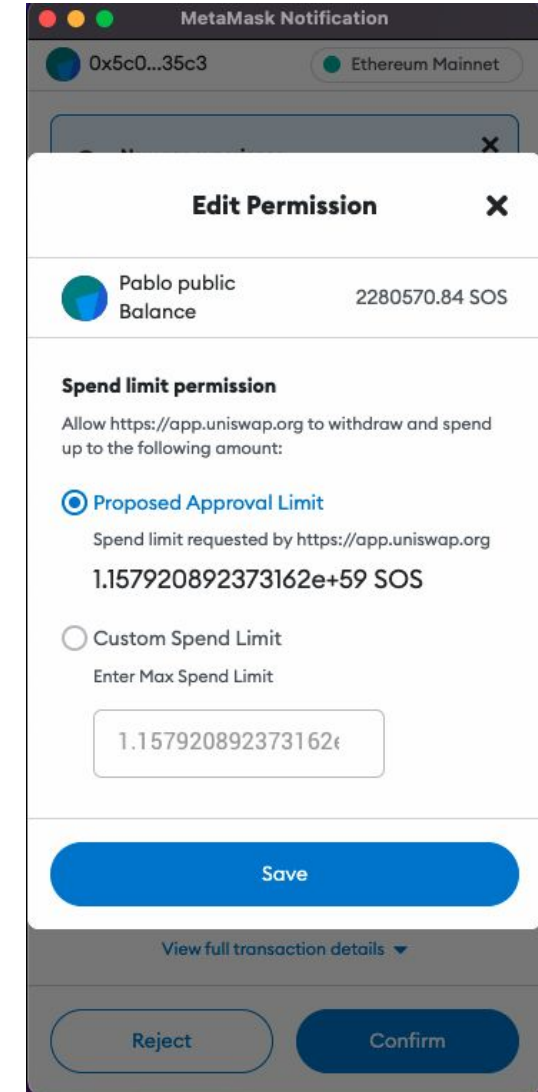
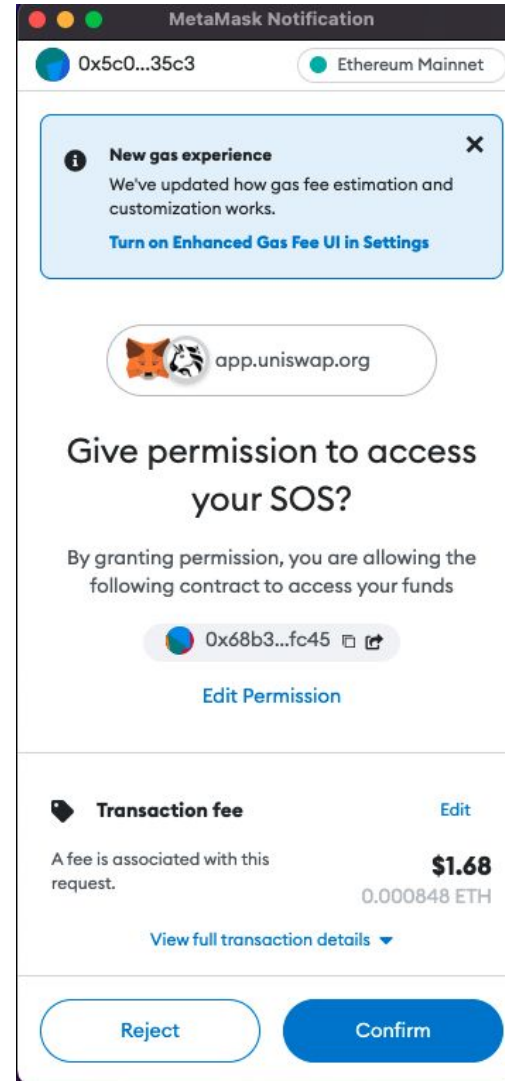
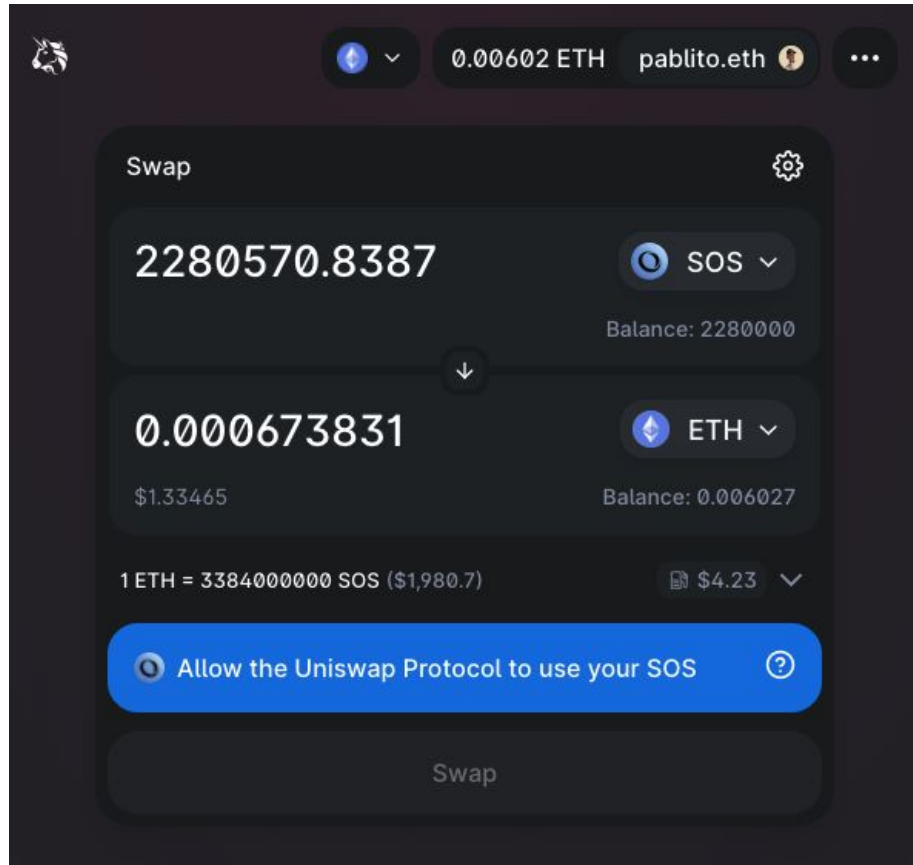
Similar Contracts

```
0x608060405234801561001057600080fd5b50600436106101d95760003560e01c80638f32d59b11610104578063bd85b039116100a2578063e985e9c511610071578063e985e9c5146110a9578063f242432a14611125578063f2fde38b14611234578063f923e8c314611278576101d9565b8063bd85b03914610fb7578063c311c52314610ff9578063cd7c03261461101b578063d26ea6c014611065576101d9565b80639e037eea14610cdc578063a22cb46514610d20578063a50aa5c314610d70578063b48ab8b614610db4576101d9565b80638f32d59b14610be957806391686f5314610c0b57806395d89b4114610c59576101d9565b80634e1273f41161017c578063731133e91161014b578063731133e91461098f57806373505d3514610a7e578063862440e214610ada5780638da5cb5b14610b9f576101d9565b80634e1273f4146107305780634f558e79146108d1578063510b515814610917578063715018a614610985576101d9565b80630e89341c116101b85780630e89341c1461032857806324d88785146103cf5780632eb2c2d61461048a5780634060b25e146106ad576101d9565b8062fd58e146101de57806301ffc9a71461024057806306fdde03146102a5575b600080fd5b61022a600480360360408110156101f457600080fd5b81019080803573ffffffffffffffffffffffffffffffffffffffff169060200190929190803590602001909291905050506112fb565b6040518082815260200191505060405180910390f35b61028b6004803603602081101561025657600080fd5b8101908080357bffffffffffffffffffffffffffffffffffffffff16906020019169060200190929190505050611343565b604051808215151515815260200191505060405180910390f35b6102ad6113f4565b6040518080602001828103825283818151815260200191508051906020019080838360005b838110156102ed5780820151818401526020810190506102d2565b505050905090810190601f16801561031a5780820380516001836020036101000a031916815260200191505b509250505060405180910390f35b6103546004803603602081101561033e57600080fd5b8101908080359060200190929190505050611492565b6040518080602001828103825283818151815260200191508051906020019080838360005b83811015610394578082015181840152602081019050610379565b505050905090810190601f1680156103c15780820380516001836020036101000a031916815260200191505b509250505060405180910390f35b610488600480360360208110156103e557600080fd5b81019080803590602001906401000000081111561040257600080fd5b82018360208201111561041457600080fd5b8035906020019184600183028401116401000000083
```

Nuevo navegador & wallet



Contratos aprobados



Approval checker

Etherscan

Eth: \$1,981.22 (+0.75%) | 16 Gwei

All Filters Search by Address / Txn Hash / Block / Token / Ens

Home Blockchain Tokens Resources More Sign In

Ethereum Token Approval

Review and revoke your token approvals for any dApp. For more information, check out our Knowledge Base [article](#).

0x5c07cbbd3f74925a362acab166e9b1c59a5235c3

Connected - Web3 [0x5c07...35c3] [Reset] \$90.86 and 2 NFT Approvals at risk

ERC-20 ERC-721 ERC-1155

Showing 7 of 7 token approvals found Filter by: Filter

Txn Hash	Last Updated (UTC)	Assets	Approved Spender	Allowance	
0x4c6f28b300b1fdb918d...	2022-03-25 02:15:02	ApeCoin	TransparentUpgradeableProxy	Unlimited APE	Revoke
0x88ef364f7abf5132ff4a...	2022-01-29 05:08:54	Universal Basic Income	Uniswap V3: Router 2	Unlimited UBI	Revoke
0xc9de5a0001b1990324...	2022-01-29 04:58:09	Universal Basic Income	0x: Exchange Proxy	Unlimited UBI	Revoke
0x3c4d92477d779d121d...	2021-12-03 18:15:10	MetaFactory	Uniswap V3: Router	Unlimited ROBOT	Revoke
0x1a9c4db93ac5093137...	2021-10-12 13:53:21	DivergenceProtocol	SushiSwap: Router	Unlimited DIVER	Revoke
0xf998415d4771864f0b2...	2021-05-05 02:56:07	Universal Basic Income	Metamask: Swap Router	90,071,992.54740991 UBI	Revoke
0x6fd886d02b07160c24...	2021-04-08 16:37:32	Universal Basic Income	Uniswap V2: Router 2	Unlimited UBI	Revoke

Link: <https://etherscan.io/tokenapprovalchecker>

¿Preguntas?



Gracias!



twitter.com/PabloSabbatella
www.defyeducation.com