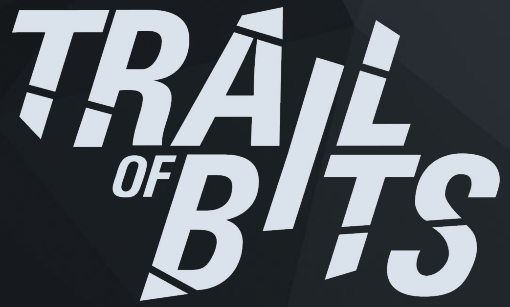

TRAIL
OF
BITS

À la découverte du métier d'auditeur Web3



nisedo
Ingénieur sécurité blockchain @ Trail of Bits

Qui suis-je ?



- nisedo (x.com/nisedo_)
- Soliditors - la communauté Web3Sec 🇫🇷
- Ingénieur sécurité blockchain @ Trail of Bits

Pourquoi devenir auditeur de smart contracts ?

La sécurité Web3 est cassée

16,6 Md $

hackés depuis mai 2016



DefiLlama.com

Web3Sec vs Web2Sec 🛡️

🥷 hack Web2

↓

🗂️ vol de données

↓

🌚 dark web

↓

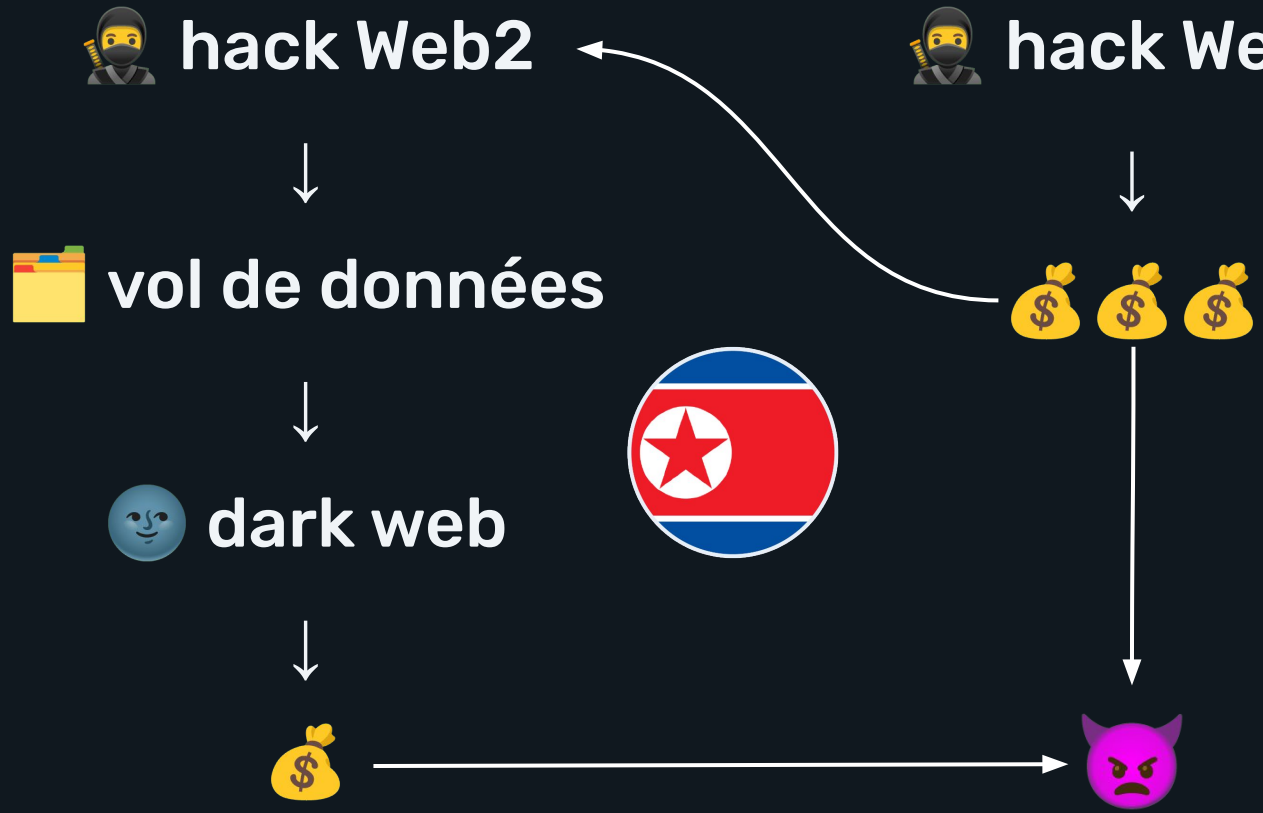
💰

🥷 hack Web3

↓

💰💰💰

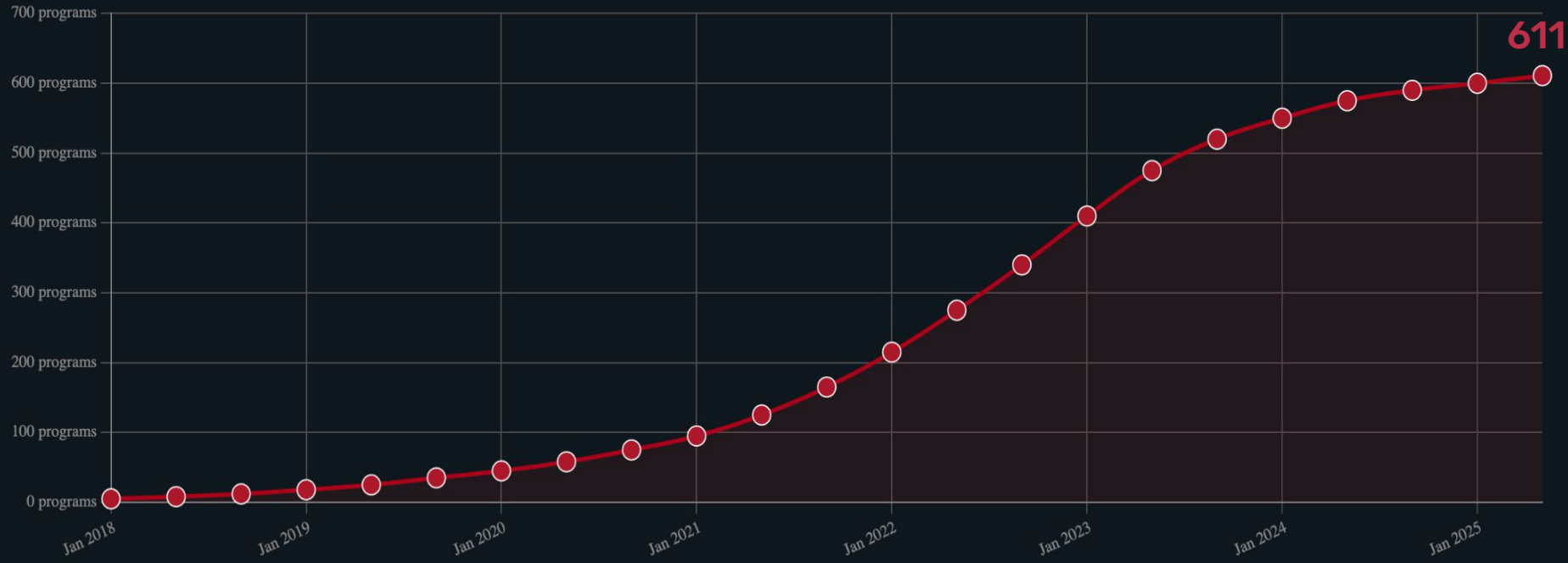
Notre travail compte vraiment 🛡️



Demande croissante

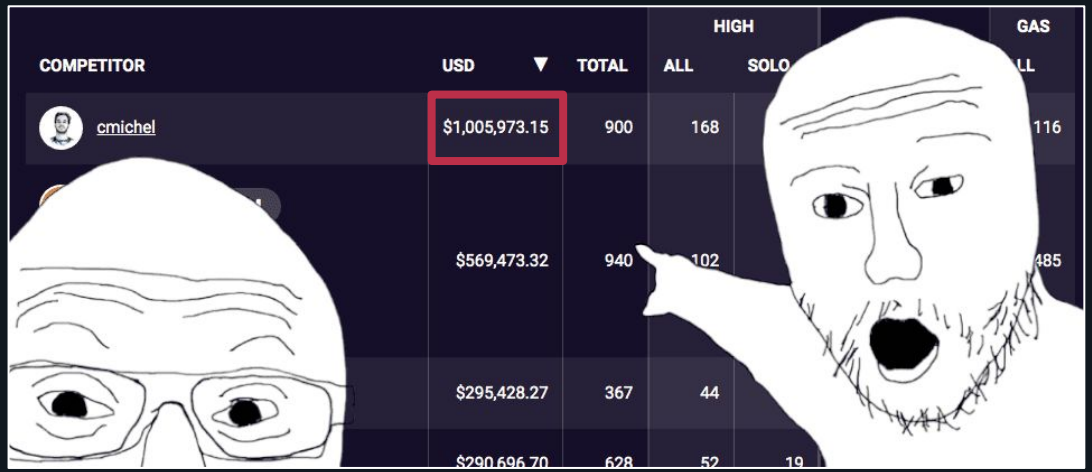
Programmes de bug bounty Web3

Croissance des bug bounties sur les plateformes (2018-2025)



Money, Money, Money 💰

1	Barracuda3172 Name	$14,439,800 Total Earnings
2	RetailDdene2946 Name	$10,020,000 Total Earnings
3	PwningEth Name	$8,000,000 Total Earnings



0x52

Security Researcher

$1.22M
Total Earnings

#3 All Time

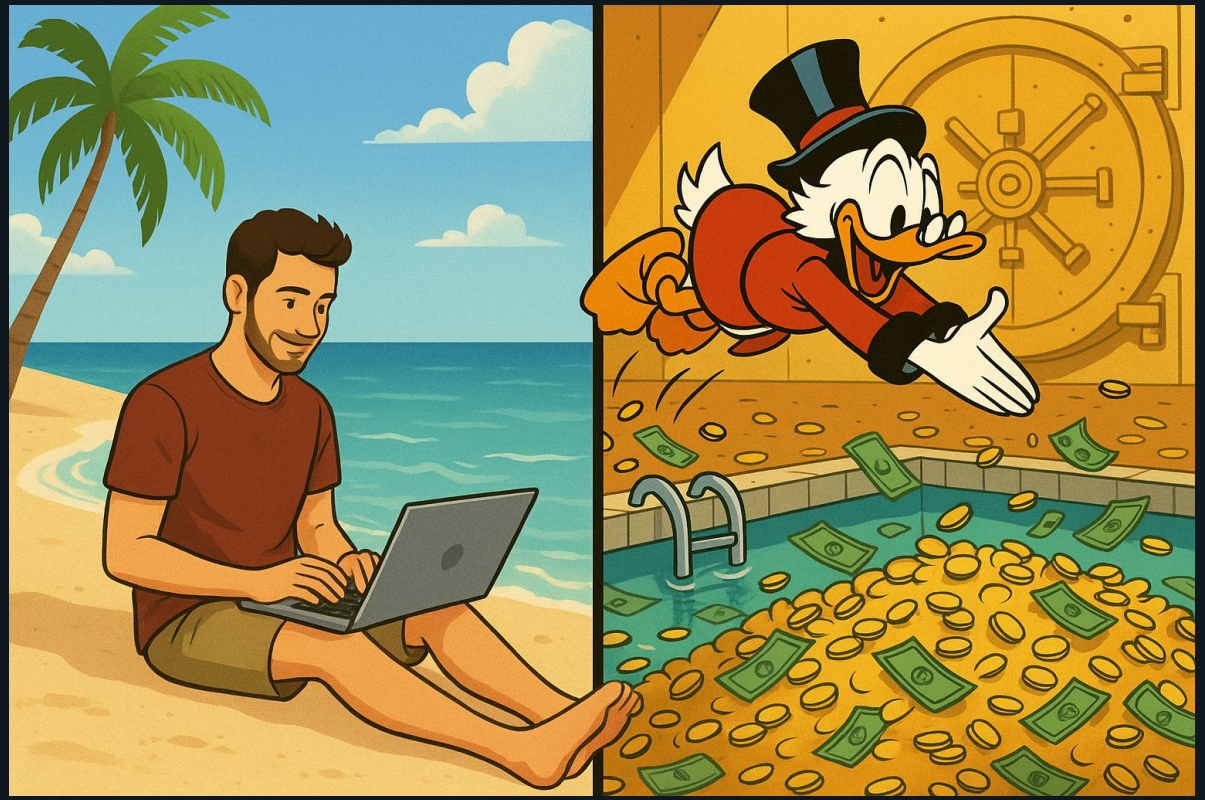
deadrosesxyz
@deadrosesxyz

proud to announce that the $1m mark was successfully crossed (and the year's not finished yet!)

a rough breakdown of the income sources:
- Contests ~$500k
- Spearbit ~$265k
- Solo audits ~$240k
- Immunefi ~40k

Mais...

Attentes

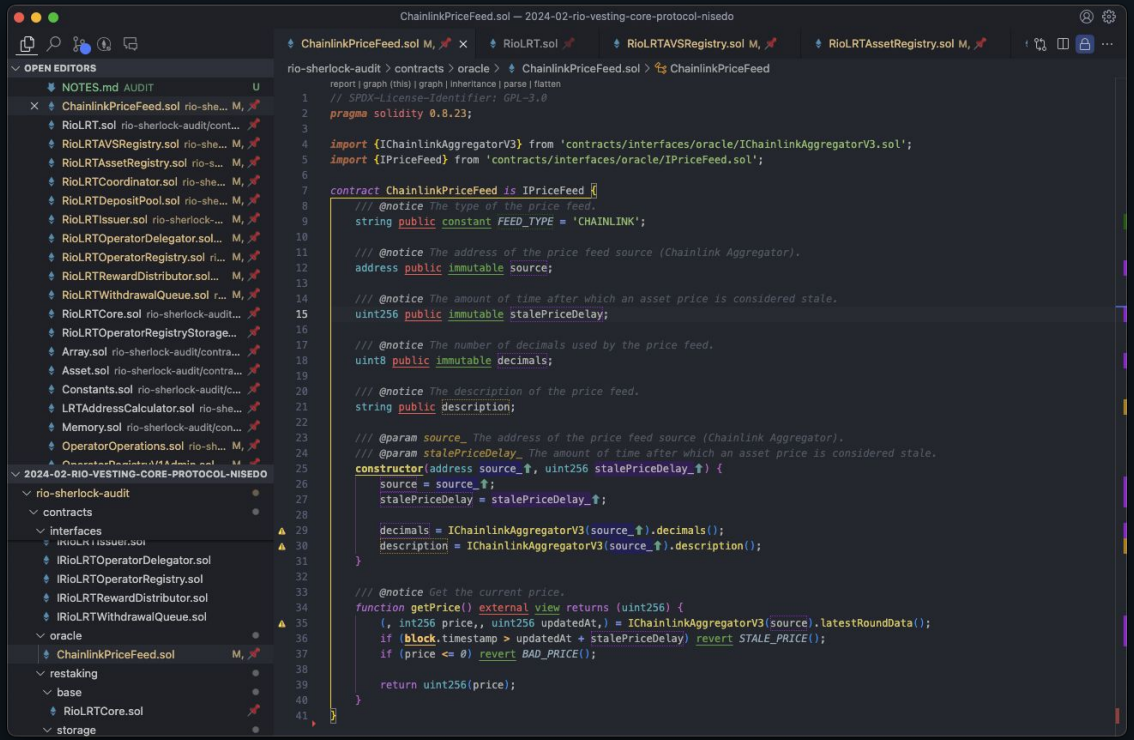


Réalité



Que font les auditeurs de smart contracts ?

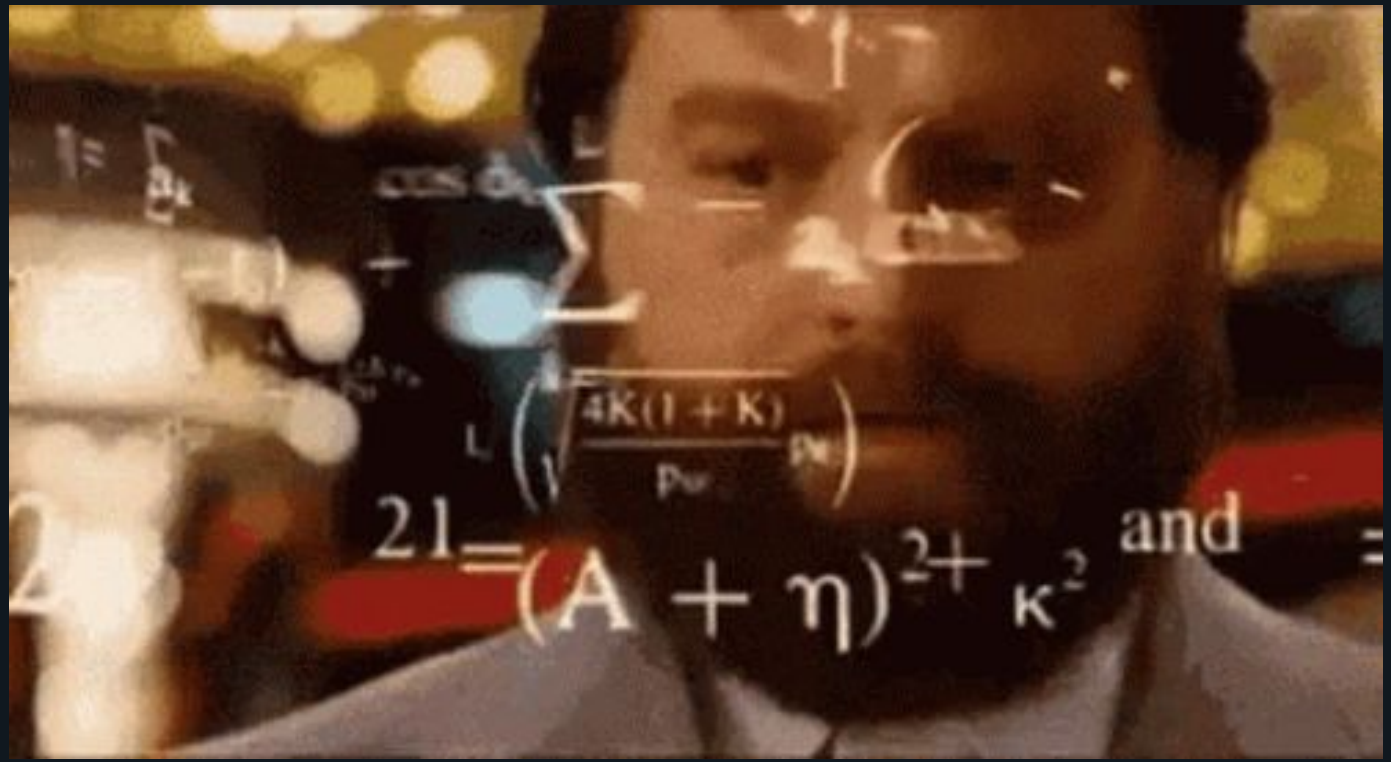
On trouve des bugs… mais comment ?



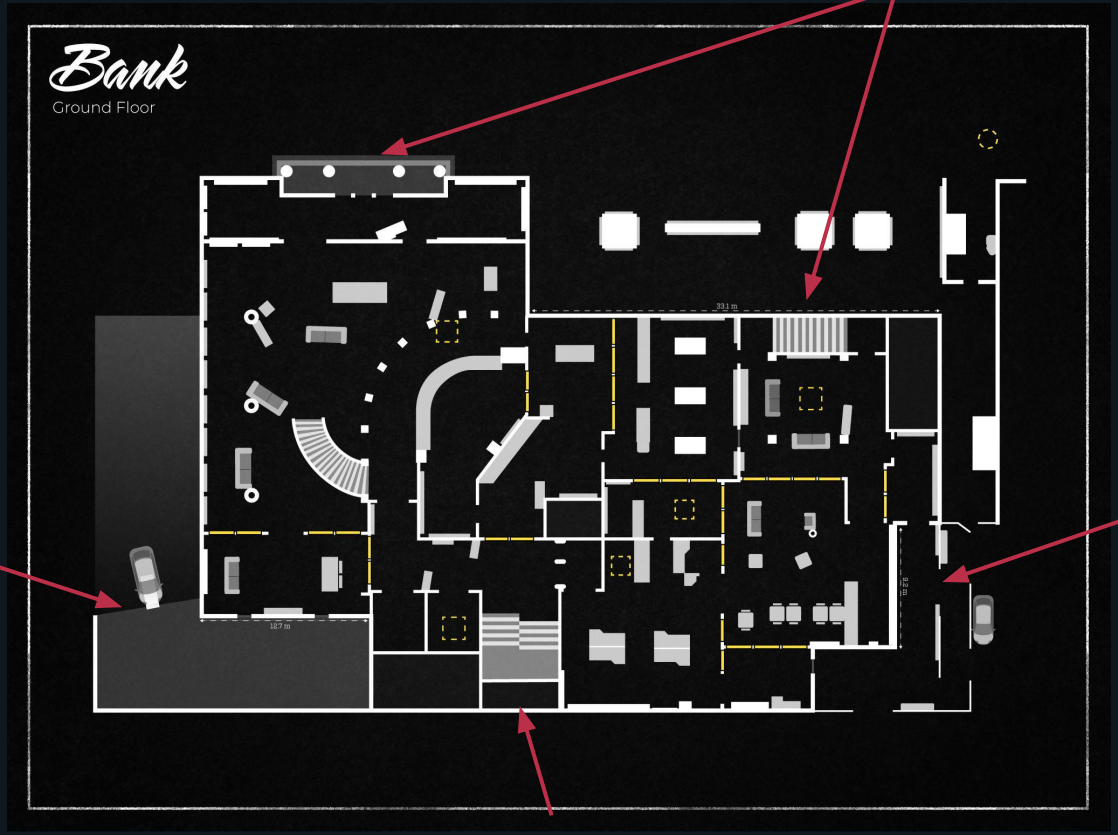
On reçoit un puzzle géant



On lit du code… beaucoup de code…



Et on assemble les pièces



Les caméras peuvent être évitées

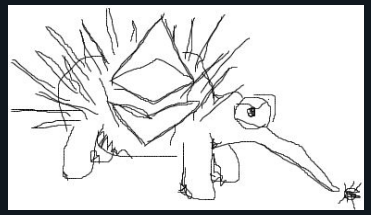
Le code d'entrée peut être bruteforcé

Pas de garde

Fenêtre ouverte

Armés jusqu'aux dents

Fuzzing



Medusa

Framework



Hardhat

Analyse statique

SLITHER

Semgrep

aderyn

Vérification formelle

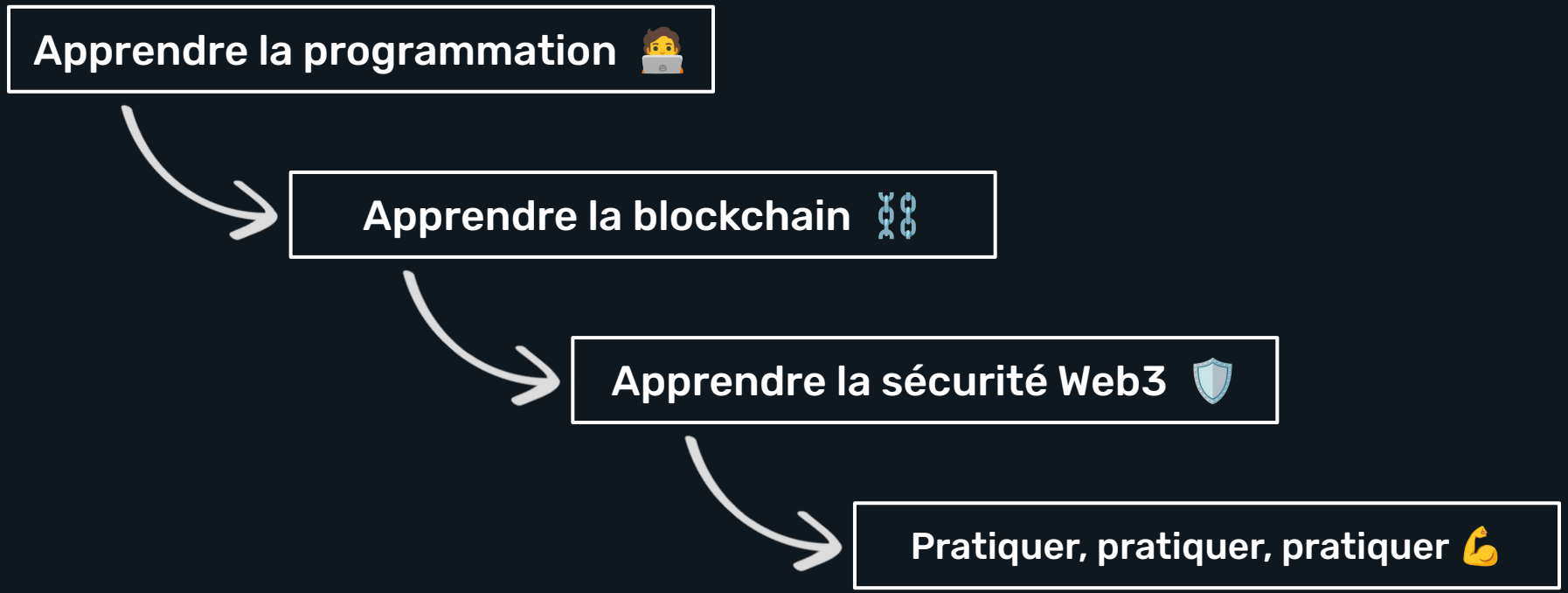
Halmos

kontrol

AI

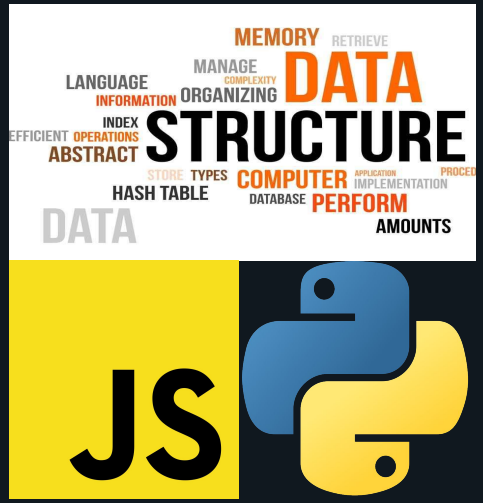
Comment devenir auditeur de smart contracts ?

Comment devenir auditeur de smart contracts ? 🎓

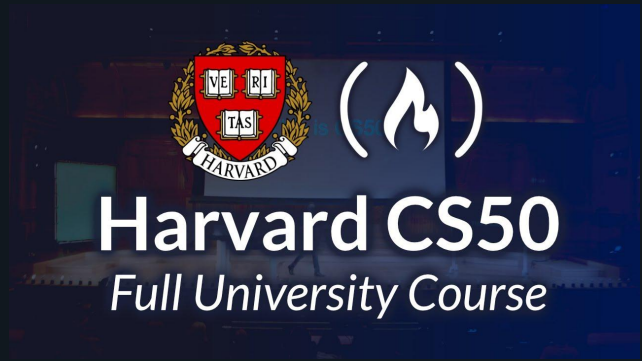


1. Apprendre la programmation 🧑‍💻

Informatique



Harvard CS50



2. Apprendre la blockchain ⛓️

EVM

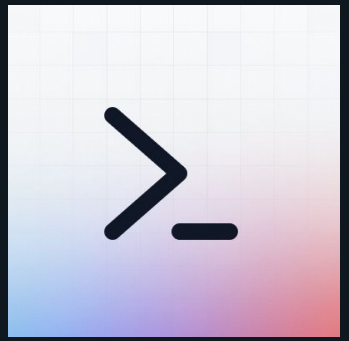


Solidity





Cyfrin Updraft



RareSkills



3. Apprendre la sécurité Web3 🛡️

Résoudre des CTFs 🚩

The Ethernaut

$DAMN VULNERABLE DEFI

ONLYPWNER

Étudier des rapports d'audit 📄

SOLODIT

4. Pratiquer, pratiquer, pratiquer 💪

Concours d'audit publics 🏆

DAILY WARDEN



Étudier des rapports d'audit 📄

SOLODIT

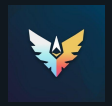
Et ensuite ?


TRAIL OF BITS
EXPERIENCED
SMART
CONTRACT AUDITOR
imgflip.

Les différents types d'audits 🔎

Concours d'audit 🏆



Audits privés 🕵️





Bug bounties 🏹






Cabinets d'audit 🏢






Le Web3 a besoin de toi 🫵



Fin

